

Official Transcript of Proceedings
NUCLEAR REGULATORY COMMISSION

Title: Advisory Committee on Reactor Safeguards

Docket Number: (n/a)

Location: Rockville, Maryland

Date: Friday, September 6, 2013

Work Order No.: NRC-208

Pages 1-80

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

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

UNITED STATES OF AMERICA
NUCLEAR REGULATORY COMMISSION
+ + + + +
607TH MEETING
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
(ACRS)
+ + + + +
OPEN SESSION
+ + + + +
FRIDAY
SEPTEMBER 6, 2013
+ + + + +
ROCKVILLE, MARYLAND
+ + + + +

The Advisory Committee met at the Nuclear
Regulatory Commission, Two White Flint North, Room T2B1,
11545 Rockville Pike, at 8:30 a.m., J. Sam Armijo,
Chairman, presiding.

COMMITTEE MEMBERS:

J. SAM ARMIJO, Chairman
JOHN W. STETKAR, Vice Chairman
HAROLD B. RAY, Member-at-Large
RONALD BALLINGER, Member
SANJOY BANERJEE, 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 COMMITTEE MEMBERS: (cont'd)

2 DENNIS C. BLEY, Member

3 CHARLES H. BROWN, JR., Member

4 MICHAEL L. CORRADINI, Member

5 DANA A. POWERS, Member

6 JOY REMPE, Member

7 PETER RICCARDELLA, Member

8 MICHAEL T. RYAN, Member

9 STEPHEN P. SCHULTZ, Member

10 GORDON R. SKILLMAN, Member

11

12 NRC STAFF PRESENT:

13 CHRISTINA ANTONESCU, Designated Federal

14 Official

15 MONIKA COFLIN, NSIR/CSD

16 RALPH COSTELLO, NSIR/CSD

17 CRAIG ERLANGER, NSIR/DSP/CSIRB

18 RUSSELL FELTS, NSIR/CSD

19 ERIC LEE, NSIR/CSD

20 TOM MOSSMAN, NRO/DE/ICE2

21 MOHAMMAD SHUAIBI, NRO/DE

22 STACY SMITH, NRO/DCIP/EVIB

23 BARRY WESTREICH, NSIR/CSD

24

25

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

TABLE OF CONTENTS

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

PAGE

Opening Remarks by the ACRS Chairman

4

Cyber Security Activities

5

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

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

(8:28 a.m.)

CHAIRMAN ARMIJO: Good morning. The meeting will now come to order.

This is the second day of the 607th meeting of the Advisory Committee on Reactor Safeguards. During today's meeting the Committee will consider the following: 1) cyber security activities; 2) future ACRS activities/report of the Planning and Procedures Subcommittee; 3) reconciliation of ACRS comments and recommendations; 4) assessment of the quality of selected NRC research projects; and 5) preparation of ACRS reports.

A portion of the session on cyber security activities may be closed pursuant to 5 USC 552b(c)(3) to protect unclassified Safeguards information applicable to this matter.

This meeting is being conducted in accordance with the provisions of the Federal Advisory Committee Act. Ms. Christina Antonescu is the Designated Federal Official for the initial portion of the meeting.

We have received no written comments or requests to make oral statements from members of the public regarding today's sessions.

There will be a phone bridge line. To

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 preclude interruption of the meeting, the phone will
2 be placed in a listen-in mode during the presentations
3 and Committee discussion.

4 A transcript of portions of the meeting is
5 being kept, and it is requested that the speakers use
6 one of the microphones, identify themselves, and speak
7 with sufficient clarity and volume, so that they can
8 be readily heard.

9 We have one item of interest that I'd like
10 to announce is that our long-time Court Reporter, Ms.
11 Kayla Gamin, will be leaving us after, I don't know,
12 I think at least four years of tremendous service. And
13 she is leaving to go to law school in Chicago, which
14 is -- I can't understand it, but --

15 (Laughter.)

16 -- I think she deserves a great deal of thanks
17 from the members of the Committee.

18 (Applause.)

19 With that, I'd like to turn it over to Mr.
20 Charles Brown, who has got the lead. Charlie?

21 MEMBER BROWN: Okay. This first agenda item
22 is obviously an update on cyber security. We know I
23 guess that Rule 73.54, and I guess the entire Rule 73.1
24 which says you've got to work on cyber, is now at the
25 point of being implemented. And the team that is doing

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 that is going to be here to try to give us an explanation
2 or an update on how they are organizing themselves and
3 how they are setting themselves up, so you can manage,
4 monitor, and ensure that the sites are in a good cyber
5 position.

6 They will also be reporting a little bit on
7 I guess the pilot project, Diablo Canyon, where the
8 initial pilot project on their I guess inspection and
9 audit, whatever they did in terms of evaluating that
10 particular plant. There will be both a closed and an
11 open -- and open and closed session, in that order.
12 I guess they will inform us when we're ready to go into
13 the closed session.

14 As a prelude to this, I guess we are going
15 to have a small lead-in here on an issue we have raised
16 in prior meetings on control of access and what their
17 general thinking is. And I feel -- I think they have
18 not gotten all of the agreements and concurrences from
19 all of the various directorates, but we will at least
20 get an idea of what some of the options are.

21 Now, Tim is here. Did you want to say
22 anything? Do you want me to go -- head over to Mo?
23 Okay. I will -- anybody else -- Barry or Monika? I
24 don't know. Who is going to lead this thing off.

25 MR. WESTREICH: I'm Barry Westreich. I'm 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

1 Director of the Cyber Security Directorate in NSIR, and
2 that's a new organization, so I think we -- Mo is going
3 to talk about a subject with the new reactor group, and
4 then we are going to talk about cyber security in general,
5 the programs and processes we have in place. So I think
6 we'll start with Mo and let you --

7 MR. SHUAIBI: Okay. Good morning. My name
8 is Mohammad Shuaibi. I'm the Acting Director for the
9 Division of Engineering in the Office of New Reactors.

10 And the purpose of my remarks -- and I'm going to try
11 to keep them brief today -- the purpose of my remarks
12 is to provide you an update on the staff's activities
13 to address the ACRS's March 19th letter on Chapter 7
14 of the mPower design-specific review standard.

15 By way of background, the Committee has
16 previously raised issues on the area of communications
17 independence and cyber security framework for new
18 reactors. Examples of where you raised issues include
19 ACRS letters of December 18, 2012, and March 19, 2013.

20 And we have responded to those two letters in
21 corresponding letters of February 6, 2013, and April
22 29, 2013.

23 In the Committee's March 19th letter, the
24 Committee comments focused on interpretation of Clause
25 5.9 of IEEE 603, which addresses control of access.

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 In that letter, the Committee referred to an earlier
2 letter that -- where you had taken a position, and you
3 wrote, "We recommend that the control of access review
4 section of the DSRS be expanded to require the reviewer
5 to assess the architecture and firewall to ensure that
6 it is hardware-based, one-way firewall."

7 The Committee's letter continued with, and
8 I quote, "No software should be involved in either its
9 operation or setup." So that's kind of where we are
10 -- where I am going to focus my remarks.

11 In our April 29, 2013, response, we indicated
12 that we are considering the Committee's recommendation,
13 and that we will update the Committee on our progress
14 as we meet with you. So this is one of these updates.

15 So then we move into ongoing activities and
16 next steps. First, specific to the mPower
17 design-specific review standard, we have engaged B&W
18 regarding Chapter 7 of the DSRS to address your
19 recommendation. We are currently in dialogue with B&W
20 on how to address the recommendation, and we are planning
21 meetings with them as a way to get a better understanding
22 of their design, discuss the issues, and reflect what
23 we need to do in our DSRS to address the recommendation
24 that you provided.

25 We owe you a letter to inform you of our

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 decision on this issue, and we plan to provide you that
2 letter before we finalize the DSRS. So you will see
3 something from us that shows you how we address that
4 for the DSRS. So that portion is specific to the mPower
5 design.

6 But more generically, as a result of your
7 March 19th letter, we held a series of meetings in the
8 staff to consider options on how to address your
9 recommendation more broadly. The meetings culminated
10 in an Office Director level meeting between the office
11 of NSIR, NRR, and NRO, on May 30th of this year. And
12 the last time when the Subcommittee met Tom Berglund
13 was here to brief you on that. And so I'm going to
14 summarize what Tom Berglund provided to you.

15 Office management was provided with the
16 staff's recommendations, and office management approved
17 moving forward to explore three concepts in parallel
18 for new reactors. I want to focus on one of these
19 concepts. It is one of the more immediate concepts,
20 and I think the one that you would probably be most
21 interested in at this time. But there are two others
22 which I could address. I think Tom covered them quite
23 a bit at the last meeting, but I think the one I'm going
24 to cover now is probably more relevant to what you want
25 to discuss for this status meeting.

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 So using this concept, we would incorporate
2 specific requirements for independence for new reactors
3 in our 10 CFR 50.55(a)(8). That's the rule that
4 addresses IEEE 603 or incorporates IEEE 603 into the
5 NRC regulations.

6 And we would also include a rule that would
7 require that if a design cert applicant were to take
8 an alternative to our new independence requirements,
9 that they would have to identify any resulting
10 communication pathways that they have introduced as a
11 result of that alternative. They would have to identify
12 those communication pathways because they may introduce
13 vulnerabilities.

14 The purpose of these requirements is to ensure
15 that the pathways created by the design and the
16 alternatives that they would take to our new requirements
17 are identified, and that there is a clear handoff between
18 the design certification applicant and the COL
19 applicant, so that the COL applicant would know what
20 they need to do and what communication pathways exist
21 that they would need to address in their future
22 activities.

23 This rulemaking approach is generic. Like
24 I said, the first item I addressed was specific to mPower.
25 The rulemaking activity would be generic. It would

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 be for design certification applications, not just
2 mPower. So it goes beyond the mPower design.

3 We are also -- I also want to note that we
4 are currently deliberating on this option as part of
5 the ongoing rulemaking activity for 50.55(a)(8). So
6 this goes back to Charlie's comment that we are not done
7 yet. I'm giving you a status that we are still
8 discussing this. And we are making good progress, I
9 believe, so we look forward to coming back and briefing
10 you again on this topic. As we indicated in our letter
11 to you, we will be briefing you and giving you status
12 as we make progress.

13 But I do want to note, final decisions have
14 not been made. So at this time, we don't expect to change
15 the interpretation of Clause 509 of 603, of IEEE 603,
16 but we do believe that our approach and the way that
17 we are proceeding is sound and has merit, and we look
18 forward to bringing that to you and having a dialogue
19 with you at the right time.

20 MEMBER BROWN: I'm certain we will have a
21 dialogue --

22 MR. SHUAIBI: I'm sure we will.

23 MEMBER BROWN: -- because there is obviously
24 some strong opinions on the use of -- and I presume you're
25 alluding to the fact that you are trying to update 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

1 rule to be 603-2009. Is it within that realm, or is
2 it going to be -- are you all trying to do this in one
3 or two pieces?

4 MR. SHUAIBI: No, you're right. It's the
5 IEEE 603-2009. I'm sorry, that was --

6 MEMBER BROWN: When you're ready to go do that
7 and make that part of the rule.

8 MR. SHUAIBI: We are doing this as part of
9 that activity, yes. The generic option that I talked
10 about here is part of the IEEE 609 -- the IEEE 603-2009
11 rulemaking activity.

12 MEMBER BROWN: Okay.

13 MR. SHUAIBI: And I believe the lead PM for
14 that rulemaking activity -- and Christian and Christina
15 have already been in dialogue about when we could come
16 to the Committee and give you an update on that activity.

17 And they are working out --

18 MEMBER BROWN: Ongoing activity to try to get
19 that -- once you are all ready to go, to get that scheduled
20 for a Subcommittee meeting and then a representation
21 at the full Committee.

22 MR. SHUAIBI: That's right.

23 MEMBER BROWN: You commented, if I'm not
24 mistaken, that there was kind of two pieces relative
25 to our letter, which we specified some thought processes

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 and then you threw in this alternative, if design agents
2 or designers or vendors or whoever, you come up with
3 an alternative path, so you still want to leave these
4 open doors for folks to tell you why they don't want
5 to do it the right way.

