

Official Transcript of Proceedings
NUCLEAR REGULATORY COMMISSION

Title: Advisory Committee on Reactor Safeguards
 Digital Instrumentation and Control Systems

Docket Number: (n/a)

Location: Rockville, Maryland

Date: Wednesday, February 23, 2011

Work Order No.: NRC-726

Pages 1-379

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 DISCLAIMER
4
5

6 UNITED STATES NUCLEAR REGULATORY COMMISSION'S
7 ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
8
9

10 The contents of this transcript of the
11 proceeding of the United States Nuclear Regulatory
12 Commission Advisory Committee on Reactor Safeguards,
13 as reported herein, is a record of the discussions
14 recorded at the meeting.
15

16 This transcript has not been reviewed,
17 corrected, and edited, and it may contain
18 inaccuracies.
19
20
21
22
23

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 UNITED STATES OF AMERICA

2 NUCLEAR REGULATORY COMMISSION

3 + + + + +

4 ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

5 (ACRS)

6 DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS

7 SUBCOMMITTEE MEETING

8 REGARDING REGULATORY GUIDE 1.152 REV. 3

9 + + + + +

10 OPEN SESSION

11 + + + + +

12 WEDNESDAY

13 FEBRUARY 23, 2011

14 + + + + +

15 ROCKVILLE, MARYLAND

16 + + + + +

17 The Advisory Committee met at the Nuclear
18 Regulatory Commission, Two White Flint North, Room
19 T2B3, 11545 Rockville Pike, at 8:30 a.m., Charles H.
20 Brown, Chairman, presiding.

21 COMMITTEE MEMBERS:

22 CHARLES H. BROWN, Chairman

23 JOHN D. SIEBER, Member

24 JOHN W. STETKAR, Member

25

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 ACRS CONSULTANTS PRESENT:

2 MYRON HECHT

3
4 NRC STAFF PRESENT:

5 STEVEN ARNDT, NRR/DE

6 TOM BERGMAN, NRO/DE

7 RICHARD CORREIA, NSIR/DSP

8 RALPH COSTELLO, NSIR/DSO

9 CRAIG ERLANGER, NSIR/DSP/ISCPB

10 PAT HILAND, NRR/DE

11 TERRY JACKSON, NRO/DE/ICE1

12 WILLIAM KEMPER, NRR/DE/EICB

13 ERIC LEE, NSIR/DSP/DDRS/ISCPB

14 TIM MOSSMAN, NRR/DE/EICB

15 DONALD J. SANTOS, NRR/DE

16 MIKE SHINN, NSIR Consultant

17 GEORGE SIMONDS, NSIR Consultant

18 DEANNA ZHANG, NRO/DE/ICE1

19 CHRISTINA ANTONESCU, Designated Federal Official

20
21 ALSO PRESENT:

22 JAY AMIN, Luminant/Comanche Peak Digital Systems

23 MATT GIBSON, Progress Energy

24 WILLIAM GROSS, NEI

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

1. Opening Remarks 4

2. Historical Perspective and Overview of
 Current Regulatory Structure on Digital
 Systems security 10

3. Regulatory Guide 1.152 Modifications and
 Overview 106

4. Industry Perspective on Addressing Cyber
 security and SDOE 182

5. Regulatory Developments to Address Cyber
 security 282

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

9:50 a.m.

CHAIRMAN BROWN: The meeting will now come to order, we're ready to go, I think, pending other changes. We should have a reporter here, he or she, whichever, is on their way.

This is a meeting of the Digital Instrumentation & Control Subcommittee. I'm Charles Brown, Chairman of the Subcommittee. ACRS Members in attendance are John Stetkar, Jack Sieber, Myron Hecht, a Consultant.

Christina Antonescu, of the staff is the Designated Federal Official for this meeting. The purpose of the meeting is to discuss draft final Reg Guide 1.152, Rev 3, and other cyber security related activities.

In particular, the staff will discuss current regulatory structure on cyber security, Reg Guide 1.152 modifications from Rev 2 to Rev 3. Current developments to address cyber security an appropriate level of protection for the Technical Support Centers that were mentioned and discussed in several other meetings.

We will also have an industry perspective on cyber security presented. The Subcommittee will

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

4 The rules for participation in today's
5 meeting. It has been announced as part of the notice
6 of this meeting previously published in the Federal
7 Register on February 11, 2011.

8 We have received no written comments or
9 requests for time to make oral statements from members
10 of the public, regarding today's meeting. Also, we
11 have no request for a bridge phone line listening to
12 the discussions.

13 In addition, portions of this meeting will
14 be closed, if need, due to proprietary information
15 discussed by the industry. The transcript of the
16 meeting is being kept and will be made available, as
17 stated in the Federal Register Notice.

18 Therefore, we request that participants in
19 this meeting use the microphones located throughout
20 the meeting room when addressing the Subcommittee.
21 The participants should first identify themselves and
22 speak with sufficient clarity and volume, so that they
23 may be readily heard.

24 We will now proceed with the meeting. I
25 would like to remind the members, to also speak 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 give your names until we have a court reporter here to
2 ensure our statements are attributed to the correct
3 individuals during the parts of this meeting when we
4 don't have the reporter here.

5 So I'll call on Mr. Rich Correia, Director
6 of security Policy in the Officer of Nuclear security
7 Incident Response to give a brief introduction,
8 followed by Bill Kemper, Reviewer for the NRR.

9 MR. CORREIA: Thank you, Chairman and
10 Committee Members, Rich Correia, Director of the
11 Division of security Policy and NSIR. With me is Tom
12 Bergman, Director of the Division of Engineering in
13 NRO and Pat Hiland, Director of the Division of
14 Engineering in NRR.

15 We have quite a group here today to
16 present and support the meeting. Four Branch Chiefs,
17 two Senior level Advisors, six Senior Tech Staff and
18 two Industry Representatives.

19 As you said, Chairman, the Agenda is
20 ambitious and comprehensive, we want to make sure we
21 cover all the issues that you requested to hear about,
22 so there's going to be a lot of technical information
23 presented.

24 We hope we cover all the issues, if not,
25 we'll get back with you. And we're hoping that

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 industry perspective too, will also bring a different
2 aspect to our cyber security implemented at their
3 sites. So, with that, we'll turn it over to the
4 presenters.

5 MR. KEMPER: Thank you, sir, good morning.

6 I'm Bill Kemper, I'm a Senior Engineer in the I&C
7 Branch in NRR, and I'm joined by my colleagues today,
8 Terry Jackson, Chief of the I&C Branch in NRO, and
9 also Craig Erlanger, Chief of the Integrity, security
10 Coordination and Policy Branch in NSIR.

11 We're here today to provide an overview of
12 the NRC's Digital Safety System security Licensing
13 Program and the cyber security Regulatory programs.

14 The purpose of today's discussions is to
15 present the modifications to Reg Guide 1.152, Rev 2,
16 that will clarify the 10 CFR 50.55A requirement for
17 secure development and operational environment or
18 SDOE, as we call it.

19 Also to provide an overview of digital
20 safety system security licensing and cyber security
21 licensing framework and oversight, including the
22 integration of these two regulatory programs. And
23 that's a very important aspect we want to try to get
24 through today. And to address any ACRS questions
25 regarding how the digital safety system security and

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 the cyber security licensing reviews and inspections
2 are conducted utilizing our integrated process.

3 Next slide, please. The desired outcome
4 of these discussions will hopefully address all
5 questions of this Committee regarding the Part 50
6 Digital Safety System and security Licensing Process
7 and the Part 73, cyber security Program, itself.

8 Also, to convey a common understanding of
9 the NRC's licensing and oversight process for Digital
10 Safety Systems and cyber security, and result in
11 ACRS's recommendation, we hope, to initiate, excuse
12 me, issue of Reg Guide 1.152, Rev 3.

13 Next slide. To bring all this into
14 perspective, we'll discuss the following things today.

15 First off, we'll provide a history of the Digital
16 Safety System security and cyber security.

17 We'll also provide an overview of the
18 current regulatory basis for cyber security Programs
19 and the Digital Safety System security Requirements
20 themselves.

21 We'll provide a discussion regarding
22 modifications to Reg Guide 1.152, the staff deems
23 necessary to implement the integrated Part 50 Digital
24 Safety System security Licensing Process, and the Part
25 73.54, cyber security program.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 And, finally, the regulatory developments
2 that establish the NRC's cyber security regulatory
3 framework itself.

4 CHAIRMAN BROWN: This is Member Brown.
5 One question, you talked about Part 50 and integrating
6 into Part 73.54. What happens to Part 52?

7 MR. KEMPER: Well, Part 52 references the
8 technical criteria from Part 50. So when I say Part
9 50, really I'm speaking synonymously about Part 50 and
10 52.

11 CHAIRMAN BROWN: Okay, thank you.

12 MEMBER SIEBER: This is Member Sieber, my
13 overall understanding of really what you're doing is
14 to try to separate Part 50 elements describing how
15 these digital systems should work and how they can
16 inadvertently fail -- I am sure you related Part 73
17 pieces of it, so that they are addressed basically in
18 two different places but still intermesh. Is that a
19 correct perception of what you're doing?

20 MR. KEMPER: Yes, it is. But, and I'll
21 get into it through my presentation, in a lot more
22 detail. Others are going to get up here, as well, to
23 try to explain that even further for you.

24 MEMBER SIEBER: Thank you.

25 MR. KEMPER: In the next couple of slides,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 I'll put all this into perspective by providing a
2 historical time line for the establishment of the
3 Agency's Part 50, Digital Safety System security
4 Licensing process and the cyber security program
5 itself.

6 The original Reg Guide 1.152, title
7 Criteria for Use of Computers and Safety Systems at
8 Nuclear Power Plants, was issued in November, 1985,
9 endorsing IEEE Standard 7-4.3.2, 1982 version, which
10 is titled Standard Criteria for Digital Computers and
11 Safety Systems of Nuclear Generating Stations to
12 provide regulatory guidance for Digital Safety
13 Systems.

14 Prior to that there was none in existence.

15 The Reg Guide and the Standard did not address
16 digital system security, other than access control,
17 which is really an artifact that's drawn from IEEE
18 603.

19 The first revision of Reg Guide 1.152, was
20 issued in January, 1996, to endorse the 1993 version
21 of 7-4.3.2. The new standard captured additional
22 guidance for computer security and computer based
23 safety systems that had evolved over the 11 years
24 since the original version of the standard was issued.

25 CHAIRMAN BROWN: Member Brown. You

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 talked about in Rev 1, endorsing, which is it, 7-
2 4.3.2? I went back and took a look at that, so I need
3 something clarified.

4 I didn't see a whole lot of cyber security
5 related stuff in there.

6 MR. KEMPER: There was none.

7 CHAIRMAN BROWN: Thank you, I thought --

8 MR. KEMPER: That's the point I'm trying
9 to make. Yes, I'm going to repeat that a couple of
10 times, actually.

11 CHAIRMAN BROWN: Okay, thank you very
12 much.

13 MR. KEMPER: In Rev 0, there was no
14 security guidance in it.

15 CHAIRMAN BROWN: Not even in Rev 1?

16 MR. KEMPER: In Rev 1, there was no
17 security guidance in there.

18 CHAIRMAN BROWN: Even though it endorsed
19 7-4.3.2, but that doesn't have anything in it?

20 MR. KEMPER: That is correct.

21 CHAIRMAN BROWN: Thank you.

22 MR. KEMPER: And my next statement was
23 this version of the standard and Reg Guide didn't
24 contain any security requirements.

25 CHAIRMAN BROWN: Sorry about that.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. KEMPER: No, problem.

2 DR. HECHT: This Myron Hecht. As a member
3 of that standards committee, we did not in anyway
4 conceive that it was necessary to consider it.

5 At that point, systems were stand-alone
6 and very different from, as a matter of fact, PCs were
7 stand-alone and there was no real attack vector.

8 MR. KEMPER: That's a very good analogy,
9 it was a different world then, than we're in now. And
10 it brings me to my next point. As we all know, the
11 terrorist attacks on September the 11th, 2001, caused
12 the staff to look much closer at security, including
13 cyber security.

14 Following the terrorist attacks, the NRC
15 issued Order EA02-026, to address the threat
16 environment at that time.

17 This order was issued in February, 2002,
18 and specified numerous interim compensatory measures
19 to address the elevated threat environment. Part of
20 this order contained cyber security requirements,
21 mandating nuclear power plant licensees to identify
22 critical digital systems, that were critical to the
23 safe operation of the facility, and to evaluate the
24 possible consequences to the facility, should those
25 systems be compromised.

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 that in essence is what that order was
2 about. The material aspects of this order were
3 withheld from the public disclosure in accordance with
4 10 CFR 73.21, requirements for the protection of
5 safeguards information.

6 The NRC issued a subsequent order, EA03-
7 086, title design basis threat for radiological
8 sabotage in April, 2003. This order supplemented the
9 design basis threat or DBT as it's called, for nuclear
10 power plants specified in 10 CFR 73.1.

11 Among other things, this order established
12 requirements for the development of a cyber security
13 program at each nuclear power plant. And, again, the
14 material aspects of this order were also withheld from
15 the public for the same reason. Next slide.

16 In recognition of the potential cyber
17 security related issues, resulting from increased use
18 of digital technology at nuclear power plants, in
19 October, 2004, the NRC published NUREG CR-6847, titled
20 cyber security Self-Assessment Method for U.S. nuclear
21 power plants.

22 The staff, assisted by its Contractor,
23 Pacific Northwest National Lab, developed a cyber
24 security Self-Assessment Methodology that could be
25 used by licensees to assess the risk to the plant,

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 excuse me, to assess the risk to systems deemed
2 critical to the operations of the nuclear power plant.

3 The method was developed utilizing a multi-
4 disciplinary team that included nuclear power industry
5 personnel as well.

6 And again, the material aspects of this
7 document were also withheld from the public in
8 accordance with 2.390.

9 So using NUREG-6847 and insights gained
10 during its development, the Nuclear Energy Institute
11 or NEI developed NEI 04-04, title cyber security
12 programs for nuclear power reactors.

13 To provide nuclear power reactor licensees
14 with the means for developing and maintaining a cyber
15 security program at their sites. The NRC staff
16 evaluated the NEI Submittal and, by letter dated
17 December 23, 2005, informed NEI that NEI 04-04,
18 Revision 1, which was dated November the 18th, 2005,
19 provided an acceptable approach for formulating an
20 interim cyber security program at that time.

21 And I have to provide a note here. The
22 guidance in that NUREG, as well as NEI 04-04, is no
23 longer acceptable to meet today's cyber security
24 requirements, which I'm going talk about the evolution
25 of those requirements, in just a minute.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 The NRC issued Rev 2, Reg Guide 1.152, in
2 January, 2006, to endorse the 2003 version of IEEE 7-
3 4.3.2. The IEEE standard still did not have criteria
4 for computer security, including cyber security.

5 So the staff took it upon itself to
6 include Regulatory positions 2.1 through 2.9, of the
7 Reg Guide, to address aspects of the implementation of
8 cyber security, within safety systems that were not
9 adequately addressed in the standard itself.

10 Reg Guide 1.152, Rev 2, guidance was
11 developed to address both malicious and non-malicious
12 events and has been used for all digital safety system
13 license reviews from that time forward.

14 On December 31st, 2007, NRC issued interim
15 staff guidance 01, or ISG-01, we call it. It deals
16 cyber security for nuclear safety systems. This
17 guidance document resolved industry concerns about a
18 perceived conflict in cyber security guidance between
19 Rev 2 of Reg Guide 1.152, and Rev 1 of NEI 04-04.

20 So the task working group for ISG-1
21 concluded that Reg Guide 1.152, Rev 2, was, and I
22 quote, an acceptable method that can be used by
23 licensees and applicants to provide cyber security
24 protection for digital I&C systems used in safety
25 related applications, unquote.

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 ISG also clarified that here was no
2 conflicts between the industry document and NEI 04-04
3 and Reg Guide 1.152, Rev 2. And some of the members
4 that were on that group, are sitting in this room right
5 now, as a matter of fact.

6 I'm sure they remember these discussions
7 quite well. ISG-01 further states that until new
8 regulatory guidance is issued licensees, permit
9 holders and applicants involved in a design
10 construction, implementation or upgrade to safety
11 related digital systems, instrumentation and control
12 systems in nuclear power plants, may address
13 applicable cyber security issues through the use of
14 either Reg Guide 1.152, Rev 2, regulatory positions
15 2.1 through 2.9, or the attached version of draft NEI
16 04-04, Rev 2, in conjunction with the correlation
17 table. And that was attached to the ISG-01. In fact,
18 all digital safety system licensing applications that
19 have been approved to date, were reviewed against the
20 cyber security criteria of Reg Guide 1.152, Rev 2.

21 And some are still in progress as we speak
22 right now. In March, 2009, the cyber security Rule,
23 10 CFR 73.54, was issued. The new rule maintains the
24 intent of the previously issued security orders and
25 requires licensees and applicants to implement an

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 effective program to detect and prevent cyber attacks
2 on plant computer based systems associated with
3 safety, security and emergency response.

4 Guidance for meeting 10 CFR 73.53, was
5 issued as Reg Guide 5.71, in January, 2010. And,
6 finally, to complete the regulatory infrastructure for
7 digital system security, the staff intends to issue
8 Reg Guide 1.152, Rev 3, this summer.

9 Which will provide guidance for digital
10 system reliability, availability and integrity. This
11 issue will be covered in much detail later on in the
12 presentation.

13 So, if there's no, yes.

14 CHAIRMAN BROWN: I want to make sure I
15 understand. You used the words, when we went into the
16 1.152, Rev 2, about resolving conflicts, I mean,
17 excuse me, ISG-01 resolving conflicts between 04-04
18 and 1.152, perceived conflicts.

19 MR. KEMPER: Perceived.

20 CHAIRMAN BROWN: You used the work design
21 in there, so I'm trying to make sure I understand that
22 that's still, we're still encompassing both the Part
23 50 and 52, realms under that umbrella that you
24 mentioned earlier?

25 And then when you translate it into 5.71,

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 still falls within that realm, as well. I went
2 back and looked at 5.71. It's not quite as crisp from
3 the new plant design search and stuff like that, but
4 we've heard about it.

5 I think my memory is correct, John, didn't
6 we hear people mention 5.71, in some of those
7 meetings when we were talking?

8 So, you're like me, you don't remember? I
9 was hoping somebody would remember better than I do.

10 MR. ERLANGER: Yes, sir, it is, it does
11 apply to applicants, it is an operational program and
12 I will speak to that.

13 CHAIRMAN BROWN: Okay, that's fine, thank
14 you.

15 MEMBER STETKAR: John Stetkar. If you're
16 going to go into this fine. Why was the decision made
17 to issue a new regulatory guide 5.71, in response to
18 the 10 CFR 73.54 requirements, rather than issuing, at
19 that time, a new revision of 1.152, to incorporate
20 that?

21 In other, that seems to be the historical
22 split that we're talking about.

23 MR. KEMPER: Well, fundamentally, the
24 reason for it is Reg Guide 1.152, endorses far, far
25 more guidance about computer based critical safety

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, than just security, cyber security.

2 So that's why the staff, NSIR, as well as
3 NRR, worked very closely to try to figure out what's
4 the best way to provide guidance to the industry that
5 would navigate through those two issues very clearly.

6 So, a decision was made to go ahead, my
7 answer, to go ahead and develop Reg Guide 5.71, to
8 provide guidance to the industry on how to comply with
9 the new rule, 73.54, specifically.

10 Because the new rule is, as you well know,
11 it's only a few paragraphs, you know, as rule language
12 normally is.

13 MEMBER STETKAR: I think the basic, I
14 understand historically what was done. The question
15 is why -- why not just integrate that into 2.5 or 2.6
16 through 2.9?

17 MR. KEMPER: The question was though to
18 leave Rev 2 of 1.152 in place, until 5.71 was
19 developed and sent out to the industry. Because we
20 still needed a regulatory infrastructure for cyber
21 security, okay.

22 So that's why where we are today, and now
23 5.71 is off, it's been developed, full endorsed and
24 integrated in the industry, so now it's time to pare
25 back the requirements in Rev 2 of 1.152, because it's

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 confusing some of the industry right now.

2 Because there are duplicate requirements
3 in both of those standards.

4 MR. ERLANGER: Sir, this is Craig
5 Erlanger. What I will add, everything we're doing in
6 cyber security tied to the requirement, 10 CFR 73.54,
7 is a new requirement.

8 One thing you'll hear today on the
9 conscious decision plan path forward was safety and
10 reliability versus malicious actors.

11 There was a need on how we approached a
12 problem, to look at it from the requirements
13 standpoint. So 5.71, is simply the guidance on how to
14 implement the rule.

15 One thing I will speak about in a moment
16 is one of the benefits and the challenges for the way
17 we set up the rulemaking, is it's a performance-based
18 regulation.

19 With that, and with the threat constantly
20 changing, we needed the flexibility and the
21 scalability. There's only, which may or may not sit
22 well. So many things we can do in the design.

23 So part of how we approached a problem was
24 based simply on that approach. I'll speak to that in
25 a moment.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MEMBER STETKAR: You know I'll telegraph
2 some of my questions, because this also, commission
3 guidance anyway indicating that the industry and staff
4 should account for both safety and security in an
5 integrated form. In other words, you shouldn't
6 necessarily design something for safety and then later
7 go try to backfit some programs or elements of how you
8 operate the system for security.

9 And that's why my concern about this
10 historical split. Because everything you've said, I
11 can see, could have been accomplished equally well in
12 a revision to Reg Guide 1.152.

13 You could have had the old, Rev 2 could
14 have been in force until Rev 3 came out, and you could
15 have addressed all of the, quote, you know the
16 performance-based issues in the security aspect and
17 the same regulatory guidance while keeping a single,
18 integrated guide that covered, you know, the whole
19 life cycle of digital systems from initial design
20 concept through implementation and operation
21 maintenance in the power plant.

22 So, I hope you'll address some of those
23 concerns.

24 MR. ERLANGER: Yes, sir.

25 CHAIRMAN BROWN: I want to amplify John,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 because we both brought this up at one of the other
2 meetings, this aspect. The, I want to say this right,
3 okay, and this is not a criticism, I'm just trying to
4 get, to open up the conversation here, so you'll
5 address the stuff that we've been concerned about.

6 I mean I did go through this, I understand
7 the breakpoint and very, very clear in both your
8 discussion in 1.152. As you go look at the breakout
9 of this, it's very clear as to what you were trying to
10 do.

11 But when I go read, look at 5.71, one of
12 the major strategies isn't in there, is the
13 architecture, the cyber security architecture. And if
14 you look at 5.71, or at least when I looked at it,
15 there's, it's a lot of process and it's not hardware
16 design oriented, per se.

17 And I think you've made that statement.
18 I've forgotten what the word you used was.
19 Performance based, stuff like that. Now and one of
20 the things I found, I thought was missing in this, is
21 that, and in the other meetings we've had.

22 Is if you don't have, and this happens
23 back in the licensing area. This is why I was
24 concerned. You don't have a hardware architecture
25 that can then be used, okay, used is probably 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 wrong word here, to develop that cyber security plan.

2 I mean when you go look at the cyber
3 security plans, they're not required to be available
4 and complete until before fuel load. If you go look
5 at the requirements in the applications that we've
6 seen.

7 So, you know, when, so in the licensing
8 world, where does that breakpoint? How does that get
9 integrated so that you have an architecture in your
10 digital I&C system. And it's not just, I understand
11 the point about in-plant, which is what you're
12 focusing 1.152 on, but it's almost, it's like it draws
13 a line or a wall between once it gets communicated
14 out, we don't deal with this anymore.

15 And the architecture as shown in your
16 licensing document may not support what you need to do
17 in order to achieve the proper levels of security.
18 Whether it's Level 2, 3 or 4. I mean 5.71 specifies,
19 you know, a kind of this defense in depth architecture
20 of fire walls.

21 I'll call it fire walls as you go along.
22 So that was a number of our, I'm just trying to
23 amplify John's comments a little bit, because that's
24 the way I thought about it.

25 MR. JACKSON: This is Terry Jackson, I'll

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 try to cover some of that when we get to my portion.

2 CHAIRMAN BROWN: Okay, I just want to make
3 sure we cover it, I'm not trying to get that answer
4 now, but as you're going through your presentations,
5 that's one of our major concerns. Steve also wanted
6 to say something, Steve Arndt.

7 MR. ARNDT: Going back to John's original
8 question associated with, why did we not try and
9 provide guidance on the security rule in the 1.152 Reg
10 Guide?

11 One of the reasons associated with that is
12 the scope of the security rule is significantly
13 different from the scope of Part 50.

14 Reg Guide 1.152, is an acceptable means
15 that the staff has found for meeting the requirements
16 in Part 50 and 52.

17 The rule in 73.54, has a much broader
18 scope than just safety systems. So, from an
19 operational standpoint it would be extremely difficult
20 to talk about things that aren't safety systems.

21 I understand we probably could have done
22 other things, but from a strictly operational
23 standpoint, that would have been a very significant
24 challenge.

25 CHAIRMAN BROWN: Go ahead John.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MEMBER STETKAR: Let's let them go through
2 it, I think we've telegraphed enough issues that they
3 should be sensitive to.

4 MR. KEMPER: I'll turn it over. Thanks
5 for your questions, I'll turn it over the Craig now,
6 who is going to answer a whole lot of those questions.

7 (Laughter.)

8 MR. ERLANGER: Thank you, Bill. This is
9 Craig Erlanger, and in a general sense we will get to
10 some of your questions in my presentation, but in the
11 staff presentation we do speak to some of this, using
12 the TSC as an example.

13 CHAIRMAN BROWN: Okay, I have one more
14 questions here, Member Brown again. The, and this is
15 just, this is my thoughts, don't attribute it just to
16 the Committee or any of my fellow members.

17 Okay, in the process for developing lots
18 of systems, when I see program focus performance based
19 process oriented and that's what applies once I get
20 farther down the line.

21 After the license is issued, I start
22 getting worried because I have a lot of experience and
23 this is not, you know, raising any great flags on me
24 or anything, it's just that I've seen a lot of things
25 that got great processes, but you don't get the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 product that you want when you're finished, unless
2 somebody, somebody, not the licensee, not the vendor,
3 is overseeing the actual design, the details of that
4 design.

5 Not just that they have a nice quality
6 process in place, and you see, you know, you can check
7 that all off. You've got to have somebody looking at
8 that and say, okay, how are you executing that
9 particular part of the program.

10 How are you going to achieve that, show me
11 type thing. And that's difficult to see when you,
12 when you look in these particular Reg Guides that are
13 addressing cyber security.

