

Official Transcript of Proceedings  
NUCLEAR REGULATORY COMMISSION

Title: Advisory Committee on Reactor Safeguards  
Digital Instrumentation and Control Systems  
Subcommittee Meeting: Open Session

Docket Number: (n/a)

Location: Rockville, Maryland

Date: Tuesday, June 4, 2013

Work Order No.: NRC-4277

Pages 1-130

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

1 UNITED STATES OF AMERICA

2 NUCLEAR REGULATORY COMMISSION

3 + + + + +

4 ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

5 (ACRS)

6 + + + + +

7 DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS

8 SUBCOMMITTEE

9 + + + + +

10 OPEN SESSION

11 + + + + +

12 TUESDAY

13 JUNE 4, 2013

14 + + + + +

15 ROCKVILLE, MARYLAND

16 + + + + +

17 The Subcommittee met at the Nuclear  
18 Regulatory Commission, Two White Flint North, Room  
19 T2B1, 11545 Rockville Pike, at 1:00 p.m., **CHARLES**  
20 **H. BROWN, JR.**, Chairman, presiding.

21 COMMITTEE MEMBERS:

22 **CHARLES H. BROWN, JR. Chairman**

23 **J. SAM ARMIJO, Member**

24 **DENNIS C. BLEY, Member**

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24

***WILLIAM J. SHACK, Member***

ACRS CONSULTANT:

MYRON HECHT (via telephone)

DESIGNATED FEDERAL OFFICIAL:

CHRISTINA ANTONESCU

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24

TABLE OF CONTENTS

ITEM	PAGE
Opening Remarks	4
Introduction	7
NSIR Overview	32
NRC Cyber Security Program Status	55
Inter-Office Framework Overview	86
Inter-Agency Intl. Activities Overview	99

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24

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

1:00 p.m.

CHAIRMAN BROWN: The meeting will now  
come to order.

This is a meeting of the Digital  
Instrumentation and Control System Subcommittee.  
I am Charles Brown, Chairman of the Subcommittee.

ACRS Members in attendance are Dennis  
Bley. Coming, will be Sam Armijo, Bill Shack,  
myself and Myron Hecht, our consultant, is  
participating by phone as a consultant for the  
Subcommittee meeting.

Christina Antonescu of the ACRS staff  
is the Designated Federal Official for this  
meeting.

During this meeting, the staff and the  
Office of Nuclear Security and Incident Response  
NSIR will brief the DI&C Subcommittee on staff's  
activities associated with cyber-security.

The Subcommittee will gather

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealrgross.com](http://www.nealrgross.com)

1 information, analyze relevant issues and facts,  
2 and formulate proposed positions and actions, as  
3 appropriate for deliberation by the full Committee.

4 The rules for participation in today's  
5 meeting have been announced as part of the notice  
6 of this meeting, previously published in the  
7 Federal Register on May 30, 2013.

8 We have received no written comments  
9 or requests for time to make oral statements from  
10 members of the public, regarding today's meeting.

11 Also, today's agenda highlights areas  
12 for which the meeting may need to be closed, in  
13 order to protect unclassified safeguards  
14 information.

15 In particular, the open session for the  
16 public will be from 1:00 p.m. to 2:45 p.m. and the  
17 closed session will be from 3:00 p.m. to 5:00 p.m.,  
18 right after the break.

19 Also during the open session, we have  
20 the following people from the public on the bridge  
21 line, listening to the discussions.

22 Skip Butler, Peter Yandow, Patricia  
23 Campbell, Matthew Bohne, excuse me if I pronounced  
24 that wrong, Brian Buckley, Sara Rudy, Lee

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealrgross.com](http://www.nealrgross.com)

1 Doughtery, all from GE Power & Water, and Bob  
2 Hirmanpour, Southern Nuclear Company.

3 If there is anyone else on the line,  
4 would they please identify themselves at this time?

5 MR. RUSSO: Scott Russo from GE.

6 CHAIRMAN BROWN: Okay, Bob Russo?

7 MR. RUSSO: Scott Russo.

8 CHAIRMAN BROWN: Okay, Scott Russo,  
9 okay, thank you. Have you got that?

10 To conclude, anyone else? Excuse me?

11 Okay, to -- we would appreciate to  
12 preclude interruption of the meeting, the bridge  
13 line will be placed on listen-in mode during the  
14 discussions and presentations and Committee  
15 discussions.

16 A transcript of the meeting is being  
17 kept and will be made available, as stated in the  
18 Federal Register Notice.

19 Therefore, we request that  
20 participants in this meeting use the microphones  
21 located throughout the meeting room, when  
22 addressing the Subcommittee.

23 The participants should first identify  
24 themselves, and speak with sufficient clarity and

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 volume, so that they may be readily heard.

2 We will now proceed with the meeting.

3 I call upon Christiana Lui, correct?

4 MS. LUI: Correct.

5 CHAIRMAN BROWN: Thank you, Director  
6 of Division of Security Policy in the Office of  
7 Nuclear Security and Incident Response, to provide  
8 some introductory remarks, followed by Tom Bergman,  
9 Director of Division of Engineering of the Office  
10 of New Reactors, who will also provide some  
11 introductory remarks for NRO, before we proceed.

12 Christiana, would you like to go ahead?

13 MS. LUI: Yes, thank you. Good  
14 afternoon.

15 As Mr. Brown has mentioned, I am  
16 Christiana Lui, currently the Director of Division  
17 of Security Policy in the Office of Nuclear Security  
18 and Incident Response.

19 Sitting with me at the table to my right  
20 are Tom Bergman, Director, Division of Engineering  
21 in the Office of New Reactors, Ron Albert, Chief  
22 of the Branch -- Chief of the Reactor Security  
23 Oversight Branch in the Office of Nuclear Security  
24 and Incident Response, and Craig Erlanger, Chief

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealrgross.com](http://www.nealrgross.com)



1 -- the Cyber-Security and Integrated Response  
2 Program Branch Chief in the Office of Nuclear  
3 Security and Incident Response.

4 Sitting at the table is Barry  
5 Westreich. He is currently the Deputy Division  
6 Director in the Division of Security Operations  
7 in the Office of Nuclear Security and Incident  
8 Response.

9 In the audience, we also have staff and  
10 management coming from the Office of Nuclear  
11 Reactor Regulations, the Office of Nuclear Material  
12 Safety and Safeguards, the Office of Regulatory  
13 -- sorry, the Office of Nuclear Regulatory  
14 Research, and I think I've seen some staff coming  
15 from FSME, but I don't see them right now.

16 All right, so, many of our past  
17 interactions on cyber-security were in the context  
18 of regulatory guide reviews and digital  
19 instrumentation and control, and cyber-security  
20 licensing actions in the past.

21 We're glad to have the opportunity to  
22 support these dedicated Subcommittee meetings on  
23 cyber-security regulatory programs today.

24 We worked very closely with the ACRS

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 staff, in developing today's agenda.

2 In the next few hours, we plan to first  
3 introduce the cyber-security staff, and followed  
4 by the Cyber-Security Regulatory Program elements.

5 Specifically, we want to provide you  
6 an overview on how we have developed and implemented  
7 the existing regulatory program, the various  
8 technical and regulatory products produced and to  
9 be produced, any notable domestic and international  
10 engagements, and how we are working the interface  
11 on those regulatory issues that have both safety  
12 and security considerations.

13 Our goal is that by the end of today's  
14 meeting, you will all have a clearer picture on  
15 the agency's cyber-security and regulatory  
16 program.

17 With that, I would like now to turn to  
18 Tom, for him to offer a few thoughts.

19 MR. BERGMAN: Yes, again, my name is  
20 Tom Bergman. I am the Director of Engineering in  
21 the Office of New Reactors.

22 Actually, the purpose of mine is to  
23 update all of you on the EMPOWER DSRS initiative.

24 We committed to periodically update you, as we

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealrgross.com](http://www.nealrgross.com)

1 make progress on that, and this is a very good  
2 opportunity.

3 So, this is a current status briefing.

4 It's subject to change. Much of what I'm going  
5 to talk about is influx. I hope that is enough  
6 caveats for what I'm going to go forward with.

7 Previously, the ACRS raised issues on  
8 communications independence and the cyber-security  
9 framework in new reactors, in numerous letters,  
10 and most recently, in the interpretation of a clause  
11 in IEEE 603, dealing with control of access, and  
12 that is the one where we committed to get back to  
13 you.

14 We've had a series of meetings in the  
15 staff. We tasked the Branch Chiefs involved from  
16 NSIR, NRO, NRR and Research, to come up with a set  
17 of options, which they presented to Division  
18 Management.

19 We refined it a bit, and late last week,  
20 we met with the Office Directors for NSIR, NRR and  
21 NRO, and they modified our proposals and added one.

22 We have engaged key stakeholders, but  
23 we need to re-engage, in particular OGC, on a couple  
24 of the options, as well as others, as we go forward.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealgross.com](http://www.nealgross.com)

1                   What was approved by the Office  
2 Directors was to move forward, to continue to  
3 explore three concepts in parallel, four new  
4 reactors.

5                   The first one is actually kind of  
6 already underway, and that is engaged licensees  
7 early during construction, regarding  
8 implementation of the cyber-security program and  
9 the I&C design.

10                  We've already had meetings with the  
11 licensee. We'll continue to do so.

12                  We're looking for an effort more like  
13 what NRR did with Diablo Canyon, and you're going  
14 to get briefed on that in more detail later, and  
15 then you'll also get briefed more specifically on  
16 the activities between NSIR and NRO on new reactors.

17                  The second item is to incorporate a  
18 requirement regarding cyber-vulnerabilities with  
19 respect to certain designs into the current 10 CFR  
20 50.55(a) (h) rule-making to endorse IEEE 603-2009,  
21 and this is still a concept. We haven't turned  
22 it over to the staff, to figure out how you would  
23 implement it, and if you can implement it.

24                  But the concept is that for those

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 designs that need an alternative or an exemption  
2 to the requirements in 50.55(a) (h), they would need  
3 to describe the cyber-vulnerabilities of their  
4 design that they've introduced through their  
5 design.

6 In other words, if they don't meet the  
7 requirements as written, and they come in under  
8 either 50.12 or 50.55(a) (a) (3), then they would  
9 need to address the cyber-vulnerabilities.

10 So, the assumption is that 50.55(a) (h)  
11 provides a decent system, all right.

12 The purpose of this requirement is to  
13 ensure that the cyber-vulnerabilities and the  
14 design are understood and there is a clear hand-off  
15 from the design certification vendor in the COL  
16 applicant and licensee, as to what aspects of the  
17 design do need to be addressed through the  
18 cyber-security program.

19 So, it doesn't really change the  
20 current framework of the cyber-security program  
21 in a safety base design. It augments or enhances  
22 the implementation of the program, by being clear  
23 up front, where there may be some vulnerabilities  
24 in the design with respect to cyber.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1           This approach is generic. It would not  
2 be specific to EMPOWER, as we currently envision  
3 it. It would -- if we can do it through this current  
4 rule-making, it would be done in a time frame that  
5 would support the EMPOWER review, as well as other  
6 new reactor reviews.

7           We believe it may address your  
8 concerns, as expressed previously, regarding the  
9 most recent letter. At this time, we do not expect  
10 to modify the staff's interpretation of what  
11 control of access is meant. We think this other  
12 requirement is more effective.

13           The third concept in parallel would be  
14 to develop a new regulation to consider the impact  
15 of design on cyber-security, and in the model that  
16 was discussed, was 2014-06, which is minimization  
17 of contamination.

18           Are you familiar with that regulation?

19           It's very short, that's why I brought the book.

20           It's actually really, only about a sentence.

21           It says -- it only applies to new  
22 reactors, and it says that, "They shall describe  
23 how the facility design and procedures for  
24 operation will minimize, to the extent practical,

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealgross.com](http://www.nealgross.com)

1 contamination of the facility and the environment,  
2 facilitate eventual decommissioning and minimize,  
3 to the extent practical, the generation of  
4 radioactive waste."

5 So, we think that sort of concept up  
6 front is workable. It's a good analogous rule in  
7 a different part.

8 That would be a long-term effort,  
9 because that is a whole new rule-making. So, it  
10 would go through prioritization and budgeting  
11 process, and with that, unless you have any specific  
12 questions for me.

13 CHAIRMAN BROWN: I guess I do have a  
14 question, in terms of -- I'm trying to connect the  
15 dots between radioactive contamination of the site  
16 during decommissioning, with --

17 MR. BERGMAN: Oh, no.

18 CHAIRMAN BROWN: -- control of access,  
19 or whatever you said.

20 MR. BERGMAN: You could replace  
21 contamination with cyber.

22 In other words, it would be that same  
23 framework of -- in new reactors, they have to look  
24 at their design and say, "Have we done things that

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 would mitigate the release of radioactivity, due  
2 to whatever?"

3 So, a lot of the plants are basically  
4 lined in stainless steel, right, to a -- certainly,  
5 anything that is handling radioactive waste is  
6 lined in stainless steel.

7 That's saying, consider the long-term  
8 consequences of operation early in the design.

9 The analogy is, you would say,  
10 "Consider the ramifications on -- of cyber-security  
11 on -- or of your design on cyber-security program  
12 later."

13 This is the longest term one that  
14 requires the most work. It's the most conceptual,  
15 but that is -- it's just a model. It's not going  
16 to be in Part 20. It would be, likely in Part 50,  
17 as a design requirement or potentially, in Part  
18 73 as a cyber-requirement.

19 But again, that is to augment the  
20 existing framework, but that would be a new  
21 rule-making.

22 So, when I say that is a long-term, I  
23 mean, typical rule-making from concept to the  
24 finalization that isn't of a crisis mode, you know,

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701



1 it's five-ish years.

2 CHAIRMAN BROWN: Right, I'll be dead  
3 by then, potentially.

4 MR. BERGMAN: Well, we do a lot of  
5 rule-making for the agency. So, it has to enter  
6 that whole process. That is why the second one  
7 is more the near-term fix.

8 CHAIRMAN BROWN: But yes, the second  
9 one, I'm trying to get a little -- that was the  
10 second question was, you talked about if a licensee  
11 or a designer, whichever, I've forgotten the  
12 terminology you used, when you went through the  
13 phrases, requires an exemption from  
14 50.55(a)(h)(2), I think you said, which (a)(h)  
15 implements 603.1991, if I remember correctly.

16 MR. BERGMAN: Yes.

17 CHAIRMAN BROWN: And the issue we  
18 brought up is, we've separated the cyber thought  
19 process from the existing regulations that require  
20 the plant design to provide control of access, and  
21 that the engineer -- the design of the plant has  
22 to do that.

23 So, are you saying that they would be  
24 exempted? They would apply for an exemption and

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 say, "No, we don't have to provide for control of  
2 access," is that the --

3 MR. BERGMAN: So, we're trying to --

4 CHAIRMAN BROWN: I'm trying to connect  
5 the dots on that.

6 MR. BERGMAN: Whether they need an  
7 exemption or an alternative, without getting too  
8 deep into 50.55(a), depends where the requirement  
9 exists in 50.55(a).

10 Some parts of it require an  
11 alternative. Some parts of it would require an  
12 exemption.

13 CHAIRMAN BROWN: Yes, but 603-1991 is  
14 very specific.

15 MR. BERGMAN: Right.

16 CHAIRMAN BROWN: And that's  
17 implemented -- you know, that is actually a part  
18 of the rule, that says you have to design your plants  
19 in accordance with that, which talks about control  
20 of access, very clearly.

21 And it says, not only do you have to  
22 have procedures to do that, you have to have a plant  
23 design that allows you to execute it. That's got  
24 to -- you know, the plant has to accommodate to

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 be able to do that.

2 Therefore, that means -- and the point  
3 we've tried to make is, we've got to consider those  
4 types of things during the DCD or the licensing  
5 process, not post, not wait. That was the point  
6 of our last -- that was the -- you know, one of  
7 the three points that we made in our last letter  
8 in EMPOWER.

9 So, I'm having a little bit of  
10 difficulty of connecting those dots, in terms of  
11 an exemption or where they -- that the --

12 MR. BERGMAN: You know, if you need it  
13 -- if you meet it, and it would be 2009 we're talking  
14 about, right. This is the new -- this is the  
15 rule-making to endorse the more recent edition of  
16 the standard.

17 CHAIRMAN BROWN: Yes, I haven't read  
18 the 2009 for control of access, but I've -- isn't  
19 it the same?

20 MR. BERGMAN: I don't know on that  
21 specific clause, but in the -- in a rule-making  
22 like this, much is -- I mean, if you look at  
23 50.55(a), most of it is staff exceptions to the  
24 codes and standards.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealrgross.com](http://www.nealrgross.com)

1           So, you have the standard, plus you have  
2 the staff exceptions to the standard. That  
3 combination of requirements, if met, we would say,  
4 they need to do nothing. We would rely solely on  
5 the -- on the existing framework.

6           If they do not meet all those  
7 conditions, then they would need to come in under  
8 -- with either an alternative -- let's just use  
9 alternatives, to keep it simple, an alternative.

10           In that case, where they need an  
11 alternative to meeting the rule, as written, then  
12 they need to address the cyber-vulnerabilities in  
13 the design, that they've introduced, by not meeting  
14 the --

15           CHAIRMAN BROWN: Okay, let me put this  
16 -- let me craft this into something I can  
17 understand.

18           I understand your general point, at  
19 least two of the new designs, I'm pulling on my  
20 memory, over the last three years now, that we've  
21 looked at maybe three, and referencing this to the  
22 concern we raised with EMPOWER.

23           In other words, you've got the  
24 safeguard systems and the reactor trip systems all

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 feeding a giant network, which goes up to the main  
2 control room, and the technical support facility  
3 center.

4 That network has a computer on it, which  
5 then connects to the outside world, either the  
6 business network or the corporate network, or call  
7 it whatever you want. It goes -- it leaves the  
8 plant.

9 MR. BERGMAN: Leaves the page.

10 CHAIRMAN BROWN: That is right, and  
11 that computer, in the earlier versions that we had  
12 talked about, has a firewall in it, but it is a  
13 software based firewall. It could have been a  
14 software -- in fact, as one said, it would be, but  
15 they hadn't really -- you know, it was part of the  
16 design, and they hadn't done it yet, and so, we  
17 had that interchange in the earlier -- in the  
18 meetings.

19 Now, the rule is -- doesn't get real  
20 specific, in terms of how you do that. We've tried  
21 to make the point that it needs to be an  
22 incontrovertible hardware one-way firewall, not  
23 something subject to a hacker, playing games with  
24 bits and bytes, to allow himself access, and I use

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealgross.com](http://www.nealgross.com)

1 -- you know.