6 MR. SHUAIBI: It's not --

7 MEMBER BROWN: I'm being a little bit
8 pejorative in that because --

9 MR. SHUAIBI: I read the transcripts before
10 coming to this meeting.

11 (Laughter.)

12 I remember the questions that were asked then.

13
14 I understand what you're saying, but within
15 50.55(a), if you read the regulations, there are -- with
16 the required standards that we have on the applicants,
17 and then there is a clause in 50.55(a)(8)(3) that says
18 that a licensee could propose an alternative to what
19 we have in there, but they would have to justify it.

20 We are proposing -- or we are working on a
21 proposal for requirements for independence. We would
22 allow an applicant to come in and say, "We would like
23 to use an alternative to what we are proposing," but
24 this is where we would -- we are considering the
25 requirement that would say, if you want to do that, 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

1 if you want to introduce complexities and communications
2 pathways, you would have to identify those communication
3 pathways, so that a COL applicant would know what they
4 have to address in terms of vulnerabilities that are
5 introduced by such pathways.

6 MEMBER BROWN: As part of the DCD or the design
7 -- the license approval --

8 MR. SHUAIBI: That's the thinking right now.
9 That's right. That's the thinking right now. So --

10 MEMBER BROWN: So we just capture it as part
11 of the licensing process, as opposed to having it kind
12 of deferred out to the future sometime.

13 MR. SHUAIBI: That's right.

14 MEMBER BROWN: Okay.

15 MR. SHUAIBI: This is not inconsistent with
16 the rest of our regulations. We have our regulations,
17 and within 50.55(a) we use the word "alternative,"
18 because that's the word in the rule. But even our other
19 regulations, there is an exemption requirement, 50.12,
20 that says, "If an applicant comes across a situation
21 where they choose to take an exemption, they could
22 propose to do that, but they would have to provide a
23 justification." And we have criteria for what we would
24 look at in order for us to be able to provide or be willing
25 to approve an exemption.

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 So the regulatory process -- and I know
2 "process" is not usually a good word in this setting,
3 but the regulatory process allows for them to try --
4 don't take those paths. But there are criteria that
5 we would follow, and we would have to do a review to
6 decide whether an alternative that they may propose would
7 be acceptable or not, if it would be acceptable or not.

8 MEMBER BROWN: All right.

9 MEMBER CORRADINI: Can I ask a question?

10 MEMBER BROWN: Yes.

11 MEMBER CORRADINI: Since I -- Charlie is the
12 expert here, so -- so if we go to Summer and Vogtle,
13 how does what you just said affect those plants that
14 are in construction?

15 MR. SHUAIBI: That's part of the rulemaking
16 activity, and that becomes the scoping requirement that
17 would be included within the rules. So that would be
18 a good discussion topic for when we talk about the
19 specific rule and how it comes out. So I don't want
20 to talk specifically about Summer and Vogtle in the
21 context of a rule that we haven't fully developed yet,
22 because that is under deliberation right now within the
23 staff.

24 MEMBER CORRADINI: Okay.

25 MR. SHUAIBI: But let me generically, just

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 -- if I may just add one statement. In the case of a
2 plant like Summer or Vogtle where they are -- where they
3 have referenced a certified design and they have received
4 a license already, we would be under the backfit
5 requirement. If we wanted to go off and do something
6 on our own initiative, that says, "We want you to do
7 something different than what we have licensed you to
8 do."

9 MEMBER CORRADINI: But I guess since we're
10 talking process and not technical, I'm still not clear.

11 Do they satisfy, under their current design and what
12 they're building, the rule? Or would they need to take
13 -- I mean, there must be some feeling from the staff
14 where they sit relative to this. So where do they sit?

15 Or there is no feeling from --

16 MEMBER BROWN: No, it was mushy. When we
17 approved the license --

18 MEMBER CORRADINI: But you agree with Mr.
19 Brown that it's fuzzy?

20 MEMBER BROWN: It's very mushy on that plant
21 design. We discussed that during the DCD and our
22 approval letters, and we got a lot of pushback. So it's
23 --

24 MEMBER CORRADINI: With all due respect, I
25 hear you. I'm curious what the staff thinks.

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 MR. SHUAIBI: As part of the activity that
2 we have undertaken, we will be looking at what it looks
3 like for previous designs and what it looks like for
4 ongoing designs and what it would look like for future
5 designers.

6 MEMBER CORRADINI: So I take that to mean it's
7 unclear.

8 MR. SHUAIBI: I think what I would rather say
9 is maybe that would be a good topic to discuss in detail,
10 probably at the time when we come back to you with --

11 MEMBER CORRADINI: I've heard that before.
12 I'll stop. Okay. Fine.

13 MR. SHUAIBI: Let me just say, in our minds
14 we have done a lot of work already, so we've got some
15 answers to those questions.

16 MEMBER CORRADINI: Okay. Fine.

17 MR. SHUAIBI: But I do think it's a longer
18 discussion. I really do think it's a longer detailed
19 discussion --

20 MEMBER CORRADINI: That's fine.

21 MR. SHUAIBI: -- of you wanted to go down that
22 --

23 MEMBER CORRADINI: I just want to understand
24 what's out there now and how it relates to what you
25 explained. That's all. Thank you.

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 MEMBER BROWN: And now there's one more piece
2 that -- you know, you talk about new reactors, but we
3 really haven't addressed yet how we may want to cover
4 existing plans when they do a backfit or an extensive
5 digital I&C upgrade where they now bring in the networks,
6 where they bring in the whole new vulnerabilities
7 relative to control of access to these systems, and that
8 has not been covered yet. That is still part of the
9 general way it is right now, and it's -- so if we get
10 this new -- my view, and I'm not sure this is right,
11 because if we get the 50.55(a)(8) modified with 2009
12 with whatever we and everybody else agrees to, and then
13 a plant -- a licensee comes in with an upgrade, do they
14 have to make it to the new guidance? And does that then
15 require them -- and how does that hand off? And how
16 is that going to match? I just don't understand.

17 So that's another subject of discussion I
18 think we --

19 MEMBER BANERJEE: Are there licensees coming
20 up or --

21 MEMBER BROWN: Some are already in place.
22 Okay? Now, I don't know what other folks have in mind
23 because we haven't -- I know Oconee has had a full
24 backfit, and I guess there's -- is there another --

25 MR. MOSSMAN: Diablo.

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 MEMBER BROWN: Diablo, that's right. I'm
2 sorry. Diablo Canyon, right. So, but I don't know what
3 else is in the queue, if anything.

4 MR. SHUAIBI: And this has been part of the
5 long discussion within the staff about, how do we do
6 this? How do we do this for new reactors? How do we
7 do this for operating reactors? Do we do things
8 differently between the new and the operating reactors?
9 Are there differences in designs? Are there
10 differences in the level of integration, the level of
11 communication between a whole new design that is all
12 integrated and, you know, possibly an old design that
13 gets updates or upgrades in different areas versus the
14 whole system? So that --

15 MEMBER BANERJEE: How urgent is the
16 situation?

17 MR. SHUAIBI: I'm sorry?

18 MEMBER BANERJEE: How urgent is it?

19 MR. SHUAIBI: I don't want to say it's urgent.
20 I don't think it's urgent that we need to be in front
21 of the Committee today or tomorrow. I think it's on
22 a good -- I think it's on a good path, and we'll deal
23 with it in a good --

24 MEMBER BANERJEE: Does that increase
25 vulnerability right now?

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 MEMBER BROWN: Yes. No, I'm not going to let
2 him answer that. I knew what Mo was going to say. No,
3 I'm just teasing.

4 The plants are out there. Oconee and Diablo
5 Canyon have been done, and they did not address this
6 issue up front during the architecture development for
7 those systems. So what -- you know, when I first looked
8 at the -- had one look at the Oconee one and -- after
9 I had been here for about three months or something like
10 that, they -- the vulnerability was there. They were
11 connecting to the outside world via little block boxes
12 with software in them and into the plant.

13 So what's the level of detail? I don't know.
14 Because it was just a box; that was it.

15 MR. SHUAIBI: And that's part of the big
16 dialogue within the staff is level of detail available
17 at different stages of time, and for different --

18 MEMBER BROWN: Well, I just wanted to give
19 you a heads up that we're going to -- you know, this
20 subject is not dead once we finish that, go to the next
21 part that's in the queue to try to get, you know, a good
22 framework established as to how we -- how the staff,
23 how the Commission and everybody else handles this on
24 the long haul.

25 MR. SHUAIBI: I came in here optimistic that

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 I could talk you out of that, but I understand.
2 Actually, I knew that. I knew that we would continue
3 this dialogue. I was just being facetious.

4 MR. WESTREICH: With regard to your comments
5 about the current -- we are going to talk about the
6 inspection program and implementation of the cyber
7 security. So that does address some of these
8 vulnerabilities on the back end. I know your issue was
9 on the front end, but we have done quite a bit already
10 to kind of address some of these issues. So we'll talk
11 about that.

12 MEMBER BROWN: No. That's why we wanted to
13 have this briefing, so the full Committee would have
14 an idea of what's going on from that regard, because
15 I have a few more questions that I didn't ask in the
16 Subcommittee meeting that -- because it just didn't dawn
17 on me. Now they have dawned on me.

18 MR. WESTREICH: Okay.

19 MEMBER BROWN: Based on your all's marvelous
20 presentation.

21 MEMBER SKILLMAN: I'd like to ask a question.
22 If in the course of the next 12 months there were to
23 be a cyber attack that allowed an outside party to get
24 control of Diablo or Oconee, what action would the agency
25 take?

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 MR. WESTREICH: Well, that's difficult to
2 answer if we don't know the specifics. You know, at
3 this point --

4 MEMBER SKILLMAN: Wait, wait, wait, wait.

5 MR. WESTREICH: -- we've taken a number of
6 actions already to isolate --

7 MEMBER SKILLMAN: And any of the plants, if
8 something goes wrong, you've got an AIT, you've got a
9 shutdown, you've got bells, lights, and whistles, you've
10 got admin, you've got all kinds of stuff coming out of
11 the sky.

12 So for a non-cyber attack, a lot of us around
13 this table have lived that life, when something really
14 goes wrong. I would say this is something that went
15 wrong. What would the agency do?

16 MR. WESTREICH: Well, we would use our same
17 process as we use now. We'd have -- we activate our
18 response mode. We do onsite activities. We have teams
19 that would go out to try to understand the issue. We'd
20 be communicating with the licensee. So we'd be in
21 incident response mode, just like we would for any other
22 event.

23 So, and we're hopeful. I think what we've
24 done in the operational programs to mitigate a lot of
25 these issues is to really address the vectors that could

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 cause that to occur. So I think we've done the major
2 things already to mitigate something like that from
3 occurring. And we're continuing to implement that
4 program, and we'll be doing that over the next several
5 years.

6 MEMBER SKILLMAN: Doesn't that kind of move
7 into the sense of urgency that Dr. Banerjee asked about?

8 MR. WESTREICH: Well, I mean, that's why we're
9 moving out pretty quickly. We had -- the rule went into
10 place, and we've had them implement these first seven
11 milestones that we'll talk about to address the major
12 vectors. That's already in place. So we've done that
13 already. I think that gives us some confidence that
14 we have a little time to address some of these other
15 issues.

16 MEMBER SKILLMAN: Okay. Thank you.

17 MEMBER BROWN: Yeah. I think it would be
18 useful to let them go through and then take -- see how
19 they address your question because I've got a couple
20 of amplifying thoughts that we didn't address as how
21 they do that. And they've done a bunch of stuff, but
22 you've got to know what that is to see what -- to kind
23 of address your thought process.

24 MEMBER SKILLMAN: Thank you.

25 MR. WESTREICH: Yeah I think once we go

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 through what we've done, you can --

2 MEMBER SKILLMAN: Okay. Thanks.

3 MR. WESTREICH: -- give us more.

4 MR. SHUAIBI: Are there any other questions
5 for me?

6 MEMBER BROWN: I'm finished. I appreciate
7 your update, and looking forward to trying to get this
8 general concurrence within the management and of the
9 staff, so that we can get on with the rulemaking revision
10 and then fight it out, letter, you know, dueling swords
11 or whatever we want to call it, but our letters and then
12 the EDO responses to see how that plays.