14 So, that's going to be another question
15 later, I'll just throw that out on the table to let
16 you know. You've heard me say that in the licensing
17 arena, you're going to hear it now in this arena, as
18 well.

19 MR. ERLANGER: Thank you, sir, this is
20 Craig Erlanger, first I'll just answer your question
21 briefly. We will be presenting on where we stand
22 regarding the oversight inspection program
23 development.

24 I will mention the telegraph a bit from
25 our side is we're in licensing right now and we're

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 going through the process so we might have to come
2 back to you, down the road, and tell you how the
3 oversight inspection program development is going.

4 We're just not, a lot of things today is
5 we're are developing, we are in licensing, so it's a
6 brand new requirement from a 2009 rulemaking and where
7 we stand today is in the licensing with a concurrent
8 development of the inspection oversight program, which
9 will mirror how we do inspections in other program
10 areas.

11 So that presentation will follow Mr. Lee's
12 this morning, on where we stand regarding oversight
13 and inspection.

14 CHAIRMAN BROWN: Okay, Member Brown,
15 again. I understand you're in licensing, and that's
16 back to the point of the architecture. How do you
17 ensure you've got an architecture that's going to be
18 able to be utilized in the manner in which you want it
19 to be, once you get into that oversight and inspection
20 type process.

21 To see, how did we get what we wanted. Do
22 we have even an architecture that can achieve that.
23 And that's, that was my, you wanted, not the only
24 issue, but one of the major issues in terms of pushing
25 this aside, this whole thought process about what it

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 looks like, what architecture are you going to provide
2 to people to achieve this cyber security plan, and
3 achieve its goals.

4 MR. KEMPER: This is Bill Kemper, I
5 believe that Eric Lee has got a presentation that will
6 shed a lot of light on those questions.

7 MEMBER SIEBER: This is Member Sieber,
8 maybe I can make a comment here, it really goes back
9 to the very first thing that I said. If you prescribe
10 exactly how to construct your architecture, then
11 everyone will end up with the same system and it's my
12 thought that what you're really trying to do is to set
13 forth a number of principles that describe the
14 boundaries in which, whatever system you have must
15 perform.

16 And that becomes the regulation,
17 regulatory guide and so forth. And it's up to the
18 licensee to design and implement the system, and it's
19 up to the Agency and its inspection process to make
20 sure that that system meets all the requirements of
21 the regulations.

22 As opposed to sitting down now, before
23 anybody has actually physically built one of the these
24 things and tell them exactly where, how the process is
25 supposed to go together, how they're supposed to

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 communicate.

2 Should they be in separate rooms, don't
3 use USB ports and all that, even though that happens
4 to be in there, and then the regulation is to set the
5 boundaries on this, as opposed to define the design.

6 And so I don't have such a difficult time
7 accepting the way the regulations are without the
8 design because before you ultimately license the
9 plant, you're going to inspect the design and make
10 sure who's attributes are met.

11 Is that really the philosophy that you're
12 using?

13 MR. ERLANGER: Yes, sir, in a general
14 sense. And we'll cover the framework aspect of how we
15 set the program up.

16 DR. HECHT: This Myron Hecht, if I could
17 just respond to your point, as well as Charlie's.
18 There's something in between prescriptive design
19 features that provide really clean acceptance criteria
20 and what you're talking about, and I've heard this
21 used in architectural discussions in some of the more
22 recent systems that we've seen.

23 And that's the notion that an
24 architectural tenant. And an architectural tenant is
25 something more than just the broad principle. But not

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 something as specific as saying, you will use this
2 kind of a guard or that kind of firewall.

3 And perhaps that's what we should be --

4 MEMBER SIEBER: That's where we should be?

5 DR. HECHT: I would suggest that because,
6 as Charlie stated, once it's in the plant and you're
7 doing you inspections, it's kind of late if there's an
8 attack vector that isn't covered.

9 CHAIRMAN BROWN: I was not, remember I was
10 not up to springboard, I was not trying to say you
11 dictate every wire and every modem and every little
12 piece of one-way whatever.

13 But if you don't have a flexible
14 architecture that can accommodate various approaches,
15 then you're toast when you get there. And then all of
16 sudden you're ripping stuff out and having to put more
17 stuff back in.

18 And we can always say, well, that's the
19 licensee's problem, but that's not necessarily always
20 the best approach if you know they're going down a
21 path that's, okay, you see they're not providing a
22 flexible enough path to accommodate the end goals.

23 So, let's, thank you. I don't know what a
24 tenant is yet, so I've going to have to talk to you
25 about that. A tenant is somebody that rents my

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 apartment, if I own an apartment building.

2
3 (Laughter.)

4 MR. ERLANGER: Good morning everyone, my
5 name is Craig Erlanger and I am the Chief of the
6 Integrated security Coordination and Policy Branch.
7 This morning I will be providing you with an overview
8 of the NRC cyber security Regulatory framework. I'll
9 explain the scope of the cyber security rulemaking,
10 what the status is regards to licensing and discuss
11 some recent staff actions.

12 After the presentation on Regulatory Guide
13 1.152, Mr. Eric Lee will be providing you with a
14 presentation on how 10 CFR 73.54, the cyber security
15 Rule, and it's associated Reg Guide, Reg Guide 5.71,
16 interface and complement Reg Guide 1.152, Revision 3.

17 My overarching goal is to set the stage of
18 the following two presentations. What we hope to
19 clarify today, in the staff presentations, is that Reg
20 Guide 1.152, provides guidance on what constitutes an
21 adequate design and Reg Guide 5.71, provides guidance
22 on what constitutes an adequate program.

23 I also hope to convey that the NSIR staff
24 is communicating and coordinating with NRR and NRO
25 staff to put a regulatory infrastructure in place 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 address the threats and challenges associated cyber
2 security.

3 10 CFR 73.54 is officially titled the
4 Protection of Digital Computer and Communication
5 Systems and Networks. I require licensees to provide
6 high assurance, not absolute assurance, the digital
7 computer and communication systems and networks are
8 adequately protected against cyber attacks.

9 The scope of the rule includes digital
10 computer and communications systems and networks
11 associated with safety functions, imported safety
12 functions, security functions, emergency preparedness
13 functions and support systems, which if they are
14 compromised, would impact, adversely impact safety,
15 security and emergency preparedness functions.

16 So, to Steven's point, it's a lot more
17 than just safety systems, what we're looking at. Also
18 important to note, and we talked about this briefly,
19 that 10 CFR 73.54, is an operational program that
20 applies to licensees and applicants.

21 The focus is on the prevention of
22 radiological sabotage. What I mean by that is any
23 deliberate act that is directed against the plant.

24 cyber security is the process by which
25 critical digital assets are protected on a continual

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 basis from intelligent and malicious threat actors in
2 the face of ever changing methods and attack and
3 compromise.

4 And that is something I'll emphasize
5 throughout my presentation to go off script here, is
6 that the threat keeps changing, because it, and we
7 have real world examples and we'll talk about them
8 this morning.

9 That we've got to build that flexibility
10 into it. There are certain aspects of the cyber
11 security rule and Reg Guide that can and should be
12 considered by licensees and applicants during the
13 design of systems.

14 Principally these are the security
15 controls that are included in Reg Guide 5.71. The
16 challenge with cyber security features and design is
17 that the adversary changes and evolves.

18 What may be adequate today, maybe obsolete
19 tomorrow. In licensing, the Agency cyber security
20 staff does not review individual systems, but looks a
21 cyber security from a programmatic perspective.

22 This is also a performance based
23 requirement, which I previously mentioned. We rely on
24 measurable outcomes, known as performance results that
25 need to be met, but we provide flexibility to

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 licensees meeting those outcomes.

2 This flexibility is key and, to go off
3 script again, if you look at the rulemaking, we talk,
4 we say need to apply security controls. The level of
5 detail of what those security controls are, based upon
6 the known threats today, are found in the regulatory
7 guide.

8 This was done intentionally and is
9 captured in a license condition, which I'll talk about
10 in a bit, because the scalability of the program needs
11 to, I guess expand and contract based upon the threat.

12 CHAIRMAN BROWN: Can I, you talk about
13 performance based. Performance, this is Member Brown.

14 I looked at, when I look at 73.54, that's what I
15 would have perceived to be the performance
16 requirements you're looking for. Is that correct?

17 MR. ERLANGER: That's correct
18 understanding and we get to the clarity of what we
19 actually, the guidance, which is, you know, pretty
20 heavy, Reg Guide 5.71, or NEI 08-09 is how you meet
21 what's in the rule.

22 What's unique is that it's not just a, you
23 can do these if you want. The commitment they're
24 making in licensing the programmatic approach means
25 that for those 148 security controls, for every

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 digital asset that screens in or screens out, that's a
2 process they follow in there.

3 They have to, at a minimum, consider those
4 security controls. And Eric will speak to this in
5 detail. But the overarching picture is you apply the
6 security control, great. You don't apply it, tell us
7 why. Maybe it's something that would adversely affect
8 safety that you don't want to do.

9 A very generalized example could be
10 putting a password for a control room operator on a
11 workstation. A bad scenario happens, he ends up
12 locking himself out.

13 That would make no sense to put a security
14 control like that on there. The other option is maybe
15 you've got a better way or an equal way do it, not one
16 of our security controls.

17 Just tell us how you thought about that
18 threat vector. And that's the flexibility of the
19 program that you'll hear about in Mr. Lee's
20 presentation.

21 What I will mention about performance
22 based regulations, this is consistent on how we
23 regulate for security, the Part 73 regulations. To
24 make a physical security analogy we say you need to
25 defend against x.

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 A licensee might say the fence is eight
2 feet high, nine feet high, ten feet high. We don't'
3 get to that level of detail in prescribing, we just
4 tell the what they the need to defend against, if that
5 helps, with an analogy to make it clear.

6 For the cyber security licencing process,
7 one thing that is unique again, is that this becomes a
8 condition of their operating license. Prior to the
9 Part 73 update that occurred in 2009, the license
10 condition for security required there security plans.

11 These were your training qualification
12 plan, your safeguard continency plan and your physical
13 security plan. With the addition of the cyber
14 security rule in '09, the license condition needed to
15 be updated to reflect this new requirement.

16 As a result, cyber security plans for the
17 operating fleet were submitted as a license amendment
18 request. I meant, I'm going to key in on license
19 amendment requirement, because it's a terminology.

20 When I take a step back I believe it
21 creates a bit of confusion of what we're doing on a
22 program look. It's just the approach we took, but we
23 were amending the license to account for a new
24 requirement.

25 Both Reg Guide 5.71, and NEI 08-09, Rev 6,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 which is the industry cyber security guidance
2 document, are unique because they contain an Appendix
3 that contains a cyber security template that can and
4 was utilizing by licensees and applicants for
5 licensing purposes.

6 The use of templates add efficiency,
7 effectiveness and shortens and simplifies the review
8 process. To date, every operating reactor licensee
9 and all the new reactor design centers have utilized
10 one of these two templates.

11 So while the license --

12 CHAIRMAN BROWN: 5.71 is pretty clear
13 template. I went off to see where NEI 08-09 was
14 endorsed. All we were able to find, in terms of
15 asking the question, was a couple of letters that went
16 back and forth, where the first, the first letter I
17 guess I saw said something about, gee, if you don't,
18 if you don't use the template in 5.71, you know,
19 you're going to get RAIs or something like that on it.

20 And something else was submitted and you
21 eventually wrote a letter. But I still couldn't find
22 where NEI 08-09, Rev 6, was endorsed in total, along
23 with the template and any formal document. So, am I
24 correct on that?

25 MR. ERLANGER: You are correct, sir, and

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 on the subsequent slide, I believe Slide Number 9, I
2 will address where we stand in regard, and answer all
3 your questions on it later on.

4 CHAIRMAN BROWN: Okay, so that will be,
5 okay, so that will be addressed?

6 MR. ERLANGER: Most definitely, and I
7 don't answer it at that point to satisfaction, I can
8 definitely give you more.

9 So while a license amendment request for a
10 safety system is individually unique process for that
11 particular system. For cyber security licensing the
12 review was simplified by the use of a template.

13 We are able to do this because of the
14 programmatic approach we took to cyber security.
15 Slide 8, please.

16 The last point is a great discussion to
17 transition, to talk about SRP 1366. Unlike the
18 license amendment request done by NRR and NRO that
19 rely heavily on the SRP to ensure key elements are
20 covered, the cyber security plans were simplified by
21 the use of the templates mentioned on the previous
22 slide.

23 We did not have to review unique
24 applications. We did use the SRP, primarily for
25 deviations to specific sections of the templates. 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 which and if an applicant or a licensee deviates from
2 the plan template, we have an will continue to look at
3 the SRP and Reg Guide 5.71.

4 But, again, if you refer to Appendix A in
5 both documents, everyone across the board has utilized
6 that. So our Rev 0 of the SRP, is a direct derivation
7 of what you'll see in Reg Guide 5.71.

8 CHAIRMAN BROWN: Are we ever going to see
9 13.6?

10 MR. ERLANGER: Sure, sir, we sent it down
11 for awareness. It was published in the Federal
12 Register, I believe, in November.

13 CHAIRMAN BROWN: I found, I went to the
14 web site and I found a Rev 0 or Rev 1, and I just kind
15 of quickly glanced at it. I saw it referred to in
16 some of the documents.

17 MR. ERLANGER: If, again, we can do
18 whatever the Committee would like. And it's, we, it's
19 a directly derived from Reg Guide 5.71 on the program
20 look.

21 CHAIRMAN BROWN: That's kind of what it
22 looked like.

23 MR. ERLANGER: It's literally verbatim,
24 yes.

25 CHAIRMAN BROWN: It looked like a template

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 checklist on those.

2 MR. ERLANGER: To a certain extent it's
3 making sure the key elements were hit and they it goes
4 into the detail.

5 CHAIRMAN BROWN: I didn't mean to refer
6 just to the template, but it covered --

7 MR. ERLANGER: It covers all the key
8 elements. But the intent we can figure out what's
9 needed for what the Committee needs afterwards. But
10 we were not intending --

11 CHAIRMAN BROWN: I'm not trying to define
12 that, I'm just trying to understand what it is.

13 MR. ERLANGER: It is a Red Zero document
14 and from where we stand today, for the initial round
15 of licensing for both operating fleet and the new
16 reactor applicants.

17 They did utilize, everyone across the
18 board utilized one the two templates that were
19 provided.

20 CHAIRMAN BROWN: Okay, thank you.

21 MR. ERLANGER: For operating reactors,
22 just to give you an update of where we are and then on
23 the next slide I'll get back to 0809 and answer your
24 question, Mr. Chairman.

25 Now plans are currently undergoing staff

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 review. We've been working closely with NRR's
2 Division of Operating and Reactor Licensing, in ODC
3 and utilizing a team approach to conduct these
4 reviews.

5 We're in the process of issuing require
6 for additional information that have been based solely
7 on the deviations from the templates.

8 The staff has also been proactive with the
9 help of NRR to develop a template for the safety
10 evaluation reports that you issued upon the completion
11 of the technical reviews. Yes, sir.

12 CHAIRMAN BROWN: You're looking at, this
13 is interesting. You put in a modification, I'm just
14 going to ask an example and maybe if you're going to
15 cover it somewhere else you can tell me, but a new
16 system is being put in to Oconee, a digital I&C
17 system.

18 That means now the while ability. The way
19 you transmit information out to other locations,
20 whether it's a technical support facility or center or
21 the EOF or wherever.

22 It's different now then it was in the
23 analog world. It was there, how was that handled?
24 Was that, I mean we didn't have all this well-defined,
25 it's going in 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 Has that been encompassed in terms of the
2 cyber security aspects of where that information is
3 going, how it's being sent to various places.

4 Similar to the (inaudible) corporate
5 network or something like that?

6 MR. ERLANGER: it's a great question and I
7 think it's a question the topic will refer to
8 throughout the day today. But in a general sense, if
9 the program approach does not have a decrease in
10 effectiveness, you wouldn't see a revised plan coming
11 in for sakes.

12 Again we're taking the program level.
13 But we are very much aware and very sensitive to this
14 transition period that we're in today from things hat
15 were licensed using Reg Guide 1.152, Rev 2, with the
16 absence of a codified cyber security regulation to
17 where we hopped to go down the road with 5.71 in Rev
18 3, complementing one another.

19 So situations like Ocone obviously and
20 I'll defer to the safety folks when I over step my
21 bound here. The safety evaluation report does speak
22 to cyber security. The licensee is very aware that
23 there is a cyber security requirement out there and
24 they need to meet that requirement.

25 And these are not a normal situations.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 There's finite number, we pay attention to them and
2 we're working through, we are, we have a plan to
3 address those types of situations as they come up.
4 But we will cover mods and plans. I know in both the
5 licensee presentations they speak through their
6 process as well as what would be on the technical
7 level.

8 But we will talk through that in the next
9 two presentations.

10 MR. KEMPER: This is Bill Kemper, can I
11 just interject. For the Oconee review, as I said in
12 my presentation earlier, at the time they made their
13 submittal for the RPS and the SFAS upgrade system,
14 ISG-1 was in place.

15 So they showed compliance to the
16 requirements that were specified in ISG-1, which
17 specified either Reg Guide 1.152, Rev 2, was adequate
18 cyber security guidance or any, 0404, Rev 2.

19 They chose to comply with Reg Guide 1.152,
20 Rev 2, and that was the basis for reviewing and
21 approving those type of security measures.

22 MEMBER SIEBER: This is Member Sieber. To
23 the extent that that's inadequate as we learn more
24 through time than that cyber security risks. How do
25 you deal with plants that were licensed in a

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 regulatory framework that was not all inclusive, that
2 we know now.

3 In other words, a licensee would come in
4 with a wide variety of different kinds of systems and
5 propose one that by yesterday's regulation was just
6 adequate. But we'll meet with the demands of
7 tomorrow. How do you plan to deal with that.

8 MR. ERLANGER: So, we'll make an
9 assumption, I think it's a valid assumption that the
10 Ocone, that will screen in as a critical digital
11 asset or a critical system.

12 It will hit that threshold that, but that
13 is a decision made by the licensee, but also can,
14 that's a pretty big system. They have to meet the
15 requirements of 73.54.

16 Now the question, and there are, what Eric
17 will outline is there's 148 security controls, there
18 bins, big picture bins. Technical and Management
19 Operational.

20 It doesn't matter the design of the
21 system, they can apply those controls. And it's just,
22 it's a program approach where, that's why when you
23 look at the different design centers, you look at the
24 different systems.

25 This applies, can be enforced today.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 There will be an implementation schedule that they'll
2 have to meet and they'll put it in place. They have
3 to meet the requirement, in summary, they've got to
4 meet the requirement of 54.

5 MR. KEMPER: This is Bill Kemper again.
6 Just as important, though, sites, you know, are
7 developing their own cyber security programs right
8 now. Each and every one of them. They started out
9 several years ago, you know when NEI 04-04 was issued,
10 basically.

11 So, like for example, Oconee, we're
12 talking about that. We approved that like one of the
13 things that comes to mind is we said, they committed
14 there will be no open ports to any of the peripherals
15 associated with the RPS.

16 So we approved it based on that. And when
17 the system is installed the Regions will inspect that,
18 to ensure that that architecture is, in fact,
19 maintained.

20 Now if they choose to modify that later
21 on, under 5059, they will have to go through the
22 evaluation, the 5059 rule to ensure that they haven't
23 deviated from that licensing basis by which that
24 program, or the system was approved.

25 So the licensees are going to have to, you

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 know, obviously they have well established expertise
2 and programs, and so they'll have to maintain those
3 commitments themselves and I'm sure they're very
4 comfortable doing that.

5 MR. CORREIA: This Rich Correia from NSIR,
6 if I could add to that. Cyber security plans that we
7 are now reviewing, also have features, if you will,
8 requirements that would force a licensee to go back
9 and reevaluate their cyber security protections if
10 something changed.

11 If there's a new threat, some information
12 that we would submit to them. If something happened
13 at another plant, through operating experience, the
14 program calls for them to go back, reevaluate and
15 adjust as appropriate their program to accommodate
16 that. So it's not static.

17 MEMBER SIEBER: This is Member Sieber
18 again. But there's nothing in the regulation or the
19 regulatory guide that makes them construct that
20 program in that way, right?

21 MR. CORREIA: There is.

22 MEMBER SIEBER: Okay, you can point it out
23 when we get to it.

24 MR. KEMPER: You mentioned 148 explicit,
25 what did you call them?

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 PARTICIPANT: They're security controls --

2 CHAIRMAN BROWN: security controls, thank
3 you. That's a lot. And we've got 148 things you,
4 which is the most, is there a thought process at NRC
5 that says which ones are important. I mean is there a
6 priority in terms of how you look at these controls or
7 is it a one size fits all and they all have to mush
8 through every one.

9 PARTICIPANT: Great question. I'm sorry,
10 were you done.

11 CHAIRMAN BROWN: No, I appreciate your
12 complement.

13 (Laughter.)

14 PARTICIPANT: It is, so we like to say, on
15 one level we took the fun out of it. And that's an
16 expression we've used for some time, where they were
17 based upon known threat factors.

18 But that question came up. How do you get
19 that high assurance, how do you get it in a timely
20 manner? So what we did is we looked at some of the
21 more probable threat vectors.

22 Things we're seeing, whether it's a, I
23 won't say attacks that, things that go on, so portable
24 media. The introduction of thumb drives and things
25 like that.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 There's obviously a security control for
2 removable media. What we've done and working with
3 industry, as Rich mentioned, there's two requirements
4 that were in 73.54. Submit a plan and submit a
5 proposed implementation schedule.

6 We did front load those more probable
7 threat vectors and things to look at on the front end,
8 because it would just make common sense to do.

9 But every control that's there was there
10 for a defined reason, intended purpose and we don't
11 put a weight on what's more important, but there is
12 some, as a learning organization, you see more
13 vectors, vectors that are being used more than other.

14 So it made sense to front load them and
15 how we organized the implementation schedules.

16 CHAIRMAN BROWN: Okay, now is that done,
17 is that done post? Is that done during your licensing
18 review of this, or is that, does that wait until
19 afterwards or what?

20 PARTICIPANT: You could say part of the
21 licensing review does include a reviews of the
22 proposed implementation schedules. And what you'll
23 see there is a, I'll be on high level.

24 The staff chose two dates that were very
25 important to them. One is the full program

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 implementation, every plan procedure, every I dotted,
2 T crossed.

3 And then we picked an interim date with
4 interim milestones such as things like portable media,
5 those threat vectors. Ensuring people are in, there's
6 something called the critical group on our access
7 authorization programs.

8 Just a laundry list of things that need to
9 be done at a much earlier interim milestone. And I'm
10 speaking to the operating reactor site because new
11 reactor, obviously the license condition is prior to
12 fuel load on the applicant's side where they've got to
13 be in full program compliance.

14 So, yes, across-the-board, we do look at
15 it in licensing and we will speak to it in the license
16 condition.

17 PARTICIPANT: Do you make the absolute
18 assumption that if you isolate a Cyber system, control
19 system, completely that the only attack you'll get is
20 from an insider?

21 PARTICIPANT: No, we don't, but we do
22 consider, I thought you were going to end up, do we
23 stop it. We definitely consider the insider but you
24 have to, if it's isolated, you still apply the 148
25 security controls.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 And what Michael, Eric and --

2 PARTICIPANT: I would think so, there's a
3 lot of smart people out there.

4 PARTICIPANT: And that's the greatest
5 challenge. But so getting something like a data diode
6 only buys you so much. Concerns with software
7 updates, things, you know, things that go on normal
8 plant life.

9 No we can't assume that just being
10 digitally isolated will buy you that level of success.
11 It will get you so far, but it doesn't get you all the
12 way.

13 PARTICIPANT: Well, you can assure that
14 you're okay as of yesterday, but today is a different
15 question.

16 MR. KEMPER: That brings up the point a
17 little, let me slip back into architecture a little
18 bit, because the data diode issue has prayed on me and
19 I'm not a designer so, but I do know that a lot of
20 these communications paths are, claim to be one way,
21 but they're from inside.

22 This is this is the isolation of the
23 inside of the plant. Can something get in, when
24 you're not aware of it?

25 Some of these one-way items, components,

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 are really software controlled. In other words, you
2 can program them to be one way, or you can program
3 them to be bidirectional.

4 Or you can buy a transmission or a
5 communication device that is literally one way only,
6 it will not doing any else.

7 And I asked that question several times
8 and the applicant, in the new reactor world and I got
9 kind of no answers. And that's one of my concerns
10 relative to the architecture.

11 It's not prescriptive, but what does one-
12 way mean. It's like independence, you're either
13 independent or you're not. You can't be half
14 independent.

15 You're either one way or you're not one
16 way, so --

17 MR. JACKSON: This Terry Jackson --

18 PARTICIPANT: Let me make sure I got the
19 point, in other words somebody could come in high, get
20 in, change the, you know, change that, get a piece of
21 software and, see these guys are smart.

22 They're a lot smarter than most people we
23 know. And they do amazing things, and all of a sudden
24 turn that around where he can actually implant or send
25 in other information into the operational equipment.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 So that's, I think that's a little bit of
2 the part of the question that -- go ahead, Terry.

3 MR. JACKSON: I was going to get into my
4 Slide, but the question you brought up with regards
5 to, like architectural aspect for data communications,
6 that's one aspect that not necessarily unique to cyber
7 security, but also something to look at in safety
8 review as well.

9 So when folks do come in and they say,
10 well, it's uni-directional data communication. And
11 you say, how do you implement that then. Some have
12 described to us how they physically limited by just
13 one, you know, like fiber optic cable going from one
14 location to the other. It's only transmitted --

15 PARTICIPANT: But what's the data on the
16 fiber optic link, has to be, not be able to be
17 switched for the source.

18 MR. JACKSON: So we look at, and using the
19 guidance in Reg Guide 1.152, we're looking at it from
20 a non-malicious aspect where you could have some kind
21 of software error or something else happening, say a
22 non-safety system and how could it impact the safety
23 system.

24 But there's some inherent benefits in the
25 safety review where we're looking at the data

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 communications and how it could affect other divisions
2 or other systems.

3 And it brings over those benefits. I
4 think the cyber security, while not intentionally in
5 their review, but it's kind of like an inherent
6 benefit, just from the safety review itself.

7 MR. KEMPER: This is Bill Kemper, if I
8 could, now we have some practical experience in the
9 Ocone application. I'm sure you all remember that
10 had a data diode, it was a commercially developed
11 device and my staff had a look at that particular
12 device in great detail, to assure ourselves that it
13 was in fact designed, configured, built and configured
14 to only provide communications in one-way direction.