2           There has been examples where plants  
3 in existence today, with some systems connected  
4 off to a business network somewhere through a  
5 firewall, somebody left the firewall in a two-way  
6 communication mode, while they were updating their  
7 software, and ended up getting some error code back  
8 in the rest of the plant, not a fun circumstance  
9 to have to clean up.

10           So, I'm trying to envision how this  
11 works, if they come in, in this design and they  
12 say, "Well, ghee, we're going to ignore the obvious,  
13 and say we're so smart, we can manage having people  
14 pound us to death with hackers for the next 40 or  
15 60 years," and constantly changing software all  
16 the time.

17           Therefore, "We're going to tell you why  
18 it's going to be okay," from a cyber -- that is  
19 -- that is what I get out of the comment that you're  
20 making.

21           They have to justify not doing it the  
22 right way.

23           MR. BERGMAN: And that is -- and there  
24 is interplay between this -- this potential new

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 requirement and what is already in 50.55(a)(h),  
2 right.

3 So, without -- that is -- that  
4 regulation is currently being worked on by the  
5 staff, and there is a healthy and diverse range  
6 of views of how restrictive, going from, you know,  
7 nothing to hardware based only, to allowing  
8 software controls under certain conditions.

9 Where we'll end up, we don't know,  
10 right. So, but where we end up does influence the  
11 effect of this new requirement.

12 So, that will be worked out, through  
13 that rule-making, and you'll have an opportunity  
14 to weigh in on that rule-making. I think we're  
15 coming to you in the October time frame.

16 So, yes, it does --

17 CHAIRMAN BROWN: Well, in 603 --

18 MR. BERGMAN: You picked up on the  
19 point --

20 CHAIRMAN BROWN: -- 2009?

21 MR. BERGMAN: Yes.

22 CHAIRMAN BROWN: And 55(a)(h)?

23 MR. BERGMAN: Yes.

24 CHAIRMAN BROWN: Whatever.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. BERGMAN: Yes, so, you're correct.

2

3 How that rule is written affects how  
4 those types of designs would be viewed and what  
5 -- whether or not they would need an alternative  
6 to that regulation, addressing their  
7 vulnerabilities.

8 But understand, this concept that has  
9 been agreed to explore wouldn't preclude a design  
10 having those vulnerabilities by itself, right.

11 It says you need to explicitly  
12 acknowledge what the vulnerability is, so that the  
13 COL applicant understands the vulnerability they  
14 will need to address, that is created by the design,  
15 through their program.

16 So, it leaves intact the safety based  
17 review we do today, coupled to a cyber-security  
18 program, but highlights very early, before the COL  
19 has, in theory, even been applied for, but  
20 certainly, before it's been issued, that this  
21 design has these features that create known  
22 cyber-vulnerabilities.

23 CHAIRMAN BROWN: Okay, I'm going to  
24 make a personal comment that doesn't reflect the

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701



1 views of the Committee, if you don't mind. Okay,  
2 Sam? Thank you, since I said that --

3 MEMBER ARMIJO: I didn't say it,  
4 because I want to make a comment too.

5 CHAIRMAN BROWN: I guess, I just want  
6 to make an observation, relative to the networks  
7 and this interplay between how you get data in and  
8 out, or if you do.

9 Obviously, zero going -- no connection  
10 is a great way to do it. You would never get any  
11 argument from me, okay, and I've made the point  
12 -- or through the Committee, which we've agreed  
13 with, that hardware one-way incontrovertible can't  
14 be modified -- can't be changed by any way, other  
15 than ripping it out and putting in some new  
16 hardware.

17 We would accept that, okay, as a  
18 satisfactory means of getting stuff outside the  
19 plant.

20 The third way obviously, we're not --  
21 I personally wouldn't be particularly happy with,  
22 although that would be one of the options, but one  
23 of the things that has been my major -- one of my  
24 major concerns, this is not -- plant is not an

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 information technology system.

2 You can't just be constantly changing  
3 cyber-security protection software down in the  
4 plant, while the plant is operating. I mean, you  
5 just can't go put patches in, every other day.

6 It's not like sitting at home, "Oh,  
7 ding, your software has been updated. Restart to  
8 fix it again," or to make it viable in operation.

9 It just doesn't work that way.

10 I mean, you've got a two-year refueling  
11 cycle, when you have an opportunity to go in and  
12 make changes, and patches, and the way these smart  
13 people that are hacking stuff are operating,  
14 they're changing stuff on a daily basis.

15 I mean, every day I come in, my software  
16 has been updated, every day, and so, it -- this  
17 thought process, you are the regulator in charge  
18 of protecting these plants, and making sure they're  
19 satisfactory.

20 So, I am just giving you a thought  
21 process here that there is an opportunity to make  
22 sure this comes out right.

23 MR. BERGMAN: We certainly understand  
24 that perspective and like I say, it's one of --

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealrgross.com](http://www.nealrgross.com)

1 we got the full spectrum of perspectives, a healthy  
2 and diverse range of views within the --

3 CHAIRMAN BROWN: I didn't say they were  
4 all healthy.

5 MEMBER ARMIJO: Yes, I don't agree with  
6 the healthy part.

7 If you just designed a new  
8 instrumentation and control system for a nuclear  
9 power plant, and you recognize that it already has  
10 existing vulnerabilities to cyber-attack, hackers,  
11 why wouldn't you just fix it? Why do you just --  
12 you know, why would you even design a system like  
13 that?

14 MR. BERGMAN: I think --

15 MEMBER ARMIJO: Sure, you can design  
16 a system that everybody agreed was great, and then  
17 in time, a new vulnerability was discovered, you  
18 know, that is fair.

19 CHAIRMAN BROWN: Probably take it to  
20 --

21 MEMBER ARMIJO: But you know, if it's  
22 just software based, it is maybe seconds later,  
23 I don't know.

24 So, just the problem is, are these

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 systems really fundamentally being -- these  
2 problems being addressed at the right point in the  
3 architecture, as Charlie has pointed out many  
4 times, of the design, and there is very --

5 MR. BERGMAN: And that will be the  
6 process we go through to develop --

7 MEMBER ARMIJO: This is very, very  
8 troubling, that --

9 MR. BERGMAN: Right, that is the  
10 rule-making process. We'll go through that, as  
11 we finalize -- I shouldn't say finalize. It hasn't  
12 gone out for proposed yet. Before it goes out for  
13 proposed rule-making.

14 CHAIRMAN BROWN: Well, the --

15 MR. BERGMAN: That is part of the  
16 debate that is ongoing.

17 CHAIRMAN BROWN: Well, 603-2009 change  
18 is a primary opportunity short-term --

19 MR. BERGMAN: Yes.

20 CHAIRMAN BROWN: -- to get it right and  
21 make it right and keep it right, and it really --  
22 and then it obviates something.

23 You can do whatever you want to with  
24 the five-year rule, but this certainly takes the

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealrgross.com](http://www.nealrgross.com)

1 issue kind of off the table, for the most part,  
2 if you get it right, and it's very easy.

3 If 2009 version has the same words as  
4 1991, you can just say, "We accept this, however,"  
5 bang, put that in the rule, and that makes it easy.  
6 It's done.

7 MR. BERGMAN: It's never easy.

8 CHAIRMAN BROWN: And it is --

9 MR. BERGMAN: Rule-making is never  
10 easy.

11 CHAIRMAN BROWN: Well, that is the --

12 MR. BERGMAN: It's a fickle beast.

13 CHAIRMAN BROWN: Anyway, all right,  
14 Sam, do you have any other comments?

15 MEMBER ARMIJO: No, I think we're just  
16 feeling disagreement, that's all.

17 MEMBER BLEY: No, I'd just note that  
18 the things we've been urging are a little bit akin  
19 to the evolution of designs towards something that  
20 hopes to be inherently safe, and we're looking for  
21 something that is inherently resistant, and it's  
22 hard to see that happening in software.

23 CHAIRMAN BROWN: I want to amplify that  
24 a little bit, since I don't know when to stop

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealrgross.com](http://www.nealrgross.com)

1 talking.

2 When going from analog systems to the  
3 digital computer based systems, we've gone from  
4 individual electrically driven, you got four  
5 temperature instruments, you got four temperature  
6 instruments. You got four pressure detectors,  
7 you've got four pressure detectors.

8 You got four neutron high range.  
9 You've got so many source range. You've got so  
10 many whatever, flow, individual pieces all lumping  
11 and making their own particular two out of this,  
12 two out of that, two out of whatever, and you can't  
13 -- nobody can touch those. The only access is to  
14 go down to the cabinet and start tweaking  
15 potentiometers.

16 But with the digital computer approach,  
17 they've -- that -- those 20 instruments have now  
18 been integrated into four trains.

19 You've got all kinds of instruments --  
20 sensors feeding one train, and another diverse set  
21 -- not diverse. Another similar set, equal set,  
22 feeding the next, and on down the line.

23 So, we've increased the integration.  
24 We've made it -- if we've increased the

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealgross.com](http://www.nealgross.com)

1 connectivity vastly with the networks and  
2 everything else that are going on, still the problem  
3 of maintaining independence and making these  
4 designs inherently safe has been compounded  
5 exponentially, by going that direction.

6 And if anything is proved that you need  
7 to pay attention to this now, it's just watching  
8 what is going on, I mean, even with the latest  
9 pilfering of our defense infrastructure and half  
10 the secrets of our defense contractors being pumped  
11 over to China.

12 MR. BERGMAN: And I think you've seen  
13 that in our reviews of the more complex designs  
14 we've had.

15 They're very difficult to -- for the  
16 applicants to show they meet the regulations and  
17 are acceptable, and for our staff to find them,  
18 right. Those are very lengthy reviews, largely  
19 driven by that connectivity and inter-dependence.

20 CHAIRMAN BROWN: Okay, well, we should  
21 probably get on with the rest of this.

22 MR. BERGMAN: Rest of this. We're  
23 going to make it up right now.

24 CHAIRMAN BROWN: That's all right,

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 this was a useful discussion. I do appreciate --  
2 Tom, I appreciate you coming down and taking the  
3 time to go through the status and the update, with  
4 what you're all doing and where you're going,  
5 because it gave us an opportunity for this  
6 interchange.

7 By the way, Bill, I didn't ask you if  
8 you had any comments.

9 MEMBER SHACK: You guys covered it  
10 pretty well.

11 CHAIRMAN BROWN: Anything else?

12 MEMBER BLEY: Yes, if you're leaving,  
13 I would like to say the idea that across NRC's  
14 divisions, you're looking at this as a whole group,  
15 is very good, and we're pleased to see that.

16 CHAIRMAN BROWN: No, I agree with that,  
17 also. Thank you very much.

18 MR. BERGMAN: Thank you.

19 CHAIRMAN BROWN: I didn't know that you  
20 intended to stay or not, and enjoy this.

21 MR. BERGMAN: Until this Panel exits,  
22 you know.

23 CHAIRMAN BROWN: Okay, all right, you  
24 all can proceed on your process.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealrgross.com](http://www.nealrgross.com)



1 MR. BERGMAN: Yes, thank you, Charlie.

2 MR. ERLANGER: Good afternoon,  
3 everyone. My name is Craig Erlanger. I'm the  
4 Chief of the Cyber-Security and Integrated Response  
5 Branch.

6 As Christiana mentioned, I'm joined by  
7 Ron Albert, who is the Branch Chief, responsible  
8 for the Oversight Branch, and that's the Reactor  
9 Security Oversight Branch. Next slide, please.

10 What we would like to do for the next  
11 couple of minutes is orient you to our organization.

12  
13 I think historically, we've done a hot  
14 start with these meetings, assuming that you  
15 understand how NSIR is organized and who is who  
16 in the organization.

17 We recognize that we don't interact  
18 with you as frequently as the other offices, so,  
19 we thought it would be helpful, just to spend a  
20 few minutes on the front end.

21 We are very sensitive to our use of  
22 acronyms today. So, we will do our best not to  
23 use them, but what we try to do is highlight a few  
24 in here that you'll probably hear throughout the

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealrgross.com](http://www.nealrgross.com)

1 day, in the hopes of just heading that dialogue  
2 off.

3 A little bit about the agenda today.

4 What I will mention is the order has been slightly  
5 modified, due to the open and closed sessions today.

6  
7 I'll be followed by Mr. Perry Pederson  
8 and Mr. Tim Mossman, who will give an overview of  
9 the cyber-security program.

10 Again, part of our thought process on  
11 that is, there is some new faces out here who weren't  
12 here the last time we met, and we thought it would  
13 be helpful to spend a little bit of time, to explain  
14 the existing requirements and what Part 73 is all  
15 about, specifically, Part 73.54 of the  
16 cyber-regulation.

17 The topics you see up there, we are  
18 definitively going to give you some insights into  
19 the oversight program, talk a little bit to extend  
20 -- to expand upon the previous comment about our  
21 inter-office coordination and how we've been taking  
22 some of the ACRS feedback and translated it to  
23 action and improvements we've made in that area.

24 Next slide, please.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealrgross.com](http://www.nealrgross.com)

1           We came up with three desired outcomes,  
2           and hopefully, they're in line with what your  
3           expectations are for the day.

4           We, first and foremost, want to give  
5           you an overview of the program and explain how it's  
6           being implemented today.

7           Since we started interacting with ACRS  
8           on this topic, and it was for the endorsement of  
9           Regulatory Guide 5.71, we are actually out there  
10          today, inspecting interim milestones.

11          So, we can share with you, some insights  
12          on how that is going and where the program is today  
13          and where it's headed.

14          We obviously want to improve our  
15          communication and coordination with ACRS, and we  
16          think this meeting is a good step to do that, and  
17          we'll continue the dialogue.

18          Throughout the day, I'm sure we're  
19          going to identify some areas of interest for future  
20          interaction, and we should take note of that, and  
21          when we wrap up the day, just agree and understand  
22          what you want to hear a bit more about. Next slide,  
23          please.

24          A little bit about NSIR. NSIR,

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealrgross.com](http://www.nealrgross.com)

1 probably similar to the many organizations in the  
2 Federal Government, was formed post-9/11 to react  
3 to some of the threats out there, and just the  
4 environment that the United States was in at the  
5 time.

6           You know, our mission is to prevent  
7 nuclear security incidents and prepare for and  
8 respond to safety and security events.

9           The regulations you'll find in Part 73  
10 are all predicated on preventing a malicious actor  
11 from doing bad things, where in historically,  
12 you've dealt more with Part 50 and Part 52, which  
13 were based on safety and reliability.

14           Those two intersect at various points  
15 throughout the regulatory framework, and we'll hope  
16 to amplify and explain that a bit more, as we go  
17 through today.

18           We have three technical divisions, and  
19 this is where you'll start hearing some acronyms  
20 throughout the day.

21           Division of Security Policy, in a  
22 general sense, we handle everything from  
23 rule-making to licensing, in that division.

24           The Division of Security Operations,

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 that is your oversight, inspection, your  
2 contemporary issues, as well as our intelligence  
3 function, as it relates to cyber.

4 The Division of Preparedness and  
5 Response, they deal with not only EP issues, but  
6 they also deal with the manning of the Operation  
7 Center.

8 As many of you are aware, the NRC has  
9 a 24 by 7 Operations Center. There is some  
10 connectivity and relationship due -- related to  
11 cyber-security and reporting, which will grow over  
12 the coming years, and they have a piece of that,  
13 as well.

14 We have, similar to most organizations  
15 with the NRC, a PMDA type function, but these are  
16 the three technical divisions that we have in our  
17 organization today.

18 Very quickly, this is the -- the current  
19 organization as it stands today, within the  
20 Division of Security Policy, there is two branches,  
21 the branch that I represent, the Cyber-Security  
22 and Integrated Response Branch. The painful  
23 acronym you'll hear is CSIRB, throughout the day.

24 We focus on rule-making, guidance,

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 licensing. A topic called the cyber-security  
2 roadmap, which you'll hear about in a later  
3 presentation, this is a -- tracked on something  
4 called SECY-12-0088.

5 It recognizes the existing regulatory  
6 framework for operating reactors and new reactors,  
7 but also discusses the path forward for fuel cycle  
8 facilities, non-power reactors ISFSI's and  
9 byproduct material licensees.

10 So, we'll give you some insights on  
11 larger agency programs, as they relate to  
12 cyber-security and where we think the agency is  
13 headed.

14 You'll see this statement,  
15 inter-governmental and international coordination  
16 throughout these next couple of slides.

17 Both divisions, Division of Security  
18 Policy, Security Operations and I'll even say  
19 Division of Preparedness Response, have  
20 inter-governmental and international ties, due to  
21 what their focus areas are.

22 So, we all interact in the  
23 inter-government. There is no one clear -- or  
24 there is no one point of contact to work with one

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 agency.

2 The best example would be Department  
3 of Homeland Security, and my folks focus on policy  
4 issues, where the Oversight Branch would focus on  
5 getting advisories from organizations like US and  
6 ICS-CERT, those type of things.

7 So, we have a -- basically, we're a  
8 matrix organization, is the thought I would leave  
9 you with.

10 Fuel Cycle and Transportation Security  
11 Branch, we will go into greater detail on this topic  
12 later today, and what they support, and this is  
13 the cyber-security roadmap and activities related  
14 to cyber-security and fuel cycle facilities.

15 They are supported to a great extent,  
16 by NMSS, so, we matrix with another organization,  
17 as well as two branches within the Division of  
18 Security Policy.

19 We'll be able to give you an update of  
20 where those activities are in a general sense.  
21 We've gone out there. We've looked and we're  
22 preparing some recommendations on a path forward,  
23 and am going to present that to Commission in the  
24 short-term, but we'll get into some details about

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealgross.com](http://www.nealgross.com)

1 that in a bit today. Next slide, please, Chris.

2 For the Division of Security  
3 Operations, as the title alludes to, they're  
4 dealing with operational real -- things that are  
5 happening today.

6 So, they're dealing with -- dealing  
7 with the threat picture, as well as overseeing the  
8 inspection programs.

9 They also deal with something called  
10 the Cyber-Assessment Team. We'll speak in detail  
11 about this later today, and how the NRC deals with  
12 real threats, when we're made aware of a piece of  
13 malware out there, how do we get that information  
14 out to our licensees? How do we share information  
15 across the board?

16 So, they'll give you some insights on  
17 how we do that in a real sense today.

18 As I previously mentioned, they also  
19 deal with inter-government and international  
20 coordination. They also serve as our liaison to  
21 the Regions, and work with them on a daily basis.