13 MR. SHUAIBI: I'm looking forward to the
14 dialogue. I think it will be a good dialogue.

15 MEMBER BROWN: Oh, yeah.

16 MR. SHUAIBI: I agree. So if there are no
17 other questions, then I'll leave and --

18 MEMBER BROWN: Thank you, Mo. Appreciate it.

19 MR. SHUAIBI: Thank you.

20 MR. WESTREICH: So, as I said, I'm Barry
21 Westreich. I'm Director of the Cyber Security
22 Directorate, which is part of our Office of Nuclear
23 Security and Incident Response. That's a new
24 organization. I'll talk about that change in a minute.

25 But here is our agenda. It's a pretty full

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 agenda. We appreciate the opportunity to come speak
2 before the Committee and discuss cyber security issues.

3 It's a current issue. There's a lot of changes taking
4 place. So this is a fairly dynamic area. We have in
5 the audience staff from a number of the other offices,
6 if questions come up related to their activities.

7 Next?

8 So the purpose is to provide you an overview
9 of our cyber security program and how it is being
10 implemented. We have a number of activities across the
11 licensee types that we want to update you on. We talked
12 to a subcommittee about that on a few occasions.

13 And so we want to continue to improve
14 communication and coordination on cyber security and
15 also identify areas of future interest, so we understand
16 what your topics that you want to discuss in the future
17 are.

18 MEMBER BROWN: I presume what you mean by
19 communication is to ensure that we have suitable meetings
20 to let us know you've hit different stages of your --

21 MR. WESTREICH: That's great.

22 MEMBER BROWN: -- development of your program
23 to make sure we're on board or understand --

24 MR. WESTREICH: Understand.

25 MEMBER BROWN: -- what you're doing to see

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 if we then want to make any suggestions.

2 MR. WESTREICH: That's correct. Yes.

3 MEMBER BROWN: Okay. Thank you.

4 MR. WESTREICH: So our new Cyber Security
5 Directorate -- so that's kind of hard to see, but that's
6 the organization chair for our Office of Nuclear Security
7 Incident Response. And prior to our reorganization --
8 I'll just -- we had three divisions -- Division of
9 Security Operations, Policy, and Incident Response.
10 And the organizations had -- two of the organizations
11 -- the Division of Security Policy and Operations both
12 had cyber security activities, both on the policy side
13 and the oversight side.

14 And in order to gain some control of the area,
15 have a focused effort, and more of an effective
16 governance structure, we decided to merge the two
17 division staff that were working on cyber security
18 activities.

19 So we created this new Cyber Security
20 Directorate, and if you look it's kind of in the upper
21 left. Hard to see. Cyber Security Directorate now
22 reports directly to the front office. I'm the Director
23 of the Directorate, and Russ Felts, to my right, is the
24 Deputy Director. And all the staff that were involved
25 in cyber security activities previously are now combined

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 into this one directorate.

2 So we've been in place since June, a little
3 bit of coordination and understanding how to merge those
4 two activities to move forward. So the focus areas
5 continue to be the areas that we were working on before.

6 Yes?

7 MEMBER BROWN: We have a question. Somehow
8 -- I don't know.

9 MR. WESTREICH: That's the closed session.

10 MEMBER BROWN: Do I have an open session?
11 Maybe I'll go -- oh, no, I guess -- sorry, didn't realize
12 I had --

13 MEMBER STETKAR: The answer to your question
14 is, Charlie, it's Friday.

15 MEMBER BROWN: I'm awake.

16 MEMBER BLEY: It's good you're finally
17 looking at the slides.

18 (Laughter.)

19 MEMBER BROWN: A positive step here. I
20 didn't get my donut in yet. That's a big problem. Thank
21 you very much for putting up with me.

22 Barry?

23 MR. WESTREICH: Can we go back one real quick?

24 MEMBER BANERJEE: Wow, that's hard to read.

25 CHAIRMAN ARMIJO: That's busy.

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 MR. WESTREICH: So the new organization, our
2 primary mission is to be the point of contact for all
3 cyber security activities involving our licensees. So
4 we don't do internal NRC cyber security, but all the
5 activities related to our licensees. And we're the
6 single point of contact for all those communications,
7 both internally and externally, industry and other
8 federal agencies, the White House, and all the various
9 stakeholders involved in cyber security.

10 MEMBER BROWN: Question on this. Which is
11 the -- from the standpoint of looking and doing all of
12 your inspections and audits, is that the left-hand column
13 over there? I see it's New Reactor Licensing Branch,
14 inspection and regulatory. Is that where --

15 MR. WESTREICH: Well, the Cyber Security
16 Directorate --

17 MEMBER BROWN: Is that the top one?

18 MR. WESTREICH: It's the dangling box, yes.

19 MEMBER BROWN: Dangling box.

20 MR. WESTREICH: We have all cyber
21 security-related activities, which includes inspection
22 oversight for cyber security.

23 MEMBER BROWN: But you don't have anybody
24 working for you, so that's just --

25 MR. WESTREICH: No, we do. We have all 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

1 this -- we have the staff that has been working on it
2 before, so the staff that was working on it from our
3 Division of Security Operations, where I was the former
4 deputy --

5 MEMBER BROWN: Okay.

6 MR. WESTREICH: -- those staff have moved over
7 to this directorate. The people doing the inspections
8 --

9 MEMBER BROWN: Okay. That was the question
10 that we had as to what is their handoff from the old
11 to the new, and that should be -- the answer is the folks
12 we used to deal with or would see, we are going to keep
13 seeing them.

14 MR. WESTREICH: Right. You're just going to
15 keep seeing, because we're all in one organization.
16 So we had some management -- a little bit of management
17 organization changes to facilitate this move, but at
18 this point we're up and running and we're continuing
19 on with the same activities that we were doing before.

20 MEMBER BROWN: Okay. Thank you.

21 MR. WESTREICH: It is considered a temporary
22 organization, because once we get to a stable program
23 across the licensee types, we will consider merging it
24 back into the line organization in NSIR. So we're
25 talking like a 2019 date that we will -- if we're there

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 and we're stable at that point, we'll merge back into
2 the organization -- previous organizational structure.

3 MEMBER BROWN: your box would drop down into
4 the same line with all of the other three, as opposed
5 to --

6 MR. WESTREICH: It would disappear and get
7 merged back into those other activities.

8 MEMBER BROWN: So the initial effort here was
9 to have a more focused group to get everything started
10 and stabilized and running smoothly, and then move it
11 into a line --

12 MR. WESTREICH: That's correct.

13 MEMBER BROWN: -- organization.

14 MR. WESTREICH: That's correct.

15 MEMBER POWERS: Are you saying that you think
16 that by 2019 all of those plants that are going to switch
17 to digital systems will switch. Is that what you're
18 saying?

19 MR. WESTREICH: No. What we're saying is
20 that the programs will be developed and stable. So
21 currently in power reactors we have an ongoing effort
22 to implement their plans that we have approved. So they
23 have implemented Milestones 1 through 7.

24 MEMBER POWERS: But when you say "stable,"
25 the technology for threatening the security of digital

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 systems won't be static.

2 MR. WESTREICH: No, that's true. It's not
3 so much --

4 MEMBER POWERS: I'm trying to understand what
5 "stability" means.

6 MR. WESTREICH: Stability from a program,
7 from an NRC regulatory program standpoint. So we will
8 have all of the plants -- power reactor plants will have
9 their cyber security plans fully implemented at that
10 point. So they will be operating under an approved plan
11 that we have inspected and we know how they do upgrades,
12 how they do maintenance activities, all of the stuff
13 that we would be concerned about, if they are going to,
14 you know, make a change.

15 Same with fuel cycle facilities. At that
16 point, we should have -- whatever path we take to get
17 cyber security rules in place and implemented should
18 be well on their way by that time. And so we'll have
19 to reassess in 2019 to see if we're there.

20 MEMBER POWERS: I mean, it's --

21 MR. WESTREICH: Okay? So our activities
22 include rulemaking. One of the things we're working
23 on is the cyber reporting rule. Guidance development,
24 we're still looking at some additional guidance,
25 regulatory guidance, and other inspector guidance. 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

1 have licensing activities for new reactors and updates
2 and changes to the cyber security plans that are already
3 approved and in place.

4 Continuation of policy issues, which is our
5 road map activities, we are now looking at fuel cycle
6 facilities and we will look at RTRs, ISFSIs, and
7 materials licensees, so that's the policy work that we
8 are still doing. And as we've talked about, we're
9 continuing to provide oversight for implementation of
10 the current rule and implementation activities for power
11 reactors. And we'll talk about all of those things in
12 the presentations in this session.

13 MEMBER BLEY: Barry, I know our role and it's
14 not to really tell you how to manage, but I just want
15 to make an observation. On the reactor side, in terms
16 of considering the impact of events that occur in the
17 plants, real-world events, we let that kind of percolate
18 through lots of places in the organization. And we built
19 this thing called AEOD some years ago to really start
20 focusing on operating experience, and then said, "Well,
21 we got that working," put it back generally, and now
22 we've got a new program to focus on.

23 It just strikes me cyber security is always
24 going to be a bit like that because the threats are
25 changing, the technology is changing, and some central

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 place to be on top of that may be something you are always
2 going to need.

3 MR. WESTREICH: Well, we will always need
4 that. I mean, we have a cyber assessment team. They
5 are integrated with our ILTAB threat folks, looking at
6 the threat.

7 MEMBER BLEY: Okay.

8 MR. WESTREICH: And we're also taking that
9 CAT activities, cyber assessment team activities, and
10 looking from an op e perspective. How is that getting
11 transmitted to the licensee community? What does that
12 mean? What are we seeing? Kind of in a broad
13 perspective.

14 So you're right, we are looking at that.
15 That's part of -- I think, Ralph, are you going to talk
16 about --

17 MEMBER BLEY: And that is linked with the op
18 e stuff.

19 MR. WESTREICH: So we'll talk about that in
20 a little more detail about the cyber assessment team.
21 But that's something we'll probably have in place
22 whether this directorate is in place or not.

23 MEMBER BLEY: Thanks.

24 MR. WESTREICH: So any other --

25 MEMBER BROWN: Yeah. Just one,

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 springboarding off Dennis'. I mean, the real point is,
2 you know, this is an area where obviously the technology
3 and the capability and what is going to be used. Things
4 are going to be constantly changing. I mean, you can't
5 breathe, go to bed one night, and all of a sudden, you
6 know, the iPhone you bought last night is no longer any
7 good and you have to have the latest whatever --

8 MEMBER POWERS: Come on, Charlie.

9 MEMBER BROWN: -- and it not only will
10 communicate with the internet, but it will also
11 communicate with satellites and the NSA, you know,
12 database and everything else, and it's just fancy, fancy,
13 fancy.

14 So, and that's -- if you want to know why I've
15 been so hard over on the control of access points issue
16 is that there is a way to avoid difficulties if you get
17 ahead of the game, where you minimize the manpower,
18 resources, and dollars, not only from the licensee
19 standpoint but from your all's standpoint of ensuring
20 that threats are not a real threat to the operation and
21 safety performance of the plant.

22 And that's why you find me kind of pushing
23 back all the time on these alternative proposals by
24 vendors that want to implement the guidelines that you've
25 put out and the way you may end up putting them out.

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 So I just want to have you keep that in mind,
2 that the cyber security role from a plant safety
3 standpoint -- I'm putting the business, you know,
4 corporate headquarters building off on this side where
5 they can do their IT thing and upgrade every software
6 thing, and they can -- if they lose their files, that's
7 their problem. I'm concerned about the plant, control
8 of the plant, the operators, and people's access to go
9 in and fudge around with what is coming in and out.

10 So that's why I kind of really get wrapped
11 around the axle on this stuff. They just -- they give
12 you a little heads up in terms of the thought process,
13 and why I continue to hammer on it, that's to simplify
14 the thing, particularly with technology changing the
15 ability to do things.

16 I mean, I can just see one of these design
17 agents or vendors or licensees proposing some wireless
18 communication thing, which is -- it's not prohibited.

19 There is not a specific statement there. So then you
20 have to have a guy justify it, and you fight your way,
21 you know, for months and months and months going back
22 and forth, and finally you give in and say, "Well, we
23 really can't tell him what to do. It's up to him to
24 make sure his stuff is safe."