15 And, you're right, some of those devices
16 do have microprocessors in them. So, it's, you have
17 to really keep your wits about you and be sure that
18 you understand how that system operates.

19 And we had to actually do a detailed
20 circuit analysis. We had to go to that level, which
21 we don't normally go to that level for reviewing these
22 types of systems, to ensure that it was one-way.

23 Because we were reviewing this system to
24 meet the requirements of cyber security, as they were
25 outlined in 1.152.

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 PARTICIPANT: And we will speak to
2 defensive architectures in the staff presentation.
3 We'll --

4 MR. KEMPER: Okay, you can see where my --

5 CHAIRMAN BROWN: I hate to keep beating a
6 dead horse because I don't think he's really dead.

7 MR. KEMPER: In NRR's case, this is Bill
8 Kemper again, that's done during the licensing review
9 or that was done during the licensing review of
10 Oconee. I would think in NRO's area, that would be an
11 ITAC, which will have to be done at the appropriate
12 time.

13 PARTICIPANT: The last thing I was going
14 to mention on operating reactors is the industry has
15 developed a cyber security Task Force. Many members
16 are present today, to help represent their collective
17 equities on the Cyber subject.

18 And this has added greatly to bringing
19 resolutions to light and very quickly and it's been
20 very helpful and it's probably similar to many other
21 programs out there.

22 When you have a new requirement the
23 industry bans together and works through problems and
24 has a unified approach to answering questions for the
25 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 For applicants, you are probably more
2 familiar with because you've been seeing some of the
3 briefs down here. They submit their cyber security
4 plans on a schedule that's consistent with their
5 overall licensing schedule.

6 To date, the staff has reviewed one cyber
7 security plan for each design center, so they're in
8 the process, and I believe we're coming down to brief
9 you on South Texas the week after next.

10 So you're probably more familiar with
11 seeing Cyber reviews coming down --

12 PARTICIPANT: No, we haven't seen, correct
13 me, I don't remember seeing a specific presentation.
14 I'm interested in that because we have --

15 PARTICIPANT: We haven't seen any design
16 since (inaudible). We haven't seen many design
17 centers yet. ESPWR was all (inaudible) out in the
18 future.

19 PARTICIPANT: (Inaudible) and ABWR both,
20 very and I've got the documents here, at least the
21 single sheets that say that security plan is not
22 required until before fuel load.

23 PARTICIPANT: That is a correct statement.

24 PARTICIPANT: And that's way down and it's
25 way after licensing. That's three or four years down

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 the path after the license has been granted. So, you
2 know, we're trying --

3 PARTICIPANT: Maybe I can clarify.

4 PARTICIPANT: -- we're trying to
5 understand how we don't lose the bubble between
6 licensing and when the security plan, but we don't
7 want to make it so restrictive either. That you lose
8 the capabilities to fight new threats. Jack, what
9 were going to say?

10 MEMBER SIEBER: That gets to the point
11 that it's really all going to be done by inspection.
12 And you spend a lot of time trying to decide whether
13 something is unidirectional or bidirectional.

14 I don't picture an Inspector going through
15 that kind of a process.

16 PARTICIPANT: That's exactly, one of our
17 concerns is where do we bring in, and I'm not, we are
18 not criticizing the competence of the Inspectors. I
19 mean that's, that's, in the site, the Regional groups
20 and the Plant Inspectors. That is a very difficult
21 task. I mean even folks vaguely familiar with how
22 they work have a difficult time.

23 And even folks that really think they
24 understand it have a difficult time with some of these
25 devices.

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 SIEBER: Well, they have a harder
2 time because they understand it.

3 (Laughter.)

4 PARTICIPANT: So just to clarify my
5 statement Vogtle and Sumner have come down and given
6 you their Chapter 13 briefs again following the
7 guidance, the Regulatory Guide or 0809, and you'll
8 see, I believe, South Texas the week after next.

9 And what you'll hear in these
10 presentations is that they submitted the plan that was
11 part of either Reg Guide 5.71.

12 PARTICIPANT: That's about all they said,
13 though, the submitted the plan.

14 PARTICIPANT: And that's where we are in
15 licensing. And we will speak to the inspection
16 program but again, I want to emphasize program look.

17 PARTICIPANT: And the last slide, recent
18 staff action. In October, 2010 --

19 CHAIRMAN BROWN: Don't forget to, I keep
20 forgetting to identify myself. Let's keep myself
21 honest as well as you guys.

22 MR. ERLANGER: Craig Erlanger, NSIR.
23 Slide Number 9, please. Recent policy development.
24 In October, 2010, the Commission clarified it's
25 position on cyber security regulations for nuclear

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 power plants versus those cyber security requirements
2 imposed by the Federal Energy Regulatory Commission
3 for Reliable Electric Power Generation.

4 On November 21, 2010, the staff provided
5 information in response to the Commission SRM on this
6 subject. The staff in this information paper
7 discussed how they would need to revise the regulatory
8 framework, cyber security regulatory framework.

9 I mention this today because the staff
10 will be updating Reg Guide 5.71, this is one of the
11 things we committed to in the info paper to reflect
12 the Commission's decision.

13 So why I'm mentioning that is upon the
14 completion of the updates the staff intends to send
15 the Reg Guide back to ACRS for a look. It's just the
16 normal process. We're going to go from Rev 0 to Rev
17 1.

18 Incorporate some of the changes that we
19 spoke about in the information paper and go through
20 the normal process of coming back with the Reg Guide.

21 Additionally, the industry representatives have
22 indicated they were advised of the cyber security Plan
23 template and the guide that's contained in 0809,
24 Revision 6.

25 I'd like to highlight your previous

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 question that the NRC staff has not endorsed any 0809
2 Revision 6. And I'm going to emphasize Revision 6,
3 and not to give all the history unless you'd like it,
4 that there were some challenges with the initial
5 industry document that was created, but we worked
6 through them.

7 There was over, if we had accepted the
8 first Revision, we would have had over 140 plus
9 generic issues on it. It's just a, the realities of a
10 new program we're working through, so we ended up with
11 Revision 6.

12 There is a bit of history on the time line
13 on how come we didn't get the document down here in
14 time for endorsement. And I'll paint a picture on a
15 macro level and can peel back as much as you'd like me
16 to do.

17 We sped up the Part 73 rulemaking, a
18 conscious decision made by the Commission. Due in
19 part to the effect it would have on the nuclear
20 renaissance. At the time a decision was made that you
21 would not license a plant under security orders.

22 As a result, we had to speed up the
23 rulemaking. That came at a price, to be quite honest
24 and that price was getting the rule out there, but not
25 the Regulatory Guides which we've been as Tier 1 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 the same time.

2 Traditionally when we do rulemakings we
3 like to get the guidance documents out there at the
4 same time. So as a result, the rule required by
5 November 23, 2009, that licensee submitted a cyber
6 security plan and propose implementation schedule.

7 January of that year, ACRS approves
8 Regulatory Guide 5.71. So there were challenges with
9 finalized guidance out there. Fast forward to the
10 spring and the NEI 08-09, Revision 6.

11 And what I will mention and it's
12 obviously, as you've seen the document, they're based
13 upon the same methodology, same approach, same
14 security controls.

15 In essence, they are virtually identical
16 documents. There's drivers why, in many programs
17 industry creates their own industry documents or
18 guidance for their licensees.

19 We're getting to a point where we will,
20 yes sir.

21 CHAIRMAN BROWN: Can I, I just want to
22 make sure, should we pause while we get the reporter
23 set?

24 (Asides.)

25 PARTICIPANT: So we haven't gotten to a

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 point yet where we have endorsed as a staff 0809,
2 Revision 6. You are correct, Mr. Correia signed out a
3 letter that said acceptable for use, pending formal
4 endorsement.

5 Again, this added greatly to the
6 consistency of the licensing reviews. We did go
7 through the document, 0809, Rev 6, with NRR, NRO,
8 found it acceptable in the interim to get something in
9 so we can continue the licensing process, but we have
10 not endorsed that document.

11 But I will tell you they are very similar
12 documents, same security controls, same approach, same
13 methodology. So, at some point you will see that
14 document as well.

15 CHAIRMAN BROWN: Why do you need both
16 them, if their both the same?

17 PARTICIPANT: I think that's a question
18 you can ask the industry representatives this
19 afternoon, and I mean that sincerely. We came up with
20 our Regulatory Guide to explain what we were looking
21 for, based upon our requirement.

22 Again, if you look at the title of what
23 Reg Guide 5.71 is, it's for nuclear facilities. We
24 took a broader, so a lot of the nuances and the
25 language change hone into the power reactor community.

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 I'm not trying to speak for them, I'm
2 sure they'll address why they --

3 CHAIRMAN BROWN: So you're saying there's
4 a little bit of narrowing down in 0809.

5 PARTICIPANT: Some of the word choices in
6 there that could make it a bit more germane to just --

7 CHAIRMAN BROWN: Well 5.71 is very
8 extensive.

9 PARTICIPANT: It has the same security
10 controls, same approach, same methodology. And,
11 again, as complement to the cyber security Task Force
12 on the industry side.

13 These were shared, a shared process we
14 went through in hammering out what security controls
15 applied to the nuclear sector. What a program, if we
16 didn't involve them from Day 1, it would be very hard
17 to implement a program without knowing what we were
18 looking for, if that makes sense.

19 MEMBER SIEBER: This Member Sieber. Your
20 Reg Guide 5.71, as it now stands does not refer to or
21 incorporate some of the insights from the NIST 853.
22 Is there a reason why you didn't reference that?

23 PARTICIPANT: Well, I guess I would have
24 to, so we did rely on NIST 853, as well as NIST 882,
25 for parts of it. And will update the 5.71, and an

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 update to 0809, at some point in the future.

2 What I would like to say, though, is
3 consistent with how we normally do rulemakings, we've
4 got to get a little bit of inspection time and monitor
5 the effectiveness of 73.54, through (inaudible).

6 Again, we're still in licensing, we're
7 going to have a program, we're going to see what was
8 good in the rulemaking, what areas for improvement.
9 If we're noticing any trending, if we need to tell our
10 guys the normal life cycle of the program.

11 So it's a new requirement and we just need
12 to get a bit of run time as well. And that will
13 further dictate whether our guidance was doing what we
14 intended it to do or if there's room for improvement.

15 And being a Rev Zero document as, you at
16 1.152 in Revision 3, I'm sure we'll go through a
17 couple of Revs to get it to be, it will constantly
18 improve.

19 The last thing I will mention is on the
20 cyber security Oversight Inspection Program. We know
21 this is of interest to the members. Following Mr.
22 Lee's presentation, Mr. Ralph Costello, of our
23 Division of security Operations, will give you an
24 update on where we are regarding to the inspection and
25 the oversight 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 This is my last slide. I can take
2 questions now. A lot of your comments, I will tell
3 you, are addressed through Mr. Lee's, but I can,
4 whatever you'd like to -

5 MEMBER STETKAR: Craig, this is John
6 Stetkar. You said that there is a planned update of
7 Reg Guide 5.71, sometime in the future. Could you
8 give us an idea of when in the future? Are we talking
9 about the next year, the next decade, the next
10 century?

11 (Laughter.)

12 MEMBER STETKAR: Next week?

13 MR. ERLANGER: A lot sooner than that, but
14 not next week. We made a commitment to the Commission
15 that we would begin updating the Regulatory Guide in
16 Q2 of FY-11, right now, to begin the update.

17 MEMBER STETKAR: Oh, okay. So we're
18 looking at --

19 MR. ERLANGER: We committed --

20 MEMBER STETKAR: -- which one?

21 MR. ERLANGER: Second Quarter of FY-11.
22 So we're wrapping up.

23 MEMBER STETKAR: Will 5.71 --

24 MR. ERLANGER: 5.71. We committed to them
25 to get it done within a year, for the changes. And

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 what we'll do, is we'll make sure we work through,
2 whether it's Christina or whoever else supporting, as
3 we get ready to, we'll make sure you have all the
4 information, redlined, strikeout, etcetera.

5 MEMBER STETKAR: This is something you're
6 gearing up --

7 MR. ERLANGER: Most definitely.

8 MEMBER STETKAR: -- even as we speak right
9 now?

10 MR. ERLANGER: Most definitely. And
11 there's a lot of editorial things we've picked up in
12 the document, we could have done better. Areas for
13 improvement and clarification, but we're in the, you
14 know, we're getting through the licensing in the
15 coming months and then our focus really shifts back
16 again to the infrastructure items.

17 DR. HECHT: Aren't we in Q2 of FY-11?

18 MR. ERLANGER: It started already. We
19 started right now updating it and we have one year
20 from now to, that's what we committed to our
21 Commission to do it.

22 CHAIRMAN BROWN: It's FY-11.

23 MEMBER STETKAR: FY-2011.

24 CHAIRMAN BROWN: Yes, I missed the nuance
25 there.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. ERLANGER: Oh, I'm sorry, so already
2 got updates.

3 MEMBER STETKAR: we're within one month of
4 the end of, Q2, FY-11.

5 MR. ERLANGER: So we committed to the
6 Commission to do that next year.

7 MEMBER STETKAR: You're looking early next
8 year to issue this?

9 MR. ERLANGER: And we'll have some more
10 clarity once we get through licensing, what the
11 schedule is looking like. But it is our intent, you
12 know, as per, the Commission was very clear to get
13 that implementation guidance back to you and we will
14 do that.

15 CHAIRMAN BROWN: Next fiscal year. You
16 said early to get it issued, early next year.

17 MEMBER STETKAR: Calendar year.

18 CHAIRMAN BROWN: Now we're switching to
19 calendar year.

20 MR. ERLANGER: It ends up in 2012.

21 CHAIRMAN BROWN: Okay.

22 MR. ERLANGER: And I'll be turning it over
23 to --

24 CHAIRMAN BROWN: Just ask me.

25 MEMBER STETKAR: Member Stetkar.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. ERLANGER: Do you want to take a break
2 now, Charlie? We didn't have one scheduled, but if --

3 CHAIRMAN BROWN: No, I did not see a
4 scheduled break. About how long do you anticipate
5 your --

6 MEMBER STETKAR: Two minutes.

7 CHAIRMAN BROWN: Because you all were
8 supposed to be finished.

9 (Laughter.)

10 CHAIRMAN BROWN: You all were supposed to
11 be finished at 10:00. We have five minutes. So my
12 question --

13 MR. JACKSON: I think we talked to a lot
14 of the information that I was going to cover. So it
15 shouldn't take me probably no more than ten or 15
16 minutes to cover it.

17 CHAIRMAN BROWN: Is that acceptable?

18 MR. JACKSON: It depends on questions.

19 CHAIRMAN BROWN: Oh, I was looking to
20 break when we finished right here, so thank you.

21 MR. JACKSON: Okay.

22 CHAIRMAN BROWN: All right?

23 MR. JACKSON: All right, so my name is
24 Terry Jackson, I'm the Branch Chief in the Office of
25 New Reactors for Instrumentation Controls and

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 Electrical Engineering Branch Number 1.

2 And Craig covered the cyber security
3 Regulatory frame work. And so what I'll do now is I
4 will provide an overview of the Digital System Safety
5 Regulatory frame work as it interfaces with cyber
6 security.

7 In the following slides, I'll also discuss
8 the technical aspects of the Digital Safety and cyber
9 security reviews.

10 There's two presentations that will follow
11 this and they will go into more detail on the items I
12 present. Craig mentioned the ones that Eric Lee will
13 present and there's also one before that which Tim
14 Mossman and Deanna Zhang will provide for Reg Guide
15 1.152.

16 One of the goals of a Digital System
17 Safety Review is to ensure that the Digital Safety
18 System reliability, availability and integrity remains
19 in the presence of non-malicious events.

20 I want to emphasize that I&C reviews under
21 10 CFR, Part 50 and 52, focus on safety systems,
22 whereas 10 CFR 73.54, is broader in scope to include
23 safety systems, security systems, and emergency
24 preparedness systems.

25 So to your question that you had raised

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 earlier on one of the reasons why we didn't just add
2 the guidance in the Reg Guide 1.152, is because that
3 scope is for safety systems, whereas the scope of Reg
4 Guide 5.71, is broader to include other systems, as
5 well.

6 MEMBER STETKAR: I think I understand a
7 bit of that, Terry, John Stetkar, again. Let me just
8 ask a probably naive question and you may get to this
9 later.

10 Who physically in the NRC Staff performs
11 the safety reviews under 1.152? Is it people in NRO,
12 NRR?

13 MR. JACKSON: Yes, the folks at my branch
14 and the branch.

15 MEMBER STETKAR: And who performs the
16 reviews under 5.71, is that all NSIR?

17 MR. JACKSON: NSIR.

18 MEMBER STETKAR: And there's no, you don't
19 all sit together in a single room and do those reviews
20 of a given design?

21 MR. JACKSON: We do coordinate with each
22 other and there's some examples during, for example,
23 the new reactor reviews. Where, if we see, as we're
24 doing our safety review and we see particular aspects
25 that we think, well, this could be a challenge from a

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 cyber security standpoint.

2 We have used our, we call them Design
3 Center --

4 MR. ERLANGER: DCWGs.

5 MR. JACKSON: Yes, DCW, Design Center
6 Working Groups, where we bring in the vendor, the
7 combined license applicants, and NSIR and ourselves
8 and we say this is what we see, while we're doing the
9 review.

10 And we ask the vendor and the applicants,
11 how are you guys going to deal with this in cyber
12 security space. So we've done that on occasions.

13 MEMBER STETKAR: On occasions. But I
14 guess I'd be interested to understand how that process
15 really works. Because this, you may have gathered
16 from the earlier question, I'm interested in
17 understanding how this sort of integrated perspective
18 is implemented.

19 I understand, eventually you have a design
20 in the plant and once it's up and running, the
21 inspection process, make sure that it meets all of the
22 rules. But from a design review, and I'll use a new
23 reactor as a good example, because it's a clean slate.

24 I'm interested in understanding how that
25 integrated perspective is actually implemented.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 Because you've mentioned a couple of times that, in
2 deed, there is some sort of integration.

3 So, perhaps later, as you get into more of
4 the detailed discussion, we can hear a bit about that.

5 MR. JACKSON: That's on one part of that.

6 I think if you're looking for a formal process
7 whereby there's kind of like an SRP Guidance or
8 something that says there's particular coordination
9 among the folks.

10 We don't have that type of formal
11 guidance. But, on the other hand, for example, when
12 Reg Guide 5.71, was being developed, the folks in NRR
13 and NRO participated and supported NSIR in the
14 development of that guidance.

15 As well as when we modified Reg Guide
16 1.152, NSIR also came along and provided assistance
17 there. There's some other aspects within the agency
18 for example, there is a cyber security Assessment
19 Team, which is related to the instant response
20 functions for the agency.

21 And so that team is made up of individuals
22 from different offices in the agency to address any
23 kind of ongoing cyber security concerns that come up -
24 -

25 MEMBER STETKAR: I understand, but that's

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 sort of in process.

2 MR. JACKSON: Right.

3 MEMBER STETKAR: I'm talking about
4 stepping way back to the design reviews.

5 MR. ERLANGER: And just to add on here,
6 one of the things, going back tot he program approach
7 that, that the, I won't say the challenge, the reality
8 of what we're doing is that I hate to say independent
9 design, because there's not.

10 There are things you consider during
11 design, but regardless of what the system is, you
12 still need to meet the requirements of 73.54. So when
13 we're doing a individual safety system, there's the
14 overall looming big ticket items like following a
15 process to identify your digital assets.

16 Applying the security controls. Selecting
17 a team that's independent of management so you can
18 make decisions. These larger program issues, which
19 complements what's being done in 1.152 Rev 3 space.

20 So it's a, it was, very much, but the
21 communication, you know, as we get to, you know, we'll
22 call them those transition systems until everyone is
23 caught up. We are aware, we are talking about it.

24 We're talking about Ocone, we talked
25 about it last week. There are groups there, but the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 Inspection Division over in NRR. You know, how do you
2 do this? These meetings are ongoing, so we are
3 cognizant of this challenging period in between where
4 we need to do a bunch of --

5 MEMBER STETKAR: Stetkar again. Are we
6 online yet?

7 COURT REPORTER: Yes, sir.

8 MEMBER STETKAR: Okay.

9 (Laughter.)

10 MEMBER STETKAR: I hate saying my name
11 because I, you know. Occasionally I mispronounce it
12 myself.

13 (Laughter.)

14 MEMBER STETKAR: The only reason I asked
15 is part of the continuing concern. You mentioned that
16 sometime in the next year you'll be updating Reg Guide
17 5.71, and any associated SRP section.

18 I was curious whether there was any move
19 afoot to formalize that integration. In other words,
20 if you are updating the SRP at least, in the near
21 future, from the security aspect, it would see like an
22 opportunity to at least, in that section of the SRP,
23 put the hooks back into the safety side and we'll
24 eventually get to a plan for updating 1.152, and its
25 associated sections of the SRP.

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 put those formal hooks in there.
2 Because, as you mentioned, there is, there is no
3 formal requirement right now.

4 CHAIRMAN BROWN: Let me amplify that, from
5 the hooks standpoint. I guess one of the things I
6 would have expected in earlier conversations, during
7 the licensing part of it, that when you finished your
8 safety review or in the process of it, you would then
9 have, okay, we're done.

10 Then have NSIR, would have said, okay,
11 yes, we've looked at this also, and there's a
12 framework there within which we will be able to
13 operate.

14 In other words, you have a sign off that's
15 kind of a more formal way, as opposed to just saying
16 we talked. And that's, that's the world I came out
17 of.

18 I mean while I owned the I&C and all the
19 electrical stuff, the reactor guys were always leaping
20 on my body, as well as the, you know, folks that owned
21 other critical components.

22 And it's not like you can't identify, you
23 know, what are critical digital assets going to be?
24 Have those been laid out? And so that you know, when
25 you make that handoff in transition, that 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 people at the next level that they're going to, to
2 this transition space, that you're set up to do that.

3 And, you know, that's what I've gotten out
4 of the earlier conversations. You said it, I think,
5 fairly clearly, there's no formal process, but you
6 talk.

7 And, you know, that's, to me, that's a
8 little bit too informal. Now, I'm not telling NRC how
9 to run their business, it's just that that's cause for
10 concern that we're going to get a transition that's
11 not as crisp and that we don't have what we need when
12 we get to the other space. You were raising your
13 hand?

14 MR. CORREIA: Yes, this is Rich Correia
15 from NSIR. You hit on a very timely topic. We
16 discussed that recently at Office Director level, and
17 it was recognized that we do need a formal process,
18 right now.

19 Not next year, right now, as we transition
20 into licensing of cyber security Plans. We have
21 Diablo Canyon coming in for an upgrade. We want to
22 integrate this cyber security and Safety Review
23 Processes together formally.

24 To, as you said, put the hooks in it to
25 make sure it happens. And then eventually get into

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 the SRP update. And I think --

2 CHAIRMAN BROWN: Is there a, when you say
3 now, I like those words. What does now, when you say
4 now, what does that mean? Next week, next month?

5 MR. ERLANGER: I can speak to it. We met
6 literally last week with the Office Directors. The
7 Staff immediately following that, between NRO and
8 NSIR, we were talking more on the new reactor site
9 for that particular example.

10 But we're very aware of the interim issues
11 we, and I don't want to make, say a Oconee is an
12 issue, but that's just an example of we need to pay
13 attention to it.

14 So these are a finite number of mods and
15 things going on that we are aware and when we say
16 we're talking is, you know, things that hit that 50.59
17 threshold, we're aware and we're working through those
18 problems.

19 What Rich is referring to would be, would
20 coincide with the updates we're doing to formalize.
21 And whether it's in the Reg Guide or the SRP or a
22 separate document, a procedure on how to communicate
23 formally, what we're doing, we're discussing that now.

24 But what I'd like to leave you with a
25 thought is that we are aware that we're in a

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 transition period between, which a new program out
2 there, new requirement, an updated to Rev 3, and we're
3 not ignoring and we know what things were licensed
4 under when and paying attention. So it's, by real
5 time we're working through the process. I don't think
6 I can give an end date when it's finalized, right now.

7 CHAIRMAN BROWN: You can see where we've
8 said this about six times now, or something like that.

9 So you can see where our concern is relative to the
10 integration and the hooks between the two groups that
11 make sure everything is done and there's always going
12 to be a loose end somewhere, you never catch
13 everything.

14 But at least you'd only have dozens of
15 them.

16 MR. KEMPER: Well, this is Bill Kemper.
17 Just, hopefully I can ease your minds a little bit,
18 since we talked about Ocone several times. And I
19 realize we're transitioning the guidance for cyber
20 security.

21 But when we wrote the Safety Evaluation to
22 approve the RPS and SFAS upgrade, we identified, you
23 know, we approved specifically many design strategies
24 aimed at dealing with cyber security.

25 We also identified specific inspection

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 items for Region 2, to pick up on once that system is
2 actually installed. So the handoff or the passing of
3 the baton, if you will, went from NRR Licensing to the
4 Inspection Forces for that particular system.

5 So all those items are very specifically
6 identified in the Safety Evaluation and those have
7 been transmitted to Region 2.

8 I've personally talked with a Branch Chief
9 down there in the inspection group several times over
10 this. And so they're developing their plans to go
11 ahead and do a site-specific inspection.

12 So I expect something akin to that will be
13 carried forward.

14 CHAIRMAN BROWN: But, bear in mind, again,
15 to bring up Jack's point, you're asking Inspectors now
16 where, how do you ensure that expertise is brought in
17 from here, Headquarters, who are actually think about
18 and issuing these guidances.

19 Because the Inspectors are going to be,
20 you've got to train a whole set of, you know,
21 microprocessor-based Inspectors that know all these
22 nuances. That's tough to do.

23 MR. ERLANGER: Well, it's ongoing right
24 now, sir. And they're the same people.

25 MR. KEMPER: For Oconee, for example,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 we've already sent members of NRR Staff down to work
2 with the Inspection Force as they started doing that
3 inspection. To serve as technical consultants and
4 assisting the inspection themselves.

5 So Headquarters is clearly positioned to
6 work with the Regions are appropriate, to provide the
7 expertise needed to execute those inspections.

8 MR. ERLANGER: And what Mr. Costello will
9 speak to you is that the Digital I&C Staff in the
10 Regions, will also be the core of the cyber security
11 Inspection Team.

12 So we're dealing with the same folks who
13 were looking at, and what you'll see in the industry
14 presentations as well, is that the Digital I&C
15 Communities and Cyber Communities are very much one in
16 the same.