22 The Intelligence Liaison Threat  
23 Assessment Branch, ILTAB, just as it says, they  
24 focus on cyber-security threat analysis and

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701



1 inter-governmental and international  
2 coordination. They are our liaison to the  
3 intelligence community.

4 We actually -- and you'll hear from  
5 Perry Pederson shortly. He has just accepted a  
6 position in that branch, where he is a  
7 cyber-security intelligence analyst over there.

8 This is the first time we've had that  
9 position at the agency. So, we're growing the  
10 program in that area, as well. Next slide, please.

11 A little bit about staff experience,  
12 and this is a, I guess --

13 CHAIRMAN BROWN: Wait a minute.

14 MR. ERLANGER: Sure, Charlie.

15 CHAIRMAN BROWN: Let me ask you one  
16 thing. Can you back up, just a second?

17 MR. ERLANGER: Absolutely.

18 CHAIRMAN BROWN: On the -- when you're  
19 talking about the Security Oversight Branch, and  
20 you talked about -- your set up, to be able to at  
21 least monitor what the threat picture is in general,  
22 in the country, or around -- or from whom, or is  
23 this via commercial threats, as opposed to those  
24 that are identified in other areas, and then you

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 pass those on?

2 Is there something that the licensee  
3 -- I mean, this is his stuff, once he's got the  
4 plants up and running.

5 MEMBER BLEY: By the way, if we ask  
6 anything that ought to be put off to the close  
7 session, let us --

8 CHAIRMAN BROWN: Yes, thank you.

9 MEMBER BLEY: You have to remind us.

10 MR. ERLANGER: Absolutely.

11 CHAIRMAN BROWN: Yes, I don't think I'm  
12 going to get into that, but my point being is that  
13 -- not specifics, but where is the division? Where  
14 does this licensee responsibility begin?

15 I mean, it would seem to me, once  
16 they've taken over and they're operating, then are  
17 they expected to have a staff that is constantly  
18 -- separate the plant --

19 MR. ERLANGER: Sure.

20 CHAIRMAN BROWN: -- that interface  
21 that I talked about, you know, that thing that talks  
22 out to the business network. They've got to take  
23 care of the rest of their site.

24 They obviously don't want all their IT

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 systems going belly-up, while they're, you know,  
2 trying to run this plant, for a lot of different  
3 reasons.

4 So, that is one set of threats. Then  
5 there is another set of threats that you wouldn't  
6 expect, if you design the thing correctly, to ever  
7 get into the plant type systems.

8 So, do you expect them to have an  
9 organization that is primarily responsible for  
10 making sure their systems are safe and secure, or  
11 it's not totally your responsibility?

12 MR. ERLANGER: I think I can answer  
13 that in this setting, but I will tell you, the level  
14 of detail we can provide in the closed setting will  
15 give you --

16 CHAIRMAN BROWN: Okay.

17 MR. ERLANGER: -- a bit more.

18 Licensees do have organizations that monitor the  
19 threat environment. They have access to  
20 information provided by the Department of Homeland  
21 Security.

22 There is the industrial control systems  
23 cyber-emergency response team and the U.S. computer  
24 emergency response team, passed the advisories.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 There is a hard-token method that they can get that  
2 information from.

3 Part of the requirements we've built  
4 into the cyber-plan is, the licensee needs to be  
5 able to be aware and monitor the threat environment.

6 That being said, we do have a  
7 responsibility, that once we learn this  
8 information, we have to get it out there in a timely  
9 manner.

10 A part of the -- I guess, what I'll call  
11 the landscape today is, there is a proposed  
12 rule-making related to reportability, Appendix G  
13 to Part 73. It's out there, and that will have  
14 a cyber component that will help codify the  
15 reporting requirements.

16 It's already been out for public  
17 comment. It's not, as I think Tom alluded to,  
18 something that we're starting fresh, that we have  
19 to go through a whole rule-making process.

20 What we did in the interim is, we put  
21 a security advisory. It's marked OOU Security  
22 Related Information, related to reportability and  
23 the type of information we would want to hear from  
24 licensees, if they find out something is going on

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 in their facilities.

2 But to answer your question, it's a  
3 joint shared responsibility, and when we learn  
4 something, we want to get it out as soon as possible,  
5 but there is also a responsibility of the licensees,  
6 to monitor the threat-scape and understand what  
7 is going on out there.

8 DHS plays a pivotal role in that  
9 function of sharing information.

10 MR. WESTREICH: Craig?

11 MR. ERLANGER: And we will talk about  
12 it in -- actually, the mechanics of it, in the closed  
13 session this afternoon.

14 CHAIRMAN BROWN: Okay.

15 MR. WESTREICH: Craig, just to  
16 respond.

17 There is some information -- there is  
18 plenty of information that licensees aren't able  
19 to get, classified Government information that we  
20 --

21 So, this Intelligence Liaison Threat  
22 Assessment Branch is the liaison to provide -- get  
23 that information from the Government intelligence  
24 community, then we package it in a way that we can

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealrgross.com](http://www.nealrgross.com)

1 provide to the licensee community, so they can take  
2 action.

3 But in some cases, we're the only  
4 connection they are going to have to that  
5 information.

6 CHAIRMAN BROWN: Okay, I can  
7 understand it at some levels.

8 MR. ERLANGER: Does that satisfy for  
9 the --

10 CHAIRMAN BROWN: Yes, I mean, one of  
11 the driving reasons for my question was, when you  
12 get into the switch yard, and I'm not talking about  
13 balance of plant, but out in the switch yard, all  
14 of the switch yard breakers and everything else  
15 are not totally under control of the local  
16 operators, in terms of how they connect to the grid.

17 Those are, in many circumstances, maybe  
18 all now, I don't know, are reportedly subject to  
19 this state of type supervisory control and what  
20 is it, data acquisition, where the remote grid  
21 operator can control those breakers and open --  
22 so, if somebody hacked in, you're subject to a  
23 complete -- a loop -- a loss of offsite power, if  
24 they trip everything off, and now, you're into a

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealgross.com](http://www.nealgross.com)

1 comp.

2 So, that is -- you don't have to say  
3 anything more. That is the reason I asked the  
4 question about, I presume the licensee doesn't have  
5 any control over that part of it, but yet, their  
6 plant has to be inherently safe, with respect to  
7 it.

8 Now, we have requirements for that, but  
9 it is -- it just seems to me, it's -- you're much  
10 more set up to end up in a circumstance where  
11 somebody can do some damage -- damage, that is the  
12 wrong word. Some -- create a problem in the plant,  
13 that you have to deal with, without -- totally  
14 outside your control.

15 MR. ERLANGER: Yes.

16 CHAIRMAN BROWN: And that was one of  
17 the reasons I was asking a little bit about their  
18 organizational capabilities.

19 MR. ERLANGER: In another  
20 presentation, that I think will add a little bit  
21 to this conversation is, our -- when Tim Harris  
22 gets up here and speaks about our  
23 inter-governmental relationships, our  
24 relationship with the Federal Energy Regulatory

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 Commission and the North American Electric  
2 Reliability Corporation for Grid Issues, we can  
3 kind of step through what -- where that relationship  
4 is, and I think that will answer some of --

5 CHAIRMAN BROWN: All right.

6 MR. ERLANGER: Some of your questions.

7 CHAIRMAN BROWN: Thank you.

8 MEMBER BLEY: Yes, and we'll be looking  
9 forward to hearing how that is formalized, how that  
10 works.

11 MR. ERLANGER: Absolutely. A little  
12 bit -- this is very briefly on staff experience.

13 Cyber-security touches so many aspects  
14 of plant life, as you're well aware, from the safety  
15 side to the maintenance side, to the operations  
16 side.

17 What we've recognized over the last  
18 couple of years is, it takes a village type  
19 mentality to get this done.

20 We have so many disciplines that  
21 support this program. You look at it, you look  
22 at a little bit about backgrounds.

23 The staff has -- they have worked in  
24 every office, virtually every major office in the

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701



1 agency. They come from private sector companies.

2 Strong backgrounds in digital I&C and industrial  
3 control systems, electrical information --  
4 electrical engineering and information technology.

5 There is no one cyber-security  
6 specialist who can do it all.

7 So, I think one thought we're trying  
8 to convey today is, and you'll hear more about it  
9 in our inter-office framework, we fully recognize  
10 and appreciate it. It takes a -- it takes a group  
11 of people to get this done, and this program really  
12 touches virtually every aspect of the plant life.

13 MEMBER BLEY: You didn't mention  
14 operations. Do you have former operators?

15 MR. ERLANGER: I'm sorry, I thought --  
16 yes, we have people who have operational  
17 experience, whether they're exactly SRO's, I can't  
18 speak to that. I know organic to my branch, I do  
19 not have a former SRO in my branch, working on this  
20 today.

21 But you have Senior Resident  
22 Inspectors, you have people who are employed by  
23 utilities, out there working in digital I&C shops,  
24 but whether they're actual operators, I can't

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 answer that right now, sir.

2 MEMBER BLEY: Okay.

3 MR. ERLANGER: Okay, next slide,  
4 please. That concludes my portion.

5 Up next is -- and thank you for allowing  
6 me to get through that pretty quickly.

7 Perry Pederson is going to come up with  
8 Tim Mossman, and we're going to begin our technical  
9 presentation, if that is -- if there is no further  
10 questions.

11 MR. HECHT: This is Myron Hecht,  
12 calling from Los Angeles. I am just wondering if  
13 I could ask a question, with regard to ICS-CERT?

14 MR. ERLANGER: Absolutely.

15 MR. HECHT: The ICS-CERT has a number  
16 of advisories. Among them, the ones I find the  
17 most interesting are the ICS vendors or others  
18 reporting on the vulnerabilities that they find  
19 in their control systems, and in some cases, these  
20 vulnerabilities can't be solved by a simple patch.

21 Leading to this in the previous  
22 presentation on -- or discussion on the three  
23 conceptual approaches, how is it that major  
24 vulnerability in the ICS, not necessary an alert

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealrgross.com](http://www.nealrgross.com)

1 due to a virus or something like that, but a major  
2 vulnerability in a I&C application that is  
3 installed at a plant, would be handled?

4 MR. ERLANGER: Myron, can I ask just  
5 a clarifying question, and I'm going to need some  
6 help from some of my oversight folks, who deal with  
7 this on a day-to-day basis.

8 Is your question -- to restate your  
9 question, if we learn from ICS-CERT that there is  
10 a vulnerability related to CERT and industrial  
11 control system, is your question, what do we do  
12 with that information? I'm not sure I'm following.

13 MR. HECHT: What is the expectation of,  
14 how shall I say it, solving that problem from the  
15 plant and from your office and the entire process,  
16 I guess?

17 How does the problem get fixed, from  
18 the time that the vulnerability is noted, and I'm  
19 pausing that as a major system vulnerability, and  
20 that might require re-installation of a -- you know,  
21 a major server, or a number of servers.

22 MR. ERLANGER: Well, I think the first  
23 step -- I can speak to it from the policy side.

24 We want to get that information out

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 there, right away. We don't maintain a catalogue  
2 of what industrial control systems are at every  
3 site.

4           Ralph, are you walking up this way?  
5 Mr. Ralph Costello, from the Division of Security  
6 Operations, who works with the Cyber-Assessment  
7 Team, is going to add some remarks.

8           But we would get the information out  
9 there, and I'll just let Ralph.

10           MR. COSTELLO: Yes, sir, I think that  
11 is a very good question.

12           Obviously, each industrial control  
13 system is different. Each potential vulnerability  
14 is different.

15           To give you a blanket answer, would  
16 probably not be answering appropriately, but let  
17 me give you an example.

18           If say, there is an industrial control  
19 system design, I won't mention any names, that has  
20 an apparent vulnerability and the licensee hears  
21 about it through ICS-CERT, obviously, they have  
22 multiple ways to secure an incident.

23           In many cases, in ICS systems, the  
24 vendors haven't done a lot of security

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 implementations, but some are doing it.

2 With that being said, there is ways in  
3 which they can prevent the spread, and this is a  
4 simple answer, first, the elimination of the  
5 pathway, and then screening for, obviously, the  
6 virus definitions, if they exist.

7 Also, there is an anomalous detection,  
8 which should be going on in your ICS system, up  
9 front. Does that answer your question?

10 MR. HECHT: In part. That is  
11 basically saying now, you've gotten an alert. The  
12 immediate response is basically, do what you can  
13 to mitigate the problem.

14 But I guess my question is, you have  
15 to do a re-install or a major upgrade. What happens  
16 next?

17 MR. COSTELLO: Well, without going  
18 into a specific scenario, it would be hard to know  
19 what they would do.

20 It may be a simple fix. Then again,  
21 it may be a more complicated fix, like you just  
22 mentioned.

23 I can tell you, the Department of  
24 Homeland Security is working closely, not only with

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 our industry, but with vendors also, and in this  
2 open setting, I can't go into more detail, but I'd  
3 like to in the closed setting, if I am permitted.

4 MR. ERLANGER: Myron, maybe -- you  
5 know, any digital asset that is brought into the  
6 environment has to go through a whole -- a very  
7 robust process.

8 This would be no different from the  
9 sense that if there is a problem with a particular  
10 system, if it's within scope of the cyber-security  
11 rule, i.e., it performs a safety/security emergency  
12 preparedness function, there would be a deliberate  
13 process to re-introduce it into the environment.

14 How to do that is spelled out in detail  
15 in the Regulatory Guide, but that would be, the  
16 licensee would follow a process, to make sure it's  
17 okay, before it's up and running again.

18 We can talk -- I mean, as Ralph said,  
19 probably if -- I don't know if we answered your  
20 question.

21 CHAIRMAN BROWN: Yes, Myron, we're  
22 going to go on, on this.

23 I don't want to get -- I understand --  
24 I think I kind of understand your question, from

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 the standpoint of, if a vendor makes a PL -- a  
2 programmable logic control, for instance, and there  
3 is -- it's installed in some industrial control  
4 systems, and they identify a vulnerability with  
5 it, and we've got it installed in say, all the  
6 circuit breakers, control circuits at one of the  
7 plants, we obviously have some vulnerability, under  
8 those circumstances. The plant has a  
9 vulnerability.

10 So, how is that dealt with? Is that  
11 an example of what you're talking about?

12 MR. HECHT: Yes.

13 CHAIRMAN BROWN: Okay, so, I guess the  
14 question was, well, how do you deal with that, and  
15 I'm not sure you can be as specific, other than  
16 to say, somebody has to figure out what to do, once  
17 they know what the vulnerability is.

18 MR. HECHT: Well, I guess the point is  
19 that we should be considering not only the --  
20 solving the problem of the vulnerability, but also,  
21 the additional impact on safety, and how do we do  
22 that?

23 CHAIRMAN BROWN: I think you have to  
24 think about that at the time, once you know what

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 it is.

2 MR. HECHT: Right.

3 CHAIRMAN BROWN: All right, we've got  
4 that on the record. Let's go ahead and proceed  
5 on, okay, Myron?

6 MR. HECHT: Okay, thanks.

7 CHAIRMAN BROWN: Thank you.

8 MR. ERLANGER: We're going to do a  
9 quick transition, sir.

10 CHAIRMAN BROWN: Okay, that's fine.  
11 Thank you.

12 MR. PEDERSON: Good afternoon. As  
13 Craig said, my name is Perry Pederson, and although  
14 I have a background in IT and general technology  
15 research and development, for many years, I've been  
16 focusing in the last 10 years on industrial control  
17 system security.

18 I first got started in this, working  
19 for DoD. I was a PM for Infrastructure Protection  
20 at the Combating Terrorism Technology Support  
21 Office.

22 I transitioned from that to the  
23 Director of Control System Security at Department  
24 of Homeland Security.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealrgross.com](http://www.nealrgross.com)



1           Just over four years ago, I joined the  
2 NRC and was fortunate enough to be part of the team  
3 developing the Regulatory Guide 5.71, and I also  
4 led the team that did the review and approval of  
5 all the cyber-security plans for the operating  
6 plants and the new reactor applicants that we had  
7 at that time.

8           I'm currently the Senior Cyber-Threat  
9 Analyst within NSIR, and today, I am going to do  
10 my best to represent the collective effort of a  
11 lot of folks in this room, but I welcome them to  
12 stand up and point out any mis-statements or  
13 mis-characterizations I might make. Next slide.

14           I'd like to provide you with a  
15 high-level view of NRC's current approach to  
16 cyber-security, by covering these topics.

17           I'm going to touch on some terms that  
18 are used repeatedly. I'm going to talk about the  
19 cyber-threat landscape, give you a view of the  
20 historical time line, touch on coordination  
21 efforts, look at the regulatory framework itself.

22           That is the regulation, the guidance, licensing  
23 and oversight, and then look at it in terms of a  
24 cyber-security life cycle, followed up with some

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealgross.com](http://www.nealgross.com)

1 Q&A at the end. Next slide.

2 I'm sharing some of these terms with  
3 you because I think it's important, because these  
4 terms are used in the cyber-security plans by each  
5 of the licensees, and then when they are reviewed  
6 and approved by the NRC, they then become part of  
7 the licensing basis, and then that drives the  
8 oversight and inspection process.

9 So, it's important to understand that  
10 we all have a common understanding of what this  
11 means, so when a licensee commits to do something,  
12 and then they go do that, and we show up to inspect  
13 it, there is a common understanding of what we're  
14 looking for. Next slide.

15 I would like to spend a little time on  
16 the cyber-threat landscape. I think anyone who  
17 reads the newspaper and watches television these  
18 days, understands that it's changing and it's  
19 getting a lot more serious.

20 I would have to say that what you see  
21 on television and read in the paper is fairly  
22 accurate. It may not be the complete picture, with  
23 all of the details, but it does give you a real  
24 sense of the dynamic nature of this threat that

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 we're facing.

2           However, some things have not changed.

3  
4           For example, the first computer virus  
5 I ever saw was on a 5 1/4 inch floppy disk, and  
6 30 years ago, it would have been easy to simply  
7 ban the use of all floppy disks.

8           Now, we can see the fallacy of that kind  
9 of an approach, that kind of prescriptive approach  
10 to dealing with the issue.

11           Therefore, the NRC staff has concluded  
12 that this performance based regulatory framework  
13 that I'm sharing with you today, is superior to  
14 a highly prescriptive approach. Next slide.

15           One take-away from this slide is that  
16 cyber-security is really not new for the NRC.

17           We started to pay attention to this back  
18 in the 1900's. None the less, security, including  
19 cyber-security, moved up several notches in  
20 everybody's mind, after 9/11.