25 Well, that's -- at some point, the regulator

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 has to kind of be the adult in the room and make sure
2 that they don't put themselves at risk. So I'm not
3 trying to tell you, again, how to do it. Yes, I am.

4 (Laughter.)

5 MEMBER CORRADINI: Yes, you are.

6 MEMBER BROWN: Just to have the thought
7 process to know where -- you know, why I consider the
8 control of access. And it's not just internet to the
9 network, but it's also control of access all the way
10 down the food chain and how you identify it.

11 So, anyway, you can go --

12 MR. WESTREICH: Of course, we agree that those
13 are important considerations. I mean, I think we all
14 agree with the wireless example. You know, the cyber
15 security plant controls are going to have to deal with
16 that. If they were to put something wireless, then we'd
17 have to have some pretty significant controls thought
18 about.

19 MEMBER BROWN: That's an understatement.

20 MR. WESTREICH: So, I mean, I don't disagree
21 --

22 MEMBER BROWN: Okay.

23 MR. WESTREICH: -- that this is an important
24 area.

25 MEMBER BROWN: All right.

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 MR. WESTREICH: Maybe how we get there is
2 where we have some discussion.

3 MEMBER BROWN: Yes. Thank you.

4 MR. WESTREICH: Okay. Russ, do you want to
5 go ahead?

6 MR. FELTS: Certainly. Okay. So I'm Russ
7 Felts, Barry's deputy. I just want to take a couple
8 of minutes to sort of set the stage for further
9 presentations by talking a little bit about the
10 regulatory framework. In order for me to get into sort
11 of a historical perspective on the NRC's involvement
12 in cyber security regulation and specifically what we've
13 done to this point, I want to talk briefly about the
14 threat.

15 So on this slide you see that we recognize
16 that there are a number of different avenues through
17 which an adversary could attempt and potentially succeed
18 in conducting a cyber attack. And we recognize -- and
19 it's in regulation in 73.1 -- that we have a
20 knowledgeable, dedicated, intelligent adversary, and
21 implied there really is the fact that the adversary is
22 looking for vulnerabilities and is smart enough to
23 attempt to figure out ways to exploit those
24 vulnerabilities. Right?

25 So our programs are intended to put licensees

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 in a condition where these vulnerabilities are
2 mitigated. And because of the fact that we recognize
3 that these vectors can't be completely eliminated, we
4 took a performance-based approach in terms of how the
5 regulation was set up.

6 Next slide, please.

7 From a historical perspective, NRC has been
8 involved for over a decade now in the cyber security
9 area. I want to call your attention to a couple of things
10 specifically on this slide, the fact that in 2009 is
11 when the cyber security rule at 73.54 became effective.

12 It was issued in 2009.

13 Licensee's cyber security plans for power
14 reactors were put in place, approved in the 2011
15 timeframe, and we are currently inspecting the interim
16 implementation. All right? So we've got a number of
17 milestones, which I'll talk more in depth about here
18 in a second.

19 We are out currently inspecting those programs
20 as we speak.

21 MEMBER BROWN: You recognize that there was
22 significant disagreement on Rev 3 at 1.152 relative to
23 the statement that says the design folks are not going
24 to look at anything. They are actually almost virtually
25 prohibited from looking at anything other than how 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

1 system implements its safety function, and that's it.

2 In other words, don't bother us; we'll do it later.

3 So we lost that battle, but it's not over.

4 MR. FELTS: We understand that was a change.

5 MEMBER BROWN: Yeah. It was a change because
6 it was different in Rev 2.

7 CHAIRMAN ARMIJO: Could you go back to Slide
8 8? In your threat vectors, where are the insider threat?
9 Is it just under vendors and vendors to vendors?

10 MR. FELTS: No. Actually --

11 CHAIRMAN ARMIJO: It seems to me that is the
12 most challenging problem.

13 MR. FELTS: I think --

14 CHAIRMAN ARMIJO: You know, your own
15 employees, for reasons of their own, decide to create
16 problems --

17 MR. FELTS: Sure.

18 CHAIRMAN ARMIJO: -- and have routine access,
19 and it seems to me that is one of the most difficult
20 problems to deal with. Do you -- if you could just tell
21 us a little bit about your thinking.

22 MR. FELTS: Right. I think that, if you look
23 at the list of threat vectors there, the only place where
24 you are really -- we are saying that someone would not
25 need either inside access or figure out a pathway to

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 exploit inside access, like giving something to someone
2 either knowingly or unknowingly to put that malicious
3 code in the system --

4 CHAIRMAN ARMIJO: Eventually, you're going
5 to need some sort of a device, right?

6 MR. FELTS: -- is really the internet, right?

7 Obviously. So an outsider could potentially exploit
8 a vulnerability that existed that had a face on the
9 internet, and the supply chain, as you pointed out.
10 All of the others, clearly there is a potential for an
11 insider to exploit any of these vulnerabilities.

12 So it certainly is an aspect of the design
13 basis threat, the insider, and we recognize that.

14 MEMBER BROWN: Sam, just a simple example.
15 Somebody could go down and say they are authorized to
16 take a laptop down. But that laptop has a USB port on
17 it, and they have to have a thumb drive where they alter
18 somehow -- don't ask me how because I'm not an expert.

19 Plug that in, and now when they update the software
20 it introduces some wrinkle in the software how it
21 executes the software, and now all of a sudden you've
22 got a problem.

23 And if you -- you've got to control that.
24 So thumb drives, any access to that laptop and how that
25 software is input to it, even down to the cabinet level,

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 how do you modify it? Do you change out proms, or do
2 you do a software upgrade via a laptop or a USB drive
3 or via a network connection into it? All of those are
4 vulnerability and access points.

5 MR. FELTS: Well, like -- you know, as in the
6 physical security realm, there are programs in place
7 to address the insider threat, which applied both in
8 physical security considerations and in terms of cyber
9 security. So, you know, there is an insider mitigation
10 program the licensee is required to have in place and
11 it's inspected.

12 CHAIRMAN ARMIJO: I guess that's the best you
13 can do, because it's really people. And you can't get
14 into their minds and --

15 MR. WESTREICH: This idea is included in our
16 interim actions, actions that have been implemented now.
17 This insider mitigation program is something they need
18 to maintain and enhance actually.

19 CHAIRMAN ARMIJO: Right.

20 MR. FELTS: Let's move on to the next slide.

21 I wanted to talk just a bit about the
22 regulation at 73.54. It currently applies to power
23 reactors, both new and operating. And I mentioned it's
24 performance-based. It's a high level regulation. It's
25 only about a page and a half. But it has -- the basic

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 requirements there are for the licensee to, you know,
2 establish and implement the cyber security plan, which
3 for all the power reactors that are operating is in place.

4 They have to protect those critical digital
5 assets, and we'll talk a little bit more about what those
6 are. And the things that are covered, the things that
7 -- the aspects that define what is a critical digital
8 asset are the fact that we require cyber security
9 protections for things that could impact safety,
10 important to safety, security, and emergency
11 preparedness functions, or systems that could impact
12 those functions.

13 So it doesn't have to be something that
14 directly performs a safety, security, or an emergency
15 preparedness function. It could be something that is
16 required to operate effectively or to function in order
17 to support the system that performs the function.

18 They have to have a defense-in-depth
19 protective strategy, which includes a defensive
20 architecture. So there's a requirement for the licensee
21 -- in guidance it discusses -- and the licensees that
22 have not committed to this in their plans, to have this
23 defense-in-depth approach through the architecture that
24 essentially isolates the most critical systems from the
25 internet with various layers of protection. And then,

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 of course it addresses technical, operational, and
2 management controls.

3 So, again, this is Reg Guide 5.71, and we
4 talked about the fact that there are interim milestones.

5 And these are some of those that you see laid out on
6 the slide here. The formation of a cyber security team
7 to actually go and identify critical digital assets,
8 and then to apply that defensive architecture, which
9 has these five levels that you see there starting at
10 Level 0, which is the internet.

11 You see that you can have two-way
12 communication between Level 0 and Level 1, Level 1 and
13 Level 2. But beyond Level 2 you are not allowed to have
14 two-way communication. You either have to have those
15 systems air-gapped or you have to have a data diode in
16 place to ensure that you don't have things that
17 potentially originate on the internet finding their way
18 into the most important systems, the highest levels of
19 protection.

20 And then the licensee needs to address -- is
21 required to address security controls for the CDAs.

22 MEMBER POWERS: Can I ask you about the first
23 step? Form cyber security team. This is an obligation
24 of the licensee to do this?

25 MR. FELTS: Correct.

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 MEMBER POWERS: So who is on that team?

2 MR. FELTS: It's a multidisciplinary team,
3 so it would include engineers, IT staff. It needs to
4 be multidisciplinary to make sure that all of the
5 appropriate perspectives are considered.

6 We don't want these teams to just be composed
7 of folks that are knowledgeable about IT systems but
8 don't necessarily understand the impacts of, say, a loss
9 of function of a CDA they are looking at. We need people
10 that have that cross-disciplinary perspective to make
11 sure that the appropriate things are being protected
12 at the appropriate level.

13 MEMBER POWERS: I'm just thinking of one or
14 two plants that I am reasonably familiar with. And I
15 can certainly find people that can outline for you in
16 some detail what the loss of a function is. There
17 probably are few on that plant staff right now that are
18 familiar with the kinds of threats that the high end
19 of your threat vector -- I mean, what are you saying?

20 I have to have somebody on my team that knows those
21 kinds of things?

22 MR. FELTS: No. I don't think the team
23 specifically has to include folks that are experts in
24 the threat, but they do need to understand those vectors
25 so that they can essentially plug the gaps and ensure

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 that vulnerabilities are addressed.

2 So, for example --

3 MEMBER POWERS: Does your guidance give them
4 enough to do that?

5 MR. FELTS: I think from what we've seen,
6 we've seen -- at least so far in our inspection program
7 we've seen fairly -- we've seen implementation that
8 indicates that, obviously, there is a range of
9 capabilities we've seen across the spectrum of plants
10 that we've inspected.

11 So I don't know if I can specifically address
12 whether or not the guidance is adequate in terms of
13 telling them who needs to be on the team. I think it
14 does fairly clearly lay out who they need to have
15 involved.

16 MEMBER POWERS: My concern is that the threat
17 vector evolves very fast, and once you get up to the
18 high end of that vector, it's very sophisticated stuff.

19 And I don't see how anybody on the -- I don't see how
20 a licensee can keep up with that, because he's got another
21 line of business that he is pursuing and that's a chore.

22 And, I mean, if your guidance provides him
23 enough --

24 MR. WESTREICH: I think the guidance provides
25 the type of people they need to have on their team.

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 So like Russ said, it's multidisciplinary, includes IT
2 people, it includes a plant --

3 MEMBER POWERS: Those IT people, you know,
4 I mean, how many IT people are there on a plant site?

5 MR. WESTREICH: Well, we're talking about
6 typically corporate IT who are dealing with protecting
7 their corporate structure from the threat as well. So
8 most of the guys we see are fairly aware of where we
9 are in the threat landscape.

10 Ralph, you had something to add?

11 MR. COSTELLO: Professor Powers?

12 MEMBER POWERS: Yes.

13 MR. COSTELLO: I'd like to answer your
14 question, if I may. This team is multidisciplined, and
15 we have it specified in intimate detail who has to be
16 on, how many people, but it had to be multi-faceted,
17 in accordance with subparagraph 3.1.2 of the 0809, which
18 is in fact our license condition cyber security plan.

19 And what we found with the first 14
20 inspections is some sites had a very good mix, a very
21 good team. They had to do very little to change it,
22 improve it. But this is not a stagnant team you just
23 make up one day and it stays that way for 50 years.
24 They are going to adapt, change, improve the team makeup,
25 so they get better and can be better.

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 For instance, we found that at some sites they
2 didn't include physical security as much as they probably
3 should have. And they realized that after we left the
4 last day of the inspection, and so they include some
5 more people that have more physical security experience,
6 et cetera, et cetera, et cetera.

7 So that's how this team composition seems to
8 be working. The good news is it seems to be improving
9 continuously. That's what we're seeing in real-time
10 inspection space.