17 With the people and they're integrated and
18 talking. So, from the NRC perspective, the Inspectors
19 that are, the Digital I&C Inspectors are also the
20 Cyber Inspectors are a core element of those teams out
21 there. And Ralph will speak to that in his
22 presentation.

23 CHAIRMAN BROWN: Okay, John, do you have
24 anything else on that?

25 MEMBER STETKAR: No.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 CHAIRMAN BROWN: Okay, go ahead Terry.

2 MR. JACKSON: Okay, I was going to say
3 that, we talked about the coordination between Safety
4 and cyber security Reviews, and I think the revision
5 to Reg Guide 1.152, Revision 3, is actually the first
6 step in that direction. Because part of it is
7 identifying who has responsibility for what parts that
8 they're going to look at.

9 And that was the first question we had
10 when we began interfacing with Reg Guide 5.71. And we
11 said, okay, we'll have to clearly define who has what
12 responsibility in what areas.

13 So that's a first step, I think, that
14 needs to be taken. And then as we see where there's
15 need for other coordination we'll put those in there.

16 MEMBER STETKAR: Terry, that's a little
17 different perspective than I had when I read Rev 3, of
18 1.152, because I looked at Rev 3, relative to Rev 2,
19 as, it might more clearly define the responsibilities,
20 but it seems to more clearly endorse the fact that
21 they're not integrated.

22 CHAIRMAN BROWN: I think that was very
23 clear.

24 MR. JACKSON: Yes, the regulatory line is
25 what we're trying --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MEMBER STETKAR: Go on, I don't want to
2 hold you up.

3 CHAIRMAN BROWN: No, we don't, okay, thank
4 you.

5 MEMBER STETKAR: It was just a comment.

6 CHAIRMAN BROWN: But the observation is
7 correct. I mean it was very, very clear in Rev 3, in
8 terms of the separation of church and state, okay.
9 And that's not meant to be a political statement, it's
10 just an analogy, okay.

11 MEMBER SIEBER: But I thought that's what
12 they were trying to do.

13 CHAIRMAN BROWN: Yes, that's what we got
14 out of that.

15 MEMBER STETKAR: It's the intent.

16 CHAIRMAN BROWN: I'm going to pony up to
17 Rich's comments, and they, it's recognized that you
18 need a formal set of hooks here to connect these,
19 connect these two sections together, and make sure you
20 get it, so there's a crossover.

21 You have a before licensing is granted,
22 you know where you're going. I mean that's
23 fundamentally the point.

24 You don't have to have it all defined, but
25 you know where you're going and what 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 MR. JACKSON: All right. Now I mentioned
2 non-malicious events and those are events where there
3 is no intent to impact the Digital Safety System.
4 These events may include human error in design,
5 operation, maintenance.

6 It could be equipment failure, or it could
7 be environmental impacts to digital equipment. Human
8 error certainly receives the most attention in Reg
9 Guide 1.152, Rev 3, in the regulatory positions.

10 Also, the synergistic effects of these
11 events could cause unexpected failures in digital
12 systems as well.

13 security controls for a digital safety
14 system may or may not be part of the safety system.
15 If a security control is part of a safety system, the
16 adequacy of that control to thwart a malicious attack
17 is covered under Part 73.

18 Now the I&C Staff performed its safety
19 review will ensure that the security control does not
20 adversely affect the digit safety system's
21 reliability, availability and integrity.

22 And that the security control is developed
23 under a high quality process. So, basically what
24 we're saying is, and I've got an example here where,
25 let's say an applicant includes an encryption feature

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 a digital safety system.

2 The I&C Staff would ensure that that
3 encryption feature does not adversely impact the
4 safety system's ability to perform its safety
5 functions.

6 So, that part of that is that that code
7 would have to be developed under a high quality
8 process and that would be part of our inspection and
9 all the activities.

10 But we wouldn't come out and say, well,
11 that encryption feature is adequate for cyber security
12 protection, we would just say, well, that feature is
13 there, it's developed under a high quality process as
14 part of the safety system, and that there's assurance
15 that it won't impact the overall safety function of
16 the safety system.

17 But later on, it would be NSIR, in their
18 cyber security program, that would look at that
19 encryption feature and say is that adequate for a
20 cyber security control.

21 Because, the concern is, is we may look at
22 it in the licensing world and say, yes, that's good
23 and it may be true for today. But tomorrow, there may
24 be a new threat and that encryption feature may not be
25 adequate.

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 they would have to then address the
2 system.

3 CHAIRMAN BROWN: But then now what
4 happens? They haven't blessed it. Now later you come
5 along and now you've got to rewrite the software to
6 modify the encryption feature. That just doesn't make
7 any sense.

8 MR. ERLANGER: So you mentioned that this
9 all needs to be resolved prior to licensing being
10 completed. I would respectfully say it doesn't,
11 because we're doing, the program commitments to these
12 controls is independent of the system, it's
13 independent of the design.

14 We're not, when you look at the security
15 controls, we're not to the level of detail where we're
16 espousing the use of a certain type of encryption. It
17 will be as high level as you need encryption.

18 We're not going to get so, to get the
19 licensing and program level done, these are, I firmly,
20 100 percent agree with Rich, I work for Rich, so I
21 definitely should agree with him.

22 (Laughter.)

23 MR. ERLANGER: We need to work on a formal
24 handoff for whether it's an office procedure or what
25 not. But these are items that may not translate to a

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 need in program-focused licensing, what we're doing
2 for cyber.

3 The controls are very, I hate to say, high
4 level, but they're not saying use this company's data
5 diode. It's not saying use this type of software.

6 It's the commitment to look at those
7 things, to have deterministic devices to ensure you
8 have encryption. To ensure you have a firewall. To
9 ensure you protect portable media.

10 So we're doing, what we're doing, again,
11 is very program-focused. And I know that's a
12 discussion we're going to get throughout the day and
13 may talk about, but that's how we approached it.

14 MEMBER STETKAR: Let me ask, since Terry
15 dug the hole, I'm not going to let you two out of it.

16 The way I understood it is Terry said that during the
17 Safety System Design Review, they will evaluate.

18 Suppose somebody did present a design,
19 with enough detail, in that the NRR, NRO folks, during
20 their review, look at the details of the encryption
21 software and assured themselves that in deed there was
22 nothing there that would adversely affect safety
23 system performance.

24 Then he said the process then continues,
25 that eventually someone somewhere will look at 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 encryption feature and determine that in deed it is
2 adequate to provide the type of cyber security
3 requirements that you require.

4 Suppose that someone somewhere determines
5 that that particular encryption feature is not
6 adequate to provide the cyber security protection that
7 you need.

8 Somebody eventually, somewhere, although
9 you say the program is at a very high level. I'm
10 assuming somewhere, somebody actually looks at that
11 design.

12 Whether it's an Inspector or whoever does
13 that. They determine it's not adequate. So somebody
14 needs now to change the software to meet the security
15 requirements and they do that.

16 Who then looks at it again to make sure
17 that the revised software still has no adverse impact
18 on safety. Where does it get thrown back in?

19 MR. JACKSON: Okay, so let's say, for
20 example, the scenario where they have a, we call it
21 built-in security feature into the safety system.

22 And then later on it's determined that
23 this feature for changing the threat environment is no
24 longer adequate. And so the licensee then has choices
25 it can make.

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 It can either try to apply some control
2 outside of the system, to compensate for it, and that
3 might be one option. So, you won't necessarily have
4 to change the safety system itself.

5 Or, they could say we can go in and we can
6 change the safety system itself. Now in that case,
7 they would do the changes that they need for cyber
8 security, but from a safety standpoint sense, then
9 they've got to look at the change process 50.59 and
10 determine, well, do I need, can I do it under 50.59,
11 do I need to acquire staff approval to make that
12 change?

13 MEMBER STETKAR: I understand.

14 MR. ERLANGER: And to complement the
15 50.54P plan changes for effectiveness. If they
16 decrease the, change the effectiveness of the program
17 that leads to a decrease, that would also trigger
18 another --

19 MEMBER STETKAR: Yes, I'm talking about
20 something that identifies as an inadequacy that is
21 then repaired from one perspective.

22 MR. JACKSON: So it is kind of, I guess,
23 prudent for the industry to think about, you know, the
24 cyber security controls and how flexible they are, as
25 well.

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 Because the threats can change and I'm
2 sure that's something they keep in their mind.

3 MEMBER STETKAR: Well, the threats going
4 to always change. I mean, you know, we're dealing in
5 that environment, but I'm talking about some more
6 fundamental, as Charlie likes to talk, architecture or
7 both hardware and software architecture to address
8 both issues.

9 MR. JACKSON: All right, Revision 2, as
10 Bill had mentioned, Revision 2 of Reg Guide 1.152,
11 contain criteria associated with cyber security. The
12 main thing, consistency with Part 73, the cyber
13 security portions are being transferred to Reg Guide
14 5.71. Reg Guide 1.152, will continue to address non-
15 malicious events.

16 And we felt the revisions necessary for
17 Reg Guide 1.152, to establish a clear regulatory
18 framework with regards to digital safety system and
19 cyber security licensing.

20 And we felt that Revision 3 of the Reg
21 Guide 1.152, supports the regulatory framework that's
22 been described. So, next slide there.

23 Okay, the following is an overview of Reg
24 Guide 1.152, Revision 3, and the next presentation
25 will go into more detail on the changes made. The

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 draft of Reg Guide 1.152, Revision 3, which was also
2 DG-1249, which issued for public comment last summer.

3 And those public comments have been
4 received and responded to. Core changes to Revision
5 3, of the Reg Guide include, the cyber security is now
6 under the domain of Part 73.

7 Thus, all references to cyber security
8 malicious actions or attacks are migrated to Reg Guide
9 5.71. Within the safety review, one of our core
10 requirements is 10 CFR 50.55-AH, which endorses IEEE
11 603 and IEEE 603 security focus of Reg Guide 1.152, is
12 being reemphasized.

13 So, for example, inadvertent actions by
14 operators should not lead to inappropriate access,
15 such that the digital safety system reliability,
16 integrity or functionality is impacted.

17 And that has to do with Clause 5.9 in IEEE
18 603. Also, undesirable behavior or communications by
19 connected systems, should not lead to a degradation in
20 digital safety system liability, integrity or
21 functionality.

22 And that is associated with Clause 5.6 in
23 IEEE 603. And then, furthermore, the development
24 environment for both the application software and the
25 platform software, should be controlled and protected

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 against inclusion of unwanted, unneeded and undesired
2 code.

3 And, in addition, as will be discussed in
4 the subsequent presentation, certain regulatory
5 positions were removed from Revision 2. And those
6 were associated with the installation, operations,
7 maintenance and retirement, which are more operational
8 aspects that are better addressed in Reg Guide 5.71.

9 Okay, the next slide. So I've discussed
10 Reg Guide 1.152, Rev 3, from the regulatory framework
11 perspective, where the staff is making a clear
12 distinction between the cyber security and safety
13 review responsibilities.

14 And I'll now talk about the technical
15 aspects of Reg Guide 1.152, Rev 3.

16 DR. HECHT: Can I ask a question about
17 1.152, Rev 3?

18 MR. JACKSON: Yes.

19 DR. HECHT: It didn't only eliminate the
20 references that you described on the previous slide,
21 it also eliminated the steps in the later part of the
22 life cycle, most importantly related to installation,
23 operation and, I guess, disposal isn't a concern, but
24 who knows.

25 And aren't there aspects of safety and,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 which do, and of security, that intersection which are
2 affected by installation.

3 And those, somehow or another, need to be
4 considered prior to the inspections.

5 MR. JACKSON: They are, and certainly, you
6 know, the installation, operation, maintenance and
7 everything can impact the safety as well as the cyber
8 security.

9 In our License Reviews we're looking at
10 the design aspects of the system, primarily. And then
11 our regional folks, who are doing the inspections and
12 so forth, are the ones who are carrying pretty much,
13 you know, the weight of ensuring that the
14 installation, the operations and the maintenance and
15 stuff is being carried out according to, you know, the
16 criteria that's set out in the regulations.

17 MR. ERLANGER: I just add that any, one of
18 the questions we thought we were going to have --

19 CHAIRMAN BROWN: Are you satisfied with
20 that answer?

21 DR. HECHT: I think I just heard, I just
22 heard the question come back.

23 MR. ERLANGER: Anything that's missing
24 from 1.152, Rev 2 from Rev 3, that was one of the
25 questions we asked ourselves.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 A great question would be, well where did
2 it go? And what we hope to clarify in the next two
3 presentations, are elements that were removed from Rev
4 2 to Rev3, how they are either taken care of by the
5 new regulation or where they're located in Rev 3.

6 So, I believe in the next two
7 presentations we will answer your question about where
8 all those elements went. If we did not, we can
9 definitely get, I feel comfortable that it will be in
10 Mr. Lee's slides, that we'll talk about.

11 MEMBER STETKAR: They didn't disappear.

12 CHAIRMAN BROWN: Okay. Is that okay?

13 DR. HECHT: For now.

14 CHAIRMAN BROWN: Okay. Let's go ahead and
15 roll. I want to get us to that break here, that I
16 promised 25 minutes ago.

17 MEMBER STETKAR: You run a tight ship,
18 Charlie.

19 CHAIRMAN BROWN: Yes, very, very tight.

20 MR. JACKSON: So what I wanted to show is
21 that there is some technical overlap between the
22 Safety Review and the cyber security Review.

23 First, many of the design features are
24 practiced addressing non-malicious events, could be
25 used by licensees to address malicious events, as

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 well.

2 For example, in the area of data
3 communications independence, which we mentioned
4 earlier. As a particular example, if an applicant has
5 no data communications or they have uni-directional
6 data communication between divisions or between safety
7 and non-safety systems, the principle of independence
8 provides a basis for reliable operation in the event
9 of a latent software error, component failure or human
10 error, which all these are non-malicious events.

11 However, restricted data communications to
12 ensure reliable operation also provides an inherent
13 benefit to cyber security, as well as it eliminates
14 the pathway for an attack to the safety division.

15 Therefore, there is inherent benefits in
16 cyber security from the secure development and
17 operational environment that reviewed this
18 performance.

19 It's not something that we intentionally
20 go out and say, well, is this providing a cyber
21 security benefit, but it's just inherently by things,
22 like you said --

23 CHAIRMAN BROWN: We're just saying they're
24 complementary, one gives to the other.

25 MR. JACKSON: Yes.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 DR. HECHT: Terry, can I ask a question?
2 With respect to what the cyber security world is
3 worried about, you know, MITRE has an inventory of
4 common vulnerabilities and common weaknesses, and
5 there are various code-scanning static analyzers and
6 other analyzers to look for those in code.

7 With those, given the fact that 5.71 or
8 NSIRs seems to be involved primarily at the back end.

9 And these would be involved at the front end. How
10 does that, how does anything like that happen or does
11 that happen or is that accounted for?

12 MR. ERLANGER: Well, 5.71, does speak to
13 those issues and it just, it, regardless of where it
14 falls in the process, these are requirements that
15 applicants and licensees need to meet.

16 So what I'm saying is that it might, you
17 have to meet it. Where it falls out in the Licensing
18 Review, you can argue that there'll be a system that's
19 in process today that we're reviewing, that was looked
20 at under old guidance.

21 They still need to meet the requirements
22 set forth in 73.54 and the associated guidance.
23 Because we have that license condition as a hook.

24 So, yes, if we looked at things on the
25 front, they have to look at it on the front end. They

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 have to, and at the end of the day, they have to meet
2 the requirement.

3 So, it's just a function of how the
4 regulations are organized but that particular example
5 you referenced is covered in 5.71. And the gentlemen
6 are nodding emphatically back there.

7 So they will speak to it. But they can
8 speak to it in detail, but we do consider it and,
9 again, a licensee or applicant needs to meet the
10 totality of the regulations.

11 DR. HECHT: So does that mean that NSIR
12 goes with the NRO people to Westinghouse and says in
13 addition to having done your static analysis for
14 safety, that you've also done your static analysis and
15 make sure there are no buffer overflows or something
16 like that?

17 MR. ERLANGER: Well, if it's something
18 like --

19 MR. JACKSON: For example, if it's
20 something like buffer overflows, I think that would be
21 a safety concern as well. So, when we were looking at
22 a lot of these, you see a lot of the potential
23 vulnerabilities and stuff or the effects of these
24 vulnerabilities are similar.

25 Whether you're looking at it from a non-

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 malicious sense or from a malicious sense. So I think
2 there's a lot of technical area that's covered by the
3 safety review but we don't have plans where NSIR is
4 doing a cyber security look at the system at the same
5 time that we're maybe inspecting the I&C system.

6 DR. HECHT: Well, if you don't have the
7 plans for that simultaneous inspection, does that
8 relate to the integration or the need for integration
9 that was spoken about earlier?

10 MR. ERLANGER: I think what we've been
11 trying to convey this morning, is the programmatic
12 look, again. And I know that it's not, it's a
13 different concept. I won't say it's the same concept,
14 that they have to meet those requirements.

15 The requirement for 54 is an operational
16 program that applies to licensees and applicants. We
17 don't control, we are very aware and observant of
18 what's happening in the vendor realm out there, but
19 the testing and going out there, as Mr. Costello will
20 speak to, that's not where the focus of the cyber
21 security Inspection and Oversight is located.

22 The requirement is for licensees and
23 applicants and we believe the operational program is
24 the place where it should be housed. So, you know,
25 again, they have to meet the totality of the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 regulations.

2 And I think both licensees will attest to
3 this in their presentations. Is they need, they are
4 aware and they are considering all these things on the
5 front end, because they know they have to meet both
6 requirements in the end.

7 So the sequencing, I think we'll hear
8 today, is that they're aware of all this stuff. And
9 it's, we don't have, I hate to say, a cyber security
10 vendor front-end-loaded look we're doing on different
11 things.

12 MR. KEMPER: This is Bill Kemper, if I
13 could inject, and I'm sorry. I know you're trying to
14 get to break, but I just --

15 CHAIRMAN BROWN: No, I'm just trying, I'm
16 starting to run, I've been letting things go because
17 it's been some pretty relevant to a lot of the
18 discussion.

19 So we're running over quite a bit on this
20 and I just want to try to get back on a little bit of
21 a time schedule. Go ahead, but be quick.

22 MR. KEMPER: If I could just say, Terry's
23 first bullet here, though, is a very significant
24 statement. The things we're talking about, your
25 example for example.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 That's a reliability issue, as well.
2 Because that falls under the current regulations in
3 Part 50. So we would review that in the Licensing
4 Review of that system.

5 Now, someone could also use that same
6 device, if you will, for malicious attacks against the
7 system. So, there's a considerable amount of overlap
8 here, between what's reviewed in the initial Licensing
9 Review, from a safety and reliability standpoint
10 versus what can and will be used later on, after the
11 fact, to satisfy NSIRs of cyber security criteria.

12 DR. HECHT: That was a bad example. I'll
13 try to give another example. These are access or
14 account control, data rights for various programs,
15 which might not at all have a safety issue, but might
16 have a cyber security aspect to them. Safety issues
17 being primarily that at the very least, every
18 essential program better have the rights it needs to
19 be in the program.

20 But other, how shall I say, lower, less
21 core programs, more peripheral programs, might have
22 lower privileges.

23 Now, it would seem to me that if the
24 safety is primarily or NRR or NRO, let me put it that
25 way, are looking primarily from a safety perspective

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 front end, that NSIR might not get their seat
2 at that table. If I'm making myself clear.

3 MR. ERLANGER: So that would fall in the
4 family of technical security controls. And those are
5 those non-human things, hardware, firmware, software.

6 DR. HECHT: You've said, yes, there's a
7 list here, I mean there's a list there basically
8 saying that these might apply. It doesn't say exactly
9 where, and access control is on this list, I noticed.

10 But how do you know that what's being done
11 in that safety system or could matter factor the non-
12 safety CDA in the design phase, to be sure that it's
13 met. If your guy's focus is at the back end.

14 MR. ERLANGER: Well, I, Eric, do you want
15 to and I can start if you want?

16 DR. HECHT: I'm sorry, maybe I should,
17 should I ask --

18 MR. ERLANGER: No, it's a good --

19 CHAIRMAN BROWN: Let's see if we can ask
20 it when he's up at the table, is that okay? Do you
21 mind?

22 MR. ERLANGER: No, no, that's fine.

23 DR. HECHT: We will have an answer?

24 CHAIRMAN BROWN: I'm going to ask you to
25 kind of churn right on through here. I mean it seems

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 to me that these next two slides, you can kind of do a
2 blast through. They seem to be repetitive to what
3 we've talked about.

4 MR. JACKSON: Okay. So also, most of
5 modifications to Reg Guide, Revision 2, transfer to
6 malicious aspects of Reg Guide 5.71. And the majority
7 of the regulatory position structure and activities
8 remain the same.

9 And then finally from our experience with
10 licensees and applicants, we see that they are
11 addressing cyber security up front in the development
12 stage. And that they're taking credit for some design
13 features and practices that address both malicious and
14 non-malicious events.

15 While regulatory framework has evolved in
16 the past few years, the framework we have today we
17 believe is an improvement because, from a technical
18 standpoint, the Staff is touching on design features
19 and practices to ensure safety and have added benefit
20 of addressing security concerns, as well.

21 Okay, and then the last slide here, this
22 is just --

23 CHAIRMAN BROWN: Oh, I thought you were
24 finished. I thought you were summarizing already.

25 (Laughter.)

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 CHAIRMAN BROWN: Let me skip the
2 summarizing. I think we can read this one, this one
3 is easy.

4 MR. JACKSON: I was going to read it to,
5 but you can read it.

6 CHAIRMAN BROWN: Because it's just
7 repetitive and I don't want this question answered
8 right now, I want it done sometime later.

9 Look at the public comments. There was
10 one in there a couple of times that talked about ISG-
11 01. And there's, where there's 20 items talked about
12 relative to security, cyber security type items.

13 They were not incorporated. You all said
14 no, we don't have to do this. I don't remember, I'd
15 have to go back and look at the reason again.

16 But, I'd like to have an answer to that at
17 some point during this discussion about why, pardon?
18 This afternoon, yes, whatever is appropriate. Was
19 that in there?

20 MR. JACKSON: The next presentation --

21 CHAIRMAN BROWN: Okay, that's fine. I
22 just want to make sure we address that. Thank you.
23 All right, thank you for your patience with the
24 management of the meeting at this point.

25 We will now take a 15 minute break and we

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 reconvene, let's, I take that back. Let's make it ten
2 minutes and we will reconvene, is that okay, subject
3 to the members? At 10:45.

4 (Whereupon, the proceedings went off the record at
5 10:34 a.m. and came back on at
6 10:49 a.m.)

7 CHAIRMAN BROWN: The meeting will come
8 back to order and we'll proceed now with the second
9 set of presentations. I guess that will be Tim
10 Mossman and Deanna Zhang. And this is going to be
11 riveting as I'm sure, as well, correct? You may
12 proceed.

13 MS. ZHANG: Good morning, thank you for
14 this option to discuss our approach for ensuring
15 integrity, availability and reliability in the design
16 and development of Digital Safety Systems.

17 My name is Deanna Zhang and I'm from the
18 Officer of New Reactors, Division of Engineering,
19 Instrumentation and Controls Branch. My colleague
20 here, Tim Mossman, who will be presenting the second
21 portion of our presentation, is from the Office of
22 Nuclear Reactor Regulations, Division of Engineering,
23 Instrumentation and Controls Branch.

24 Before I begin my presentation, Chairman
25 Brown had a question about the comments we've

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 received for Reg Guide 1.152, Revision 3, and I would
2 like to answer that at a high level before we go into
3 more detail with Tim's portion of the presentation.

4 CHAIRMAN BROWN: This is ISG-01?

5 MS. ZHANG: Yes, the comments regarding
6 ISG-01 and cyber security. Specific comments that we
7 received in the Reg Guide comments. And the reason we
8 did not incorporate those comments in, is because a
9 high level, what the comments were, that we had other
10 guidance addressing all these access control
11 independents and cyber security, why do we need this
12 guidance in Reg Guide 1.152, Revision 3.

13 And the reason we did not accept those
14 comments is that we feel that this guidance, Revision
15 3, provides additional clarity and criteria for
16 addressing a secure development and operational
17 environment.

18 And, therefore, we do not feel that we
19 should remove this guidance and just defer to other
20 existing guidance, such as that, those that are in Reg
21 Guide 1.152.

22 CHAIRMAN BROWN: You're saying that 2.1
23 through 2.5, but they're the same as Rev 2. They
24 effectively didn't change.

25 MR. MOSSMAN: They're very close.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MS. ZHANG: Very close.

2 CHAIRMAN BROWN: And ISG-01, came after
3 that.

4 MS. ZHANG: Yes.

5 CHAIRMAN BROWN: I mean Rev 2 was in place
6 before ISG-01 was put in place. And so, you know, I'm
7 talking about the list of 20 items, the do's and
8 don'ts.

9 In other words, here's some guidance that
10 if you do these things you're going to have some
11 trouble. If you don't do them, you won't have as much
12 trouble when you submit them to us, or vice versa, if
13 I said that wrong.

14 MR. MOSSMAN: Are you talking about ISG-01
15 or ISG-04?

16 CHAIRMAN BROWN: I don't know, whichever
17 one does, maybe it's ISG-04, because --

18 MR. MOSSMAN: Oh, yes, yes.

19 MS. ZHANG: Yes, that's the --

20 CHAIRMAN BROWN: I'm sorry, did I say one?
21 I apologize for that.

22 MR. MOSSMAN: Yes, okay, yes.

23 CHAIRMAN BROWN: It's the one with the
24 list of --

25 MR. MOSSMAN: Yes, we'll address both of

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 those, actually kind of, two nuances to what Deanna is
2 saying. Yes, we had a number, in fact, one of our
3 drafts of Rev 3, we actually did reference ISG-4, but
4 per our internal review process, kind of the rules of
5 the road were, it was considered not good practice to
6 reference an Interim Staff Guidance, when a lot of the
7 criteria therein are ultimately destined for more
8 permanent regulatory guides or other documents,
9 industry standards.

10 And so we have, in Section 2.1, Regulatory
11 Position 2.1, we kind of have, I don't have the exact
12 statement in front of me, but we reference other NRC
13 positions and guidance will cover uni-directional and
14 bi-directional communications.

15 That was the statement that replaced our
16 original grant referenced ISG-04, since it was
17 considered not good practice to reference ISG-04.