21           I won't go through every milestone on  
22 this chart, but if you'd like information on any  
23 one of them, certainly, we can provide additional  
24 details.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealgross.com](http://www.nealgross.com)

1           But in summary, key points are the  
2 cyber-rule was introduced or issued in 2009. The  
3 Regulatory Guide 5.71 was published in 2010, and  
4 subsequent to that, all operating plant  
5 cyber-security plans were reviewed and approved  
6 in 2011, and inspections began this year. Next  
7 slide.

8           The main point of this slide is that  
9 regardless of the perspective, be it intra-agency,  
10 inter-agency, international or industry,  
11 coordination on cyber-security has taken place on  
12 multiple levels and continues today, as you would  
13 expect.

14           Multiple NRC offices work together on  
15 various aspects of this framework, and Tim Mossman  
16 to my left, will provide some additional  
17 information on the inter-agency coordination and  
18 the latest on the inter-office instruction.

19           Furthermore, Tim Harris will provide  
20 you with some details on NRC's efforts in the  
21 inter-agency realm. This would include DHS, and  
22 as mentioned previously, FERC and NERC, as well  
23 as international fronts.

24           As for the last bullet on this slide,

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 I think you're well aware of the transparent and  
2 open process that the NRC is known for and has --  
3 and the public has provided valuable input to this  
4 process.

5 For example, based on some recent  
6 research that I was doing on this topic, I learned  
7 that it was public input, was not the driving  
8 factor, but it was a factor for including cyber  
9 in the design basis threat.

10 So, I think it's important to note that  
11 all the brains, when it comes to cyber-security,  
12 don't sit at the NRC, and we recognize that and  
13 we accept input from many stakeholders. Next  
14 slide.

15 So, just as a way to depict the  
16 regulatory framework, you know, it seems obvious  
17 that every element in this framework is necessary,  
18 and each one informs the other three.

19 Although the NRC process is tried and  
20 true, and the staff leveraged the experience from  
21 other major program implementations, cyber is  
22 different.

23 The NRC is breaking some new ground  
24 here, and there is no doubt that lessons will be

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealrgross.com](http://www.nealrgross.com)

1 learned and the next iteration of this  
2 cyber-security framework will be an improvement.

3 Next slide.

4 Ten CFR 73.54, you already know about  
5 the rule, but just to hit a couple of highlights.

6 Licensees are required to provide high  
7 assurance against a cyber-attack.

8 On numerous occasions, I've been asked  
9 to define, well, just what does that mean? High  
10 assurance? My answer is always the same,  
11 Regulatory Guide 5.71.

12 In other words, if you follow the  
13 guidance in 5.71, by definition, that will provide  
14 high assurance. Next slide.

15 I'd like to explain a little bit about  
16 how this came about and the pedigree behind it,  
17 and there was a tremendous amount of work, as I'm  
18 sure you're aware of, done by NIST in this arena.

19 So, there wasn't a need for us to  
20 reinvent the wheel, and as outlined in the NIST  
21 guidance, they recommend that you take their set  
22 of security controls, their security program and  
23 you tailor it for you industry and for your specific  
24 application, and that is exactly what we did in

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 this case.

2 Therefore, with Special Publication  
3 853, as the base set of security controls, with  
4 input from many contributors, the staff created  
5 the guidance for implementing a cyber-security  
6 program for nuclear power plants. Next slide.

7 Now, I'd like to get into a little bit  
8 of the details of Reg Guide 5.71, and just step  
9 you through this process.

10 I'm not going to touch every detail,  
11 but one of the first things you need to do is  
12 recognize, as Craig had mentioned earlier, is that  
13 this really takes a multi-disciplinary  
14 cross-functional team, to really do this right.

15 You need the IC engineers. You need the  
16 nuclear engineers. You need the IT folks at the  
17 table. You need a lot of folks involved in this  
18 process.

19 So, after you form a team, then you go  
20 through identifying what is a critical digital  
21 asset.

22 Once a CDA has been identified,  
23 regardless of whether its function is safety,  
24 important to safety, security, emergency

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 preparedness or a system that supports those  
2 functions, there is the same three-step process  
3 that is required.

4 But just imagine a large funnel.  
5 Everything in the plant really is considered, and  
6 only those systems that are tagged as a critical  
7 digital asset come out the bottom of this funnel,  
8 and those are the ones -- those are the systems  
9 that we apply security controls to.

10 The defensive architecture is one  
11 thing, and we've already touched on this issue early  
12 on this afternoon. The defensive architecture is  
13 an important aspect of a defense in-depth concept.

14 In this slide, for example, you'll see  
15 five levels, and you might consider that levels  
16 of trust, Level 0 being the internet. In other  
17 words, zero trust.

18 Level 4 being typically where you would  
19 find safety systems, and that is my highest level  
20 of trust.

21 But a critical digital asset could sit  
22 in Level 0. It could sit in any of these levels,  
23 and it would have to be protected in the same way.

24 In other words, we don't employ a graded

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701



1 approach and say, "Well, security systems are not  
2 as important as safety or EP systems are not as  
3 important to safety, so you don't have to do as  
4 much."

5 We can see a lot of these systems may  
6 reside on the same network. There may be pathways,  
7 whether it's wired, wireless or sneaker-net, that  
8 connect a lot of these systems. So, you have to  
9 protect them all equally.

10 If it is a critical digital asset, then  
11 you have to apply the security controls.

12 MEMBER ARMIJO: Could you give an  
13 example of a critical digital asset that would be  
14 at Level 0 in a nuclear plant?

15 MR. PEDERSON: Probably some emergency  
16 notification systems. EP is one of those cases,  
17 where an EP system could be compromised, and it  
18 may not directly lead to radiological sabotage,  
19 but none the less --

20 MEMBER ARMIJO: It could confuse --

21 MR. PEDERSON: -- it wasn't important  
22 enough -- pardon?

23 MEMBER ARMIJO: It could confuse  
24 people, mis-inform people --

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. PEDERSON: Right.

2 MEMBER ARMIJO: -- things like that.

3 MR. PEDERSON: Correct.

4 MEMBER ARMIJO: Okay, but not actually  
5 in the control of a pump or --

6 MR. PEDERSON: Correct.

7 MEMBER ARMIJO: -- some other system?

8 MR. PEDERSON: Right. So, that was  
9 considered during the rule-making process, that  
10 emergency preparedness systems and notifying the  
11 NRC and the public of any potential event was as  
12 important to protect from a cyber-attack, as a  
13 safety system.

14 MEMBER BLEY: You're probably going to  
15 get into it in a minute, but if not, I guess I'd  
16 have a little trouble seeing how you can protect  
17 something up at Level 0, as well as you can protect  
18 something down at Level 4.

19 MR. PEDERSON: Well, the protection  
20 comes as a result of a couple of things.

21 Certainly, if you have a safety system  
22 sitting at Level 4, there is that extra measure  
23 of protection by the additional boundaries and the  
24 boundary in the flow control devices between those

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealrgross.com](http://www.nealrgross.com)

1 boundaries.

2 So, you could say that a safety system  
3 has those additional measures of protection, right.

4 Like for example, in the diagram  
5 between Level 4 and 3, we'd certainly like to see  
6 some kind of a deterministic device there. You  
7 could call it a data diode. Certainly, I'd be happy  
8 with an air gap, but something to enforce the data  
9 flow at that point.

10 You get out to between Level 1 and Level  
11 0, you need bidirectional flow, and so, you may  
12 need some additional controls, in order to address  
13 that protection of that device.

14 So, that would be the difference. So,  
15 it --

16 MEMBER BLEY: Yes, but me at least,  
17 that's a pretty substantial difference.

18 MR. PEDERSON: Well, it is a  
19 substantial difference, but in our Regulatory  
20 Guide, there is -- I forget the number exactly,  
21 147 or 148 controls.

22 If you identify a CDA and it's in Level  
23 0, you have to address all 148 of those controls.  
24 Doesn't matter where it resides in this

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 architecture.

2 MEMBER BLEY: Okay.

3 MR. PEDERSON: Next slide. Similar to  
4 the physical security plan, the cyber-security plan  
5 contains essentially, a commitment to implement  
6 a program as outlined therein.

7 However, the plan is reviewed. After  
8 the plan is reviewed and approved by the NRC, it  
9 becomes part of the licensing basis, and as I  
10 mentioned, drives the inspection and oversight  
11 process.

12 One thing I'd like to add to this first  
13 sub-bullet under the essential elements, is that  
14 while everyone would expect the inspectors to look  
15 at a list of CDA's that licensees maintain onsite,  
16 we're likewise interested in those things they  
17 considered were not CDA's.

18 We really need to understand their  
19 thought process, and we want to make sure that they  
20 didn't accidentally, or through a misunderstanding  
21 or mis-interpretation, identify a system to not  
22 be a CDA, when in fact, it is a CDA.

23 This is something, as you can imagine,  
24 would have a serious consequence. Next slide.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealrgross.com](http://www.nealrgross.com)

1 CHAIRMAN BROWN: Before you leave that  
2 one.

3 MR. PEDERSON: Sure.

4 CHAIRMAN BROWN: Question. Have you  
5 -- a CDA -- I'm looking at the essential elements,  
6 after the basic plan part.

7 Have you all been involved in  
8 evaluating a specific plant yet, relative to its  
9 defensive model? A plant? Not a -- I'm asking  
10 this in the context of your earlier slide, where  
11 you talked about the threat vectors.

12 I mean, if I look, and I look at, say  
13 the reactor trip system, I'm picking one in the  
14 plant, not in emergency -- not up in the Level 0  
15 world, but down in the Level 4 world.

16 There are still things you have to do,  
17 if you -- because there is a communication path,  
18 and if -- I don't want to get back into how that  
19 path is executed.

20 But if it's not executed in a manner  
21 that is totally secure, then you have to start  
22 looking at the access -- I hate to use that word,  
23 but the control of access to the things that are  
24 accessible through that path, whatever they may

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealrgross.com](http://www.nealrgross.com)

1 be, whether they're controls, whether they're data  
2 that is going to inhibit a trip or actuation of  
3 a safeguard system, or whatever.

4 MR. PEDERSON: Well, I would think  
5 Ralph Costello --

6 CHAIRMAN BROWN: So, my question -- let  
7 me finish.

8 So, my question is, if -- I was thinking  
9 about this, when I was going through your slides  
10 the other -- you know, couple of nights ago, and  
11 trying to think of circumstances, based on my own  
12 experience, when we were first in the Naval Nuclear  
13 Program, when I was first doing this kind of stuff.

14 We put it in proto-type plants, not ships, which  
15 were kind of disconnected from everybody.

16 One of the things we looked at was, we  
17 made sure you couldn't -- you didn't just connect  
18 up a laptop to something. You didn't do business  
19 that way, or you did not have a USB -- a thumb-drive  
20 port, or there were certain -- you just didn't build  
21 those in. There was no way.

22 The only way you could change the  
23 software would be to pull out the card, take off  
24 a programmable read-only memory, put a brand new

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealgross.com](http://www.nealgross.com)

1 one in. That is really hard to have.

2 Doesn't mean it can't be compromised  
3 at a vendor's place, as Stuxnet has illustrated,  
4 when you build stuff into a design somewhere that  
5 gets in, although that one got in via thumb-drive,  
6 I guess, or something like that. That is the  
7 hypothesis.

8 But you could postulate somebody doing  
9 that maliciously from some other source when it  
10 was brought in. But that is hard.

11 So, I was looking for again, a strategy  
12 -- well, I keyed on your words 'protected strategy'.

13 I mean, you have to look at the assets, and you  
14 start having to look at, well, what are the touch  
15 points? What are the controls of access?

16 I remember one of the designs we were  
17 looking at, where there is a maintenance computer.

18 So, whenever they update software or  
19 anything else, it is done through that, I think  
20 -- this is my memory again, old memory, so, it might  
21 not be working right all the time, but it goes  
22 through the maintenance computer set up, to go into  
23 each of the individual trains.

24 So, that is why I was asking you if

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealrgross.com](http://www.nealrgross.com)

1 you've actually done this, for a particular  
2 installation, and then walked through the strategy  
3 of how you were going to -- how you were going to  
4 do that?

5 Maybe that is a 'yes' or 'no' answer.

6 I don't know.

7 MR. PEDERSON: I think the answer is,  
8 we have an answer.

9 CHAIRMAN BROWN: I'm sure.

10 MR. PEDERSON: And well, Ralph  
11 Costello, and perhaps in more detail later during  
12 the closed session --

13 CHAIRMAN BROWN: Okay, in closed  
14 session, fine.

15 MR. PEDERSON: -- we could get into  
16 some of those details.

17 CHAIRMAN BROWN: That's fine.

18 MR. PEDERSON: But he may be able to  
19 speak to it now, to some degree.

20 CHAIRMAN BROWN: We'll wait, we'll do  
21 it at the other time. There's no sense in doing  
22 this twice.

23 MR. WESTREICH: Well, I'm Barry  
24 Westreich, Deputy Director in DSP.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701



1           We are, in fact, doing that for types  
2 of systems that we're inspecting against.

3           So, licensees have identified their  
4 critical digital assets, and then in this current  
5 version, in these interim steps for what we call  
6 target set equipment, the most sensitive equipment,  
7 they have implemented controls for each one of those  
8 target sets to use, and we look at the controls  
9 and we look at all the vectors associated with those  
10 CDA's, to determine, have they considered all the  
11 vectors that are associated with that system? Is  
12 it vulnerable to, you know, portable media?

13           Are there -- is it in the right level  
14 in the architecture? You know, we talked about  
15 the Level 4. Are they in Level 4 as they're  
16 supposed to be? Have they placed the data diode  
17 in place?

18           So, we do look at that specifically,  
19 related to the systems on a sampling basis, that  
20 we address during these inspection activities.

21           But we're in this interim  
22 implementation phase. So, it's not the breadth  
23 of the plant now, it's associated with what we're  
24 calling target sets.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealgross.com](http://www.nealgross.com)

1 CHAIRMAN BROWN: These are existing --  
2 these are operating plants, right?

3 MR. WESTREICH: These are operating  
4 plants.

5 CHAIRMAN BROWN: Not the -- one of the  
6 points of my -- one of the -- the thrust of my comment  
7 is that on a go-forward basis in new plant designs  
8 in -- you can certainly simplify the vulnerability  
9 problem by -- I love to use, not allowing certain  
10 assets to have access via certain means.

11 In other words, you make sure that you  
12 don't have those vulnerabilities built in, in the  
13 beginning, even though you can't theoretically  
14 dictate it, you can certainly encourage it during  
15 the design and licensing stage via the  
16 architecture, because we do have fairly complete  
17 block diagram, functional diagrams of what these  
18 look like.

19 It's irrelevant, what the technology  
20 is. Blocks are blocks.

21 MR. WESTREICH: Right.

22 CHAIRMAN BROWN: So, anyway, that is  
23 just a thought process. We'll wait until the  
24 closed session, to hear the --

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealrgross.com](http://www.nealrgross.com)

1 MR. PEDERSON: Yes, and it's a perfect  
2 segue to the next slide.

3 CHAIRMAN BROWN: Okay, thank you.  
4 You're doing a good job of catching up, after our  
5 half-hour digression, by the way.

6 MR. PEDERSON: No problem. So,  
7 recognizing that full implementation is down the  
8 road for some sites, we prioritize some of those  
9 activities and developed these interim milestones.

10 These interim milestones focused on,  
11 as you were just mentioning, some of these key  
12 threat vectors, with an emphasis, as Barry was also  
13 just mentioning, target set equipment, where these  
14 were identified and licensees committed to complete  
15 all of these interim milestones by December 31,  
16 2012, and that is also what Ralph and his team are  
17 inspecting, and have begun to inspect this year.

18 So, for example, Milestone 3 is  
19 installing a deterministic one-way device between  
20 Levels 3 and 4, or between 4 and 3.

21 Another example -- and that would  
22 essentially isolate those most critical systems  
23 in Level 4.

24 Milestone 4, another example,

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealgross.com](http://www.nealgross.com)

1 implementation of security controls related to  
2 portable and mobile devices, recognizing one of  
3 the threats that we all learned recently, otherwise  
4 known as Stuxnet, is a really good example and very  
5 illustrative of just what an air gap buys you.

6 It's not your sole savor. It has to  
7 be part of an entire programmatic approach.

8 In that, you know, just to point out,  
9 I think it's worthwhile pointing out, I've had this  
10 discussion, that it really doesn't matter how much  
11 malware is loaded on a USB stick, if you don't let  
12 it in the door. That is a critical point.

13 Then there is Milestone 6, for example,  
14 application of security controls to target sets.

15 So, for those particular CDA's that are  
16 part of a target set, then all 148 controls have  
17 to be addressed.

18 So, we're trying to make sure that right  
19 up front, the most cyber-sensitive systems are  
20 identified, isolated and protected, and that is,  
21 in a nutshell, the essence of these interim  
22 Milestones 1 through 7.

23 CHAIRMAN BROWN: One of the -- just a  
24 comment on your thought, relative to, if you don't

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 ever let the USB in the door.

2 That is a different -- that is a  
3 different -- that is an administrative control type  
4 thing.

5 MR. PEDERSON: Right.

6 CHAIRMAN BROWN: Okay, and it's  
7 considerably simpler to apply that administrative  
8 control and checks to prevent that, than it is to  
9 protect yourself from somebody who has -- can hack  
10 through your network, through a communications  
11 network, where it feeds both the control room and  
12 the plant.

13 I am beating this horse. It's not a  
14 dead horse. It's a very live horse, in case you  
15 hadn't noticed, because that is an interactive set  
16 of threats that is constantly bearing.

17 The other one is one that you can look  
18 at and take care of, and control with a different  
19 level of controls.

20 I mean, the purpose of the discussion  
21 is to see that -- or at least to provide thought  
22 process, that keep that thought in mind, when we  
23 are doing these -- the thought process, well, like  
24 you say, your diode, your data diode from 4 to 3

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealrgross.com](http://www.nealrgross.com)

1 and from 3 to 2. Those are the two levels that  
2 we have, supposedly one-way communications, and  
3 we don't want to be able to be compromised.

4 But it -- because it goes to the point  
5 I made earlier, that you just can't be in the mode  
6 of constantly trying to patch, and you don't want  
7 cyber-software on any of your applications, safety  
8 safeguards. You just don't want it in there. It's  
9 just -- it's a threat to actually having it perform  
10 its function.