11 MEMBER POWERS: It's slopes that I'm worried
12 about. And, you know, if we demand too much, you know,
13 I cannot -- I worry about asking the sites or even the
14 corporate IT organization to have the same level of
15 knowledge on cyber security that people on your staff
16 have, because I just don't think it's possible. I mean,
17 they just can't -- they have other missions.

18 MR. WESTREICH: And, frankly, they're not
19 privy to some of the information because it's classified.

20 So it's our job to provide that information to them,
21 which is part of what the cyber assessment team does.

22 And these inspection activities are -- you know, it's
23 the first time through. There's a little bit of a
24 learning that is going on where they understand what
25 the expectation is.

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 So I think, as Ralph said, as we move forward,
2 the teams are getting more robust. We have an obligation
3 to provide them that threat information if it's -- if
4 we think it's affecting them.

5 CHAIRMAN ARMIJO: There are cyber security
6 consultants and organizations that provide support or
7 reviews. What is the -- your view of their role in either
8 advising or participating in some way in these cyber
9 security teams?

10 MR. FELTS: Well, I think we've seen certainly
11 licensees using consultants to assist them, if they may
12 not have the expertise necessary to do an effective job
13 resident in their organization. And we have definitely
14 seen a mix -- at a particular site we've seen a mix --
15 at each site we've seen a mix of staff that work at that
16 site and corporate support people, and in many cases
17 contract support to bring the right expertise to the
18 cyber security team to put the adequate protections in
19 place.

20 But I really think that the point is they are
21 not necessarily focused so much on the threat as they
22 are in plugging the vulnerabilities, understanding what
23 is -- what infrastructure is at the plant and how an
24 adversary might exploit that and making sure that those
25 pathways are addressed.

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 MEMBER RAY: But do you envision at some point
2 having a designated particular point of contact between
3 the agency and the licensees on this topic?

4 MR. WESTREICH: Well, I think that's -- do
5 you mean in terms of a specific individual or --

6 MEMBER RAY: Well, or a position, a position
7 to which the licensee would designate people, rather
8 than, you know, just, well, somebody from corporate will
9 respond to this particular communication that we're
10 having. I mean, there are positions in the operation
11 of the plant that traditionally have been established,
12 and people hold those positions. I'm just wondering
13 if in this area there ought to be something similar.

14 MR. WESTREICH: Well, I think we've seen that
15 licensees are coming around to the notion that this --
16 and, clearly, I understand --

17 MEMBER RAY: I'm asking, do you think as an
18 agency, not that we just observe that they're doing it,
19 but that should become part of the requirement that,
20 okay, we want a designated point of contact for this
21 subject.

22 MR. WESTREICH: I don't think that's
23 something we've thought about.

24 MEMBER RAY: Okay. Well, I'll just give it
25 to you to think about.

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 MR. WESTREICH: Yeah. I think --

2 MEMBER RAY: I mean, you have lots of other
3 things if that's the case. It seems like, following
4 up on the comment the Chairman was making, that it would
5 be maybe worthwhile if we said, "Okay. It's time that
6 everybody have somebody who is designated." It may not
7 be their only job, but --

8 MR. WESTREICH: We currently do have
9 designated points, but there are people that are
10 designated as the lead procurement activity. And that's
11 primarily because they're trying to implement this
12 thing, and they're going to go out through 2015, '16,
13 '17, so there is a designated point of contact. We have
14 a lot of communication with them. Downstream I'm not
15 sure if that's something we need to think about.

16 MR. FELTS: Aside from the cyber security
17 team, there is no prescribed requirement for a particular
18 point of contact. But I think we've seen licensees
19 recognize the importance of cyber security, and those
20 that have multiple facilities certainly have sort of
21 a core group of experts that are implementing --

22 MEMBER RAY: Yeah. But it's natural, it's
23 an observation that you've made. But, you know, there
24 is always the outlier, somebody who is -- maybe the job
25 has been vacant for a while, and that's not good.

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 MEMBER SKILLMAN: Let me ask you to go back
2 to 10, please, on the requirements. Is there a
3 requirement to identify that the security system has
4 been pinged, that there has been an attempt to gain access
5 and to mine that information for usefulness?

6 MR. FELTS: Well, there is a requirement in
7 the cyber security plan, not the regulation but the cyber
8 security plan, for detection and response capability.

9 And, as Barry mentioned earlier, we are working on a
10 reporting requirement right now, a rulemaking for
11 reporting requirements for cyber security that would
12 -- you know, depending on how that works through the
13 rulemaking process would require licensees to report
14 to us that they have experienced a cyber attack.

15 So I'm not sure which part of that addresses
16 specifically your question. I presume you're asking
17 about detection and response capability or detection
18 and --

19 MEMBER SKILLMAN: What I'm really thinking
20 about is how the fleets have generally implemented some
21 form a near miss process, where -- whether it was an
22 injury or avoidance of a trip, or a near miss on a cycle
23 or a process failure that could have resulted in some
24 significant event, and it did not occur, the employees
25 are on their honor to say, "Hey, this is what I did.

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 This is what happened. This was truly a near miss
2 event."

3 And I'm thinking of a cyber attack being a
4 near miss event when your protection systems have
5 repelled incoming, but the need to disseminate that
6 information for learning, which is why the near miss
7 process is so effective out in the fleets. People say,
8 "Hey, you know, this could have happened. It didn't
9 happen. This is why it didn't happen." Maybe we'd
10 better make a stronger letter, a better gate, more
11 protection on the switchgear, or something such as that.

12 I'm thinking of a true threat that was
13 repelled. Is there a requirement to report it and to
14 mine the information, so that the next time it happens
15 it is more robustly reported.

16 MR. FELTS: Right. I think that's really the
17 focus of the rulemaking effort we have ongoing for a
18 cyber reporting requirement.

19 MEMBER SKILLMAN: Okay. Thank you.

20 MEMBER BROWN: I want to make one observation
21 relative to Dana's lead-in. If you go back to Slide
22 -- the threat one, the landscape -- 8. One way of looking
23 at this -- and this springs from all of your all's
24 questions -- is if you look at that list -- and whether
25 I'm right or wrong, it's kind of the way I've categorized.

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 There's active dynamic threats, which are real-time.
2 They are happening bang, bang, bang, but you've got
3 to fight them off.

4 And then there is what I call the slower moving
5 threat, such as somebody -- a person taking a USB drive
6 or a laptop, test equipment, whatever it happens to be,
7 into the plant and doing something. I mean, so there
8 is active dynamic in the threats, and then there is the
9 more administratively controllable type threats that
10 are not real-time where you are trying to fight off the
11 latest worm, malware, or whatever the fancy new
12 terminology that the world comes up with for these
13 threats.

14 And that all goes back to literally the
15 defensive architecture from the dynamic. If they have
16 to fight these dynamic threats every day, hour in and
17 hour out, they're going to lose. They will not have
18 the staff at the plant. They will not have the resources
19 at the plants. Even the corporate umbrella will not
20 have the ability to protect those plants from that.
21 The financial community has proved that.

22 I just got a letter the other day from DOE.
23 All of my data was compromised. My entire -- all of
24 my PII was compromised. It's out there, they gave away
25 Social Security numbers, addresses, phone numbers, work.

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 Everything I've ever done has been thrown out in the
2 wide world. I don't know what the hell I'm going to
3 do with that, but DOE lost it. So I'm really happy.

4 So that was a dynamic threat, came in and took
5 the stuff out of their databases. So the key is the
6 architecture that just literally puts a wall that can't
7 be penetrated from the dynamic threat, so that they can
8 concentrate on those that can be handled internally.
9 So internet, intranet, wireless, Bluetooth, all that
10 stuff, dynamic threats.

11 Look at the rest of those. You can deal with
12 those on an administrative basis. Doesn't mean they're
13 not important or critical or complex, but you can deal
14 with vendors, vendor to vendors, laptops. All those
15 are just -- I mean, you can, you know, go to bed one
16 night, I've got a procedure, I can do that. You can
17 check a guy. You can check the thumb drive. You can
18 do all kinds of things before he goes down there. And
19 you can know what your threats are that you'd have to
20 -- and you're going to probably miss some at some point.

21 But that's a different -- it's not as dynamic as these
22 other ones.

23 So if you listen to me beat the dead horse,
24 that defensive architecture is extremely critical, and
25 you've got to have it mapped in the plants. You've got

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 to know where those touch points are that give you the
2 vulnerabilities to dynamic threats.

3 Sorry, just had to -- based on the discussion,
4 I thought I'd throw in that thought process.

5 MEMBER SCHULTZ: I think it's important,
6 because everything we've heard since the opening
7 discussion has reinforced your comments and the
8 discussion and the need to create and isolate the
9 environment in which the threat can occur.

10 MEMBER BROWN: And you can't -- they can't
11 put people on --

12 MEMBER SCHULTZ: Programmatically, it's
13 going to be difficult to control.

14 MEMBER BROWN: -- these teams that are going
15 to be able to do all of this. Okay. I'm --

16 MR. WESTREICH: That's a good segue to the
17 next slide.

18 MR. FELTS: All right. Let's talk a little
19 about implementation. Okay? All licensees were
20 required to implement the first seven milestones by
21 December 31st of last year, and that's what we're out
22 currently inspecting now.

23 So those Milestones 1 through 7 address the
24 key threat vectors, including controls for portable
25 media. But they are focused on target set equipment,

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 so CDAs that are related to target sets are the ones
2 that we were focused on because they are the most
3 significant.

4 Milestone 8 --

5 MR. WESTREICH: One of the key threat vectors
6 is this architecture issue. So Milestone 3 is
7 installing data diodes or some other deterministic
8 device that doesn't allow internet access, to address
9 your --

10 MEMBER BROWN: Yes. But 5.71 doesn't --
11 that's guidance.

12 MR. WESTREICH: Well, that's in the cyber
13 security plan, so that's not guidance, that's required.

14 MEMBER BROWN: Yes. I understand that. But
15 you've -- they do have -- they don't have to have --
16 they can come to you with a non-one-way data diode that
17 is software controlled.

18 MR. WESTREICH: They could, but --

19 MEMBER BROWN: They just have to fight off
20 the hordes of --

21 MR. FELTS: They have all committed to the
22 architecture in their cyber security plans, which is
23 now a condition of their license. So certainly when
24 they came to us with their plan for approval, had they
25 requested approval of an alternative, we would have had

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 to consider it.

2 MEMBER BROWN: That's these 14 plants you have
3 gone off and looked at? They've committed to --

4 MR. FELTS: I'm talking about all of them.
5 All the plants require the defensive architecture. No,
6 operating plants.

7 MEMBER BROWN: So they've committed to a
8 hardware-type data diode --

9 MR. FELTS: Right.

10 MEMBER BROWN: -- non-software controlled?

11 MR. FELTS: Correct.

12 MR. COSTELLO: Ralph Costello, Office of
13 Nuclear Security Incident Response. Thank you, Mr.
14 Brown.

15 Your question is a good one, Mr. Brown, in
16 terms of, yes, they could by way of the requirements
17 opt to maybe try something like firewalls. But we all
18 know they are ineffective. We all know they're
19 insecure. Someday they may become secure.

20 And licensees ultimately, going back to the
21 one and a half page rule, which is a gem in and of itself,
22 because it says they have to protect against cyber
23 attacks, so we don't tell them specifically, there's
24 no mention how to do things, but we tell them what the
25 ultimate performance objective is, and there is no way

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 I know of, unless somebody else in the room does, that
2 a firewall is a good way to do it.

3 So the end result, as what Russ has mentioned,
4 is they are using data diodes, hardware-related data
5 diodes, not software, because otherwise when we inspect
6 it, the first question --

7 MEMBER BROWN: I understand.

8 MR. COSTELLO: -- we're going to ask them is,
9 tell me how you're protecting against this event.

10 MEMBER BROWN: Okay.

11 MEMBER BALLINGER: I have a question. Maybe
12 it's in the closed session. But is there the equivalent
13 of -- in the organization of the physical threat teams
14 that go out and try to get access physically to a plant?
15 Are there teams that --

16 MR. FELTS: I think you're asking --

17 MEMBER BALLINGER: -- "cyber terrorist teams"
18 -- in quotes -- that try to get access to the plant,
19 that probe the plant, just like these physical threat
20 teams do?