18 MEMBER STETKAR: Tim, I read that in the
19 responses to the public comments. Could you point me
20 to the other guidance that in deed does that or is
21 that guidance to yet --

22 MR. MOSSMAN: Right now it's ISG-04.

23 MS. ZHANG: ISG-04, the guidance in there
24 has been incorporated in IEEE Standard 74-7432, 2010
25 version, which was issued last summer.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MEMBER STETKAR: Let's wait until Slide
2 17, because I want to follow up on some of this stuff,
3 too.

4 CHAIRMAN BROWN: Okay.

5 MEMBER STETKAR: And there is a slide that
6 addresses upcoming things.

7 CHAIRMAN BROWN: All right.

8 MEMBER STETKAR: Let's wait until that, if
9 we can.

10 MS. ZHANG: So during today's presentation
11 we will be discussing the NRC's treatment of visual
12 I&C safety system security, hereafter referred to as
13 Establishment of a Secured Development and Operational
14 Environment, or SDOE, for additional safety systems as
15 described in Revision 3, of Reg Guide 1.152.

16 Specifically, we'll be discussing the
17 modifications made to Reg Guide 1.152, to address the
18 predictable challenges to safety systems development
19 and operation that may affect the integrity,
20 availability and reliability of the system.

21 We will also address the changes made in
22 the regulatory guide to focus the Part 50, focus the
23 guidance on Part 50 and 52 reliability requirements.
24 Lastly, we will discuss the paths forward for future
25 work to enhance the existing regulatory guide. Next

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 slide, please.

2 In Revision 2 of Regulatory Guide 1.152,
3 Regulatory Position C.2.1, through C.2.9, provided
4 security requirements, development process controls
5 and high levels of cyber security Program elements to
6 address the security and reliability of visual safety
7 systems, as shown on the lefthand portion of this
8 figure.

9 Positions 2.1, through 2.2, provided
10 guidance on security assessments and development of
11 security requirements, based on the results of the
12 assessment.

13 Positions 2.3, through 2.5, provided
14 guidance on the implementation of the security
15 requirements and security during the development
16 process.

17 Positions 2.6, through 2.9, provided
18 guidance on the operational life cycle phases. This
19 guidance contained very high level security
20 objectives.

21 As discussed in the previous presentation,
22 the issuance of 10 CFR 73.54, and the supporting Reg
23 Guide 5.71, provided a more comprehensive set of
24 requirements and criteria for cyber security.

25 It required the licensee or applicant 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 submit a cyber security Program Plan that provided
2 clear licensing requirements to ensure that critical
3 digital assets are protected from Cyber attacks.

4 Again, I'd like to emphasize that it's
5 critical digit assets that perform safety, security
6 and emergency preparedness functions.

7 Whereas before, in Reg Guide 1.152, we
8 only had guidance for safety systems. So it's
9 expanding guidance. The next presentation will
10 discuss the cyber security requirements and guidance
11 in detail.

12 But I just wanted to highlight a few
13 sections that provide a comparable guidance to that of
14 Reg Guide 1.152, Revision 2. This includes Section
15 C.12.2, which is on incorporation of security
16 controls.

17 Section C.12.3, through 12.5, which
18 provides guidance on securing the development of these
19 systems. And Section C.12.6, which provides guidance
20 on cyber security Program Implementation operations
21 and maintenance.

22 To ensure clarity in big regulatory --

23 CHAIRMAN BROWN: Can you connect the two
24 squares for me? I'm trying to, just pick Section 2.3,
25 2.5, Q/A, CM, arrow, 5.71, there's an equivalent

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 Section 12.3, 12.5.

2 I guess that's all part of it. And then
3 you say plus?

4 MS. ZHANG: So if you look at the lefthand
5 side, where originally we had guidance for both
6 reliability and cyber security. Now we have guidance
7 in Reg Guide 5.71, Section 12.3, through 12.5, for
8 cyber security.

9 We have guidance in Reg Guide 1.152,
10 Revision 3, Sections 2.3, to 2.5, for reliability. So
11 together they form what's comparable to what was in
12 Reg Guide 1.152, Revision 2.

13 CHAIRMAN BROWN: But they're roughly the
14 same. And if I go read the words, and if I read 2.3
15 to 2.5, in Rev 2, and read Rev 3 --

16 MR. MOSSMAN: They're very close.

17 CHAIRMAN BROWN: Very, very close to each
18 other, a few wordsmithings a little bit.

19 MR. MOSSMAN: Yes, the total amount of
20 word changes was not --

21 CHAIRMAN BROWN: Minimal for 2.1 through
22 2.5.

23 MR. MOSSMAN: Was minimal. And the way we
24 were given direction for this task, was that this was
25 to be a kind of a surgical change to Reg Guide 1.152,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 where we were strictly going in, very, very limited
2 scope revision where we were just going in, taking the
3 Cyber pieces, the Cyber language out.

4 Taking other language out that referred to
5 malicious attacks or anything that would imply --

6 CHAIRMAN BROWN: I was a few deletions,
7 but that was about all I saw.

8 MS. ZHANG: So that portion that refers to
9 malicious, that guidance has been expanded and is now
10 in Reg Guide 5.71, and it applies --

11 CHAIRMAN BROWN: Oh, it's considerably
12 expanded, I don't disagree with that. A lot more
13 detail in 5.71.

14 MEMBER STETKAR: Deanna, on this slide
15 there's a notable green wasteland in the lower right-
16 hand corner of the slide, and it, Myron is not here,
17 but that wasteland addresses his question in the
18 previous presentation.

19 Insofar as what, how does the current
20 process now assure continued reliability from a
21 hardware and software safety system functional
22 performance perspective, in the installation,
23 operations and maintenance phases?

24 That's where that green block does not
25 exist right now. It seems that we've eliminated that.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MS. ZHANG: Yes. The reason we chose to
2 remove that portion of the guidance is that Reg Guide
3 1.152 is meant for a licensing document. Those
4 guidance are specific for inspection or post-licensing
5 activity.

6 And that guidance is now in inspection
7 procedures.

8 MEMBER STETKAR: But you're saying Reg
9 Guide 5.71, has guidance in that regime of plant
10 operations.

11 MS. ZHANG: Yes, from a security
12 perspective.

13 MEMBER SIEBER: Right, only from cyber
14 security.

15 MS. ZHANG: But there's other operational
16 programs like configuration management programs,
17 quality assurance programs that will cover the
18 reliability portion.

19 MR. MOSSMAN: To date, the limited
20 examples where we've used Reg Guide 1.152, Rev 2,
21 we've had to make our licensing determinations only up
22 through those things that the applicant and vendor had
23 accomplished by the time we issued the safety
24 evaluation.

25 Which really ended with Regulatory

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 Position 2.5, which got you up through Factory
2 Acceptance Test. In limited cases like Oconee, where
3 they provided us some documentation to, they pointed to
4 their program.

5 And kind of a future commitment that
6 they'll come up with a retirement strategy for the
7 system. We would document those. We would hand those
8 over to the Region, but we would not use those
9 commitments or pointers as a basis for our licensing
10 determination and a safety evaluation.

11 MEMBER STETKAR: I understand sort of that
12 thought process. I have to think about it a little
13 more, though, thanks.

14 MEMBER SIEBER: Why does retirement
15 disappear altogether?

16 MR. MOSSMAN: I would point over to Eric.
17 I know, because I don't remember the reference off
18 the top of my head. There is actual controls in 5.71,
19 that addresses media disposal, which essentially,
20 which mapped pretty well to what the high level
21 language we had in regulatory position 2.9.

22 MS. ZHANG: As well as evaluation.

23 MEMBER SIEBER: It's your system, that
24 would be a source of information as to how to do it.

25 MS. ZHANG: Yes, as well as the, doing

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 another evaluation if you were to remove a particular
2 security control, you would need to do a particular
3 evaluation to see if that reduced your security
4 posture.

5 You know, are you really putting a
6 different system that could provide the same level of
7 security. So that's all under the guidance Reg Guide
8 5.71.

9 CHAIRMAN BROWN: Okay, let me springboard
10 from John's question, 2.6 through 2.9. When I read, I
11 mean I look at those and it looks like they apply to
12 licensing as well.

13 Because if you look at the design, I just
14 talking new reactors right now. That whole
15 certification includes, you know, operational aspects.
16 It involves, you know, testing aspects, and there's
17 in-service testing.

18 It includes acceptance testing, it
19 includes ITAAC, for various types of things. So there
20 is, as well as maintenance consideration. And yet,
21 and if 1.152, is only licensing, it looks like --

22 MEMBER SIEBER: It ought to be something.

23 CHAIRMAN BROWN: -- it ought to be, it
24 ought to still be there from a licensing standpoint,
25 not the cyber security aspects, but for, you know,

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 what are the thoughts when you are going to put the
2 stuff into service and then operate it.

3 MR. KEMPER: This is Bill Kemper. If I
4 could, I'd like to try to answer that because I was
5 one of the principals in making that change to our
6 licensing process.

7 Basically, we were challenged by our own
8 staff and our management to really evaluate the steps
9 in the design, development and implementation of a
10 safety system that really are involved with licensing
11 that system.

12 Basically, once the system is licensed,
13 our licensing process carries through with the
14 system's development, all the way up to the point
15 where the analogy I use is, it's ready to be shipped.

16 Basically, it's shrink wrapped and ready
17 to ship to the site. So, by the time we write the
18 safety evaluation for that system, it should have
19 been, we should have verified that it complies with
20 all the regulations in terms of its design, the way it
21 was built, right up to the point of installation.

22 Now, installation in the plant, that's
23 when typically a system is turned over from vendor's
24 program to a licensee's program.

25 So, at that point, the licensee takes

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 custody of that equipment. So it's up to them to use
2 their, as Deanna said, configuration management
3 systems, the QA program and so forth, to ensure that
4 the system that they pay for, we ship to the site and
5 they've got the same system that they actually, that
6 was licensed.

7 And it stayed that way. So that's really
8 outside of licensing's place. The licensee's program
9 has to take custody, I mean take control of that, if
10 you will, and take ownership of it.

11 So that's why we felt as though, after
12 thinking about this quite a bit, it would be better to
13 take those sections that were originally in 2.6
14 through 2.9, and defer that to the on-site inspection
15 program of the Regions.

16 So that's why we made that change.
17 Beforehand, for many years, it was Section 2.1 through
18 2.9, that was considered part of the licensing regime.
19 So whether that was the reason for the change, because
20 once it's designed and built, and it's written up and
21 approved accordingly, and is complying with the
22 regulations, it's no longer in licensing's face.

23 It's really up to a licensee to ensure
24 that it is, in fact, installed in accordance with a
25 configuration that the system was approved by. So

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's a long-winded answer probably.

2 CHAIRMAN BROWN: Well, it's not long-
3 winded, but from the standpoint of -- that almost
4 sounds like an NRR type. But even when a licensee
5 comes and says I want to put in a new Digital RNC
6 system and they come in with their License Amendment
7 to put it in and install it, they have provide that,
8 you know, the design. What is the design going to
9 look like?

10 And whatever framework it's supposed to
11 be, similar to what we see in the new reactor's world.

12 And as part of the new reactor's world, you get
13 operation, maintenance, testing regimens.

14 It's in there. So is you tech specs, you
15 know, they're laid out, and says we're going to test
16 them so often, blah, blah, blah.

17 So the licensee has identified, you know,
18 up front during the licensing thing, not the details,
19 but they will do certain things in accordance with
20 certain standards, you know, Reg Guides or whatever
21 you're required to do, they're identified as part of
22 that design cert or whatever.

23 So I'm just relating this. I understand
24 your point, but now it's saying, okay, we're stepping
25 aside from that, and now it gets delivered. All we're

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 going to look at for licensing is what is the design
2 going to look like and it goes out and they build it.

3 And after that it's the licensee, on his
4 own, that doesn't, so there's not licensing thought
5 process about how this stuff is going to used or
6 tested, etcetera, as part of the overall licensing
7 process.

8 It gets defined later by the licensee and
9 I guess the local --

10 MR. KEMPER: The inspection group, right.

11 CHAIRMAN BROWN: -- inspection group.

12 MR. KEMPER: You picked lower region,
13 right.

14 CHAIRMAN BROWN: If that's your decision,
15 I mean that's a decision. I'm just saying it doesn't
16 have the same level of oversight that you have during
17 the initial licensing, from a Headquarters standpoint.

18 Now, I don't know if that's good or bad,
19 I'm just saying that's the way I viewed. John or
20 Jack, Jack, I'm sorry.

21 MEMBER SIEBER: Yes, there should be some
22 requirement someplace that tells the licensee what to
23 expect to do an operation and maintenance.

24 CHAIRMAN BROWN: Well, is there?

25 MR. KEMPER: Yes, that would be technical

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 specifications, primarily. In other words, we would
2 approve the tech specs associated with the system,
3 during the licensing review.

4 Because many times that's predicated on
5 the reliability, availability, test ability of the
6 system. And then the baton against the, regulatory
7 baton is passed off to the Regions again, to verify
8 that in inspection service.

9 CHAIRMAN BROWN: Well, that part is fine.

10 But the definition is what I was talking about. And
11 that seems, seems to have been taken out of Reg Guide
12 1.152.

13 I thought that would have been where it
14 came from.

15 MEMBER STETKAR: Let me ask you a specific
16 question if I can, Bill. I'm looking at Rev 2, of
17 1.152. In Section 2.6.1, which is under installation
18 checkout and acceptance testing.

19 It says the licensee should ensure that
20 the system features enable a licensee to perform post-
21 installation testing of the system to verify and
22 validate, etcetera.

23 That says that, under the old Reg Guide,
24 part of the design review made sure that the design of
25 the system facilitated post-installation maintenance

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 and testing.

2 That's now been removed. So I can't read
3 anything in the current revision of the Reg Guide that
4 says when I design a system, I have to think about
5 post-installation testing and maintenance.

6 So could you explain how, that specific
7 example for, you know, how that has been abrogated to
8 the licensee and the inspection process.

9 Because that's a fundamental feature of
10 the design.

11 MR. KEMPER: Well, I'll tell you how we
12 handled it in the Oconee review.

13 MEMBER STETKAR: No, I want to understand
14 for current regulatory guidance going forward, not the
15 special conditions for Oconee.

16 MR. KEMPER: Okay. Well, what I would
17 expect is in the future, licensees would submit all of
18 the plans for each one of those sections.

19 In other words, each of the planning
20 aspects, which right now is contained in Branch
21 Technical Position 7-14.

22 Now some of those deal with installation,
23 operations and post-maintenance testing, that sort of
24 thing. So, NRR and NRO, I presume, would review those
25 for consistency with the regulatory guidance in those

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 areas, but not approve them specifically.

2 In other words, we would weigh in on
3 those, if you will, and say that the plans are
4 consistent with the guidance provided in various
5 documents, regulatory documents.

6 And then serve that up to the Regions, to
7 do a site-specific inspection. And I'm talking about
8 NRR space here now, I can't speak for NRO. For the
9 Regions to do a site-specific inspection at the
10 appropriate time to verify that licensee has in fact
11 implemented the plans the way they described them in
12 the licensing documents themselves.

13 MEMBER STETKAR: I guess I'm being dense.

14 I still don't understand that under my
15 interpretation, maybe I'm interpreting something wrong
16 here. Under Rev 2, of the guidance, if I am a staff
17 member performing a review, this section says that I
18 need to assure myself that the system design includes
19 features that will enable post-installation testing
20 and maintenance of the system.

21 And I guess, you know, if I'm concerned
22 about safety functions, that those features do not
23 interfere with performance of the safety of the
24 system, such that you can perform testing and it
25 doesn't substantially affect the reliability of 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 performance of the safety function.

2 And I just don't see that guidance now. To
3 me, as a Reviewer, to say that I need to be concerned
4 about that when I'm looking at the design.

5 MS. ZHANG: I think if you take it one
6 step back, you know, this guidance was originally in
7 there for cyber security purposes. You look at that
8 line, you know --

9 MEMBER STETKAR: Okay, and I purposely
10 didn't complete the sentence. I said, etcetera,
11 etcetera, because I'm allowed to do that.

12 (Laughter.)

13 MEMBER STETKAR: I recognize that in deed
14 the entire, quote, validate that the security
15 requirements have been incorporated into the system
16 appropriately. But I'll step back and say the heck
17 with security, I want to be able to test and maintain
18 this system in a way that does not interfere with the
19 safety functions of the system.

20 And that when I'm reviewing the design of
21 this system, I need to have assurance that those
22 testing and maintenance functions do not interfere
23 with the safety performance of the system.

24 MS. ZHANG: I gave you, if you could take
25 a step back.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MEMBER STETKAR: I think you can do it.

2 MS. ZHANG: If you take a step back and
3 look at all safety system requirements. We want to
4 make sure, you know, any safety feature we want to
5 make sure that, you know, it's of course the overall
6 safety function, that be performing, you know, this
7 one particular safety feature won't degrade another
8 safety feature.

9 If you look at independence, right? We
10 want to make sure that, you know, it supports the
11 overall safety function.

12 We don't take it into isolation, you know,
13 from other security requirements. You know, we don't
14 say, you know, you must need some independence
15 requirements, but if you can't achieve the safety
16 function by, you know, meeting the independence
17 requirement then, you know, it would defeat the
18 purpose --

19 MEMBER STETKAR: No, I understand that,
20 and in deed the current version of the Reg Guide does
21 talk about independence and communications. I've just
22 done a word search, I cannot find the word test or
23 testing anywhere being addressed in the Reg Guide.

24 So, the Reg Guide currently does not
25 address that issue.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. MOSSMAN: The Reg Guide still doesn't
2 endorse 7-4.3.2, 2003, and I don't have an
3 encyclopedic knowledge of every work in there, but I
4 know in 603, there is some coverage of test-ability
5 and I believe 7-4.3.2, also does pick up test-ability
6 of the system.

7 MR. ARNDT: I'm trying not to jump in the
8 middle of this, but the real issue here, John, is that
9 the very first paragraph of Section C of the Reg
10 Guide, basically says conformance with IEEE 7-4.3.2,
11 that is where all the standard safety aspects are
12 included, including the review of the design, the
13 review of the application, the life cycle, the
14 testing, the test-ability and those kinds of things
15 are picked up.

16 CHAIRMAN BROWN: Let me take a moment for
17 a minute. If somebody's, I just heard some ringing
18 sounds going on. I don't if, oh, it's yours? You
19 turned it off. I'm sorry, it's our fault.

20 (Laughter.)

21 CHAIRMAN BROWN: What paragraph were you
22 talking about in 5.71?

23 MR. ARNDT: Well, not in 5.71, 152.

24 CHAIRMAN BROWN: Oh, in 152, okay.

25 MR. ARNDT: The first paragraph of Section

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 C, Functional and Design Requirements.

2 MR. MOSSMAN: Conformance with the
3 requirements IEEE standard 7-4.3.2, 2003, --

4 MR. ARNDT: And if you go back and look at
5 7-4.3.2, plus 5.3, talks about the requirements
6 associated with all the different things you're
7 supposed to do under 7-4.3.2.

8 CHAIRMAN BROWN: Does it include the
9 things we're talking about?

10 MR. ARNDT: Yes, the entire life cycle.

11 MR. KEMPER: Yes, that was the point I was
12 trying to make a moment ago. I guess I didn't make
13 myself clear. So, John, if I could try again?

14 (Laughter.)

15 MR. KEMPER: BTP 7-14, is a very
16 comprehensive document. That's the document we use to
17 verify that the high quality life cycle development
18 process that was used for the safety system, complies
19 with the regulations or our requirements, in the
20 Standard Review Plan, which as Steve Arndt just said,
21 are embodied in IEEE 7-4.3.2.

22 So the staff would request that licensees
23 send in information to demonstrate how they comply
24 with all 12 of the life cycle processes. I believe
25 there's 12 plans that are spell out in BTP 7-14.

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 Some of those are directly applicable to
2 licensing, in our judgement, some of those we'd review
3 for a compliance with the requirements stated in BTP
4 7-14. However, we would not render a final judgement
5 on that, because that's post-installation or post-
6 licensing effort.

7 And therefore we would ask that Regions
8 take responsibility for inspecting that criteria. To
9 ensure that what they stated in the License Amendment
10 itself, was in fact executed while the system was
11 being installed and started up, tested and then
12 maintained on a regular basis.

13 So this wouldn't be a one-time only
14 inspection, this could be an ongoing inspection for
15 years to come.

16 CHAIRMAN BROWN: But you make the
17 judgement that they're adequate?

18 MR. KEMPER: Yes --

19 CHAIRMAN BROWN: You're not judging that
20 the execution is satisfactory, you pass that on?

21 MR. KEMPER: That's correct.

22 CHAIRMAN BROWN: But you do make a
23 judgement in the licensing that those are adequate --

24 MR. KEMPER: That is correct.

25 CHAIRMAN BROWN: -- in order to make sure

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 the equipment continues to perform.

2 MR. KEMPER: That is correct. That's the
3 best we can do. Because until they install it --

4 CHAIRMAN BROWN: Well, I don't see your
5 contemporaries over here shaking their head up and
6 down, they're just frowning.

7 (Laughter.)

8 MR. SANTOS: You've got to look this way.

9 MR. KEMPER: That's my boss, that's not my
10 contemporary. I hope he's shaking his head in the
11 same direction as I am.

12 (Laughter.)

13 MR. KEMPER: I hope that's clear, John.

14 MR. HILAND: This is Pat Hiland, I'm the
15 Director of Engineering for NRR. Just big picture
16 what we hoped to achieve was, you know, at one point
17 several years ago, when I looked at some of these
18 earlier drafts, we were expecting our Licensing
19 Reviewers to actually go down to the level of, show me
20 that maintenance procedure.

21 I want to see the maintenance procedure
22 before I sign off on this licensing. And so big
23 picture-wise, what we've tried to do is separate a
24 licensing decision, where you can go and put this
25 equipment on the shelf and install it at your leisure.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 When you've met your license under Part
2 50, all of those requirements that are imposed on you,
3 for your operational phases. All of your maintenance
4 requirements, all of our procedural requirements, all
5 of your test-ability requirements.

6 And so, big picture-wise, we got away from
7 having our Licensing Reviewers asking the licensees,
8 at initial review of a product, let me see the
9 maintenance procedure, how are you going to fix that
10 widget when it breaks in a year or two, after
11 installation? That's not the goal of a licensing
12 purpose, that all.

13 CHAIRMAN BROWN: I don't have any
14 disagreement with that.

15 MR. KEMPER: That would be under the
16 maintenance rules.

17 MR. HILAND: A lot of my people did.

18 MEMBER SIEBER: How do you know when it
19 broke?

20 CHAIRMAN BROWN: Yes, go ahead John, I'm
21 sorry.

22 MEMBER STETKAR: I was just trying to do
23 some searches here in real time because I sort of
24 understand the philosophy, I guess, but I'm getting
25 lost in the details.

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 did look up IEEE Standard 74.32, 2003,
2 and with regards to testing and maintenance, there's
3 one statement in there that says this standard does
4 not apply to requirements for testing and maintenance.

5 And there's another section though, that
6 does say capability for testing calibration. It says
7 no requirements beyond IEEE Standard 603-1998, are
8 necessary.

9 I don't have IEEE Standard 603-1998, in
10 hand here, so I was curious what that might say, as if
11 we're walking down a chain here.

12 DR. HECHT: 74.32 was supposed to be a
13 daughter standard to 603.

14 CHAIRMAN BROWN: Yes, it amplifies 603.

15 MR. KEMPER: It amplifies exactly. But
16 clause, by clause it's almost a parallel
17 representation of the criteria.

18 MR. MOSSMAN: And there were a number of
19 places in 74.32, where they don't provide any
20 additional language over what's already covered.

21 CHAIRMAN BROWN: And they say that,
22 nothing additional.

23 MEMBER STETKAR: But in deed the
24 requirements in 603 are, do have the testing and
25 maintenance capability requirement? Okay, 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 DR. HECHT: However, having said that --

2 (Laughter.)

3 DR. HECHT: You know one of the, I guess,
4 I read, been reading about the Stuxnet, the worm or
5 whatever it was. And one of the key features of that
6 worm was that if output of normal status, when in fact
7 it was doing badness inside the actual I&C system.

8 And this is a situation where the code can
9 be okay. At least the code under the, what is it,
10 SDOE, Secured Development Operating Environment, is
11 okay.

12 And somehow or other it got changed during
13 the installation or operations phase, and the test-
14 ability that you might think you have, would not
15 detect the presence of that particular --

16 MR. MOSSMAN: I think you're hitting upon
17 something that's really critical and I think Craig
18 touched upon it earlier, with the importance of the
19 programmatic approach that they've gone to under
20 73.54, is that security is a moving target.

21 At the point in time where we may license
22 something, it may have no known vulnerabilities. We
23 look through at a Topical Report. They have no known
24 vulnerabilities.

25 It may be, you know, as far as our

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 criteria, it may be very good, but every day they're
2 coming out with various zero day vulnerabilities and
3 that's the importance of the programmatic approach, to
4 keep that living look, that constant update of things
5 that can attack your system.

6 Zero day vulnerabilities in my mind are
7 not always, they're not always viewed as flaws when
8 the software is originally put out.

9 DR. HECHT: Well, I'm not relating to,
10 zero day really reflects a time, that's when it's
11 introduced. What I'm really talking about is the fact
12 that test-ability for, how should I say it, alteration
13 of code, is something which is a design feature, which
14 you may not think about until operations.

15 MR. MOSSMAN: That actually is something
16 we saw in the Oconee application, and I don't want to
17 go into too much detail, because some of that is
18 protected under 2.390, but they did have mechanisms in
19 place to detect any corruption in the code.

20 Any alteration, and it was a, part of
21 their, I forget what the millisecond operating cycle
22 was. But every operating cycle they would do a check
23 on the integrity of the code.

24 DR. HECHT: That's great.

25 MR. MOSSMAN: And if there was something

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 altered they would get a different value and that
2 would, that would flag --

3 MS. ZHANG: From a reliability perspective
4 you do worry about, you know, just random failures
5 that could alter the code. That's why we do have
6 things like CRC, you know, just to make sure nothing
7 was changed from when the code was shipped out to when
8 it was received.

9 You know, something could have, you know,
10 random failures.

11 DR. HECHT: Yes, but that's a different,
12 what you, the checks on the correctness of the
13 installed code is part of CM and I would agree with
14 you on that.

15 And that's party of a standard process.
16 But this kind of thing, this malicious kind of thing,
17 I agree that an online check of a code is something
18 you wouldn't necessarily do under a conventional
19 system.

20 At least I haven't done it because every
21 time you do a check like that, introduce a possibility
22 of the check fails and, you've got a trade off.

23 But now this the malicious code of course,
24 all of a sudden, that trade off all of a sudden weighs
25 much more to the side of, well, you've got to do it

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 because even though the cost of it, from a reliability
2 perspective of a false positive on that test, is
3 there.