11 And so, you want to have all that stuff  
12 off somewhere else, and you don't want to have to  
13 fool with it.

14 So, anyway, I've just --

15 MR. PEDERSON: Yes.

16 CHAIRMAN BROWN: It was -- I liked --  
17 I appreciated your thoughts, your comments on what  
18 these milestones were and what they did. That  
19 provided some illumination of what your thoughts  
20 were and --

21 MR. PEDERSON: Yes, it's a very good  
22 point, that vulnerabilities are everywhere. There  
23 is no system without them.

24 CHAIRMAN BROWN: And you need --

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. PEDERSON: If anyone claims such,  
2 then I'd be immediately suspect.

3 CHAIRMAN BROWN: Absolutely. Air  
4 gaps are nice, but they're not the sole thing.

5 MR. PEDERSON: And so, the  
6 vulnerability is a necessary condition. The  
7 threat might be considered the root cause.

8 And so, if you have a vulnerability,  
9 you have to be able to separate it from that root  
10 cause, so, that you can continue to operate with  
11 that known vulnerability, and there are different  
12 ways to address that.

13 CHAIRMAN BROWN: Yes.

14 MR. PEDERSON: Rule sets, air gaps,  
15 additional administrative controls.

16 So, there are things you can do to  
17 mitigate vulnerability, known vulnerabilities, and  
18 there is a lot of things that you do, just in your  
19 architecture, to try to mitigate the things that  
20 you don't know about, that may emerge.

21 CHAIRMAN BROWN: See, I like the way  
22 you said 'architecture', because if you don't do  
23 that during the design stage, and you try to do  
24 it a year before fuel load, it's --

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. PEDERSON: Kind of late.

2 CHAIRMAN BROWN: -- kind of late in the  
3 game, to do anything.

4 MR. PEDERSON: Yes.

5 CHAIRMAN BROWN: That is where the NRC  
6 is, and I think it's very, very important, up front,  
7 to make sure you have that control of it and you  
8 don't have those vulnerabilities, and limit them  
9 to those that you can deal more easily.

10 So, anyway, you can keep rolling here.

11 MR. PEDERSON: So, then Milestone 8 is  
12 simply the full implementation of the entire  
13 program. Next slide, please.

14 This diagram provides you just a  
15 snapshot of how that milestone will be phased in  
16 for different sites, over the next few years.

17 Note that the 'y' axis for the sites,  
18 and sometimes there are multiple reactors on a site.

19 Next slide.

20 The one thing to kind of wrap this up,  
21 and this is my last slide, you know, I wanted to  
22 leave you with the notion that although you may  
23 not look into the Reg Guide and see a section that  
24 is titled 'Cyber-Security Life Cycle', if you read

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701



1 the details and you read through the security  
2 controls, you'll see this life cycle emerge from  
3 there, that we really address every phase in a  
4 nominal life cycle of these digital systems, these  
5 critical digital assets.

6 New reactor licensees, of course, are  
7 required to have the full program up and implemented  
8 and verified prior to fuel arriving onsite.

9 The operating reactors are allowed to  
10 phase the program in over time, as I was just  
11 discussing. So, they'll touch each one of these  
12 phases, as they go through implementing their full  
13 program.

14 But eventually, when they get the full  
15 program implemented and let's say, a site that has  
16 primarily analog safety systems, and they want to  
17 do an upgrade, they're going to be working their  
18 way through this entire process.

19 There is a lot of analysis that has to  
20 be done, even touch points on the supply chain.

21 So, there are controls in the Reg Guide  
22 that address supply chain. I'm not suggesting we  
23 have the perfect solution for the supply chain,  
24 but it is there. We recognize it, and licensees

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 are committed to doing their best to fill those  
2 requirements.

3 MEMBER BLEY: Perry, before you close,  
4 couple more general questions.

5 Few years ago, we had ISG in this area.  
6 Now, we have Reg Guide 5.71. We have inspection  
7 guidelines that look like they've picked up what  
8 was in the IG's.

9 Do we have something similar in SRP  
10 space yet? Is there guidance for reviewers? I  
11 don't know if you're the right guy to ask about  
12 this.

13 MR. ERLANGER: Perry, I can --

14 MEMBER BLEY: Yes, yes.

15 MR. PEDERSON: Yes, go ahead.

16 MR. ERLANGER: Yes, sir, there is an  
17 SRP Chapter. It is --

18 MEMBER BLEY: And it's brought up to  
19 date now?

20 MR. ERLANGER: Up to date, and it  
21 reflects Reg Guide 5.71.

22 MEMBER BLEY: Okay.

23 MR. ERLANGER: Similar to the  
24 framework.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealrgross.com](http://www.nealrgross.com)

1 All these lessons learned we have --  
2 when we update the Regulatory Guide and the  
3 framework, we'll update the SRP at that time. But  
4 we do have one related to 5.71 today.

5 MEMBER BLEY: Okay, and then I had  
6 another question, because I've seen something  
7 similar in the fire risk assessment area lately.

8 You have, in the inspection guide, and  
9 I don't know if we talk about this here or somewhere  
10 else, some things you call FAQ's, and the fire folks  
11 have FAQ's.

12 Theirs are to further define the  
13 methodology they've been working on.

14 Yours, I'm curious about, you know,  
15 where they came from, why they're there, and you  
16 know, is -- are they going to stay the way they  
17 are or do they get integrated into other guidance  
18 some time in the future?

19 MR. ERLANGER: I think I'm the right  
20 one to answer that as well, Perry.

21 Yes, we have a security frequently  
22 asked question program. It's the -- the  
23 instructions can be found in a document called  
24 NEI-0510, that kind of governs the whole process.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealrgross.com](http://www.nealrgross.com)

1           As a point of reference, I would say  
2 the physical protection program has roughly 80  
3 security frequently asked questions today. Cyber  
4 is up to about seven or eight at this point.

5           MEMBER BLEY: Right.

6           MR. ERLANGER: We would use those to  
7 inform and improve our guidance down the road.  
8 The purpose of the program is to provide regulatory  
9 clarity, not to provide additional guidance or  
10 requirements.

11           So, it's just a bit more detailed, when  
12 there is a different understanding of what the  
13 requirement means. This is used to provide  
14 clarity.

15           MEMBER BLEY: So, these are coming  
16 along as sort of interim agreement, because they  
17 are issued jointly by --

18           MR. ERLANGER: Yes, sir, there is a  
19 Panel process, where the industry signs it out,  
20 as well as an NRC representative.

21           I think it's probably typical of any  
22 new requirement, that questions are going to come  
23 up and there is going to be a different  
24 understanding of --

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MEMBER BLEY: No, it seems reasonable.

2 I just wanted to --

3 MR. ERLANGER: And this is the method  
4 through which we would work through it and find  
5 resolution.

6 MEMBER BLEY: At least in  
7 cyber-security, there are -- I think they are  
8 attached to the inspection guide now, so, the  
9 inspectors get to see --

10 MR. ERLANGER: They exist in a form.  
11 There is a database that --

12 MEMBER BLEY: Maybe that isn't where  
13 I saw them. I thought I saw them there.

14 MR. ERLANGER: But the industry gets  
15 access to them, once they're published.

16 MEMBER BLEY: Okay.

17 MR. ERLANGER: And the various --

18 MR. WESTREICH: Yes, they're not  
19 attached to the inspection procedures, but they  
20 are issued jointly --

21 MEMBER BLEY: Okay.

22 MR. WESTREICH: -- between us, and you  
23 know, we endorse the NEI guidance document --

24 MEMBER BLEY: Right.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. WESTREICH: -- so, they distribute  
2 those, and then the inspectors use those as part  
3 of their inspection process. They could use that  
4 clarity for what the expectation was.

5 MEMBER BLEY: Okay.

6 MR. WESTREICH: So, we have a --  
7 currently, they're just used for each of the  
8 milestones. So, there is seven FAQ's.

9 MEMBER BLEY: Yes.

10 MR. WESTREICH: One for each  
11 milestone, because when we were doing pilot  
12 inspections, we identified a number of generic  
13 issues that we were trying to clarify before  
14 inspection activities started.

15 MEMBER BLEY: Okay, good, thanks.

16 MR. PEDERSON: Next slide. Unless  
17 there is any other questions?

18 CHAIRMAN BROWN: Okay, we're -- you did  
19 a great job. We picked up about 15 minutes, in  
20 addition to getting some good answers.

21 Tim, I'd like to try to get you and the  
22 follow-on one done, so we can just have a completed  
23 closed session.

24 So, I see you're all scheduled for about

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 15 minutes apiece, if we could go walk through both  
2 of those.

3 MR. MOSSMAN: All right.

4 CHAIRMAN BROWN: You're next, I think.

5 MR. MOSSMAN: Absolutely. Thank you.

6  
7 CHAIRMAN BROWN: Tim, you might want  
8 to move that off the microphone, move that  
9 microphone a little bit. Yes, thank you very much.

10 MR. MOSSMAN: All right. Good  
11 afternoon. My name is Tim Mossman. I'm a security  
12 specialist in the Cyber-Security and Integrated  
13 Response Branch. That is Craig's branch in the  
14 Office of Nuclear Security and Incident Response.

15 I've been with the NRC for a total of  
16 five years, since I've -- I've been with NSIR since  
17 January.

18 Prior to joining NSIR, I was with  
19 actually John Thorp's branch, working  
20 instrumentation and control in the Office of  
21 Nuclear Reactor Regulation, and if I can segue for  
22 a minute.

23 One of the amusing things about this  
24 topic was one of the last assignments, I worked

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealrgross.com](http://www.nealrgross.com)

1 with John was the inter-office instruction, and  
2 shortly before I left, NSIR volunteered to pick  
3 that up, and I was more than happy to send it over  
4 to NSIR, and a few months later, I got an opportunity  
5 to join NSIR, and the first assignment I got was  
6 an inter-office instruction.

7 CHAIRMAN BROWN: Well, the Panel was  
8 back in place.

9 MR. MOSSMAN: Pretty much, yes. So,  
10 prior to joining NRC, I supported development of  
11 command and control systems for missile defense  
12 applications, which don't sound a lot like  
13 instrumentation and control systems for nuclear  
14 reactors, but although they're on very vastly  
15 different scales, they have a lot of the same  
16 challenges.

17 We had a lot of communications. We had  
18 a lot of software dependability issues. It was,  
19 actually, it was fun, actually to work there.

20 My educational background. I have  
21 degrees in nuclear and reliability engineering,  
22 and so, I'm not sure exactly how I got into  
23 cyber-security, but that's where I am today.

24 So, today, I'll be talking about an

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701



1 ongoing effort to formalize the inter-office staff  
2 activities, with respect to cyber-security.

3 In the very recent past, one of the  
4 things that ACRS has expressed to staff is that  
5 with the separation of cyber out of the Part 50  
6 and Part 52 licensing process, that some aspects  
7 of the safety/cyber-security interface may not be  
8 adequately addressed.

9 That is something that staff is very  
10 sensitive to, and previously did commit to ACRS,  
11 to provide a more formal vehicle to define this  
12 inter-office working relationship.

13 Up until now, a lot of the things we  
14 had been doing had been some formal, some very  
15 informal, but we didn't have any kind of governing  
16 document or management guidance that said, "This  
17 is the way we expect to work together." Next slide.

18 As has been noted previously,  
19 regulation of cyber-security is still a relatively  
20 new item.

21 However, we have already seen the  
22 impact that cyber-security may be felt at many  
23 different points in the regulatory process.

24 Staff has an interest in making certain

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 that appropriate cyber provisions are taken  
2 throughout a digital system's life cycle, within  
3 the context of our regulatory structure.

4 One of the primary benefits of enhanced  
5 staff interaction on topics related to  
6 cyber-security is reduced regulatory uncertainty  
7 for licensees, basically ensuring that  
8 cyber-security issues are identified early, not  
9 letting them slide in the regulatory process, until  
10 it's expensive to fix.

11 Selfishly, enhanced staff interaction  
12 regarding cyber-security should also benefit  
13 staff, as it should result in a more efficient use  
14 of our resources.

15 Basically, we never want to get in a  
16 situation where we're ping-ponging licensees  
17 between cyber staff, licensing staff and back and  
18 forth. We do not have enough staff to do that.

19 Evolution of the cyber framework. As  
20 I mentioned earlier, this is something that ACRS  
21 has previously recommended to staff. Staff did  
22 commit to follow up on this recommendation.

23 Since that time, we've had a number of  
24 opportunities to learn from inter-office

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 activities, where we've collaborated on topics that  
2 relate to cyber-security.

3 Most notably, NSIR has been working  
4 with NRR on a pilot study, regarding the Diablo  
5 Canyon digital safety system replacement. It's  
6 an opportunity for us to view first-hand, how our  
7 cyber-security supply chain controls are being  
8 handled in the context of the procurement of the  
9 digital safety system.

10 NRO has also participated in that  
11 effort, as it has ramifications for new reactor  
12 procurement.

13 Eric Lee, who is in the audience, from  
14 our group, will provide details on the pilot study  
15 during the closed portion of the briefing.

16 Also, another area we've had a lot of  
17 interaction on, and Tom Bergman probably stole most  
18 of my thunder at the beginning of the meeting, and  
19 hopefully, he took most of the arrows at the  
20 beginning of the meeting too.

21 We've had a lot of interactions with  
22 new reactors on the safety/cyber-security  
23 interface for new reactors.

24 Monika Coflin, who is also with our

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 staff, will be providing a briefing on the current  
2 status of new reactor cyber-security.

3 Since the beginning of the calendar  
4 year, NSIR and the Regional Offices have been  
5 actively involved in NRC's first inspections, as  
6 we just discussed, of the interim implementation  
7 milestones, and Perry provided an overview of  
8 those.

9 Again, in the closed session of the  
10 briefing, Ralph Costello will talk about the  
11 oversight program and our experiences in the last  
12 four or five months on that.

13 So, although there is still much to  
14 learn, staff has had the benefit of learning from  
15 various inter-office interactions on  
16 cyber-security.

17 Okay, in developing the cyber-security  
18 framework, we've had participation from not only  
19 our office, Nuclear Security and Incident Response,  
20 but also the Office of New Reactors, the Office  
21 of Nuclear Reactor Regulation, and the Office of  
22 Research, as well as having gotten some feedback  
23 from our Regional Offices.

24 The framework that we developed

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealrgross.com](http://www.nealrgross.com)

1 contains expectations for the various headquarters  
2 office and the region, regarding regulatory  
3 activities that may have implications for  
4 cyber-security.

5 If you go to the next slide, I'll give  
6 you some examples of some of the things we tried  
7 to address.

8 Although it's challenging to figure out  
9 all the possible regulatory situations where  
10 coordination should occur between the offices, and  
11 we actually did try to come up with a set of  
12 use-cases of situations where we should be  
13 interacting, things that we at NSIR may find, things  
14 that NRR may come across, things that NRO or the  
15 Regions may come across.

16 I cannot guarantee we got everything,  
17 but here were some of the big ones we did identify,  
18 and tried to lay out expectations.

19 For things like a digital safety system  
20 amendment, something that NRR may receive, that  
21 is something that NSIR should be notified of. If  
22 it's something as simple as a set point change to  
23 a digital instrument, that may be something that  
24 NSIR has very little interest in.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealgross.com](http://www.nealgross.com)

1           However, if it's a more grandiose whole  
2 replacement of a digital safety system, that is  
3 an opportunity for us and NSIR to review our  
4 guidance, to make sure it applies to the kind of  
5 change that is being made, evaluate whether or not  
6 a pilot study, like what we're doing with Diablo  
7 is appropriate, or at the very least, notify our  
8 NSIR and/or Regional Inspectors that, "Hey, there  
9 is a big change coming down, and this ought to be  
10 in your cue for the next cyber-security inspection  
11 at that site."

12           In addition, one of the other  
13 interactions that we already have with NRR, the  
14 cyber-security assessment team, which is led by  
15 NSIR, John Rycyna in the back, currently handles  
16 a lot of these duties.

17           We receive a lot of input from NRR's  
18 operating experience program, specifically any  
19 events involving instrumentation and control  
20 systems that may have a cyber implication do get  
21 sent to the CAT team, and the IOI formalizes that  
22 agreement.

23           Having some experience with some of the  
24 things we see, they do tend to err on the side of

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealrgross.com](http://www.nealrgross.com)

1 conservatism, because we've gotten a handful of  
2 events that wind up being for analog systems, when  
3 we finally run on the ground.

4 Then also in the -- with respect to new  
5 reactors, although the vendors are not subject to  
6 the 73.54 rule, it does apply to licensees.

7 It is also important for NSIR staff to  
8 know that new reactor designs either have been  
9 received or will be received.

10 Very recently, we did have a vendor that  
11 NSIR staff participated in telecon with. They had  
12 a lot of questions regarding cyber-security  
13 guidance. They actually demonstrated a pretty  
14 reasonable understanding of our guidance, and they  
15 wanted to clarify a few points.

16 Again, just from their perspective,  
17 they are looking to hand over a cyber-ready design  
18 to a licensee, and that was an area where we at  
19 NSIR could have some value, in talking to them.

20 Then also, NSIR has an interest with  
21 NRO's vendor quality staff, regarding control and  
22 protection of the supply chain.

23 The vendor quality staff approaches it  
24 probably more from a quality assurance standpoint.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1       Our vent is a little more a malicious activity,  
2       but there is a significant amount of overlap in  
3       that area.

4               CHAIRMAN BROWN:  Have you provided  
5       them with the supply chain guys?  I mean, they're  
6       buying piece parts, some of those EP piece parts  
7       are active piece parts.

8               They have installed software on them,  
9       that are designed by vendors for -- I use -- you  
10      can use -- for radiologic control or those things  
11      that are -- or one set of things, or other sets,  
12      as well.

13              Have you all tried to put together a  
14      -- this is way down the food chain.

15              So, I mean, you're starting to look at  
16      experience levels of people that are buying these  
17      pieces, to build a bigger system, and there may  
18      be something buried in those things, or  
19      vulnerabilities that people ought to be asking  
20      about up front.

21              Have you all started a list of any kind,  
22      or do you all look at different types of piece parts,  
23      before you -- I don't know how you would do this.

24              MR. MOSSMAN:  Yes.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701



1 CHAIRMAN BROWN: I thought about it,  
2 but I am not --

3 MEMBER BLEY: I think one of the  
4 concerns, I think especially in the electrical  
5 business, is the issue of counterfeit parts.

6 A vendor makes something, and it's got  
7 a part in it that has got the logo and everything  
8 of the right manufacturer, and yet, it's not, when  
9 you open it up, something different.

10 MR. MOSSMAN: Yes, in fact, there is  
11 really three different flavors of the CFSI problem  
12 and I apologize, I might start to get a little bit  
13 on thin ice, because I'm not technical expert in  
14 this area.