21 MR. FELTS: I think what you're asking about
22 is force on force.

23 MEMBER BALLINGER: Yeah. That kind of thing.

24 MR. FELTS: No. We're not currently -- we
25 don't have a separate FOF team that is going out 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

1 trying to attempt a cyber intrusion.

2 MEMBER BALLINGER: Because that would be one
3 way to quickly sort out the vulnerabilities that you
4 -- you think you've covered all of your bases, and then
5 all of a sudden one of these teams goes out there and
6 you get a bunch of 25-year old, you know, gamers, and
7 then all of a sudden they're in the plant.

8 MR. WESTREICH: It is an attribute of the DBT.

9 So we could test it, but we likely wouldn't test actual
10 hacking on an operating facility no matter what we do
11 because that's not how we can get --

12 MEMBER BALLINGER: Well, but hacking to a
13 point --

14 MR. WESTREICH: Yeah. We have to simulate
15 it when we -- we just haven't got there yet, to think
16 about how we would do that. That may be something --

17 MEMBER BALLINGER: Because that's one way to
18 solve Dana's issue of this continuing evolution of
19 methods that people have. You know, I come from a
20 university, and, believe me, you do need a couple of
21 23-year olds.

22 MR. WESTREICH: We have some capable people
23 involved in the inspection activity that are looking
24 for things a licensee might have missed.

25 MEMBER BALLINGER: But inspection is a lot

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 different than hacking.

2 MR. WESTREICH: That's true.

3 MR. FELTS: So for Milestone 8, those are
4 site-specific dates. They range from dates in 2014 out
5 to 2017. And for Milestone 8, they're going to have
6 to have full program implementation, which really
7 requires them to have procedures in place, policies and
8 procedures in place, for training, attack mitigation,
9 incident response, continuity of operations, and so
10 forth.

11 And rather than just focus -- being focused
12 on target set CDAs, this is the broad scope where they
13 have to go through and evaluate the necessity and
14 application of additional controls, cyber security
15 controls, on all CDAs across the plant, which is a
16 substantial number.

17 So in terms of life cycle of a plant system,
18 there is nothing in the reg guide that specifically talks
19 about life cycle, but it does touch on all of the various
20 stages from acquisition of technology all the way through
21 its use and retirement, use at the plant and retirement.

22 So there are requirements associated with every one
23 of these stages.

24 And I wanted to touch on one point just to
25 potentially brush up against the topic that we were

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 earlier discussing, and that is for operating reactors
2 it's a phased approach, like we just talked about, the
3 fact that there's Milestones 1 through 7 now, Milestone
4 8, plant-specific dates, but for new reactors the full
5 program implementation all the way through Milestone
6 8, essentially everything, the whole ball of wax, has
7 to be done before fuel is loaded. So they have to have
8 their full program in place before fuel loading.

9 MEMBER BROWN: As part of this initial round
10 of whatever you all did, are you going to talk about
11 it, supply chain aspect of this thing, which is -- you
12 know, that's -- now you're down with the licensee and
13 they're out buying stuff and things like that.

14 Have you all had any interface or interaction
15 on their supply chain? Or is it just a programmatic
16 issue where they're supposed to do that and tell you
17 that they're doing it. And if they tell you they're
18 doing it, and then you say, "Okay, check the box," and
19 that's -- I'm not trying to be critical. I'm just --
20 is that -- how far down do you dig on the supply chain
21 side?

22 MR. WESTREICH: Well, they do have
23 requirements for what they need to procure, some
24 procurement requirements, right? So we look at that
25 aspect of it. We really haven't gone out and looked

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 at the vendor side yet.

2 MEMBER BROWN: My point being is that, you
3 know, how do the vendor -- how does the vendor control
4 the development of his software? And how is it managed,
5 such that -- when it's accessed to who can get to it,
6 and then who goes and looks to see a compromise of the
7 code or whatever it is in terms of the development of
8 the code.

9 MR. WESTREICH: Yeah. We really haven't
10 gotten that far yet. I think that's something we've
11 been talking about with the vendor group here, how do
12 we go do activities to look at the vendors and assess
13 how they're implementing those procurement
14 instructions.

15 MS. SMITH: Hi. My name is Stacy Smith. I
16 work in the Office of New Reactors in the Division of
17 Construction, Inspection, Operational Programs. So in
18 the vendor group there is a couple of things we're doing
19 now.

20 There was a paper a couple of years ago,
21 Counterfeit, Fraudulent, and Suspect Items. As part
22 of that paper, there's a cyber security supply chain
23 working group. So there was five actions that came out
24 of that that we're implementing currently.

25 And we updated our inspection procedures for

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 routine and reactive inspections of vendors, where we
2 included cyber security requirements. And we are going
3 out to the major vendors, the new reactors right now,
4 looking at the planning phases for software.

5 So it's stuff that we are looking at now, even
6 though the rule is in effect. Our procedures are updated
7 to look at this as they are going through the process.

8 MEMBER BROWN: When you say "looking at the
9 vendors and software," is that how they manage the
10 software, how they control it, and who has access to
11 it? Is it a dedicated computer on which -- or server,
12 or whatever it is, which is not connected to anything
13 else?

14 Aside from the dynamic threat, one of the more
15 vulnerable threats is somebody planting something in
16 the base software that doesn't show up for some period
17 of time. I mean, there's a clock in there that clicks,
18 clicks, clicks away, and three years later it says, "Oh,
19 it's time to play games."

20 MS. SMITH: The only questions we're starting
21 to ask -- we have been interfacing with Eric and going
22 to vendors now, and we are going to Westinghouse next
23 week, and they are the kind of questions that are in
24 the plan to ask them. And we're following the whole
25 software life-cycle 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

1 So we are now looking at the planning phase
2 for some of the software that is going into the new
3 reactors, so we are just in the planning stage right
4 now, but we're asking those type of questions for what
5 they consider vulnerabilities. I mean, that's to come
6 in a couple of weeks. We haven't done it yet.

7 MEMBER BROWN: Yeah. Okay. That's the one
8 other area that I -- that if you've exited the plant
9 where, you know, all of your other administrative
10 controls and controlling who can touch what, you've got
11 the dynamic, you've got the in-plant, but that supply
12 chain side and what that computer -- I've forgotten who
13 it was that -- we had one presentation where their
14 software was actually on the corporate computer. And
15 I'm sitting there saying, "Oops, what do you -- oh, well,
16 there's a firewall." I'm sorry. That is not a wall
17 in terms of separation from access.

18 Now, they explained something else to me, and
19 I think something was resolved, but I'm not quite --
20 I'm just too old to remember what it was. So that's
21 a critical area that you really need to focus on I think
22 in terms of the isolation of wherever that software
23 resides, who has access, how the versions are controlled,
24 so that as each version is developed and it has been
25 "inspected, tested," or what have you, there is no access

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 to it by other than one particular guy that owns the
2 whole thing, even though he may not be the primary
3 program. Just a thought.

4 That's what I did in my programs, in the naval
5 nuclear program. We just -- it was very, very tightly
6 controlled in terms of version control and who had --
7 who could make a change to the master set and what were
8 the processes they went through before it ever got there.

9 It's cumbersome, but it's the only way to control what
10 you've got. So just a thought to pass on to you when
11 you're doing your staff.

12 MS. SMITH: Yeah. And version control is
13 part of design control, which we'd be looking at anyway
14 for software, since it is a safety-related component.

15 MEMBER BROWN: But think about access.

16 MS. SMITH: Okay.

17 MEMBER BROWN: Okay?

18 MR. WESTREICH: Thanks, Stacy.

19 MEMBER BROWN: Yeah. I appreciate that.

20 MR. FELTS: That is my last slide. I'll turn
21 it over to Monika to talk about interagency and
22 international.

23 MEMBER BROWN: Are we ahead or behind here?
24 We've got until 9:50 before we head into the closed
25 session. I think we're -- we're okay.

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 MS. COFLIN: I'm Monika Coflin. I'm a cyber
2 security specialist in NSIR. I've been with NRC for
3 five years and worked in cyber security at NRC for those
4 five years.

5 I'm going to discuss the NRC's recent
6 intergovernmental and international cyber security
7 activities.

8 As you are probably well aware, NRC's
9 authority is derived from the Atomic Energy Act, while
10 FERC's authority for grid reliability is tied to the
11 Energy Policy Act of 2005. These two authorities
12 relative to cyber security intersect at nuclear
13 powerplants.

14 Back in January 2008, FERC issued Order 706,
15 which specified critical infrastructure protection, or
16 CIP, reliability standards to safeguard cyber critical
17 assets. NRC facilities were exempt from those
18 requirements.

19 NRC and FERC recognized the need to ensure
20 that there was no gap or overlap between the regulatory
21 programs. FERC subsequently issued Order 706 Bravo,
22 which clarified that the balance of plant and equipment
23 within the powerplants that were not within the scope
24 of NRC's regulatory requirement would be within the scope
25 of the NERC order.

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 As a result, NERC asked all nuclear
2 powerplants to determine which structures, systems, and
3 components would be potentially subject to the six
4 standards, and which would be potentially subject to
5 NRC regulation. This analysis was known as the bright
6 line process.

7 All of their plants indicated that, if
8 compromised, balance of plant structures, systems, and
9 components would affect reactivity and were important
10 to safety, and, therefore, would fall within the scope
11 of NRC's regulation. The Commission determined, as a
12 matter of policy, that NRC's cyber security regulation
13 should be interpreted to include structures, systems,
14 and components in the balance of plant that have a nexus
15 to radiological health and safety. Licensees and
16 combined license applicants subsequently updated their
17 cyber security plans to reflect that Commission
18 decision.

19 NRC staff maintains periodic communications
20 with staff from FERC and NERC to exchange information
21 and to ensure that the requirements that are in place
22 are effective to meet both organizations' interests.

23 Back on February 12th of this year, President
24 Obama issued an Executive Order on improving critical
25 infrastructure for cyber security and an associated

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 Presidential Policy Directive. The Executive Order
2 requires federal agencies to produce unclassified
3 reports of threats to U.S. companies, and requires the
4 reports be shared in a timely manner.

5 It also establishes a voluntary program to
6 promote the adoption of the cyber security framework
7 that is currently being developed by NIST.

8 Independent regulatory agencies such as the
9 NRC are encouraged to leverage the voluntary framework
10 and to consider prioritized action to mitigate cyber
11 risk for critical infrastructure consistent with their
12 authority. The Executive Order also calls for the
13 review of existing cyber security regulations.

14 NRC of course will review our requirements,
15 as directed by the Presidential Policy Directive, and
16 although we're confident that our cyber security program
17 is strong, we will implement any improvements that are
18 identified from that review. Because NRC is an
19 independent agency, the NRC is not obligated to take
20 actions as a result of the Executive Order.

21 However, NRC is voluntarily participating in
22 a number of areas. For example, NRC management and staff
23 have interacted with national security and DHS staff
24 on policy issues. NRC staff is also participating in
25 the integrated task force working groups that have been

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 formed by DHS to implement the Presidential Policy
2 Directive.

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

8 Turning to some other intergovernmental
9 activities, NSIR participates in numerous interagency
10 working groups, such as the Joint Cyber Subcouncil.
11 The Joint Subcouncil includes members from the
12 Department of Homeland Security, FBI, NRC, and private
13 sector representatives, and the Subcouncil identifies
14 cyber security risks potentially affecting the nuclear
15 sector, serves as a forum for sharing relevant
16 information within the critical infrastructure
17 framework, and helps the nuclear sector participate in
18 cross-sector bodies such as the cross-sector cyber
19 security working group and industrial control system
20 working group.

21 This last slide provide examples of bilateral
22 and multilateral activities relative to cyber security;
23 for example, NRC staff who have had specific technical
24 exchanges with Korea and Spain on cyber security. Staff
25 has also shared cyber security best practices 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

1 organizations such as the World Institute for Nuclear
2 Security.

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

11 NRC also reviews IAEA's safety standards to
12 ensure that proper and adequate interfaces with cyber
13 security are occurring.