4 It's now definitely outweighed by the
5 benefit of being able to detect a malicious intrusion.

6 MS. ZHANG: And that's why we have, you
7 know, the cyber security Program would kick in and
8 they do have anomaly-based intrusion detection to
9 detect that type of changes to your system. You know,
10 not changes from the baseline.

11 DR. HECHT: I think the net result of this
12 discussion has been that we don't necessarily know
13 when, where the boundary is between the design and the
14 operation.

15 And, in fact, it seems to change a lot,
16 back and forth.

17 MR. MOSSMAN: I would disagree. Our,
18 we've been pretty consistent, our regulatory
19 evaluation goes up and through factory acceptance
20 test.

21 DR. HECHT: Well, if in fact there's a new
22 vulnerability that's introduced which requires a
23 change in the code, are you going to go through an
24 entire 5059 process which might take years?

25 MR. KEMPER: Yes, this is Bill Kemper, yes

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 they would. They're required under the rule to go
2 through a 5059 Evaluation.

3 CHAIRMAN BROWN: I think they would like
4 to avoid that if they can. Find some other
5 alternative.

6 MR. KEMPER: A software change is a
7 configuration change, it's just like a hardware
8 change.

9 MR. MOSSMAN: And to that end, and not to
10 steal Eric's thunder, I mean, I think he'll cover this
11 later, not every technical security control has to be
12 built into the safety system itself.

13 I mean they can be built, depending on the
14 nature of the technical control and I can't, I don't
15 want to speak to all of his presentation, but they can
16 be built around. And it could also be an, in fact, if I
17 was designing it, I'm not, because that's not my job.

18 I probably wouldn't put a lot of that
19 stuff in, specifically so I wouldn't have to do that.

20 DR. HECHT: That's a reason for 5.71 being
21 separate from 1.152.

22 CHAIRMAN BROWN: Okay, let's roll here.
23 I'm being a little liberal with the time because we do
24 have time this afternoon and there's a lot of details
25 coming out.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MS. ZHANG: So, just to finish off this
2 slide, to ensure clarity into the regulatory treatment
3 of cyber security, Reg Guide 1.152, Revision 2, has
4 been modified to separate the guidance for reliability
5 and security.

6 The security portions are now addressing
7 Reg Guide 5.71, while the reliability portion of Reg
8 Guide 1.152, has been enhanced and clarified in
9 Revision 3 for this Guide.

10 Together elements of Reg Guide 5.71, and
11 Reg Guide 1.152, Revision 3, cover the same level of
12 guidance as in Reg Guide 1.152, Rev 2.

13 The staff has finalized the changes to Reg
14 Guide 1.152, Revision 3. The core changes to Revision
15 3 of Reg Guide 1.152, include, first, cyber security
16 is now under the domain of Part 73, that's all
17 references to cyber security, intention malicious
18 actions or attacks have migrated to coverage under 10
19 CFR 73.54.

20 The security focus of Reg Guide 1.152, has
21 been clarified to address integrity and reliability
22 requirements of 10 CFR Part 50 and 52. In addition,
23 regulatory positions covering post-licensing life
24 cycle phases such as those beyond factor acceptance
25 testing, as the move to 10 CFR 73.54 in Reg Guide

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 5.71.

2 So this is what we just addressed in
3 detail, so I won't go into that. The next
4 presentation on cyber security will cover additional
5 information on the operation and programs. Next
6 slide, please.

7 The Part 50 and 52 Licensing Evaluation
8 focuses on ensure reliable operation integrity of
9 visual safety systems. Therefore, safety systems are
10 to be protected during both the development
11 environment and operational environment from a
12 predictable set of non-malicious events, that could
13 challenge integrity, reliability or functionality of
14 visual safety systems.

15 And Tim will cover what we mean by
16 securing the development environment and operational
17 environment, and what we mean by a predictable set of
18 non-malicious events. To avoid confusion between Part
19 50/52 and Part 73, use of the term security, Parts 50
20 and 52 have adopted the use of the term secure
21 development and operational environment, in its place.

22 Again, just to focus on protection of
23 safety systems from a predictable set of anomalies.

24 CHAIRMAN BROWN: Excuse me, that's your
25 separation then from the licensing aspect, and its

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 review from this --

2 MR. MOSSMAN: From the bad guy world.

3 CHAIRMAN BROWN: -- from the bad guy
4 stuff. So it doesn't sound like Cyber, you're filling
5 in, but Cyber is used for everything --

6 MS. ZHANG: The lawyers told us to change.

7 MR. MOSSMAN: Yes, we tried a lot of
8 different terms and a lot of the candidate terms had a
9 lot of baggage associated with them, so this is the
10 one we came up with.

11 (Laughter.)

12 CHAIRMAN BROWN: I didn't want to say
13 that.

14 MS. ZHANG: Next slide. Reg Guide 1.152,
15 Revision 3, focuses on three primary objectives. The
16 first one is the protection of the development
17 environment from inclusion of undocumented, unneeded
18 and unwanted code.

19 Such extra software may challenge the
20 reliability and integrity of the system, should it be
21 inadvertently activated during operations.

22 This criteria survived from the
23 requirements specified in Criteria 3 of 10 CFR Part
24 50, Appendix B. The second objective is to establish
25 controls to prevent inadvertent access to the systems

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 during development or operation.

2 This is, you know, to prevent maintenance
3 personnel from inadvertently changing the system
4 software or changing set points. This criteria is
5 derived from the access control requirements and IEEE
6 Standard 603-1991, Clause 5.9.

7 CHAIRMAN BROWN: Question. Somebody
8 mentioned in the other discussion a minute ago about
9 stuff that's in 603-1998. But I guess it's my
10 understanding the only IEEE Standard endorsed is 603-
11 what is it 1993 or 1991?

12 MS. ZHANG: 1991.

13 CHAIRMAN BROWN: Ninety-one.

14 MEMBER STETKAR: It's in there, I have
15 that one.

16 CHAIRMAN BROWN: No, I got that, yes, but
17 you referenced, I've forgotten who it was. I thought
18 it was somebody on this side of the aisle. It
19 definitely wasn't over there.

20 (Laughter.)

21 CHAIRMAN BROWN: Who was talking about
22 1998. So, why is 1998 operational if it hasn't been
23 endorsed?

24 MR. ARNDT: It's not operational. The
25 reference that was discussed by Dr. Stetkar, was from

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 7432 that was referencing a different version of 603,
2 that's not endorsed.

3 CHAIRMAN BROWN: It's not endorsed. But,
4 you're --

5 MR. ARNDT: It's not included.

6 CHAIRMAN BROWN: But had you all endorsed
7 or accepted, I'm sorry, John, I'm stealing, 7432-2003?

8 MR. ARNDT: Yes, it's a little bit
9 complicated.

10 (Laughter.)

11 MR. ARNDT: 603-1991, is referenced in
12 5055-AH as part --

13 CHAIRMAN BROWN: It's in the rule.

14 MR. ARNDT: -- it's part of the rule.
15 7432, which version is it?

16 MS. ZHANG: 2003.

17 MR. ARNDT: 2003 is endorsed by Reg Guide
18 1.152, as one method of meeting the regulations.

19 CHAIRMAN BROWN: And 2003, had the
20 reference to 1998?

21 MR. ARNDT: Correct. But that version is
22 not endorsed or referenced.

23 CHAIRMAN BROWN: As a rule.

24 MR. ARNDT: As a rule or as a Reg Guide.

25 MEMBER STETKAR: So now if I come back to

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 my example of a design that assures test-ability --

2 MR. ARNDT: Correct.

3 MEMBER STETKAR: -- I look at 74, I've
4 lost all of them, 7432-2003, it refers me specifically
5 to 603-1998, which is not something that is endorsed
6 by the staff.

7 So, now, I as a designer, must fall back
8 to 603-1991, the Clause for Test-ability. Is that the
9 way the world works?

10 MR. ARNDT: Identical to the one in '98.

11 MEMBER STETKAR: Okay, I'll take your word
12 at that, but --

13 MR. KEMPER: There's two paths. Oconee
14 pursued that very path, okay. The regulations
15 endorsed, 1991 version of 603. However, 10 CFR 5055-
16 A-3, I believe it is, says that they can provide for
17 an alternative or a deviation to the regulation. So
18 that's what they did.

19 So Oconee submitted their application
20 against the '98 version of the 603, and we approved it
21 accordingly.

22 MEMBER STETKAR: Why doesn't, I'll ask
23 this, I will, they make me do this. Why doesn't Reg
24 Guide 1.152 then endorse 603-1998?

25 MR. KEMPER: Well, --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 (Laughter.)

2 MEMBER STETKAR: Given the fact that it's
3 being issued in June of 2011, perhaps.

4 MR. KEMPER: Well, let me take a crack at
5 this. I've got Geary Mizuno here, he's our expert in
6 this area, so he can correct me if I'm wrong.

7 But, at any rate, since the 1991 version
8 is codified, it would be inappropriate for us to
9 endorse another standard without going back through
10 that rulemaking process, to rectify that.

11 So that's why we didn't endorse the '98
12 version with the latest Rev 2, Reg Guide 1.152, Rev 2
13 of 1.152. You all probably are aware that rulemaking
14 is in progress right now, to codify the 2009 version
15 of IEEE 603.

16 And that will be coming before you all, I
17 presume, as a matter of process, when we get to that
18 part. So at this point, licensees have a choice of
19 either showing compliance with the '91 version, or
20 applying for an alternative to whichever version they
21 choose to comply with.

22 In which case, by rule, they are required
23 to submit an analysis to show why the version they're
24 requesting to be approved, has an acceptable
25 alternative safety solution, as the '91 version, 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 we would approve it accordingly.

2 MEMBER STETKAR: Thanks, that helps me
3 somewhat. We'll get to Slide 17, here, I think this
4 will all come -- because there's a pass forward head
5 slide.

6 MR. MOSSMAN: At risk of stealing your own
7 thunder, there's another version of 7432, that once we
8 get this one --

9 MEMBER STETKAR: Eventually, hopefully all
10 of this will get tied together when we get to Slide
11 17, I hope.

12 CHAIRMAN BROWN: The other point I get out
13 of this, if I'm not mistaken, is while you've got the
14 1991 is the rule, if you read the rule, and I'm trying
15 to remember, I did do this, actually, but I'm not sure
16 my memory is correct.

17 Alternatives are always allowed to almost
18 everything in there.

19 MEMBER STETKAR: The Reg Guides.

20 CHAIRMAN BROWN: No, in the rule.

21 MEMBER STETKAR: Oh, in the rule?

22 CHAIRMAN BROWN: When it references the
23 IEEE standards, it allows alter, it's very, they're
24 kind of mushy in terms of they mix statements about
25 how independence should be in one circumstance, but

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 yet you can do, if you really don't want to be
2 independent, just tell us why it's not or it doesn't
3 have to be, or something like that.

4 That's my poor paraphrasing. But anyway,
5 so all these, it sounds like it's just, there's
6 flexibility all the way down the line. It would be
7 nice if they kind of got all these nuances
8 straightened out over the years. New rulemaking
9 sounds good.

10 MEMBER STETKAR: I was going to say, Bill,
11 because I'll probably forget by the this afternoon, I
12 wasn't aware of the rulemaking for 10 CFR 5055. Well,
13 maybe I am, but I'm not aware of it this morning.
14 What's the time schedule for that?

15 MR. KEMPER: Let's see, actually it's
16 somewhat protracted. It takes a couple, two or three
17 years to get through these things. We've completed
18 the regulatory evaluation, I think it is, and
19 submitted that to the Policy and Rulemaking Branch.

20 And it's in the schedule next year for the
21 regulatory analysis to be produced, and I presume
22 that's when it will come before you all.

23 And then the following year, it should go
24 to the Commission for a final approval. So actually
25 it goes out until 2012, I believe, before the rule is

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 finalized.

2 MEMBER STETKAR: So you're looking late,
3 probably late 2012?

4 MR. KEMPER: Yes, that would be my guess.

5 MEMBER STETKAR: Okay, thank you.

6 CHAIRMAN BROWN: For issuance or for us to
7 see it?

8 MR. KEMPER: For issuance, final issuance.
9 So you all would see it, I would think, next year
10 sometime? I was hoping it would be a lot sooner than
11 that.

12 MEMBER STETKAR: Next year is 2012, are we
13 talking 2013?

14 MR. KEMPER: I'm sorry, you're right,
15 you're right, 2013 is when it would finally be issued.

16 It's two years from now. We've been dealing with,
17 working with the Branch Chief of the Rulemaking Group
18 for a couple, two or three weeks now to firm up that
19 schedule.

20 MEMBER STETKAR: Thank you.

21 CHAIRMAN BROWN: Just to make sure, we're
22 going to see this?

23 MEMBER STETKAR: We always have the
24 opportunity.

25 CHAIRMAN BROWN: I think it's a

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 rulemaking, so we get the opportunity, we'll know in
2 time.

3 MR. BERGMAN: You have the option, 5055-A
4 is at the option of the ACRS, because it's typically
5 just an update rule. The ACRS does occasionally pass
6 on reviewing it, but you always are given the option.

7 CHAIRMAN BROWN: Okay, well we, help me
8 keep that in mind so we ought to think about a, please
9 help me keep this in mind.

10 MS. ANTONESCU: Yes, okay, I will.

11 CHAIRMAN BROWN: We've got to get a
12 consensus from the Committee on what we want to do
13 with that, okay?

14 MS. ZHANG: So I just wanted to --

15 CHAIRMAN BROWN: I'll forget.

16 MS. ZHANG: -- finish this slide.

17 CHAIRMAN BROWN: I agree with you, finish
18 it. Do you want to turn the page, you can go on. I
19 think we've had the discussion.

20 MS. ZHANG: The last objective is just
21 basically protection against undesirable behavior, and
22 that's the sources independence from connected systems
23 which is 6.3, which this finishes my portion, so I'll
24 hand it over, the presentation to Mr. Mossman for the
25 second portion of this presentation.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. MOSSMAN: Thank you. This portion of
2 the presentation, I'm going to focus in on what
3 Deanna --

4 CHAIRMAN BROWN: One point, I would like
5 to make, when you all get to the right point, Tom,
6 whatever it is, you ought to ask us. I mean make sure
7 we don't forget also, Christine is going to help me.

8 (Laughter.)

9 CHAIRMAN BROWN: But I'd just like to make
10 sure we get timely notification of when, so we don't
11 get caught behind the --

12 MR. MOSSMAN: Yes, I'm on that Steering
13 Committee so we'll pass that on to the Project
14 Manager, that you're interested in that one.

15 CHAIRMAN BROWN: Yes.

16 MR. MOSSMAN: Because usually it's done
17 with an ASME Code. There will be one, it's about to
18 go final now. So, again, we have the same option
19 there.

20 CHAIRMAN BROWN: And we just like to have
21 the option and have it in a timely manner, so that
22 we're not burdened.

23 MR. MOSSMAN: All right, will do.

24 CHAIRMAN BROWN: Thank you.

25 MR. MOSSMAN: Thank you. As Deanna

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 started to introduce, one of the aspects we're still
2 focused on in Revision 3 of Reg Guide 1.152, is
3 establishment of a secured development environment.

4 What we mean by that, for digital safety
5 systems, notionally simpler design is preferred to
6 more complex implementations, and the presence of any
7 unwanted, unneeded or undocumented code, we believe
8 increase the potential for undesirable system
9 behavior.

10 To that end, NRC's NRR and NRO staff, as
11 part of our Licensing Evaluations, will be looking to
12 conclude that an applicant has taken reasonable
13 measures to ensure that such superfluous code is not
14 introduced into the deployed system. Go to the next
15 slide.

16 Secure development guidance. We recognize
17 that each new development of a safety system may be
18 unique and each development phase has its unique
19 characteristics.

20 To that end, Reg Guide 1.152, directs
21 applicants to perform a concepts phase assessment. As
22 part of this concepts phase assessment, applicants
23 should identify opportunities in the development
24 process for unwanted, unneeded or undocumented
25 requirements, design features or code, to be

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 introduced into the development.

2 The NRC's evaluation of the measures taken
3 to protect against this introduction of superfluous
4 code and functions will depend on the potential
5 challenges identified by the applicant.

6 A concepts phase assessment for the
7 development environment may cover things like
8 opportunities to inject unreviewed requirements into
9 the requirements documentation or database.

10 Opportunities to inject design features
11 into the design documentation that are not driven by
12 requirements. Physical and logical access to the
13 coding environment.

14 Physical and logical access of the test
15 environment and test tools, and any opportunities to
16 manipulate final test data.

17 To date we have seen applicants take
18 credit for things such as strict controls on their
19 requirements and design documentation to ensure only
20 approved personnel have access to those documents.

21 Processes to perform forward and backward
22 traceability of requirements to design and designed to
23 implemented code. To ensure no new features pop up
24 late in the process that weren't driven originally by
25 design.

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 Strict controls on the implemented code,
2 including physical security of the development
3 facility, control of access and network connections to
4 the development environment systems including, in some
5 cases, isolation of these networks, where they are a
6 separate network from the rest of the company's
7 operation.

8 As well as the use of software librarian
9 tools to track all changes and revisions to code as
10 it's undergoing development.

11 We've seen controls on the test
12 environment, including strict controls on test
13 hardware and software, including physical isolation,
14 controlled physical access, both physically and
15 network access to the test environment.

16 And, finally, we've seen control, take
17 credit for controls on their test products and data.

18 MEMBER STETKAR: Tim.

19 CHAIRMAN BROWN: Go ahead, John.

20 MEMBER STETKAR: Mine is going to take
21 some time.

22 CHAIRMAN BROWN: Real quick, I mean what I
23 got out of that, this is test and development
24 environment, and so I want my takeaway here. This in a
25 vendor's facility?

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. MOSSMAN: Yes.

2 CHAIRMAN BROWN: Fundamentally?

3 MR. MOSSMAN: It could, the licensee could
4 do it themselves, hypothetically.

5 CHAIRMAN BROWN: But by and large --

6 MR. MOSSMAN: Yes.

7 CHAIRMAN BROWN: -- that's going to be
8 subcontracted?

9 MR. MOSSMAN: Right.

10 CHAIRMAN BROWN: I would think, for the
11 most part, by and large.

12 MEMBER SIEBER: It doesn't have to be.

13 CHAIRMAN BROWN: I understand that, Jack.

14 MEMBER SIEBER: But, by and large.

15 MR. MOSSMAN: Yes.

16 CHAIRMAN BROWN: And there, they have
17 their factory, they have their design, they have their
18 engineerings, they have all their big networks and
19 everything.

20 And you're effectively saying that you're
21 looking at how isolated are there networks to ensure,
22 and their communications within their facility.

23 I mean are you really doing that, to see
24 how accessible they are from various groups? Because
25 they develop their engineering environments to be

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 accessible, their codes, their methodologies to be --

2 MR. MOSSMAN: One of the recent Topical
3 Reports we just looked at, that's not out yet, the
4 vendor, we went and visited them. They took credit
5 for software librarian tools.

6 Where, you know, they were able to show us
7 in an audit how only certain people had access to
8 actually be able to check out code and check code back
9 in, and it tracks, you know, every check in, check
10 out.

11 You could do line-for-line comparisons to
12 different version.

13 CHAIRMAN BROWN: But how that, you know, a
14 smart hacker can mask his track. He can --

15 MR. MOSSMAN: Again, a smart hacker would
16 fall under cyber security. And that's, we're not --

17 CHAIRMAN BROWN: You're not there yet in
18 the vendor facility?

19 MR. MOSSMAN: We're not evaluating the
20 Cyber controls of those facilities.

21 CHAIRMAN BROWN: That's an interesting
22 thought. Okay, go ahead.

23 MEMBER STETKAR: I'll let you get a couple
24 more slides into it, a more relevant place for me to
25 ask the question.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 (Laughter.)

2 DR. HECHT: Can I follow up on that point
3 that you just made? So, is any, and I guess really
4 starting out from Charlie's question. So I go in and
5 I steal a Developer's password and I go in and I check
6 out the code and make modifications to it.

7 Are the people from 5.71, going to come
8 and visit the vendor's plant to assess whether that's
9 going to happen?

10 MR. MOSSMAN: Eric will talk to that
11 later, but the licensee is, Eric, stop me if I'm going
12 off the reservation.

13 But they have responsibilities to put
14 contractual items in place to, and for the vendor to
15 maintain certain documentation of the controls they
16 had in place.

17 MR. LEE: That is absolutely correct. In
18 addition to that, that particular section requires a
19 Developer to incorporate security controls that are
20 equivalent to what's provided in the Regulatory Guide
21 5.71.

22 So we do require the licensees to require
23 their Developers to implement security controls, to
24 ensure that, you know, to protect the integrity of
25 their system being developed, until it's being

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 developed. Until it's delivered to the licensee.

2 CHAIRMAN BROWN: So you're effectively
3 answering the question that I asked, and saying, yes,
4 there is -- Eric?

5 MR. LEE: Yes, sir.

6 CHAIRMAN BROWN: I'm trying, did I hear an
7 answer to my question relative to the cyber security
8 aspects of the vendor's plant, his environment? And
9 it's protections to keep somebody from accessing it
10 and covering their tracks. I mean, they got, the
11 licensee is required to get his Developer, his vendor,
12 to have a 5.71 secure environment, such that it can't
13 be hacked?

14 MR. LEE: Yes, sir.

15 CHAIRMAN BROWN: And that's verified by
16 whom, the licensee? And is there any --

17 MR. LEE: They are required to have
18 already documentation associated with, you know --

19 CHAIRMAN BROWN: So you audit that, then?

20 MR. LEE: So after they develop, I guess
21 during the inspection phase, then we check and make
22 sure that they have documentation to show that there
23 is a, show that they have done exactly that.

24 CHAIRMAN BROWN: Okay, let's go on.

25 MR. MOSSMAN: Okay, next slide. Of

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 special note, when we're talking about development of
2 digital systems, is the fact that we, at the NRC, do
3 recognize that for digital systems many of them have
4 both a platform operating system, a software operating
5 system, and an application software.

6 Very frequently these two are developed at
7 different times and different facilities, often by the
8 same vendor, but maybe not the same personnel.

9 For these kinds of systems the NRC would
10 want to evaluate both the development environments of
11 the operating system and the application software, to
12 ensure they have been protected from introduction of
13 unwanted, unneeded and undocumented code.

14 It is understood that many platforms, some
15 of our pre-approved Topical Reports were developed
16 many years ago and in some cases developed in foreign
17 countries.

18 And why we understand, this doesn't make
19 for an easy process of going back and looking at
20 development environment. It is something we did for
21 the Oconee Application, as that platform was developed
22 in a foreign country many years ago.

23 The next slide. The other aspects that
24 we're still focused on in Reg Guide 1.152, Rev 3, are
25 establishment of a secure operational environment. 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 that end, we would like the applicant's Concept Phase
2 Assessment to identify potential challenges to the
3 system's reliable operation while in the operational
4 environment.

5 This assessment should focus on, and
6 Deanna kind of ghosted these already, undesirable
7 behaviors from connected systems. In many cases these
8 manifest themselves as communication issues, as well
9 as the potential for personnel to inadvertently access
10 the digital safety system, either physically, either
11 via direct connection to the safety system, or
12 logically from a user interface on a system that may
13 be connected on the same network as the safety system.

14 Next slide. Independence from other
15 systems. The term undesirable behavior was
16 specifically chosen and introduced into Reg Guide
17 1.152, Rev 3, to encompass those events that can
18 occur, not only as a result of a failure of a
19 connected system, which a lot of times we think about
20 in terms of independence of other systems, but also as
21 well as abnormal or unusual behavior that would not
22 rise to the level of a true failure of a connected
23 system, but may not be routinely expected.

24 And I'll have an example of something like
25 that in a slide or two. These kinds of behaviors

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 include things like excessive data transmission,
2 corrupt or missing data, out of sequence messages.

3 Transmission of nonstandard message
4 formats. Maybe receipt of a standard message with out
5 of range data. Or transmission of a message when the
6 safety system is in mode where it's not expecting that
7 kind of message.

8 To date, we and the staff have seen
9 applicants take credit for things, and the first
10 thing, perhaps, is one of the easiest solutions, is
11 device isolation. The less things you're connect to,
12 the fewer things that can impact your operation.

13 We've also seen devices that are
14 introduced that physically prevent the transmission of
15 data to the safety system, such as data diodes. We've
16 seen use of message filters, such as essentially
17 white-listing, that only pass specific messages to the
18 safety system.

19 So, screen out anything that doesn't look
20 like, that doesn't fit in a prescribed message format,
21 a documented message format. We've seen systems use
22 out of range checks on data fields, as well as use the
23 CRC checks to filter out corrupted messages.

24 DR. HECHT: But done primarily for safety,
25 not for security.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. MOSSMAN: Yes.

2 MEMBER STETKAR: Now I get to ask my
3 question. As I read through this, in both the
4 regulatory positions on 2.1 on the concept phase and
5 2.4.2 on development activities, let me read a couple
6 of quotes, to put it in context.

7 The licensee should assess the digital
8 safety system's potential susceptibility to
9 inadvertent access and undesirable behavior from
10 connected systems over the course of the system's life
11 cycle that could degrade its reliable operation.
12 That's in 2.1.

13 2.4.2 says the Developer should account
14 for hidden functions and vulnerable features embedded
15 in the code. Their purpose and the impact on
16 integrity and reliability of the safety system, these
17 functions should be removed or, as a minimum
18 addressed.

19 For example, as part of the failure modes
20 and effects analysis of the application code, to
21 prevent any authorized access or degradation of the
22 reliability of the safety system.

23 So, my reading of at least those two
24 regulatory positions, requires some type of assessment
25 to be made to identify potential susceptibilities.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 You could call them hazards, you could call them
2 vulnerabilities.

3 In fact, in one of the responses to public
4 comment, the term vulnerability assessment was used
5 for 2.1. Now, the Reg Guide explicitly does not
6 endorse Annex D of IEEE Standard 74.32-2003, which
7 refers to failure modes and effects analyses and fault
8 tree analyses as tools to do this type of assessment.

9 Because it says the NRC has not endorsed
10 this annex because it provides inadequate guidance
11 concerning the use of fault tree assessment NFMEA
12 techniques.

13 If I need to do an assessment, and I,
14 according to this guidance, I need to do an
15 assessment. And I don't have any endorsed tools to
16 perform that assessment, how do I perform an
17 acceptable assessment and how does the staff review
18 that assessment for both scope, detail and technical
19 acceptability. What guidance do you use?