15 But there have been a log of public  
16 information reports out there. There are parts  
17 that are much like counterfeit bolts from 20 or  
18 30 years ago, where people will manufacture a part,  
19 that is just hard to get, for purposes of making  
20 a profit.

21 It may function like the part you're  
22 looking for, but it may not be qualified like the  
23 part you're looking for.

24 There are also recycled parts, it's an

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 issue, people salvaging e-waste, you know, which  
2 in theory will be the same part, might actually  
3 be the real part, but it may have tens of thousands  
4 of hours of operating time on it, plus it may or  
5 may not have been soldered three or four times,  
6 by the time you receive it.

7 Then the last category is one that  
8 probably is of most interest, or is of more specific  
9 interest to cyber, which would be like if malware  
10 is implanted.

11 So, there are different flavors of  
12 things out there. There are different tools. Dan  
13 Pasquale has been leading a lot of the efforts on  
14 CFSI, and --

15 CHAIRMAN BROWN: Say that. What does  
16 that mean again?

17 MR. MOSSMAN: Counterfeit and  
18 fraudulent --

19 CHAIRMAN BROWN: Okay, got it, yes.

20 MR. MOSSMAN: I apologize, and we, at  
21 NSIR, have been working with him, just to -- on  
22 some of his efforts, and interfacing with industry  
23 on that.

24 I don't know that I can give you a whole

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 lot more detail off the top of my head, on that.

2 CHAIRMAN BROWN: Yes, I wasn't  
3 expecting you guys to go work with the part  
4 suppliers, themselves. But I mean, obviously the  
5 person building the systems are the point at where  
6 those parts come in, and they're the first touch  
7 point.

8 MR. MOSSMAN: Yes, I am aware that  
9 there are databases out there, and I want to say,  
10 Stacy might be able to help me in the back.

11 CHAIRMAN BROWN: I think I've done  
12 enough.

13 MR. MOSSMAN: Yes.

14 CHAIRMAN BROWN: Unless you've got  
15 another comment, Dennis. I thought we'd move on,  
16 on this one, okay.

17 MR. MOSSMAN: Okay, so, very good, the  
18 next slide. Okay, we're already there.

19 All right, in summary, very recently,  
20 the Branch Chiefs, affected Branch Chiefs in NSIR,  
21 NRR, NRO and Research signed out an internal  
22 memorandum that detailed the inter-office working  
23 arrangement for regulatory activities and cyber  
24 implications.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealrgross.com](http://www.nealrgross.com)

1                   Basically, it's the working  
2 arrangement that everybody agreed to, and I  
3 apologize if you did not get a copy yet. I know  
4 it was something that did not get signed out in  
5 time for the main distribution package. So, it  
6 got to Christina very late.

7                   CHAIRMAN BROWN: It's the closed part,  
8 you mean?

9                   MR. MOSSMAN: No, it was an internal  
10 memorandum.

11                  CHAIRMAN BROWN: Okay, yes, no, that  
12 is what you sent out?

13                  MR. MOSSMAN: Okay, yes.

14                  CHAIRMAN BROWN: Yes, I got it, yes,  
15 okay.

16                  MR. MOSSMAN: And so, anyway, that is  
17 -- constitutes an internal agreement that everybody  
18 has signed off on, and referencing back to the ACRS  
19 recommendation to formalize that, our next step  
20 is to actually get that under an inter-office  
21 instruction header, so, it's in a formal tracked  
22 document, and when we get that published as a formal  
23 IOI, we can provide that to the ACRS.

24                  MEMBER BLEY: That's great. I am

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealrgross.com](http://www.nealrgross.com)

1 really glad to see you've moved on now.

2 CHAIRMAN BROWN: Thank you.

3 MR. MOSSMAN: Yes.

4 CHAIRMAN BROWN: Tim Harris.

5 MR. MOSSMAN: Okay, thank you very  
6 much.

7 MR. HARRIS: I never know whether it's  
8 good to talk before a break, after a break, before  
9 lunch, after lunch.

10 CHAIRMAN BROWN: You could help us out.

11 MR. HARRIS: I'll try to help you out.

12

13 Good afternoon. My name is Tim Harris.

14 I am the senior program manager in the Division  
15 of Security Policy.

16 After joining the NRC in 1994, I've held  
17 a number of technical and managerial positions  
18 related to byproduct, source, special nuclear  
19 safety and security.

20 Over the last eight years, I've worked  
21 on a variety of policy issues, ranging from  
22 materials and reactor security, to cyber-security  
23 a nuclear installations.

24 I've also had extensive experience with

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealrgross.com](http://www.nealrgross.com)

1 the International Atomic Energy Agency in the  
2 development of its nuclear security series  
3 fundamentals and recommendations level documents.

4 So, this afternoon, I'll discuss some  
5 of NRC's recent inter-governmental and  
6 international cyber-security activities. Next  
7 slide, please.

8 So, this is kind of an overview of my  
9 talk.

10 I'll begin my presentation with some  
11 history on the interactions with the Federal Energy  
12 Regulatory Commission or FERC, and the North  
13 Atlantic Electric Reliability Cooperation, NERC.

14 I'll also discuss some of our other key  
15 inter-governmental interactions.

16 Then I'll discuss some of NRC's  
17 involvements with the recent Presidential  
18 Executive Order and Presidential Policy Directive  
19 to improve critical infrastructure of  
20 cyber-security, which includes the development of  
21 a voluntary framework for the -- for reducing cyber  
22 risk through critical infrastructure.

23 Last, I'll talk about some bilateral  
24 and multi-lateral international efforts that we've

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealrgross.com](http://www.nealrgross.com)

1 been involved in.

2 This slide provides some history and  
3 recent interactions with both FERC and NERC.

4 As you are probably well aware, NRC's  
5 authority is derived from the Atomic Energy Act,  
6 while FERC's authority for grid reliability are  
7 tied to the Energy Policy Act of 2005.

8 These two authorities relative to  
9 cyber-security, intersect at nuclear power plants,  
10 and I think you had some questions earlier. So,  
11 hopefully I'll be able to clarify some of those.

12 Back in January 2008, FERC issued Order  
13 706. This order specified critical infrastructure  
14 protection or CIP, reliability standards to  
15 safeguard cyber-critical assets.

16 This order also exempted NRC facilities  
17 from those requirements. Both NRC and FERC  
18 recognize the need to ensure that there was no gap  
19 or overlap between their regulatory programs and  
20 their regulatory programs.

21 Subsequent, FERC issued Order 706  
22 Bravo, which clarified that the balance of plants  
23 and equipment within the power plant that are not  
24 within the scope of NRC's regulatory requirement,

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealrgross.com](http://www.nealrgross.com)

1 would be within the scope of the NERC order.

2 As a result --

3 CHAIRMAN BROWN: Tim, to sum up --  
4 maybe you're going to answer the question.

5 As a result, go ahead and finish your  
6 --

7 MR. HARRIS: That is actually the next  
8 words right here, "As a result."

9 So, you can ask a question if you like  
10 or --

11 CHAIRMAN BROWN: Finish.

12 MR. HARRIS: Okay.

13 CHAIRMAN BROWN: And then I'll ask.

14 MR. HARRIS: So, as a result, all  
15 nuclear power plants were asked by NERC, to  
16 determine which structures, systems and components  
17 or SSC's would be potentially subject to the CIP  
18 standards, and which would be potentially subject  
19 to the NRC regulations.

20 This analysis was known as the Bright  
21 Line Process. So, it was basically a process  
22 whereby plants tried to define when that bright  
23 line, where NRC regulations would apply and where  
24 CIP standards would apply.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealrgross.com](http://www.nealrgross.com)



1 CHAIRMAN BROWN: Did you get to vote?

2 MR. HARRIS: Did I get to vote?

3 CHAIRMAN BROWN: Did NRC get to vote?

4 MR. HARRIS: I think NRC was intimately  
5 involved in the discussions.

6 CHAIRMAN BROWN: There is a memo of --

7 MR. HARRIS: Yes, there is a memo --

8 CHAIRMAN BROWN: I'm just asking, is  
9 there a memorandum of understanding --

10 MR. HARRIS: Yes, sure, sure.

11 CHAIRMAN BROWN: -- that you know what  
12 is yours and they know what is theirs? If there  
13 was an agreement or a consensus reached?

14 MR. HARRIS: Yes.

15 CHAIRMAN BROWN: Okay, that is what I  
16 meant by, did you get a vote? I apologize for being  
17 obtuse.

18 MR. HARRIS: Just staff. They don't  
19 typically let me vote.

20 MR. ERLANGER: We had an opportunity  
21 to review the framework and to -- we basically just  
22 reflected in a Commission policy decision, which  
23 came down in a staff requirements memorandum.

24 The staff subsequently wrote an

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 information paper on how we interpret it, the  
2 Commission's policy decision.

3 CHAIRMAN BROWN: Okay.

4 MR. ERLANGER: So, we were intimately  
5 involved in the process.

6 CHAIRMAN BROWN: Okay, now, you  
7 answered my question. I didn't have to ask it.

8 MR. HARRIS: Okay, so, basically, all  
9 power plants indicated that if compromised, balance  
10 of plant SSC's would affect re-activity and were  
11 important to safety.

12 Licensees further stated for this  
13 reason, all balance of plant SSC's fall within the  
14 scope of NRC's regulation, which I think is what  
15 you were getting at.

16 I think Craig mentioned that the -- it  
17 wasn't an SR. I think it was a COM.

18 Basically, the Commission determined  
19 as a matter of policy, that the cyber-security  
20 regulations NRC 73.54 should be interpreted to  
21 include SSC's and the balance of plants that have  
22 a nexus to radiological health and safety.

23 Licensees and combined license  
24 applicants subsequently updated their

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 cyber-security plans, to reflect that Commission  
2 decision.

3 I'll also note that NRC has a memorandum  
4 of agreement with FERC that provides a basis for  
5 cooperation on subsequent bright line processes  
6 to discuss things of mutual interest, and  
7 similarly, we have a memorandum of understanding  
8 with NERC, which helps also in the bright line  
9 process. Next slide, Perry.

10 So, NRC staff maintains periodic  
11 communications with staff from FERC and NERC, to  
12 exchange information and to ensure that  
13 requirements that are in place are effective and  
14 meet both organization's interest.

15 For example, NRC and FERC staff  
16 recently met to discuss FERC establishing its  
17 Office of Energy Infrastructure Security, which  
18 addresses cyber-security, and we also discussed  
19 future coordination.

20 In addition, Commission level meetings  
21 have occurred to discuss issues of mutual interest,  
22 such as the scope and boundary between FERC and  
23 NRC cyber-security programs.

24 Most recently, the Office Director of

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 NSIR Jim Wiggins, met with FERC last month, and  
2 it was agreed that a meeting between the Chairman  
3 of NRC and FERC would occur later this year.

4 So, now, I'll turn to some other  
5 inter-governmental activities.

6 MEMBER BLEY: I'm just a little  
7 curious, since you have agreements with both FERC  
8 and NERC, and I don't know those guys completely,  
9 but I know that CIP seems to originate in NERC,  
10 but then FERC issues regulations based on it.

11 I'm not sure how these --

12 MR. HARRIS: FERC issues orders and  
13 approves -- Perry can jump in, if you like.

14 FERC issues order. NERC is actually  
15 the one that issued the CIP's, which were approved  
16 by order through FERC.

17 MEMBER BLEY: So, it's not --

18 MR. HARRIS: So, it's not the --

19 MEMBER BLEY: FERC has got regulatory  
20 authority and NERC develops things that sometimes  
21 FERC uses?

22 MR. PEDERSON: Yes, NERC is the  
23 executor of the regulation. So, they are the ones  
24 that develop the standards, do the inspections and

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealrgross.com](http://www.nealrgross.com)

1 levy the fines.

2 MEMBER BLEY: Oh, they do the fines,  
3 as well?

4 MR. PEDERSON: Yes.

5 MR. HARRIS: But it's a little --

6 MEMBER BLEY: So, because regulation,  
7 FERC has the --

8 MR. HARRIS: -- different situation  
9 then the --

10 MR. PEDERSON: Yes, so, they've been  
11 split up, you know. In the NRC, we are all under  
12 one roof.

13 MEMBER BLEY: Yes, okay.

14 MR. PEDERSON: Where we have all those  
15 functions, all within the NRC umbrella, but they've  
16 been split up that way.

17 MR. HARRIS: Go ahead, Craig.

18 MR. ERLANGER: I just think it's  
19 important to note that we did a side-by-side  
20 comparison of our requirements and our guidance,  
21 as compared to the NERC/CIP standards, and Perry,  
22 correct me if I'm wrong, but the verbiage we used  
23 at our requirements were equivalent, if not --  
24 equivalent requirements for both type, and they

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealrgross.com](http://www.nealrgross.com)

1 were asked -- they were satisfied --

2 MEMBER BLEY: You don't really go  
3 further? They're essentially equivalent?

4 MR. ERLANGER: We leave it at that.  
5 They did a side-by-side and they felt comfortable  
6 with us, looking out for some of their activities  
7 --

8 MEMBER BLEY: Okay.

9 MR. ERLANGER: -- out there, and the  
10 MOU and LOA leave the door open though, if they  
11 have an interest to explore a particular topic  
12 further down the road.

13 But we did a side-by-side of the  
14 standards and Reg Guide 5.71.

15 MEMBER BLEY: Okay, thank you.

16 MR. HARRIS: Yes, for example, FERC  
17 would construct NERC to develop standards. NERC  
18 would develop the standards and they'd be approved  
19 by FERC. It's a little different done situation.

20 MEMBER BLEY: Okay, but this gets into  
21 something Charlie was getting at earlier, in that  
22 the things they have responsibility for in  
23 enforcing, can affect our plants, because of the  
24 power connections.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealrgross.com](http://www.nealrgross.com)

1 CHAIRMAN BROWN: Yes, the switch yard,  
2 or the grid side of the switch yard, not necessarily  
3 the generator side.

4 MR. HARRIS: Yes, I mean, that could  
5 be an initiator for loss of offsite power.

6 MEMBER BLEY: Yes, or some unusual  
7 configuration, okay.

8 CHAIRMAN BROWN: Just, let me ask one  
9 question on that.

10 Have you -- I mean, the loss of offsite  
11 power thing, which has -- because it seems the SCADA  
12 stuff seems to hit periodically, keep popping up,  
13 if you read -- you know, from what I read in various,  
14 you know, publications and things.

15 Have you actually looked at their  
16 oversight or what things they have tried to oversee  
17 or put in place, to maintain -- ensure that the  
18 control of those grid connections are protected?

19 MR. ERLANGER: Can you clarify, by  
20 look, do you mean have we physically gone out there  
21 and seen the --

22 CHAIRMAN BROWN: No, I don't mean that.

23 I mean, what processes do they have in place?  
24 Do they have something in place with the grid

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 operators that people look at the systems, or how  
2 do they maintain the security of the ability to  
3 maintain control of those, without having somebody  
4 come in and trip them inadvertently -- not  
5 inadvertently, but maliciously?

6 MR. ERLANGER: Perry, do you have any  
7 concession on the CIP standards that are --

8 MR. PEDERSON: Well, we have looked at  
9 their -- as Craig mentioned, we did a cross-walk  
10 between the requirements and the NERC/CIP, one  
11 thing to note about their process, to distinguish  
12 it from the NRC process, is they maintain an ANSI  
13 standard process.

14 In other words, it's by consensus of  
15 the regulated, unlike the NRC, where we accept input  
16 and then we make a decision.

17 And so, this is my personal opinion,  
18 but as I read some of those standards, there are  
19 things that are not perhaps, as rigorous and there  
20 are things that would fall out that -- you know,  
21 if our process were applied, we might call it a  
22 critical digital asset, and maybe in the case of  
23 the NERC/CIP, if it's a device that has a -- for  
24 example, and non-routable protocol, then they may

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealgross.com](http://www.nealgross.com)



1 not call it a critical digital asset.

2 They have different terminology and a  
3 different framework, but their focus, of course,  
4 at the grid is on reliability, where our focus is  
5 on safety.

6 So, you would expect some of those  
7 differences.

8 MR. ERLANGER: And I would offer, their  
9 program, similar to ours, it's evolving, and  
10 they're learning, and we meet with them, at the  
11 staff level, on a much more frequent basis, to share  
12 information, and learn what they're doing and  
13 approve our requirement and vice-versa.

14 CHAIRMAN BROWN: Yes, the reason I --  
15 there is a number of -- publically, you read about  
16 some of the -- what I would call the independent  
17 consultants and others, who rail-on in the various  
18 -- like the various electrical publications,  
19 whether it be IEEE publications or what have you.

20 There is a considerable skepticism,  
21 relative to the vulnerability of the grid, not just  
22 for nuclear power plants, but the grid in general,  
23 relative to mischief, because of the communication  
24 methodologies to now control it.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealgross.com](http://www.nealgross.com)

1           It's so -- so convenient, with the  
2           ability to not have hard wires going everywhere,  
3           and having little computer sitting around in places  
4           that -- that it's very hackable, or at least they  
5           maintain it's very hackable.

6           MEMBER SHACK: It's getting smarter  
7           all the time.

8           CHAIRMAN BROWN: Yes, but that means  
9           it's probably even more hackable, okay. That's  
10          the problem with complexity is, it increases the  
11          opportunities for malicious and -- in reality.

12          MEMBER BLEY: It doesn't garner  
13          confidence, but the distribution system and the  
14          sub-stations physically are scattered all over the  
15          place.

16          CHAIRMAN BROWN: That is true.

17          MR. PEDERSON: Well, and that's also  
18          --

19          MEMBER BLEY: For non-liberal, as  
20          well.

21          MR. PEDERSON: Yes.

22          CHAIRMAN BROWN: Yes.

23          MR. PEDERSON: The limit of the NERC  
24          relations, the NERC CIP doesn't go through the

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealgross.com](http://www.nealgross.com)

1 distribution layer. It's through the generation  
2 and transmissions layers of the grid.

3 CHAIRMAN BROWN: Oh, is that right?  
4 So, it's just been applied to the switch yard  
5 itself, in terms of its connection to the plants  
6 --

7 MR. PEDERSON: Yes, it touches us at  
8 the switch yard, of course --

9 CHAIRMAN BROWN: Yes, yes.

10 MR. PEDERSON: -- where generation --

11 CHAIRMAN BROWN: But outside of that,  
12 they don't go.

13 MR. PEDERSON: Yes, like whatever  
14 happens if your house and in your local --

15 CHAIRMAN BROWN: Yes, I'm not really  
16 worried. If my house goes out, nobody is going  
17 to worry about it, except my family, or I should  
18 say my wife.