14 In general, we are ahead of other countries
15 in establishing a regulatory framework that considers
16 cyber security. Staff believes that sharing their
17 experience in developing NRC's cyber security program
18 will contribute to a more robust global cyber security
19 program for nuclear facilities.

20 We have also been able to consider the efforts
21 and approaches of other international partners in
22 relation to NRC's cyber security program and will use
23 those insights as the program evolves.

24 That concludes my presentation.

25 MEMBER BROWN: Has there been any thought

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 given -- this is a very perverse thought. Okay? It
2 just occurred to me as you were talking. Sharing of
3 the details of the NRC's cyber security program, what
4 you assess, how you assess, et cetera, et cetera.
5 Doesn't -- while I'm all for international
6 communication, doesn't that somewhat tell other folks
7 to assess where your weaknesses are, such that their
8 nasty people, whoever, whichever country they're
9 associated with, now have a better understanding of where
10 they can throw -- I mean, has there been any thought
11 -- I'm not -- I said it was a perverse thought.

12 CHAIRMAN ARMIJO: I don't think there's
13 anything perverse about it.

14 MR. WESTREICH: We don't share information
15 with other government organizations, unless we have an
16 agreement that we can share this information. So we
17 have to have standing agreements in place for like the
18 sharing of Safeguards information and how they can
19 control it. So we have to have an established
20 relationship before we'd share any information, and then
21 --

22 MEMBER BROWN: I'm talking about them taking
23 this, you know, and their bad guys that are out there
24 wanting to snoop now say, "Oh, they've protected against
25 this, that, that, and that, but, hmm, we've got an end-run

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 over here that may give us some access." I don't know.
2 It's just a -- I told you it was a perverse thought.
3 I hadn't come to this point with it.

4 MR. ERLANGER: Good morning. Craig
5 Erlanger.

6 MEMBER BROWN: You're back.

7 MR. ERLANGER: I'm back. Can't get rid of
8 me, Charlie. I have just transitioned from the cyber
9 program, but I was involved in many of the international
10 activities. To date, the majority of the sharings have
11 been basically conceptual concepts, a programmatic
12 approach versus looking at an individual asset,
13 prescriptive versus performance-based, nothing with an
14 appreciable level of detail, definitely nothing we're
15 seeing in inspections-based for what areas can be
16 improved.

17 So we're not at that level yet, so I don't
18 -- it's something for us to be mindful of, but we haven't
19 had those interactions yet.

20 MR. WESTREICH: Although we do have requests
21 for that information, so we're working through that.

22 MEMBER BROWN: I'm glad you said that. It
23 wasn't necessarily a bad question.

24 MR. WESTREICH: No. I mean, we have -- Korea
25 is very interested. Speaking of -- other countries are

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 very interested in what we're doing and how our programs
2 are established. I think as Monika said, you've got
3 to look at the broader picture. Would we rather have
4 people more protected, or are we -- so we've got to
5 balance those two pieces.

6 MEMBER BROWN: It's a balance. It's just
7 that you have -- somehow you have to make sure our
8 interests are protected in that manner.

9 Let me ask one other -- I'm going to ask this
10 question again later when you go through the Diablo
11 Canyon pilot program and your discussions of Ocone,
12 since you've done those. But, you know, we issued Reg
13 Guide 5.71, and you've had -- since then that was about
14 four years ago, 2008 or 2009, whatever. You have now
15 had a number of inspections. I think Ralph alluded to
16 14 plants.

17 And you've had these interactions with these
18 other organizations. And if you go back -- and I'm
19 trying to remember, but I think we made some comment
20 that stuff you learned, we ought to see if we need to
21 update or do any revision work to 5.71 to improve what
22 we have -- improve upon that based on what we have found
23 over the last four years.

24 Is there anything in play to start providing
25 an assessment of that, what we ought to do with that?

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 I mean, 14 plants to go out and inspect and see, we
2 should have seen a pretty wide variety. I mean, Ralph
3 alluded to some were pretty good and some were
4 bottom-feeders, so --

5 MR. WESTREICH: Yes. Well, I think there are
6 plans to update Reg Guide 5.71. I'm not sure what the
7 schedule is.

8 MS. COFLIN: Yeah. I think we have committed
9 to beginning that update in 2014.

10 MEMBER BROWN: Okay.

11 MR. WESTREICH: But there is other things
12 we're doing based on the inspection experience.

13 MEMBER BROWN: Okay. I would appreciate it
14 if you would communicate with Christina to let us know
15 when we might see -- you know, just -- it doesn't have
16 to be something where we have to -- you know, where we
17 have to take massive handlers or anything. We'd just
18 like to know where are the areas in 5.71 that you've
19 got on potentially -- or that you've learned which may
20 help that guidance as we then provide it out to the
21 various vendors.

22 Yes, hi.

23 MR. LEE: Eric Lee from NSIR. I don't know
24 whether you remember from last briefing, I think one
25 of the reasons that we may hold up on this revision at

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 this time is to provide stability during this interim
2 period with the implementing of this cyber security
3 program. And we are collecting all of this information
4 as you have mentioned.

5 And when we complete -- a licensee completes
6 implementing their full cyber security program, we will
7 be, you know, updating the Regulatory Guide 5.71.

8 MEMBER BROWN: Okay. Yeah. I wasn't
9 insisting on, you know, every year you have to go change
10 stuff while we're in the process of trying to develop
11 these things, but, you know, it shouldn't be a 2025 type
12 issue either, so --

13 MR. FELTS: I'd like to add that there are
14 other mechanisms we have to communicate to industry when
15 we believe there may be a lack of common understanding
16 of a requirement, particularly a requirement that is
17 in a plan. And we have exercised the security frequently
18 asked questions process to provide additional
19 information to the licensee community where we found
20 there may have been some misalignment in their
21 understanding of what is required to implement
22 Milestones 1 through 7.

23 So that's a little more nimble. We can get
24 those out more quickly than a reg guide update. And
25 typically when we go through the reg guide updates 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

1 go back and look at all of the security frequently asked
2 questions and roll in any information we think is
3 appropriate in that update.

4 MEMBER BROWN: Okay. I guess --

5 MEMBER SKILLMAN: I'd like to ask a question
6 before we go to the closed session, please. I'm one
7 of the people that was in the industry before there was
8 SALP. I was a director at plants during SALP. I was
9 a director at plants with ROP. And so I've got firsthand
10 experience and bruises from all of those changes.

11 I'm wondering how the agency is going to
12 integrate, if you find a deficiency in cyber area, with
13 the ROP. Is it going to be an initiating event,
14 cornerstone item? Is it going to be a mitigating system?
15 Is it going to be a barrier to integrity, or is it going
16 to be secure?

17 MR. WESTREICH: I think it's currently in the
18 security cornerstone. So that's where it exists. Of
19 course, you know, each one of these deficiencies live
20 in some kind of other system, like either it's a safety
21 system, security system, so we're actually fully
22 integrated into the ROP. There are significance
23 determination processes for each one of these findings.

24 We are part of the ROP process and function,
25 and security now has reintegrated back into that 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

1 So it's -- there is good communication between our
2 findings and the current programs for ROP in assessing
3 overall licensee performance based on all of the
4 cornerstones.

5 MEMBER SKILLMAN: Let me go a little bit
6 further. If this agency were to be hacked, would you
7 get a red finding for the agency? And if that same
8 ability to hack --

9 (Laughter.)

10 -- is some plant manager going to get fired
11 when that man doesn't have, or that woman doesn't have,
12 clairvoyance? Because that's the way the system works.

13 Out in the plants, if you're the poor guy on watch,
14 or the poor woman on watch, and an event occurs, and
15 it's determined that it might kind of have been avoided,
16 normally somebody gets a change in position.

17 And so what I'm really wondering here is, to
18 what degree has this been thought through? Because some
19 of the events that lie ahead for the industry affect
20 people, affect their careers, and the same difficulties
21 that would affect the team here at White Flint can affect
22 those individuals who are out in the plants. And often
23 there are threats that those individuals really can't
24 imagine or determine.

25 MR. WESTREICH: Yeah. Well, you know, 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

1 I guess we don't control what the licensees do to the
2 people. And I don't -- I agree with you, I don't
3 necessarily agree with the actions that are taken if
4 there's an event or a finding. But if you look at our
5 SDP, I mean, one of the things you might want to look
6 at is our significance determination process.

7 To get to a significant finding, you really
8 have to have a direct impact on a safety system function.

9 So you really have to get fairly far down the road.
10 You're actually -- there is some vulnerability
11 associated with the safety system function, which is
12 pretty far in.

13 MEMBER SKILLMAN: Well, clearly, it's the
14 SDP. I understand that. But I'm kind of taken by
15 Charlie's comment that here you have this little black
16 box with a timer, and it has been latent for 36 months
17 and it says, "Now is the time to wake up, and control
18 rods do this." And here is some poor plant manager
19 saying, "What happened?"

20 MR. WESTREICH: We agree. I mean, if it's
21 beyond the control of the licensee to be able to figure
22 that out, it's not even a finding, right? You know,
23 in the ROP world, they have to have a performance
24 deficiency. So it's got to be something that they would
25 have been able to identify correct. If it's some latent

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 embedded software from --

2 MEMBER SKILLMAN: I'd like to make sure that
3 what you just mentioned is well carved on the record.

4 MR. WESTREICH: Yeah. We can look at --

5 MEMBER SKILLMAN: Because that's the heart
6 of it.

7 MR. WESTREICH: I mean, I think it goes to
8 this performance deficiency issue. If it's something
9 beyond their control, we typically don't hold them liable
10 to that because they have no way to control that.

11 MEMBER SKILLMAN: Good. I'm done. Thanks.

12 MEMBER BROWN: How did they get into the plant
13 in the first place? If it's intentionally inserted,
14 that's why I made the point the way I did, that this
15 is -- somebody with malicious brainpower, if he had
16 control of the software at the vendor, now there's a
17 routine that is buried that gets triggered. And when
18 you've got a half a million lines of code, they're going
19 to find it.

20 MR. WESTREICH: Yeah. I mean, the comment
21 was, if it is beyond the licensee's ability to control
22 and identify --

23 MEMBER BROWN: I'm not saying that is easy
24 to do, okay, because it's really not. But anyway, that's
25 -- the point is valid. Somebody is going to get shot

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 anyway.

2 Okay. I guess we've got to go into the closed
3 session.

4 (Whereupon, at 9:56 a.m., the proceedings went
5 into Closed Session.)
6
7
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



U.S.NRC

UNITED STATES NUCLEAR REGULATORY COMMISSION

Protecting People and the Environment

Cyber Security Update (OPEN SESSION)

Cyber Security Directorate
Office of Nuclear Security and Incident Response
September 6, 2013

Agenda

OPEN SESSION:

- Control of Access Update - NRO
- Overview of the NSIR Cyber Security Directorate – NSIR/CSD
- NRC’s Cyber Security Program/ Regulatory Framework – NSIR/CSD
- Interagency / International Activities – NSIR/CSD

CLOSED SESSION:

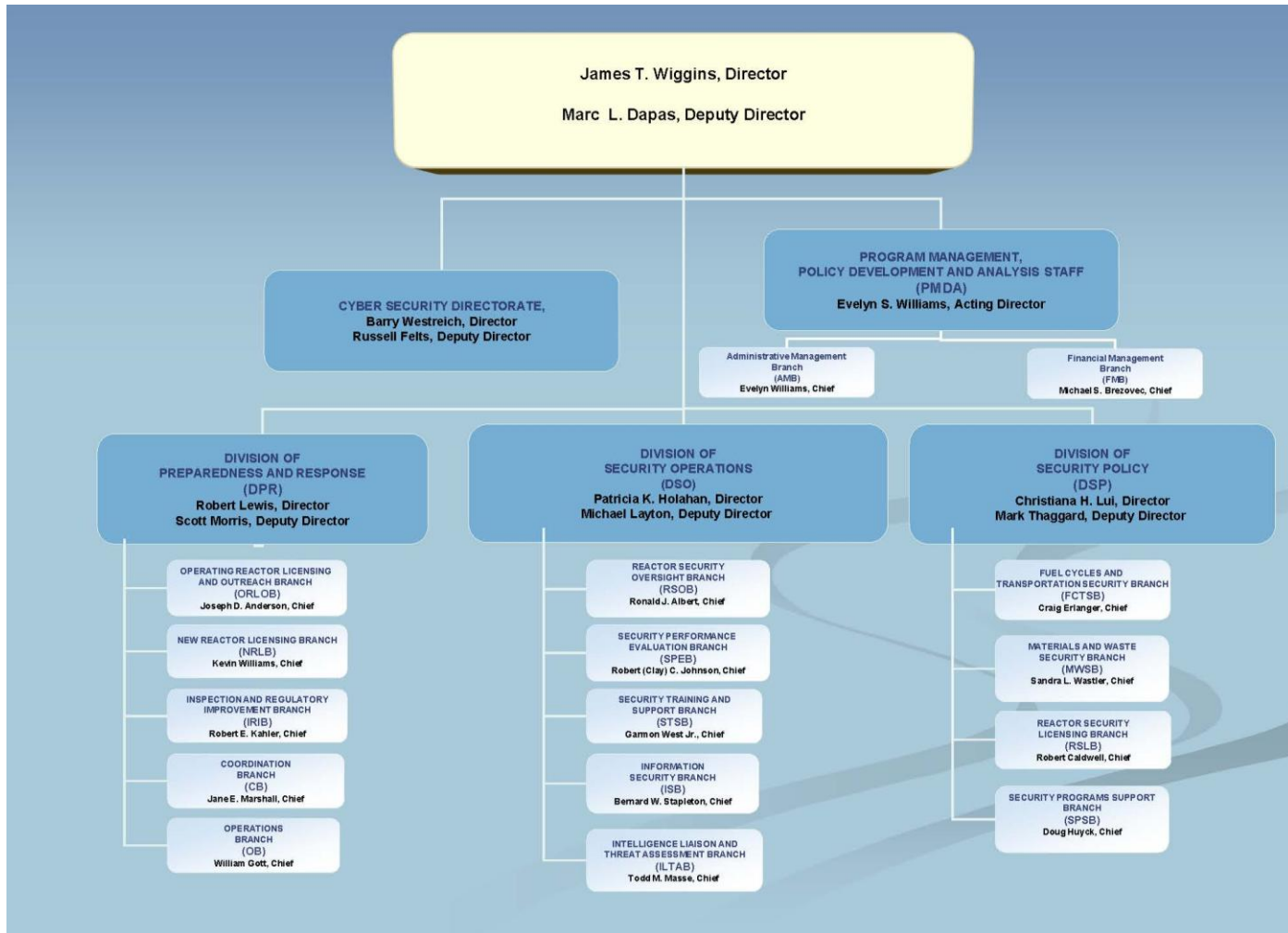
- Cyber Security Oversight Program – NSIR/CSD
- Inter-Office Coordination Activities – NSIR/CSD
- Cyber Security Roadmap Activities – NSIR/CSD

Purpose

- 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.

Overview of the NSIR Cyber Security Directorate

NSIR Organization Chart



Cyber Security Directorate (CSD)



- Established in June 2013
- Focus Areas:
 - Rulemaking
 - Guidance
 - Licensing
 - Policy Issues
 - Oversight Related to Cyber Security Requirements

NRC's Cyber Security Regulatory Framework

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

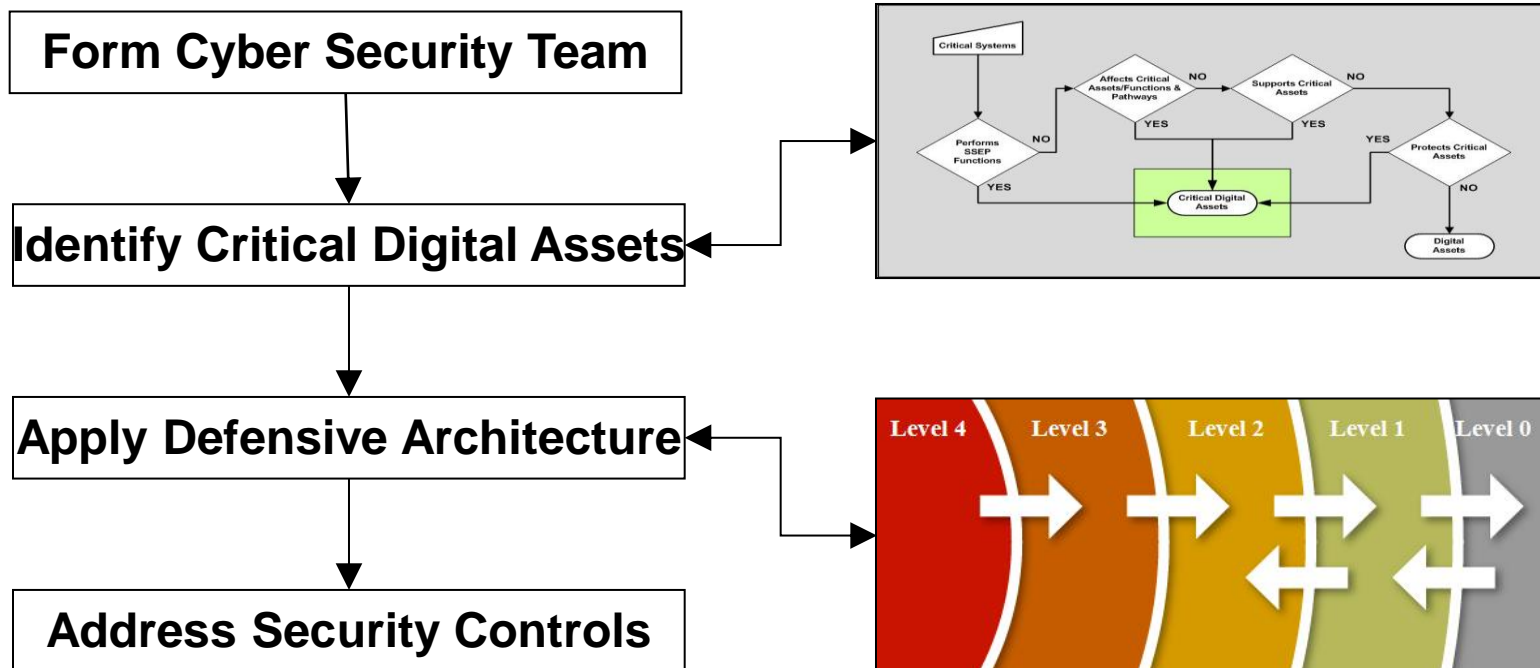
1998	Presidential Decision Directive 63 (PDD-63)
2001	Executive Order on Critical Infrastructure Protection (CIP)
2001	Issued advisory to NPP to enhance cyber security
2002	Required NPP to implement Interim Compensatory Measures
2003	Issued Design Basis Threat Order
2004	Published NUREG/CR-6847 – Cyber Risk Assessment
2005	Endorsed NEI 04-04 Rev. 1 – Cyber Security Program
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	Published RG 1.152, Rev. 3 – computers in safety systems
2011	NPP Cyber Security Plans approved
2013	Inspection of Interim Milestones begin

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
 - Provide high assurance against cyber attack
 - Integrated with Physical Security Program (10 CFR 73.55)
- Basic Requirements
 - Establish, implement, and maintain a cyber security plan
 - 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 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

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

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"> • Security planning & requirements analysis 	<ul style="list-style-type: none"> • Supply chain security • Functional security design • System test & evaluation 	<ul style="list-style-type: none"> • Audit of security control effectiveness (operational focus) • Vulnerability scanning 	<ul style="list-style-type: none"> • Continuous monitoring & assessment 	<ul style="list-style-type: none"> • Design control • Media sanitation (digital and non digital) • Disposal testing

Interagency and International Activities

FERC/NERC Activities

- Memorandum of Agreement with FERC
- Memorandum of Understanding with NERC
- Gap Analysis by NRC and FERC
- “Bright-Line” survey
- Commission Policy in SECY-10-0153
- Commission level meetings
- FERC Office of Energy Infrastructure Security established

Cyber Executive Order 13636/PPD-21

Improving Critical Infrastructure Cybersecurity

- Issued February 12, 2013
- 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

International Activities

NRC provided support and perspectives to the following:

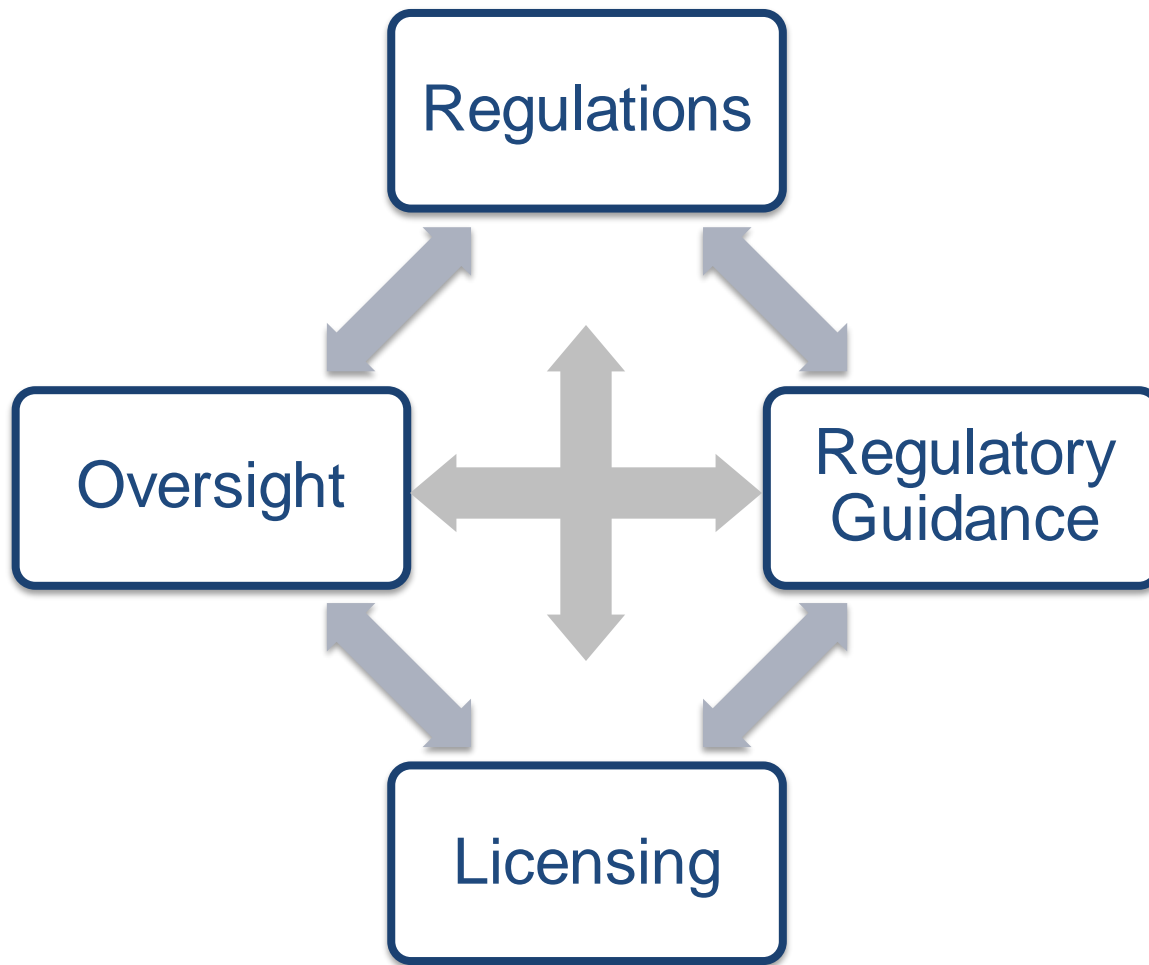
- IAEA TM - Computer Security At Nuclear Facilities (May 2011)
- WINS – Workshop on the development and integration of cyber security programs (Feb 2012)
- IAEA Consultancy Meetings
- Korea Atomic Energy Research Institute (KAERI) -NRC's cyber security and safety-security interface regulations (May 2012)

Questions



Backup Slides

Regulatory Framework



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

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

Other Intergovernmental Activities

- Joint Cyber Subcouncil
- Cross-sector Cyber Security Working Group
- Industrial Control Systems Joint Working Group

NRC involvement in 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