20 MR. MOSSMAN: You're hitting on two of the
21 areas that did come up in public comment. And two of
22 the things, I know Deanna and I have talked at length
23 about, it's both a challenge for industry and a
24 challenge for us where I think both industry and we
25 realize that two of our areas where we need additional

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 guidance, and I'm kind of ghosting ahead several
2 slides.

3 MEMBER STETKAR: Okay, if you're going to
4 address it now.

5 MR. MOSSMAN: I'll try to summarize real
6 quick. Is that concepts phase assessment and both in
7 terms of format, content, is an area that we would
8 like to see additional guidance generated.

9 And that's an area that we would like to
10 work with industry to develop.

11 MEMBER STETKAR: I'm going to interrupt
12 you, that I understand that you'd like to do things.
13 We're issuing this regulatory guidance today, such
14 that the industry will start using it, hopefully, in
15 June or whatever the target date is. What will people
16 use? I mean what --

17 MS. ZHANG: So far we've been working just
18 directly with the applicants to leverage industry best
19 practices, as well as technical expertise and just
20 working through the assessment.

21 So we hope to bring our previous reviews,
22 our experience with, and offering that guidance to the
23 licensee in the meantime and we will be developing
24 this guidance shortly.

25 MR. MOSSMAN: It's a case-by-case basis.

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 STETKAR: Well, I'll wait until
2 Slide 17.

3 MR. MOSSMAN: It's been a case-by-case
4 basis up to this point and it's not --

5 MEMBER STETKAR: I understand that, but we
6 are issuing regulatory guidance hopefully with the
7 idea of moving forward in a more coherent process,
8 rather than a case-by-case sort of ad hoc process.

9 And I'd like to understand where we are
10 and where we're going.

11 CHAIRMAN BROWN: To that point, when we
12 issued our report on ISG-06, there was a specific
13 comment of exploring the use of FMEA tools and/or, you
14 just got to one of my questions earlier, okay.

15 And the answer we got then was, well,
16 nobody really has any and nobody really has those
17 defined, etcetera, etcetera. And then we read and we
18 see where we talk about FMEA, you know, in 1.152, we
19 talk about using the methods.

20 But, yet, the answer is nobody has got
21 any. So, that makes it a little bit, it's a little
22 incongruous to, it's part of the Reg Guide, we'll talk
23 about methods for which nothing exists, at least the
24 answers we were given.

25 CHAIRMAN BROWN: John, the point is valid,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 if we're going to do them.

2 MEMBER STETKAR: Well, the assessments
3 techniques are very valid. I mean, you know, we have
4 the guidance that's saying you should do an integrated
5 assessment, is excellent.

6 But if the guidance doesn't provide any
7 further guidance on --

8 MEMBER SIEBER: What it is.

9 MEMBER STETKAR: -- what it is or what a
10 Reviewer, what a Staff Reviewer has to determine what
11 the acceptability of that assessment is. I could have
12 two people sit around for ten minutes in a room and
13 say I did an assessment.

14 And the staff has no guidance to determine
15 whether that's an adequate assessment or not.

16 MR. MOSSMAN: I think that's a fair
17 comment.

18 MEMBER STETKAR: Okay.

19 CHAIRMAN BROWN: I'm not disagreeing with
20 the concept, as we've already noted.

21 MR. MOSSMAN: Very quickly, because I know
22 we're pushing time. Just real quickly, just to
23 highlight what we, a couple of examples of what we
24 mean by undesirable behavior connected systems.

25 And both of these examples involve non-

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 safety systems. These were not safety system related
2 events. Browns Ferry, Unit 3. There was a failure of
3 a condensate demineralizer controller in August, 2006.

4 That failure of the condensate
5 demineralizer controller generated excess network
6 traffic, which impacted the function of the variable
7 frequency drive controllers on the plant recirculation
8 pumps.

9 They happen to be on the same network.
10 Those variable frequency drive controllers were not
11 protected from the impact of that failure of another
12 system on its network. Its reliable operation was
13 undermined, the end result was a scram of that plant.

14 CHAIRMAN BROWN: In other words, it was a
15 non-deterministic system that was relying on low or
16 high bandwidth but low data rates to meet its
17 performance requirements and it couldn't. Now where
18 have I heard that comment before?

19 Relative to a platform that's in common
20 use now, in a couple of the new reactor platforms
21 which are dependent upon maintaining loading less than
22 a certain amount.

23 MR. MOSSMAN: There is another one, just
24 to give a little different example. At Oconee, Unit
25 3, in November, '08, this was, they have a 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 control rod drive system.

2 They simply got a, they were simply
3 receiving a standard time signal for purpose of data
4 logging into their platform, so all their vital
5 systems would receive, would have the same absolute
6 time.

7 They got a noisy time signal, the time
8 standard device at this particular unit, when it got
9 the noisy signal, sent out a standard format message,
10 but with all zeros.

11 And the platform wasn't designed to handle
12 Day 0 and it froze on receiving that message. And
13 that was a case where that particular system was not
14 designed for out of range data.

15 And they never anticipated receiving an
16 out of range data in that particular standard message.

17 CHAIRMAN BROWN: But they had a high
18 quality design process?

19 MR. MOSSMAN: It was a non-safety system,
20 so I don't, I can't speak to what the process was.

21 DR. HECHT: It's a requirements issue.

22 CHAIRMAN BROWN: I understand that. Go
23 ahead, John.

24 MEMBER STETKAR: We're roughly on time, I
25 think. I'll let Charlie be the guide on that.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 CHAIRMAN BROWN: He's got 15 or 20
2 minutes.

3 MEMBER STETKAR: Do you, he's only got
4 three or four slides left. Do you, the two examples
5 that you mentioned here are both Browns Ferry and
6 Oconee. If I read through, I'm not coming down on one
7 side or the other in terms of endorsement of the, at
8 least the FMEA fault tree section of IEEE Standard
9 74.32-2003, but if I read through that they have
10 extensive discussion about identifying what they call
11 hazards.

12 And both of those are examples of things
13 that they do in deed call out, to say you need, when
14 you're doing your assessment, to be aware of these
15 things. So, I'm curious, and maybe I'm not asking the
16 right person, but why did the Staff not endorse that
17 particular annex of the IEEE Standard?

18 I understand the quantitative reliability
19 part.

20 MR. MOSSMAN: Yes, those particular
21 annexes were not endorsed in Rev 2, and that was
22 something we did not revisit in Rev 3. I'm sorry, I
23 don't know that I know the answer.

24 MR. ARNDT: It's a somewhat complicated
25 issue, but let me try and put it a little bit in

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 perspective. There's two aspects of endorsing and not
2 endorsing something.

3 One is whether or not we think it is
4 appropriate guidance to be used. The other one is
5 whether or not we think it is an acceptable method of
6 meeting the requirements. Two issues, with this
7 particular annex of this particular guidance.

8 One is when we originally reviewed it in
9 Rev 2, we did not sufficiently complete to meet our
10 requirements. And had we endorsed it, that would have
11 been an endorsement associated with that.

12 Now, the other issue, which is a broader
13 issue, is it going in the right direction, is it
14 something the people can use?

15 There's a lot of debate in the technical
16 community about that. And in point of fact, you can
17 go to the most recent version of 7432.

18 The industry has removed that annex.
19 There's an annex that says Annex D, this has been
20 removed from the standard.

21 MEMBER STETKAR: Is that right? I didn't
22 have the most recent one.

23 MR. ARNDT: And the reason for that is the
24 broader issue that this is an area of open debate
25 within the technical community. What's acceptable.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 And we do have a section in the SRP,
2 albeit not very good and it could be improved, on
3 failure modes analysis. But it's an open research
4 issue, it's an open technical issue, associated with
5 what is the appropriate way of doing this. I hope
6 that helps.

7 MEMBER STETKAR: That does, to some
8 extent, thanks.

9 CHAIRMAN BROWN: Are you finished, can we
10 go on?

11 MEMBER STETKAR: I am.

12 MR. MOSSMAN: Thank you. The other aspect
13 of the secure operational environment is access
14 control, which dates to Clause 59 of IEEE-603. And in
15 this, for this particular aspect and applicant's
16 concept phase assessment, should identify those
17 physical and logical points of access to a safety
18 system that may present an opportunity for personnel
19 to inadvertently access the system.

20 Physical points of access include open
21 communication ports, on the system, that someone may
22 mistakenly attempt to connect into. Logical points of
23 access include any points of human interface on
24 systems connected to the same network on which the
25 digital safety system resides.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 To date we've seen applicants take credit
2 for, things like locked in alarmed rooms and/or
3 cabinets in which the safety systems reside. A system
4 that has disabled, any unused external communication
5 ports.

6 Either in a particular mode or entirely.
7 Password protection on any user interfaces, and use of
8 key switches for anybody to make changes to a system.
9 You look like you have a question.

10 CHAIRMAN BROWN: What was one of the, run
11 back that list, there's one of them I didn't, removing
12 the ability, something like that.

13 MR. MOSSMAN: Oh, disabling external
14 communication ports.

15 CHAIRMAN BROWN: Yes, there's, I guess
16 this is one of my hangups. I mean, again, some of the
17 communication ports you can enable and disable the
18 software commands and other ones where you can just
19 drop a line, hardware-wise.

20 Drop it to ground and it can't, you can't
21 do anything with it. That's a classic way to do it on
22 certain types of e-squared primes, it's tough to
23 prevent people from writing into them without lifting
24 a wire.

25 So, I mean, some of these small details on

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 how that, communication bi-directional, the ability to
2 get into something while my attention to detail is
3 higher, at a lower level than what you'd like to
4 think, I think those points are important relative to
5 your understanding of how it's being done.

6 Somebody has to understand that and
7 recognize it, that it can't be undone inadvertently.

8 MS. ZHANG: We do recognize that. In
9 fact, in ISG-04.10 --

10 CHAIRMAN BROWN: I'm well aware of that,
11 yes. Thank you. I didn't mean to interrupt you, but
12 I did. Because that is right on the money, it is in
13 there. It's not like you all haven't thought about
14 it.

15 But sometimes I get a little bit concerned
16 about the level of detail. People are reviewing the
17 designs to be actual designs when they're developed so
18 the vendors don't think about that. They, oh, gee,
19 you know, software code, I put it in there, it's just
20 perfectly fine.

21 Wrong. And it might be in an area where
22 there's a real concern, relative to the ability to
23 access that thing. And is an Inspector going to
24 figure that out?

25 How do they do that? As opposed to

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 somebody that's got a real deep experience in digital
2 design. All right, you can go on, I've said my piece.
3 I'll probably say it again.

4 MR. MOSSMAN: It's all good. An example
5 of operational event for non-malicious inadvertent
6 access. Event, again, non-safety system. This is
7 March, '08, at Hatch Unit 2.

8 There's a plant staff member who was
9 testing an upgrade to the plant's condensate
10 demineralizer system on his business LAN. Unbeknownst
11 to the plant staff member, the upgrade he was testing,
12 inadvertently synced because it was logically
13 connected to the actual plant system.

14 The interaction between his upgrade and
15 the actual plant system caused a lot of valves to
16 close via the actual plant condensate demineralizer
17 system and it eventually shut down, scram the plant.

18 But that was a case where the plant staff
19 member never should have been able to access the
20 operational system from the network he was working on.

21 The next slide. Terry Jackson kind of
22 addressed this in his opening brief. Cyber security
23 features. We do recognize that there are going to be
24 features for which licensees seek both Part 50 and
25 Part 73 credit.

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 We would certainly want to see those
2 features, however, our review under Part 50, would be
3 limited to their ability to meet Part 50 requirements.

4 We would not make a judgement as to
5 whether or not they would meet their intended Part 73,
6 purpose. For things that serve an exclusive cyber
7 security purpose, we would also expect to see those
8 for digital safety system.

9 And, again, we would not make a judgement
10 as to whether or not they met their Part 73 purpose,
11 but we would be very interested to ensure that they
12 did not, the implementation of those features, if they
13 were to be implemented on the safety system, did not
14 undermine the response time, the functionality, the
15 reliability of the safety system.

16 CHAIRMAN BROWN: That goes back to our
17 earlier, at least an earlier comment about where's the
18 hook? Where's the integrated look, more formal look?

19 Even though you don't want to, I'm sorry, I didn't
20 mean to phrase it that way.

21 You don't look at it or don't intend to,
22 from your perspective.

23 MR. MOSSMAN: Officially, I can't make a
24 judgement but --

25 CHAIRMAN BROWN: No, I understand that,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 but --

2 MR. MOSSMAN: But I have Eric's number so
3 I know who to call.

4 CHAIRMAN BROWN: Yes, I understand that,
5 I'm just looking for that formal connection, so that
6 those don't get lost.

7 MS. ZHANG: I think, you know, we've
8 talked about development --

9 CHAIRMAN BROWN: We don't need to go
10 through that again. I agree with you, Deanna.

11 MR. MOSSMAN: Public comments, we did
12 solicit public comments on this document. We did
13 receive 38 comments from the public. We accepted
14 nine, including six that actually changed some wording
15 in the regulatory positions themselves.

16 A handful that we did not incorporate, we
17 talked about one at the onset, about not referencing
18 interim staff guidance. We had another five that were
19 deferred for reasons I kind of ghosted earlier about
20 seeking additional guidance and that's something that
21 we endorse, but couldn't fit into the limited scope of
22 this revision.

23 MEMBER STETKAR: Actually, if I read it,
24 the incorporation of the ISG-04 was also fundamentally
25 deferred because it basically says you'd consider it

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 future revision to the Reg Guide.

2 CHAIRMAN BROWN: There were two early
3 comments. It was Comment 2, Comment 2, in your list
4 and Comment 4 or 5 or something like that.

5 MEMBER STETKAR: It just says
6 consideration would be given to referencing non-
7 interim documents containing the ISG-04 guidance in
8 future revisions to Reg Guide 1.152. So that's also,
9 I read that as a deferral.

10 MR. MOSSMAN: Yes.

11 MEMBER STETKAR: It doesn't make any
12 difference.

13 MR. MOSSMAN: Yes, the statement,
14 officially the statement we put in here was other NRC
15 staff positions in guidance govern uni-directional and
16 bi-directional data communications between safety and
17 non-safety digital systems.

18 Since we couldn't put a direct reference
19 to ISG-04. Future 1.152 activities as we mentioned
20 earlier, IEEE 7-4.3.2-2010, was recently issued, which
21 does include security criteria that was not in 2003.

22 We and the staff anticipate, we will
23 review very shortly the 2010 version and the
24 acceptability of this standard will be addressed in
25 the forthcoming Revision 4 to Reg Guide 1.152.

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 addition, as we move on to work on Rev
2 4, the staff does desire to work with industry to
3 provide further guidance on secure development and
4 operational environment.

5 Regulatory positions to improve
6 consistency of their submittals and our reviews, as we
7 both gain experience. And two areas of need, as I
8 mentioned earlier. Content and format for the
9 concepts phase assessments.

10 And, as well as, we received comments on
11 treatment of preexisting systems, systems that may
12 have predated the regulatory positions of Reg Guide
13 1.152.

14 MEMBER STETKAR: Just to keep this theme
15 going, what, it's clear that you're thinking about Rev
16 4. What's your current plan and time schedule for Rev
17 4?

18 MR. MOSSMAN: We actually got some e-mail
19 taskers from research, they were ready to move out
20 with Rev 4, before we were done with Rev 3, but our
21 hope is to get Rev 3 on the books and then as soon as
22 we're done Rev 3, get moving on Rev 4. I don't have
23 a, I don't control --

24 MEMBER STETKAR: I mean what does that
25 mean in a practical, are we talking about six months,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 a year?

2 MR. KEMPER: Yes, this is Bill Kemper
3 again. Yes, we're talking six months to develop it.
4 We actually, like Tim said, research wanted to get
5 ahead of the curve and they wanted to start moving
6 forward with Endorsement 2010.

7 So we asked them to just hold on for a
8 while, let us get Rev 3 out, so we can clear up this
9 confusion that currently exists right now between the
10 guidance and 1.152 and the new Cyber rule, relative to
11 cyber security.

12 And then start moving forward with 2010.
13 The current version 2010, of 7432, has quite a few
14 changes, as you all have said. You know, it provides
15 security information, it provides a lot of additional
16 information on commercial grade dedication.

17 So it's been changed quite a bit, so it's
18 going to take a while to really digest that and
19 endorse it properly.

20 So, I would say, Research is probably not
21 here now, but it will take six months to a year to
22 actually get to the point where we're ready to issue
23 it for public comments, I would say?

24 CHAIRMAN BROWN: Within six months?

25 MEMBER STETKAR: Roughly, within the next

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 year or so.

2 MR. KEMPER: Yes, roughly within the next
3 year, you all should have a chance at reviewing and
4 commenting on that document.

5 And as Tim and Deanna's slide says here,
6 we hope to provide more guidance on some of the very
7 issues that you're talking about, John, right now.

8 About, you know, what constitutes an
9 acceptable vulnerability assessment, for example.

10 MEMBER STETKAR: Yes, thanks, that helps a
11 lot. I'm just trying to get an idea of the near to
12 intermediate term time scale for updates to the
13 various things that we're talking about.

14 So we have a feel for what we're looking
15 at there. So, thanks.

16 MR. KEMPER: Okay.

17 MR. MOSSMAN: And I know they're already
18 kicking off the 20XX version of 7432 and I'm
19 representative to that Working Group, I provided needs
20 assessment for some of these same things, so industry
21 might work on these same things relative to the next
22 version of 7432.

23 Next slide. This is my final slide, just
24 a summary, kind of the same way Deanna led off. 1.152
25 Rev 3, it's addressing predictable challenges to 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 safety system development and operation.

2 It's focused on Part 5052, reliability
3 requirements. We're going to continue with enhancing
4 this guidance going forward, as we just talked about.

5 And 7432-2010 is on the streets now, but
6 we expect that 1.152, Rev 3, provides an acceptable
7 method to ensure integrity, reliability and
8 dependability of digital safety systems during design
9 and development.

10 CHAIRMAN BROWN: One question, at least
11 from me, and nobody else has anything? And this may
12 sound like I've just forgotten everything I've heard.

13 So I'm getting mis-wired and brain burnt.

14 Secure development and operating
15 environment. I mean it's used throughout. What
16 explicitly defines, in some way, shape or form, a
17 secure development and operating environment?

18 And you've got little tidbits, but is
19 there paragraphs in here that really wack it up or
20 not?

21 MR. MOSSMAN: I don't know if we have an
22 explicit definition in 1.152, Rev 3.

23 MS. ZHANG: I think we just say here,
24 after referred to as, in the beginning.

25 CHAIRMAN BROWN: But is there some place

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 else where that, when a vendor looks at this or a
2 licensee looks and he says, well, what is that? And
3 there's, you go through and you've got to protect a
4 few things.

5 But their old stuff would have said,
6 regardless of whether you had the word security
7 development. It almost sounds like there's a little
8 umbrella under which you'd like people to operate.

9 But you haven't laid out what are the
10 boundaries of that umbrella?

11 MS. ZHANG: I think that's where the life
12 cycle process will drive you to the establishment of a
13 secure development and operational environment. But
14 we have not specifically --

15 DR. HECHT: Paragraph 2 says what you
16 should, and that's the title of it, and it says what
17 it should do. But elsewhere you've said it involves
18 access control, protection of the code and the
19 protection of the operating environment.

20 CHAIRMAN BROWN: Paragraph C-2, in the
21 thing?

22 DR. HECHT: This is on Page 8, yes, C-2.

23 CHAIRMAN BROWN: Yes, it says the NRC will
24 evaluate the secure development and environment
25 controls applied to safety system developments

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 throughout the design, blah, blah, a secure
2 operational environment, etcetera, etcetera.

3 MS. ZHANG: I think the guidance we just
4 talked about or the information we just presented here
5 is what we hope to put into the next version of this
6 guidance, as far as the security assessment, what
7 we're looking for.

8 What kind of security controls or security
9 or SDOE features we're hoping to see to mitigate
10 those, the vulnerabilities found in that assessment.

11 CHAIRMAN BROWN: Go ahead, John.

12 MEMBER STETKAR: I think, you know, I got
13 the point, I was in the same place you were, Charlie.
14 I got really confused. I looked around to see if I
15 could find some other document that even uses that
16 term, and I couldn't find any.

17 MR. MOSSMAN: We're the first.

18 MEMBER STETKAR: Yes, so I got to thinking
19 of SDOE as, you know, as a euphemism for Ralph. I
20 didn't try to, I didn't try to imply anything by it.
21 Primarily, all facetiousness aside, I think there
22 needs to be some thought and some care taken in that
23 most of the guidance that I read in the current
24 revision of this regulatory guide, talks about other,
25 there are two aspects up in the discussion of 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 regulatory guide and I highlighted them both earlier.

2 I can't find them in my notes right now.
3 But one is essentially, I found it. Vulnerabilities
4 are considered to be, Number 1, deficiencies in the
5 design that may allow inadvertent, unintended or
6 unauthorized access or modifications to the safety
7 system, that may degrade its reliability, integrity or
8 functionality during operations.

9 Or, Number 2, an inability of the system
10 to sustain the safety function in the presence of
11 undesired behavior or connected systems.

12 Most of the guidance and this notion of a
13 SDOE, whatever that is, seems to address the first
14 vulnerability. Very little of the guidance seems to
15 address the second vulnerability, which is where I was
16 getting to in terms of the fault tree failure modes
17 and effects analysis.

18 Inherent features of the design itself,
19 that may be susceptible to certain types of hazards.
20 It wasn't real clear to me how this guidance addressed
21 that.

22 And that was the genesis of my earlier
23 question. That's why something bothered me about this
24 notion of a secured development operating environment.

25 Because most of the discussion around that

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 context seems to address the first set of
2 vulnerabilities, protections against the other stuff
3 that can come in from the outside.

4 Whatever that other stuff is and however
5 it might be introduced. That's why I kind of gave up
6 on what this, I understand, earlier you said well the
7 lawyers essentially needed a different term so you
8 didn't use cyber security.

9 So it's something you may want to be
10 sensitive in the next revision of this. Either better
11 define what that really means and how it encompasses
12 the full context of the type of vulnerabilities or
13 assessments or whatever you want to call them, you
14 want performed.

15 MS. ZHANG: That's a great suggestion and
16 we'll definitely look into enhancing this guidance,
17 yes.

18 MEMBER STETKAR: Because it certainly
19 isn't a definition, and it's just a thing. That's the
20 point I finally got to on that. I gave up.

21 CHAIRMAN BROWN: Well, yes, I did too.
22 And I didn't look at the specific paragraph to pull
23 out the difference between one and two, I just was
24 trying to figure out what it was, in the first place.
25 You're finished, correct?

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. MOSSMAN: This is the final slide.

2 CHAIRMAN BROWN: Thank you.

3 MR. MOSSMAN: Anything else?

4 CHAIRMAN BROWN: John, Jack, Myron?
5 Steve?

6 MR. ARNDT: Just wanted to make sure that
7 John got the answer to his earlier question on where
8 are the other phases of the safety review, and they're
9 in 603-7432, as endorsed by the Standard, the Standard
10 Review Plan BTP-14.

11 MEMBER STETKAR: I got that.

12 MR. ARNDT: Okay.

13 MEMBER STETKAR: I think I understand it
14 now, Steve, so thanks.

15 MR. SANTOS: We can walk you through it
16 offline.

17 MEMBER STETKAR: No, I think I've got it.
18 I'm not sure how it all fits together, but I
19 understand the basic philosophy, so thanks, that
20 helps.

21 MR. MOSSMAN: Thank you very much for your
22 time.

23 CHAIRMAN BROWN: Okay, a little scheduling
24 information. We are now about probably an hour and a
25 half behind, but there is some, we've got plenty of

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 room, headroom in here, because I think we've asked
2 lots and lots of questions at this point.

3 So my plan is right now to take a lunch
4 break until 1:15, make it a nice even number, if
5 that's acceptable to the members, John, Myron,
6 consultant, okay. And we will reconvene at that time.

7 And we will start with the regulatory developments to
8 address cyber security from Mr. Lee. Is that
9 acceptable? All right, we're off the record.

10 (Whereupon, the proceedings went off the
11 record at 12:22 p.m. and came back on at 1:16 p.m.)

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 A-F-T-E-R-N-O-O-N S-E-S-S-I-O-N

2 1:16 p.m.

3 CHAIRMAN BROWN: I'm going to call the
4 meeting back into session, and also to make an
5 announcement that in order to meet some scheduling
6 commitments, we are shifting and going to have the
7 industry reviews done at this time, as opposed to
8 after the presentation by Eric Lee from NSIR, so
9 we're going to do that last.

10 He has graciously consented to going last.

11 So, I believe we have Luminant, is that right,
12 correct, yes. I can read the viewgraph. Mr. Amin,
13 did I say that right?

14 MR. AMIN: Yes.

15 CHAIRMAN BROWN: Amin, okay. And Mr.
16 Gibson. Subject to anything else, why do you all go
17 ahead and proceed.

18 MR. AMIN: Okay, good afternoon. I'm Jay
19 Amin, the Manager of Digit Programs and cyber security
20 Program with Luminant Power Nuclear Business Unit.
21 Luminant Power comprises of two operating reactors,
22 Comanche Peak Unit 1 and 2, and the a future two-unit
23 new building at the same location.

24 It is my privilege this afternoon to
25 present to the this ACRS Subcommittee of our views on

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 cyber security would be addressed during a safety
2 related digital upgrade and how the handoff would
3 occur at various phases of the system development life
4 cycle.

5 Including related activities at the
6 vendor-integrated facilities. About my background, I
7 have been involved in the nuclear power industry for
8 the last 25 plus years, with experience in design of
9 nuclear power plant, I&C and digital systems.

10 Several years of system engineering,
11 maintenance and project management aspects of nuclear
12 power plant, digit and I&C designs. In addition, for
13 the last 15 years I've been very active in a
14 leadership role in several industry initiatives and
15 NEI, INPO, EPRI and NITSL.

16 In the area of digital I&C modernization,
17 Y2K and cyber security. I'm also the lead for the
18 STARS Alliance for the cyber security Working Group.

19 Those that do not know STARS, it's an
20 alliance of seven single-site licensees and comprising
21 of 13 units. In the presentation I am about to make
22 is something that the Alliance agrees that that's the
23 approach that they're going to take going forward on
24 digital upgrades.

25 Before I go into my presentations, I also

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 wanted to let the Chairman know that the presentation
2 is a bit lengthy. I do not plan to cover each item on
3 each slide, but my goal is to cover the process and
4 how the process flows from one phase to another and
5 how we address cyber security. So that's the goal.