19 MR. PEDERSON: But this is one of the  
20 short-comings of the current NERC CIP, and they're  
21 on Version 5 now, I think it is, and looking down  
22 the road --

23 MR. HARRIS: I think they're looking  
24 at Version 6.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. PEDERSON: Yes, so, another  
2 version is coming because they keep trying to  
3 address these issues, like the distribution layer,  
4 which is where you find a lot of the smart grid  
5 evolving now, and the smarts is operating at that  
6 layer. But the NERC CIP doesn't touch that.

7 CHAIRMAN BROWN: Okay, I'm glad I asked  
8 the question then, because I didn't understand that  
9 completely. Thank you. Okay, you can --

10 MR. HARRIS: And luckily from a safety  
11 standpoint, plants know what to do when they don't  
12 have offsite power.

13 CHAIRMAN BROWN: No, I recognize that.  
14 I'm not saying that is -- I mean, that's one of  
15 the things they have to cover, so --

16 MR. PEDERSON: Right, and we do -- just  
17 as a footnote, we do coordinate a lot with NERC  
18 and FERC on sharing the threat, as well.

19 CHAIRMAN BROWN: Okay.

20 MR. HARRIS: So, slide five, as you may  
21 be aware, DHS is -- or Division of -- Department  
22 of Homeland Security is responsible for critical  
23 infrastructure protection.

24 DHS's national infrastructure

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 protection plan, or NIPP, provides a unified  
2 structure for the integration of critical  
3 infrastructure and key resource protection.

4 The NIPP includes 16 sector-specific  
5 plans that detail the application of an overall  
6 risk management framework for each sector.

7 As part of the nuclear sector, NRC  
8 participates in the Joint Cyber Sub-Council. The  
9 Cyber Sub-Council includes members from Department  
10 of Homeland Security, FBI, NRC and private sector  
11 representatives.

12 The Joint Sub-Council identifies  
13 cyber-security risk, potentially affecting the  
14 nuclear sector, serves as a forum for sharing of  
15 relevant information within the critical  
16 infrastructure framework, and also helps the  
17 nuclear sector participate in cross-sector bodies,  
18 such as the cross-sector cyber-security working  
19 group and the industrial control system working  
20 group.

21 So, now, I'll move on to the next slide,  
22 Perry, thanks, to the executive order.

23 Back in February 12<sup>th</sup> of this year,  
24 President Obama issued an executive order on

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealgross.com](http://www.nealgross.com)

1 improving critical infrastructure for  
2 cyber-security.

3 Also issued was a Presidential Policy  
4 Directive PPD-21 Critical Infrastructure Security  
5 and Resilience.

6 The executive order requires Federal  
7 agencies to produce unclassified reports of threats  
8 to U.S. companies and it requires the reports to  
9 be shared in a timely manner.

10 The executive order establishes a  
11 voluntary program to promote the adoption of the  
12 cyber-security framework, again, voluntary  
13 program.

14 Because NRC is an independent agency,  
15 the NRC is not obligated to take actions as a result  
16 of the executive order.

17 However, NRC is voluntarily  
18 participating in a number of areas.

19 For example, NRC management and staff  
20 have interacted with National Security and DHS  
21 staff on policy issues.

22 NRC staff is also participating in the  
23 integrated task force working groups that have been  
24 formed by DHS to implement the Presidential Policy

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealrgross.com](http://www.nealrgross.com)

1 Directive.

2 We believe that given the state of our  
3 cyber-security program compared to those in other  
4 critical infrastructure areas, that we can make  
5 a significant contribution towards meeting the  
6 deliverables from the Presidential Policy  
7 Directive. Next slide.

8 CHAIRMAN BROWN: Who audits the  
9 voluntary -- voluntary is one thing. I mean,  
10 people work on a business model. If they -- they're  
11 going to make a profit somewhere.

12 MR. HARRIS: Well, I think that --

13 CHAIRMAN BROWN: So, the cost is really  
14 going to --

15 MR. HARRIS: With the framework of an  
16 executive order, it's not like a regulation or a  
17 law --

18 CHAIRMAN BROWN: No, I understand  
19 that.

20 MR. HARRIS: -- which requires that --

21 CHAIRMAN BROWN: I was reading  
22 something else, relative to the executive order,  
23 and then it was interesting, the ability to see  
24 the -- how voluntary -- voluntary, they've got a

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealgross.com

1 lot of choices to make it a cost benefit analysis,  
2 which says that doesn't improve my bottom line.

3 So, I'll take the risk, that this is  
4 not going to happen to me, because I think the risk  
5 is manageable. You don't have any control over  
6 that.

7 MR. PEDERSON: In recognizing that,  
8 one of the working groups established under the  
9 executive order, is focused on incentives.

10 CHAIRMAN BROWN: Does the taxpayer  
11 subsidize those incentives or what? I said that  
12 facetiously, okay.

13 MR. ERLANGER: One of the challenges  
14 is that you got a -- try to make -- have a 'one  
15 size fits all' model for 16 very diverse sectors  
16 ---

17 MR. PEDERSON: Yes, right.

18 MR. ERLANGER: -- unlike the other --  
19 and by 16 sectors, what I mean is, DHS has basically,  
20 just broken up the United States into their  
21 functional areas.

22 So, everything ranging from financial,  
23 dams, nuclear, across the board, unlike the nuclear  
24 sector, not every sector has a regulator with

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701



1 requirements.

2 So, the attempt of this was to  
3 capitalize on a lot of these voluntary efforts,  
4 in order to improve cyber-security practices across  
5 the board.

6 CHAIRMAN BROWN: Is the nuclear sector  
7 a voluntary sector?

8 MR. ERLANGER: No, we're -- as Tim  
9 mentioned, we're -- because we're an independent  
10 agency, and the existence of the --

11 CHAIRMAN BROWN: So, I mean, so the  
12 critical -- I'm trying to think of this in terms  
13 of critical sectors. Do the critical sectors have  
14 some regulatory --

15 MR. PEDERSON: Not all of them.

16 MR. ERLANGER: Not all of them.

17 CHAIRMAN BROWN: Okay.

18 MR. ERLANGER: Chemical has just  
19 started being regulated by DHS. That was one for  
20 a while. There is -- dam sectors vary in degrees.  
21 Regulators, obviously, and banking is obviously,  
22 a diverse one and the --

23 CHAIRMAN BROWN: So, that is still a  
24 work in progress, is what you're saying.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. ERLANGER: Yes, but to answer your  
2 question, not every sector has a regulator.

3 CHAIRMAN BROWN: Okay.

4 MR. HARRIS: But you can see that the  
5 establishing this voluntary framework on a --  
6 applicable to a large number of sectors, could later  
7 be used to refine to go into a sector specific,  
8 or be adapted.

9 CHAIRMAN BROWN: Yes, I wasn't  
10 advocating that one size fits all, don't get me  
11 wrong. I was just trying to get a feel for what  
12 voluntary meant, and I think you've given me an  
13 answer on that.

14 MR. HARRIS: Good. So, the executive  
15 order also calls for the review of existing  
16 cyber-security regulations.

17 Regulatory agencies are encouraged to  
18 use a voluntary framework to assess their programs  
19 and to determine if the existing requirements are  
20 sufficient.

21 Independent regulatory agencies, such  
22 as the NRC, are encouraged to lever -- leverage  
23 the voluntary framework and to consider prioritized  
24 actions to mitigate cyber-risk for critical

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealrgross.com](http://www.nealrgross.com)

1 infrastructure, consistent with their authority.

2

3           So, I think what that means is, you  
4 know, if you have a program, look at the framework,  
5 see if you can glean anything that might help  
6 improve your program.

7           NRC, of course, will review our  
8 requirements, as directed by the Presidential  
9 Policy Directive, and although we're pretty  
10 confident that our cyber-security program is  
11 strong, we will of course, implement any  
12 improvements that are identified from that review.

13           So, NRC works closely with  
14 international counterparts to enhance nuclear  
15 safety and security worldwide. This includes  
16 exchanging information, expertise, operating  
17 experience, research and best practices.

18           The next two slides provide examples  
19 of bilateral and multi-lateral activities relative  
20 to cyber-security.

21           For example, NRC staff has had specific  
22 technical exchanges with Korea and Spain on  
23 cyber-security.

24           Staff has also shared cyber-security

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 best practices with organizations, such as the  
2 World Institute for Nuclear Security. Next slide.

3 NRC has also participated in a number  
4 of IAEA consultants meetings and larger technical  
5 meetings. In these multi-lateral meetings, topics  
6 have included developing guidance for computer  
7 security at nuclear facilities, including nuclear  
8 power plants, applying cyber-security controls to  
9 digital instrumentation and control systems, and  
10 developing assessment methodologies for cyber  
11 risk.

12 NRC staff has also assisted IAEA in  
13 developing guidelines for evaluating computer  
14 security during the IAEA advisory missions, and  
15 then updating training materials for computer  
16 security.

17 Review of documents also includes  
18 review of safety standards, such as DS431, entitled  
19 'Design of Information and Control Systems for  
20 Nuclear Power Plants'.

21 We review these documents, the safety  
22 documents, to ensure that proper and adequate  
23 interfaces with cyber-security are occurring.

24 IAEA has documents specific to

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 cyber-security for power plants, so, the technical  
2 content for cyber-security are contained in those  
3 documents, but the purpose of the review of the  
4 safety documents is to make sure that there is  
5 linkages in both documents, so that the interfaces  
6 are covered.

7 In general, we are ahead of other  
8 countries in establishing a regulatory framework  
9 that considers cyber-security. Staff believes  
10 that sharing their experience and developing NRC's  
11 cyber-security program will contribute to a more  
12 robust global cyber-security program for nuclear  
13 facilities.

14 We have also been able to consider the  
15 efforts and approaches of other international  
16 partners, in relations to NRC cyber-security  
17 program, and as additional input for future changes  
18 in the program -- we'll use those insights as their  
19 program evolves. Next slide.

20 So, that basically concludes my  
21 presentation. I'd be happy to entertain  
22 questions, if time allows.

23 MR. HECHT: This is Myron again, from  
24 Los Angeles. Can I ask a question?

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 CHAIRMAN BROWN: Yes.

2 MR. HECHT: Okay, in the bright line  
3 work between NERC/FERC and the NRC, there is some  
4 equipment from the switch yard which -- or I should  
5 say there is some distribution and power  
6 distribution, which goes back into the plant, and  
7 there's equipment associated with that, and of  
8 course, there are relays associated with that, and  
9 in many cases, these relays are directly attached  
10 to the internet.

11 Do those relays fall under the category  
12 of CDA, which makes it belong to the NRC or might  
13 those relays actually be vulnerable through direct  
14 internet attachment?

15 MR. HARRIS: Yes, I don't have that.

16 I mean, I guess it may be plant-specific. I don't  
17 have that granularity on where the actual bright  
18 line was drawn. I don't know if others in the room  
19 do.

20 MR. PEDERSON: One way to describe it  
21 is that our regulation covers the balance of plant,  
22 out to that first inter-tie in the switch yard.  
23 But there may be relays and such, that are  
24 physically on the other side, that are impacted

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 by systems on the inside of that point.

2 And so, it will, as you say, require  
3 a site-specific assessment to determine if it is  
4 a critical digital asset under our rule.

5 If it is not, part of our agreement with  
6 FERC and NERC is that we will tell them, everything  
7 that is discovered, and licensees are required to  
8 report those items that are not specifically  
9 identified as a CDA under our regulation, they're  
10 required to report that, so that they are covered,  
11 and this is to ensure that there is no gap.

12 MR. HECHT: Okay, so, basically you're  
13 saying that in the -- in case of doubt, the NRC  
14 covers it?

15 MR. HARRIS: No, I think there is a  
16 process that determines what is covered by NRC and  
17 what would be covered by the NERC CIP.

18 So, there is no ambiguity. No gap, as  
19 Perry said.

20 CHAIRMAN BROWN: Let me rephrase it.

21 The way you're saying it is the plant is required  
22 to inform NERC and FERC, for those which are not  
23 under NRC control.

24 So, there is a positive action taken,

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 as opposed to an ambiguous, let somebody else figure  
2 it out type action?

3 MR. HARRIS: Correct.

4 MR. PEDERSON: Right.

5 CHAIRMAN BROWN: Okay.

6 MR. HECHT: Okay, thanks.

7 CHAIRMAN BROWN: Thanks, Myron. Any  
8 other questions? Dennis? Bill? Sam?

9 MEMBER ARMIJO: No.

10 CHAIRMAN BROWN: Okay.

11 MR. PEDERSON: Did you have a question?

12 MR. GROSS: A comment from the audience.

13 Actually, relative to this particular topic.

14 MS. ANTONESCU: Can you please state  
15 your name?

16 MR. GROSS: My name is William Gross  
17 from the Nuclear Energy Institute.

18 While it's not one of the NERC critical  
19 infrastructure protection reliability standards,  
20 there is a NERC standard that has been approved  
21 by FERC. It's been around since as long as I've  
22 been engaged in cyber-security that's called  
23 NUK-001, or Nuclear Utility Interface  
24 Requirements.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealrgross.com](http://www.nealrgross.com)



1           That was developed on -- at the request  
2 of the industry to address specifically, the issue  
3 of the relationship between the plant and the  
4 transmission system, regarding the reliability of  
5 the transmission system to address the concern of  
6 the station black-out.

7           So, there are interface agreements  
8 currently between each plant and the transmission  
9 provider, to coordinate on a wide range of topics.

10           I don't -- I haven't looked at that  
11 close enough to understand how much that addresses  
12 cyber-security. I met with some of the transmission  
13 folks that -- from the Nuclear Utilities, just a  
14 few weeks ago, to talk about this issue of where  
15 that segmentation is.

16           They assured me that actually in the  
17 NUK-interface agreements, there would be likely  
18 a diagram or a textual description of exactly at  
19 which point the plants ownership of the switch yard  
20 ends and the transmission system begins.

21           What the transmission system picks up,  
22 those facilities would be subject to the NERC  
23 critical infrastructure protection reliability  
24 standards, for protection from cyber-attack.

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 Everything from the plant side in, would be subject  
2 to the NRC's requirements.

3 CHAIRMAN BROWN: Okay, thank you very  
4 much. With that, we will recess for 10 minutes,  
5 until -- or 11 minutes, until 3:30 p.m.

6 (Whereupon, the open session in the  
7 above-entitled matter adjourned at 3:18 p.m.)  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24

**NEAL R. GROSS**

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

[www.nealrgross.com](http://www.nealrgross.com)



**U.S.NRC**

UNITED STATES NUCLEAR REGULATORY COMMISSION

*Protecting People and the Environment*

# **Cyber Security Update**

Craig Erlanger and Ron Albert  
Office of Nuclear Security and Incident Response  
June 4, 2013

# Agenda

- Opening Remarks – NSIR management
- Overview of the NSIR Cyber Security Organization
- History and Current Status of NRC’s Cyber Security Program / Regulatory Framework
- Overview of the Cyber Security Oversight Program
- Inter-Office Coordination Activities
- Interagency / International Activities
- Cyber Security Roadmap Activities
- Path Forward

# Desired Outcomes

- Provide an overview of NRC's cyber security program and explain how it is being implemented.
- Improved communication and coordination with ACRS on cyber security.
- Identify areas of interest for future interactions.

# NSIR Organization

- NSIR was established in 2003.
- Mission: To prevent nuclear security incidents and prepare for and respond to safety and security events.
- Three technical divisions:
  - Division of Security Policy (DSP)
  - Division of Security Operations (DSO)
  - Division of Preparedness and Response (DPR)

# Division of Security Policy

## *Cyber Security Roles*

- **Cyber Security and Integrated Response Branch (CSIRB)**
  - Focus Areas: Rulemaking, guidance, licensing, roadmap implementation, and intergovernmental and international coordination.
- **Fuel Cycle and Transportation Security Branch**
  - Focus Area: Fuel Cycle Facilities Cyber Security related activities. Supported by CSIRB.

# Division of Security Operations

## *Cyber Security Roles*

- **Reactor Security Oversight Branch:**
  - Focus areas: Cyber Security Oversight Program, Cyber Assessment Team (CAT), regional coordination and intergovernmental and international coordination.
- **Intelligence Liaison Threat Assessment Branch**
  - Focus areas: Cyber Security threat analysis, intergovernmental and international coordination.



# Staff Experience

- Cyber Security relies on a team approach:
  - Staff supporting the cyber security program has worked in multiple NRC offices and private sector companies.
  - Strong Cyber Security, Industrial Control Systems, Digital Instrumentation and Control, Engineering and Information Technology backgrounds.

# Questions





**U.S.NRC**

UNITED STATES NUCLEAR REGULATORY COMMISSION

*Protecting People and the Environment*

# **NRC Approach to Cyber Security**

Perry Pederson

Office of Nuclear Security and Incident Response

June 4, 2013

# Agenda

- Definition of Key Terms
- Cyber Threat Landscape
- Cyber Security Historical Timeline
- Coordination Efforts
- Regulatory Framework
  - Regulation, Guidance, Licensing, & Oversight
- Cyber Security Lifecycle
- Q&A

# Definition of Key Terms

- Cyber Security
  - Those measures and controls, implemented to comply with 10 CFR 73.54, to protect digital systems against the malicious acts of an intelligent adversary up to and including the design basis threat, as defined by 10 CFR 73.1
- Cyber Threat
  - An individual, entity, or action that by cyber-means has or indicates the potential to harm life, information, operations, the environment and/or property
- Critical Digital Asset (CDA)
  - A subcomponent of a critical system that consists of or contains a digital device, computer or communication system or network
- Adverse Impact
  - A direct and deleterious effect on a CDA.
- Defense-in-depth
  - An approach to security in which multiple levels of security and methods are deployed to guard against failure of one component or levels

# Cyber Threat Landscape

## Threat vectors

- Hard-wired networks
  - Internet
  - Intranet
- Wireless
  - Wifi
  - Bluetooth
- Mobile media
  - USB thumb drive
  - CD/DVD
- Portable equipment
  - Laptops
  - Test equipment
- Supply chain
  - Vendors
  - Vendors to the vendors

## Threat characteristics

- Motivated
- Opportunistic
- Persistent
- Adaptive
- Learning
- Good at info sharing

# Cyber Security Historical Timeline



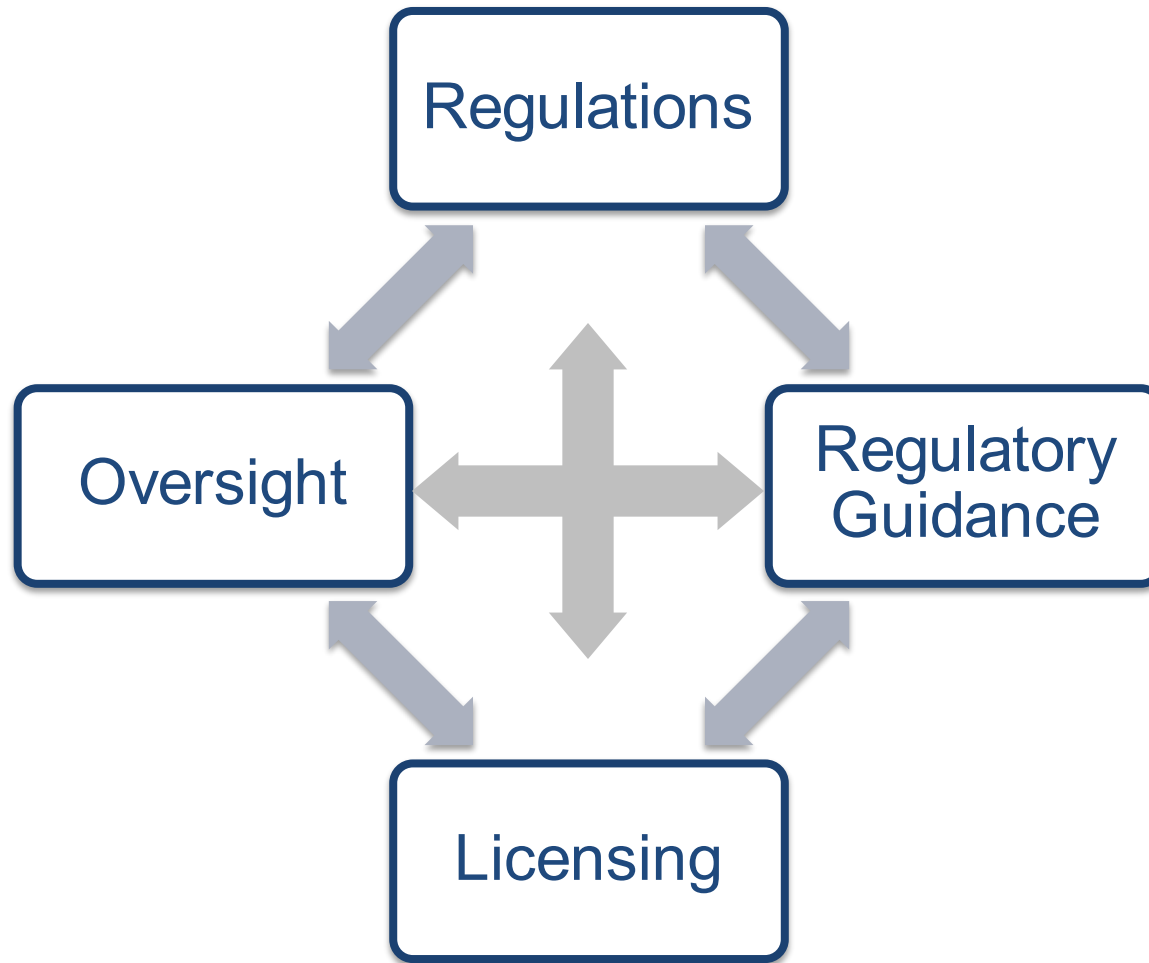
1998	Presidential Decision Directive 63 (PDD-63)
2001	Executive Order on Critical Infrastructure Protection (CIP)
2001	Issued advisory to NPP to enhance cyber security
2002	Required NPP to implement Interim Compensatory Measures
2003	Issued Design Basis Threat Order
2004	Published NUREG/CR-6847 – Cyber Risk Assessment
2005	Endorsed NEI 04-04 Rev. 1 – Cyber Security Program
2006	Published RG 1.152 Rev. 2 – computers in safety systems
2007	Design Basis Threat Rule 10 CFR 73.1/RG 5.69
2009	Issued Cyber Security Rule 10 CFR 73.54
2010	Published Cyber Security Regulatory Guide RG 5.71
2010	NEI publishes NEI 08-09 – used by operating NPPs
2011	NPP Cyber Security Plans approved
2013	Inspection of Interim Milestones begin

# Coordination Efforts

- **Intragency**
  - NSIR, NRR, NRO, RES, and Regions have worked and continue to work together
  - IOI Memorandum
- **Interagency**
  - DOE, FERC/NERC (Brightline), FBI, DoD, and others
  - DHS under the National Infrastructure Protection Plan (DHS as the Nuclear Sector SSA)
- **International**
  - International Atomic Energy Agency (IAEA)
  - Bilateral cooperation with South Korea, Spain
- **Industry**
  - Owners / Operators
  - Nuclear Energy Institute (NEI), EPRI



# Regulatory Framework



# 10 CFR 73.54

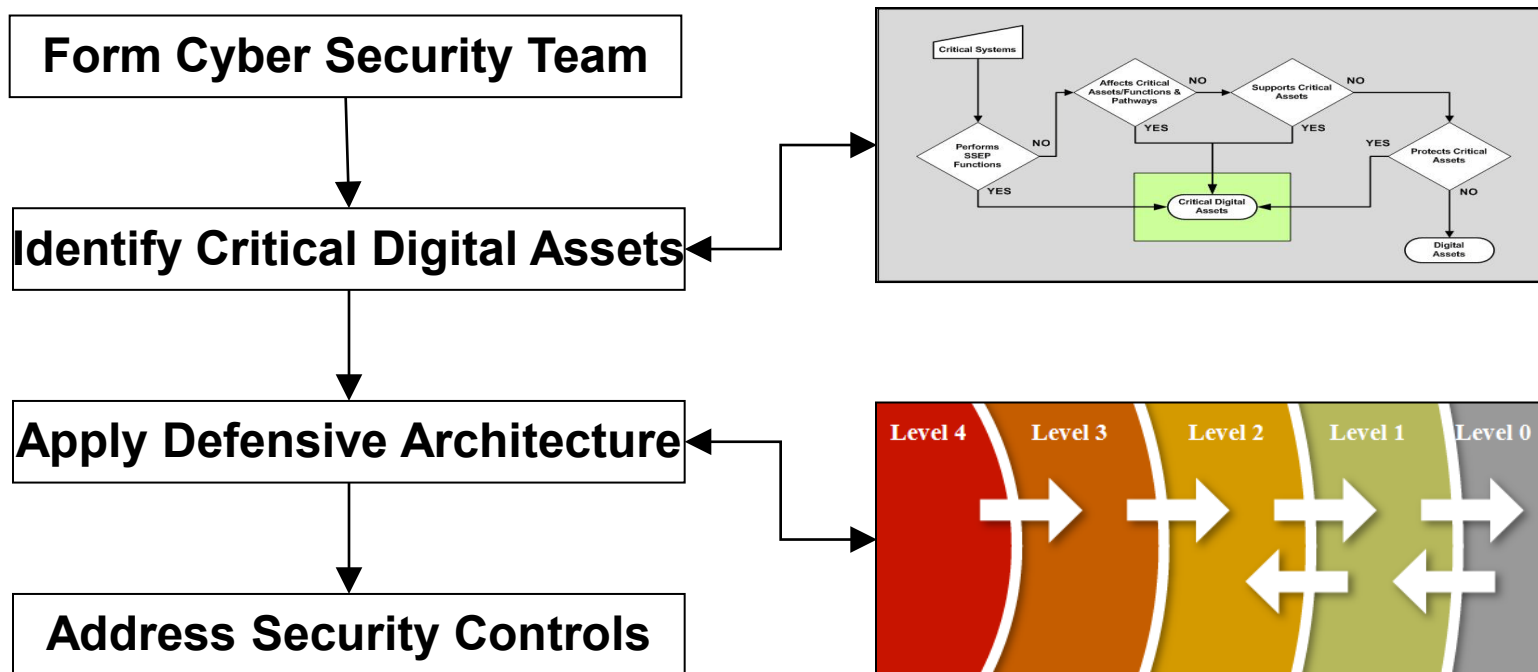
- Title: Protection of digital computer and communication systems and networks
  - Applies to power reactors – operating and new reactors
- Performance-Based, Programmatic (< 2 pages)
  - Provide high assurance against cyber attack
  - Integrated with Physical Security Program (10 CFR 73.55)
- Basic Requirements
  - Critical digital assets must be protected
  - Protect safety, important-to-safety, security, and emergency preparedness functions and support systems that can impact those functions
  - Provide defense-in-depth protective strategy
  - Implement a defensive architecture
  - Address technical, operational, and management controls

# Regulatory Guidance Pedigree

- Primary Sources
  - National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53
  - NIST SP 800-82
- Contributors
  - NRC staff from NSIR, NRR, NRO, RES
  - National Laboratory
  - Industry / Public Stakeholders
  - Private industry experts

# Regulatory Guide 5.71

## Title: Cyber security programs for nuclear facilities



1. Address each control for each CDA, or
2. Apply alternative measures, or
3. Explain why a control is N/A

# Cyber Security Plan

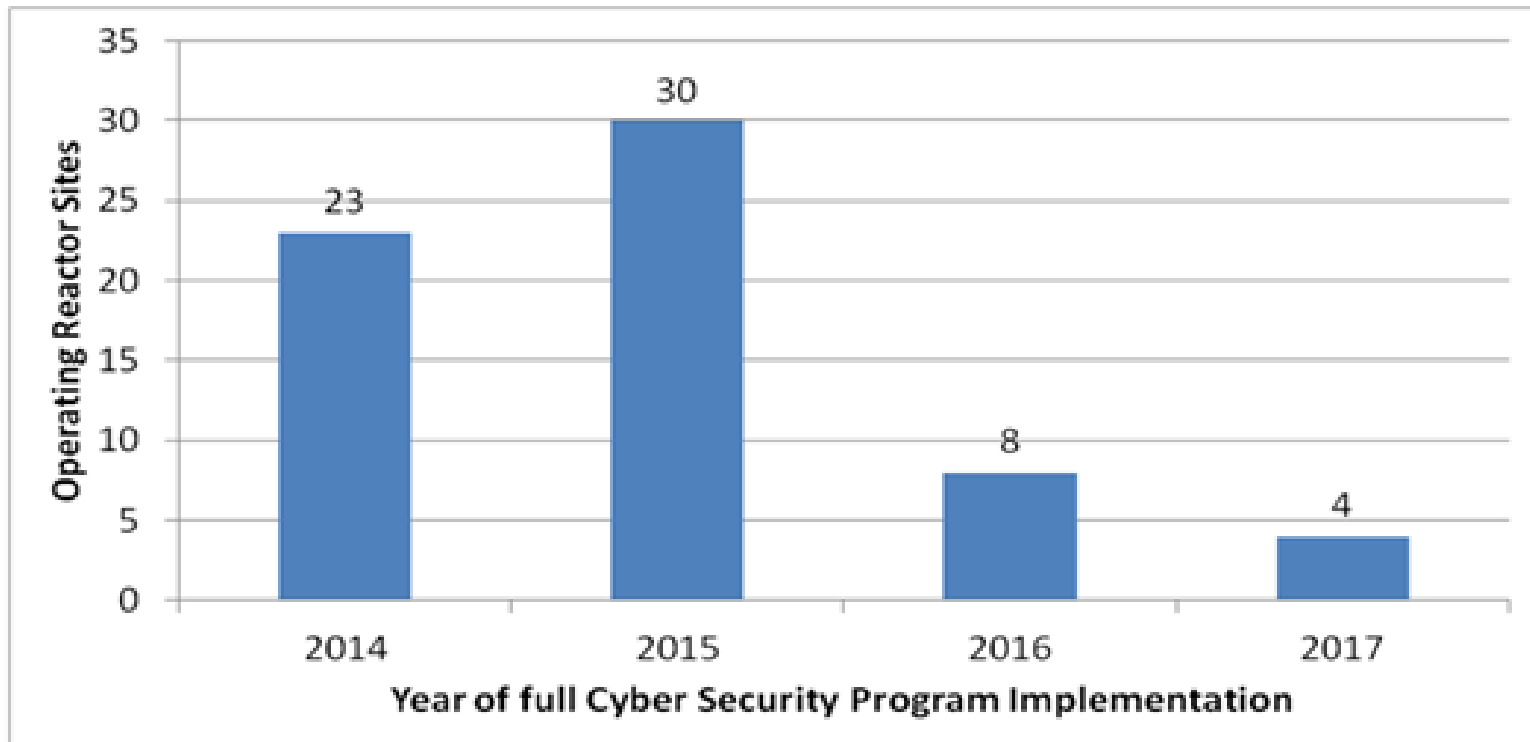
- Cyber Security Plan
  - Licensing document / required by regulations
  - Describes how cyber security program is established and maintained
- Essential elements:
  - Describe the process for identifying CDAs
  - Describe the defensive model (protective strategy)
  - Reference a comprehensive set of security controls
  - Describe the process for addressing each control
  - Commit to maintaining adequate documentation

# Implementation

- Interim Milestones 1-7 (December 31, 2012)
  - addresses key threat vectors
  - emphasis on target set equipment
- Milestone 8 (site specific date – 2014-17)
  - full cyber security program implementation
  - policies and procedures: training, attack mitigation, incident response, continuity of operations, etc
  - completion of all design remediation actions including those that require a refuel outage for implementation
  - Address all security controls for all CDAs

# Milestone 8

## Full Program Implementation



# Cyber Security Lifecycle

- Operating NPPs start in the Operation & Maintenance phase
  - Earlier phases of the lifecycle are implemented as needed based on licensee approved Cyber Security Plan
- New NPPs begin at the Concepts & Requirements phase
  - All regulatory requirements must be met before fuel arrives onsite

## Digital system security lifecycle as outlined in RG 5.71

Concepts & Requirements	Design, Implementation, & Test	Installation, Checkout & Acceptance Testing	Operation & Maintenance	Retirement
<ul style="list-style-type: none"> <li>• Security planning &amp; requirements analysis</li> </ul>	<ul style="list-style-type: none"> <li>• Supply chain security</li> <li>• Functional security design</li> <li>• System test &amp; evaluation</li> </ul>	<ul style="list-style-type: none"> <li>• Audit of security control effectiveness (operational focus)</li> <li>• Vulnerability scanning</li> </ul>	<ul style="list-style-type: none"> <li>• Continuous monitoring &amp; assessment</li> </ul>	<ul style="list-style-type: none"> <li>• Design control</li> <li>• Media sanitation (digital and non digital)</li> <li>• Disposal testing</li> </ul>



# Questions





**U.S. NRC**

UNITED STATES NUCLEAR REGULATORY COMMISSION

*Protecting People and the Environment*

# **Cyber Security Inter-Office Collaboration**

Tim Mossman

Office of Nuclear Security and Incident Response

June 4, 2013

# Inter-Office Coordination

- Cyber security concerns may arise at many points in the regulatory process
- Ensuring appropriate cyber protections are taken throughout digital life cycle
- Minimize regulatory risk to licensees
- Efficient use of staff resources

# Cyber Framework Evolution

- Commitment to ACRS
- Framework has been informed by on-going activities:
  - NSIR / NRR coordination on digital licensing\*
  - NSIR / NRO coordination on new reactors\*
  - NSIR / Regional cyber inspection activities\*

\* Closed portion of meeting

# Cyber Framework Development

- Multi-Office participation
- Addresses expectations for HQ Offices and Regions

# Example Regulatory Activities

- License amendment involving digital system
- Licensee event report (Operating Experience program)
- Combined License (COL) application / modification
- Design Certification (DC) application / modification
- Vendor inspection that raises supply chain questions
- Standards development activities

# Summary

- Staff from all NRC Offices work in an integrated fashion on Digital I&C safety and security issues
  - Collaboration has occurred through coordination by the staff on particular cyber-related topics and licensing actions
- Staff recognized the need for more explicit framework to facilitate interactions on cyber security regulatory activities
  - Commitment to ACRS
- Affected Branch Chiefs recently signed out a framework detailing the types of regulatory activities that have cyber considerations and staff interactions that result
  - The framework is intended to be formalized into an Inter-Office Instruction

# Questions







**U.S. NRC**

UNITED STATES NUCLEAR REGULATORY COMMISSION

*Protecting People and the Environment*

# **Intergovernmental and International Interactions**

Tim Harris

Office of Nuclear Security and Incident Response

June 4, 2013

# Overview

- Federal Energy Regulatory Commission and the North American Electric Reliability Corporation Activities
- Other Intergovernmental Activities
- Executive Order/Presidential Policy Directive Activities
- International Activities

# FERC/NERC Activities

- Memorandum of Agreement with FERC
- Memorandum of Understanding with NERC
- Gap Analysis
- Bright line survey
- Commission Policy in SECY-10-0153

# FERC/NERC Activities (2)

- Commission level meetings
  - Joint FERC NRC Meeting – March 16, 2010
  - Joint FERC NRC Meeting – June 15, 2012
- Periodic staff/management meetings
- FERC establishes Office of Energy Infrastructure Security

# Other Intergovernmental Activities

- Joint Cyber Subcouncil
- Cross-sector Cyber Security Working Group
- Industrial Control Systems Joint Working Group

# Executive Order

## IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY

- New information sharing programs to provide both classified and unclassified threat and attack information to U.S. companies
- Development of a Cyber Security Framework
- Establishes a voluntary program to promote the adoption of the Cyber Security Framework
- Includes strong privacy and civil liberties protections
- Review of existing Cyber Security Regulation

# NRC EO/PPD Activities

- Review our requirements, as directed
- Implement any improvements identified by the review
- Participate in executive level meetings and staff level working groups

# International Activities

- IAEA TM - Computer Security At Nuclear Facilities (May 2011)
- WINS – Workshop on the development and integration of cyber security programs (Feb 2012)
- IAEA CM – Revise Guidelines for computer security advisory/assessment Missions (March 2012)
- Korea Atomic Energy Research Institute (KAERI) -NRC's cyber security and safety-security interface regulations (May 2012)



# International Activities (2)

- IAEA CM - Application of security controls to instrumentation and control systems (June 2012)
- IAEA CM - Review and update the current training material on computer security at nuclear facilities (Sept 2012)
- IAEA CM - Application of security controls to instrumentation and control systems (Nov 2012)
- IAEA CM - Cyber threat assessment methodologies (Jan 2013)
- IAEA CM – Applying security controls to instrumentation and control systems: Security and Safety Considerations (Feb 2013)

# Questions