6 Next slide. We support the proposed
7 Revision 3, of the Reg Guide 1.152. Keeping focus on
8 the Reg Guide on safe, secure, reliable safety design
9 is the key.

10 For us, safe and secure all equates to
11 security of the safety system to ensure that the
12 safety functions are not compromised in any way. The
13 design under Reg Guide 1.152, will address protection
14 against non-malicious events.

15 The licensee cyber security Program under
16 10 CFR 73.54, will address the malicious attacks to
17 ensure that the safety functions of the CDA are not
18 compromised or further compromised.

19 The combination of the Reg Guide 1.152,
20 and Reg Guide 5.71, or even NEI 08-09, Rev 6,
21 seamlessly addressed the secure design development
22 integration, implementation, installation and
23 operation of the safety related digital systems in the
24 plant.

25 Collectively, both regulations address the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 complete spectrum of threats to the CDAs. The next
2 three slides are basically, lay the foundation for the
3 cyber security program at Luminant and basically at
4 all of the nuclear stations. So, I'll quickly go over
5 that.

6 CHAIRMAN BROWN: Before you, a brief
7 interruption. You hit at first with the plants in
8 which you are looking to utilize this. You said it
9 was Comanche Peak?

10 MR. AMIN: Yes, Comanche Peak is what
11 Luminant owns. The STARS Plants are Wolf Creek,
12 Callaway, South Texas Project, SONGS, which is
13 Southern California Edison.

14 CHAIRMAN BROWN: Is this a backfit? I
15 mean is this, the instrumentation you're putting in,
16 is this, I'm trying to recall some memory here. Is
17 this a new plant? It's an upgrade, right?

18 MR. AMIN: No, these are upgrades, this is
19 an operating plant.

20 CHAIRMAN BROWN: Great, okay, thank you.
21 I just wanted to make sure it wasn't, one of the other
22 ones that I hadn't connected the dots with yet.

23 MEMBER STETKAR: You're not talking about
24 Comanche Peak Unit 2?

25 MR. AMIN: Well, Unit 1 and 2 is what I'm

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 talking about. These are operating, and Units 3 and
2 4, is the new builds.

3 MEMBER STETKAR: Three and four.

4 MR. AMIN: No, I'm not talking about any
5 new builds, here. Okay.

6 CHAIRMAN BROWN: That's Units 1 and 2?

7 MR. AMIN: Yes. The key elements of all
8 U.S. nuclear power plant cyber security Programs are
9 the station's cyber security plan, which will become
10 part of the operating license.

11 And the cyber security policy programs and
12 implementing procedures. The station's cyber security
13 defensive strategy, the security controls, which are
14 broken down into three categories.

15 These are technical security controls,
16 operational and management. Next slide. The
17 defensive strategy is the key element of any cyber
18 security Program.

19 At Luminant Power our defensive strategy
20 follows the principles that are illustrated in this
21 diagram. Our strategy is based on diversity and
22 defense in depth.

23 The safety related assets are located in
24 Level 4. We will isolate all plant systems related
25 CDAs from any and all external attacks using

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 deterministic means, air gaps, diodes, whatever people
2 call them nowadays.

3 Our diodes will be placed at Level 3,
4 between Level 3 and 2, so that's where the air gap
5 occurs, and there are no connectivities from Level 4,
6 directly into Level 2, or Internet or any modems of
7 any sorts.

8 Each layer and level has a separate
9 boundary device.

10 CHAIRMAN BROWN: Let me, can I, when you
11 talk about Level 3, plant computer, technical support,
12 SPDS, in other words, those are all links within that
13 level.

14 There's, I mean you've got your own
15 separate system for doing that part of the
16 communication. It's not integrated. I read that as
17 no connection to anything else on the business,
18 corporate, any other type of network that you've got
19 flowing around. It's all internal?

20 MR. AMIN: Correct, that is correct. To
21 Level 3, that is absolutely correct. When it goes to
22 the EOF --

23 CHAIRMAN BROWN: That's different.

24 MR. AMIN: -- from Level 3 to Level 2,
25 that's different. But there will be communication

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 rules in place that will drive that, you know, how
2 data flows outside.

3 CHAIRMAN BROWN: But there is
4 communication back end, relative, so that EOF --

5 MR. AMIN: No, there is no communication
6 to any CDA through any kind of back feed. It would be
7 a one-way, logically and physically isolated and one
8 way.

9 CHAIRMAN BROWN: I understand 3 to 2, and
10 I'm looking at the EOF, the Emergency Operation
11 Facility, correct?

12 MR. AMIN: Correct, yes.

13 CHAIRMAN BROWN: So that will then be
14 subject to two-way communication to the outside world?

15 MR. AMIN: That is correct. That is
16 correct.

17 But that, there is not way that the EOF is going to be
18 able to take out the plant computer which --

19 CHAIRMAN BROWN: No, I'm, that's, there is
20 no connection. I'm just looking at the one-way arrows
21 and making sure that's --

22 MR. AMIN: Correct.

23 CHAIRMAN BROWN: Okay.

24 MR. AMIN: It is also important to note
25 that most aspects of this particular design of the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 defensive strategy is addressed under Reg Guide 57.1
2 or NEI 08-09.

3 In other words, under 73.54, and is more
4 or less independent of Reg Guide 1.152. If you were
5 doing a safety-related upgrade, you wouldn't be
6 addressing or designing any parts of this particular
7 defensive strategy. The defensive strategy will be
8 leveraged and you'll see how, as we move into the
9 other slides.

10 DR. HECHT: Can I ask a question?

11 MR. AMIN: Yes.

12 DR. HECHT: On the previous slide, where
13 do you put things like HVAC, internal power regulation
14 control, all those supporting systems that are part
15 of --

16 MR. AMIN: They would all be in Level 4.
17 They are all Level 4 systems. The HVAC systems at a
18 plant, HVAC control systems, electrical power systems,
19 they are all in Level 4, in Cyber protected area.

20 DR. HECHT: Even if the support non-Level
21 4 assets?

22 MR. AMIN: When you say non-Level 4
23 assets, say the plant computer is in, it depends, the
24 plant computer is located in the Level 3, but Level 3
25 plant computer is inside the protected area.

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 We have just chosen to call it a separate
2 logical layer. In other words, you have safety-
3 related systems in the current operating plants, which
4 doesn't have much technology, have these data links
5 that provide outputs to the plant computers so data
6 can be read by the Operators and Engineers and that
7 kind of thing. So that's why we have distinguished
8 the plant computer in Level 3.

9 DR. HECHT: I see, so it's like if you
10 basically have nothing more than a dumb motor that's
11 based, that has a tachometer output, that you would
12 consider to be a Level 4?

13 MR. AMIN: Yes, mostly the information-
14 type systems are in that level.

15 DR. HECHT: Okay, thank you.

16 MR. AMIN: So currently we're in the
17 process of updating our site policies, programs,
18 procedures to integrate the cyber security, 10 CFR
19 73.54 rule for us.

20 cyber security is just another attribute
21 added to many attributes of the plant digital systems
22 that we have to address. Therefore, integrating the
23 technical aspects into the product makes sense for us.

24 And you will see that as I go into the
25 life cycle. It is important to understand the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 complexities also associated with this one statement
2 that I made.

3 And if I provide a correlation, physical
4 security is more or less a stand-alone parameter
5 system and does not integrate into many site programs
6 and processes.

7 cyber security is different. It
8 integrates into almost all site programs and processes
9 due to the fact that the cyber security is one of the
10 many attributes of digital systems that control the
11 plants.

12 So it is very important that we integrate
13 cyber security into our existing programs and
14 processes, in order to ensure consistency and, of
15 course, continuous improvement via the data captured
16 in our corrective action programs and the self-
17 assessments and audit programs that exist today at
18 nuclear power plants. Next slide.

19 So, having laid the foundation for the
20 program, we will next see how cyber security is
21 addressed in system development life cycle. How do we
22 assure that the upgrade satisfies both the
23 regulations, Part 50, as well as 73.

24 And how are the hand-offs accomplished
25 during this life cycle. Next slide. This slide

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 provides an overview of the complete system
2 development life cycle and key considerations for each
3 phase.

4 As you can see, the 10 CFR Part 50/52,
5 which is associated with safe, secure and reliable
6 design, is addressed during the first four phases of
7 the life cycle. Then, that becomes the transition
8 point where the rest of the Part 73 Regulations are
9 addressed, once the asset is commissioned in the
10 plant.

11 And I think we talked about it this
12 morning as to what happens during the operations and
13 maintenance, how do we ensure integrity of the asset
14 when it moved from the design phase into the plant
15 environment and how do we continuously manage and
16 maintain the secure configuration.

17 Overall, the 10 CFR 73.54 covers and
18 envelopes the 10 CFR 5052 aspects of the cyber
19 security regulations. If you look at all the security
20 controls and convert them into requirements, I don't
21 think so there is any requirement left that you have
22 to address in cyber security.

23 And I hope Eric Lee and his staff feels
24 the same way. Because it's a deterministic rule,
25 therefore, you know, you have to go through 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 address each of those controls.

2 So next I will briefly go to each phase,
3 through each phase. So, next slide.

4 MEMBER STETKAR: Jay, can I interrupt?

5 MR. AMIN: Yes.

6 MEMBER STETKAR: One of the questions I
7 asked the staff this morning was, as part of the Reg
8 Guide 1.152 Guidance, they talk about the need to
9 perform assessments.

10 Some people call them fault tree analysis
11 failure modes and effects analysis, they're called
12 vulnerability assessments, to satisfy, to examine
13 vulnerabilities for the safety-related functions under
14 10 CFR 50 or Part 52.

15 And Reg Guide 5.71, also talks about the
16 performance of assessments. It is somewhat less
17 clear, but the words assess, risks and vulnerabilities
18 show up.

19 Where in that whole process, that sort of
20 chain that you showed on the last slide, are those
21 assessments performed and who performs them? And are
22 they integrated or are they separate?

23 MR. AMIN: So you're talking about, let me
24 understand your question. You're talking about the
25 assessments for cyber security?

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MEMBER STETKAR: I'm talking about
2 assessments, no actually I'm talking about an
3 integrated assessment that looks at various threats
4 and vulnerabilities. Some of those might be cyber
5 security threats, some of them might be hardware
6 related threats.

7 Some of them might be support systems
8 related threats. You know, I don't want to be as
9 precise and as compartmentalized. That's why I'm
10 asking about where are those assessments performed and
11 who does those assessments in your organization?

12 MR. AMIN: At a high level, the first
13 opportunity for looking at the Cyber assessments for
14 us, it begins at the conceptional design phase.

15 MEMBER STETKAR: Well, I'll ask the
16 question when you finish this slide, if you want to do
17 that.

18 MR. AMIN: No, I mean I will address that
19 as we go through each life cycle and you will see
20 that, it's going to be apparent.

21 MEMBER STETKAR: Okay.

22 MR. AMIN: But my slides focus strictly on
23 cyber security. I didn't include the other aspects,
24 but when I --

25 MEMBER STETKAR: I understand 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 also within the context of the cyber security
2 Regulatory Guide, there are the, there are, there's
3 guidance about the performance of assessments.

4 MR. AMIN: Correct.

5 MEMBER STETKAR: The vulnerabilities and
6 the weaknesses and things like that.

7 MR. AMIN: Right. And I think that's a
8 great question and I hope I'll address them as we go
9 forward into each phase.

10 MEMBER STETKAR: Good, okay, thanks.

11 CHAIRMAN BROWN: Let me, if you look at
12 your Slide 6, in the top echelon, under the 10 CFR
13 50/52, under the design phase, there's a line bullet
14 that says preliminary cyber security Assessment.

15 So that's done during, I presume, this is
16 during your licensing, is this licensing phase? Or is
17 this --

18 MR. AMIN: Okay, if they asset or if the
19 upgrade is performed under the LAR process, then under
20 ISG-06, when we submit the submittals to the NRC for
21 preapproval, then we would have to address many of
22 those elements as part of that requirement.

23 CHAIRMAN BROWN: So that's one of your
24 early phases then, ISG-06?

25 MR. AMIN: Yes.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 CHAIRMAN BROWN: So you've actually done a
2 Cyber, you're saying you'll be doing some type of a
3 Cyber Assessment. It's just not, I'm just trying to
4 get at John's question, as to when you're doing this.

5 Because you're really doing it to some of
6 this before you get through with the licensing
7 process?

8 MR. AMIN: That is correct. See the
9 process is such that we will begin the assessment at
10 the conception phase, we will conceptualize.

11 Then when the requirements are specified,
12 we will make sure that system level requirements, even
13 Cyber-type requirements are explicitly specified in
14 the requirement specs.

15 And then you go through, and when you're
16 into your design phase and your design is getting
17 finalized, that's when we will start the assessment,
18 because for us assessment is deterministic.

19 That means we need to make sure we have
20 addressed each of those 148 security controls, during
21 the assessment process. And we will complete the
22 assessment for say, a design complete phase and then
23 we will again revisit that assessment when we
24 implement in the field to make sure that all of our
25 assumptions have not changed and our assessments 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 still valid when the asset was moved from a
2 development environment into the plant environment.

3 So at the end, before the system is turned
4 over to Operations, we have to complete that
5 assessment. Make sure that all the requirements of
6 the plan are satisfied, before we turnover the system
7 draft.

8 CHAIRMAN BROWN: Okay. It's kind of
9 getting to what we've talked about a little bit as to
10 when you start and who's involved. Design phase, you
11 said it very clear, Preliminary cyber security
12 Assessment.

13 Then, during your integration and test
14 phase, this is the development of the system.

15 MR. AMIN: And I will cover that in detail
16 when I go through this.

17 CHAIRMAN BROWN: Okay, well, I'll just, it
18 talks about cyber security Assessment approved, pre-
19 installation approval.

20 MR. AMIN: Yes.

21 CHAIRMAN BROWN: So, it's, as opposed to
22 having a handoff, sounds like there's an integrated
23 look at the cyber security Requirements of 5.71, done,
24 during the design phase.

25 MR. AMIN: For us --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 CHAIRMAN BROWN: And during the licensing
2 phase. This is a phase in which you would be doing
3 your, you know, LAR preparations before you got your
4 final license request approved.

5 MR. AMIN: Correct. You are absolutely
6 correct. Whenever we submit to the NRC an LAR, we
7 will have traceability matrix that will really spell
8 out what Reg Guide 5.71, or NEI-08-09 security
9 controls are we addressing as part of the design.

10 Because, for us, we look at cyber security
11 in an integrated fashion. If I try to segregate both,
12 then at the end it is too late. When somebody finds
13 an issue, I cannot go back to design phase because,
14 guess what, I'm incurring a huge loss of investment
15 because the safety system cost a lot of dollars.

16 So for us, as licensee, we have to look at
17 the big picture from the starting to the end point.

18 CHAIRMAN BROWN: So, I see, okay, that's
19 from your perspective, I can understand that. But now
20 how do you get NRC buy in that you've done the second
21 phase? You know, this is all now done, okay, you're
22 getting their buy in up in the licensing phase where
23 what we've just heard this morning, was there's a
24 separation of church and state in this case, between
25 the licensing venue and the post-licensing, you know,

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 installation and all that other type stuff that was
2 talked about.

3 MR. AMIN: And I can, the way I would
4 address that is that when the NRC talks about safe,
5 secure and reliable designs, basically we are now
6 going to do something that is going to overlay some
7 complexity on the safety related design.

8 And I'll pick on Westinghouse, since they
9 are here in numbers.

10 (Laughter.)

11 MR. AMIN: If I was buying the reactor
12 production system, I'm not going to expect
13 Westinghouse to put in this fancy widget that I came
14 across and said, my god, this is, you know,
15 technology-driven, will make my life easy.

16 If I tell them to put it in as part of
17 that particular reactor production system, now it
18 increases the complexity because the failure modes,
19 all that have to be considered, interactions and all
20 that.

21 So we would rather not do that. So what
22 are we doing? When I talk about technical controls,
23 we are talking about simple things that we do today,
24 access controls.

25 Like, you know, make sure we have

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 function-based passwords so we can have control over
2 who access what part of the applications or, you know,
3 connectivities.

4 The direct connectivities and indirect
5 connectivities are something that are important to
6 safe, reliable design.

7 The NRC in the morning's presentation used
8 some examples in the industry. I consider them as
9 flaws in the requirement specs, flaws in the design
10 configuration management and change management.
11 Because those are the ones that introduce the
12 susceptibilities that show up during some event.

13 Call it a Cyber, or call it some other
14 event. So, yes, all those things need to be addressed
15 up front in the life cycle. And that's what we will
16 do.

17 CHAIRMAN BROWN: So, your LAR, when you
18 submit it, would have what you've, thank you, if I'm
19 putting words in your mouth tell me. Would have the
20 aspects necessary, in your mind, to meet the 5.71
21 requirements?

22 MR. AMIN: Yes.

23 CHAIRMAN BROWN: Or guidance, excuse me.

24 MR. AMIN: Guidance.

25 CHAIRMAN BROWN: The guidance. And you

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 would expect, again I may be putting words in your
2 mouth, that when you get your license approval, so
3 they sign off and give you a letter, that you would
4 say, okay, NRC has bought in on those. And I'm
5 sitting here thinking that --

6 MR. AMIN: No.

7 CHAIRMAN BROWN: -- that's not the case,
8 based on what I've heard this morning.

9 MR. AMIN: And I'll answer it a little bit
10 differently. I would say that the NRC, 10 CFR Part
11 50/52, is satisfied. However, I still have to address
12 the remainder of the security controls, that I still
13 have to address as I move the asset into the plant
14 environment and complete my cyber security assessment
15 where at that point would be the final assessment that
16 documents the final security configuration for that
17 particular asset for the life of the plant.

18 CHAIRMAN BROWN: But your equipment is
19 designed at the point that gets there.

20 MR. AMIN: That is correct.

21 CHAIRMAN BROWN: And I'm looking at the
22 way that we heard this morning, that now you're going
23 to get a second review or input that says, well, is
24 your security stuff really okay?

25 And you've now got the hardware and the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 software and the controls on site.

2 MR. AMIN: See, the way I would do it is -
3 -

4 CHAIRMAN BROWN: Do you get what I'm
5 saying?

6 MR. AMIN: Yes.

7 CHAIRMAN BROWN: Now you're going to get,
8 I don't want to use the word second guess because
9 that's not right. But you're getting a second --

10 MR. AMIN: I know where you're coming from,
11 and if I were in a real situation, if I was
12 uncomfortable with a high assurance that this thing is
13 going to be challenged by NSIR, guess what, I'm in
14 their offices, laying out a process, making sure that
15 I am not going to be incurring a loss of investment at
16 the tail end where it stops my entire modification in
17 its track and then we go through that one agency
18 accepted and one didn't.

19 So, I don't see that happening with what
20 we are doing, but that could happen in real life.

21 CHAIRMAN BROWN: It sounds like you want
22 to have control of this.

23 MR. AMIN: Yes.

24 CHAIRMAN BROWN: And all I'm trying to do
25 is figure out how I can get a copy of the transcript

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 in the future, so I can, because I'll never remember
2 all this.

3 Because it just emphasizes the point that
4 the three of us have made here about the earlier
5 integration of the cyber security requirements during
6 the licensing phase to make sure that stuff is in
7 place and hooked, before you get to this post-delivery
8 time, which is too late.

9 It's not too, too late, but it's before,
10 you know, before you've actually told the guy go build
11 it and look this, so that you don't incur that
12 expense.

13 So I'm just trying to probably say the
14 thing we've said seven or eight times last time.

15 MR. CORREIA: And that goes, Rich Correia,
16 that goes back to my earlier statement that we need to
17 develop that integrated plan now. That's, it's done
18 informally now.

19 CHAIRMAN BROWN: Yes.

20 MR. CORREIA: But we need to document it,
21 memorialize it for the future.

22 CHAIRMAN BROWN: Okay, I'm just, I'm just
23 trying to make, emphasize the point in my normal,
24 laborious way here.

25 MR. AMIN: I has some feeling that this

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 question was going to come up in my presentation.

2 (Laughter.)

3 CHAIRMAN BROWN: Okay, John, Jack, did you
4 all have anything to add to this, or did I hammer it
5 enough?

6 MEMBER SIEBER: I agree with you.

7 CHAIRMAN BROWN: Okay, Myron?

8 DR. HECHT: Yes, I'd like to ask some
9 questions about what you put in the Level 4 non-safety
10 systems at the conceptual phase and whether, how much
11 interaction or oversight one has?

12 MR. AMIN: For the non-safety systems
13 would mean that things are important to safety could
14 be NSSS control systems, or it could go to the other
15 end of the spectrum under the new regulations.

16 Now NRC will regulate the so-called
17 reactivity transient initiating systems like turbine
18 controls. Even though it is a non-safety system, it
19 can cause a plant trip or hit a drain trips, or hit a
20 drain system that may be digital.

21 All those assets, fortunately for us, are
22 all in the protected areas, so they are all in Level
23 4. So they will be in Level 4. All the control
24 systems will be in Level 4, for us.

25 DR. HECHT: Well, that's physically where

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 they're located. I'm talking about what the
2 developmental pre-installation rigor is going to be?

3 MR. AMIN: The pre-installation rigor,
4 like you're talking about, I assume, you're leading
5 toward the secure development environment?

6 DR. HECHT: No, that's for, we believe
7 that that's for the 1.152 aspect of, earlier you
8 showed that the 5.71, or 08-09 aspects do incorporate
9 all of the life cycle, but we distinguish between
10 safety and non-safety systems.

11 So I'm talking about non-safety system.
12 Let's just consider something as, the emergency
13 notification system.

14 MR. AMIN: See, for us, the process is the
15 same, whether we are pursuing a turbine control system
16 or whether we are pursuing a reactor protection
17 system.

18 The difference is the rigor. In a safety
19 system we have to follow all the specific guidance,
20 we'll have more, we have to address many other
21 regulatory required elements into our LARs.

22 And we have an independent V&V that we
23 will have to go through. So those elements are not
24 there. But, some of these fundamental elements of a
25 life cycle are still followed for all non-safety

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 control systems also.

2 Because, for us, if the turbine trips, we
3 are not producing any electricity so, you know, that
4 system becomes even more important to make sure that
5 we address cyber security and that's what our plan is.

6 DR. HECHT: Okay, I was trying to get to a
7 lower level of operational significance, but that's
8 still within the Level 4 containment.

9 So I was trying to give an example of an
10 emergency response system or maybe some access control
11 system, I mean physical access control system, that
12 probably is at a Level 4, and which you're probably
13 buying largely off the shelf. And the vendor is
14 probably selling that system to many other
15 applications besides nuclear.

16 And so what, given that there is
17 connectivity or the potential connectivity between
18 that and the reactor protection system, what does
19 that, what implications does that have for your design
20 process or your pre-installation process, let me put
21 it that way.

22 MR. AMIN: Well, pre-installation process,
23 what we do is, if we have a safety system that
24 connects to a commercially available product, okay,
25 for example like what you are mentioning, and say

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 there was some connection, that connection would have
2 to be fully analyzed.

3 In our case, if it's going to connect to a
4 safety or part of a safety system, we would spend that
5 extra dollars to go inside the box and make sure that
6 we fully understand, through the right experts, what
7 kind of connectivities are there.

8 For all human purposes we are currently
9 pursuing an approach of a standardized scholar
10 defensive strategy where we are saying that anything
11 going from a high level to a lower level system, has
12 to be physically and logically one way only.

13 So we do not want two-way communications,
14 physical and logical, that is very important. Because
15 we discuss there are many that feel, oh, I am
16 protected, but physically they're not.

17 Physically there is a common, you know,
18 more bacteria that will get them. So that is our
19 approach going forward, is what we plan to do.
20 Because we are very sensitive towards safety and non-
21 safety interactions.

22 And all these incidents that occurred, you
23 know, we believe firmly that energies put forth during
24 the conceptual design and requirement phase and how do
25 you connect systems, is very important in ensuring a

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 safe, reliable operating system. I hope I answered
2 your question.

3 DR. HECHT: Yes, thank you.

4 CHAIRMAN BROWN: Okay.

5 MR. AMIN: Okay, the concept phase. Our
6 goal for the concept phase is to ensure that the
7 pertinent security controls are addressed consistent
8 with the station cyber security defensive strategy and
9 to establish a foundation for success in the more
10 detailed phases.

11 The information that is compiled on the
12 endpoint vision of the upgrade and key high level
13 requirements, including improvements based on previous
14 operating expedience. What we also do in this
15 particular phase is also consider things like how do
16 we plan to maintain the CDA integrity from a cyber
17 security standpoint?

18 We think about all this during the
19 conceptual design phase. How will we be conducting
20 security related surveillance and how can we simplify
21 that. And these things are important to us, so that
22 we can then look into the vendor products so during
23 this phase we will also pay a visit to the potential
24 vendors to assess their products from a cyber security
25 standpoint.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 Review what kind of secure development
2 environment do they have? What kind of internal, in-
3 house cyber security process are they following?

4 And this is currently a challenge since
5 there is no consistency in this area due to the fact
6 that it is evolving and it is new for the vendor, as
7 well as it is new for the licensee.

8 So the industry is, through NEI, is trying
9 to see what we can do to establish consistency and
10 make sure we capture the right requirements with our
11 vendors, so we make sure they understand what our
12 expectations are.

13 And we also make sure that we are
14 providing clear requirements rather than ambiguous
15 requirements or attaching them in Reg Guide 5.71, and
16 telling the vendor, here, comply.

17 So from the, now that we, we will have, at
18 the conclusion of this concept phase we have captured
19 the high-level requirements and the concepts that then
20 become a starting point for the requirement phase.
21 Next slide.

22 MEMBER STETKAR: Jay.

23 MR. AMIN: Yes.

24 MEMBER STETKAR: Before you get off the
25 concepts phase, I'm going to try again to ask you the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 question I asked before. One of the major elements
2 of Reg Guide 5.71, is the convening of what it calls a
3 cyber security Team.

4 And one of the roles and responsibilities
5 of the cyber security Team is evaluating or
6 reevaluating assumptions and conclusions about current
7 cyber security threats, potential vulnerabilities to
8 and consequences from an attack, the effectiveness of
9 existing cyber security controls, defensive strategies
10 and attack mitigation methods.

11 And cyber security awareness and training
12 of those working with or responsible for CDAs and
13 cyber security controls throughout their system life
14 cycles. Could you tell me where in the concept phase,
15 how is Luminant implementing the cyber security Team
16 at this stage of the design life cycle and what does
17 that cyber security Team do, in practice, since you
18 have this process?

19 MR. AMIN: That's a perfect question,
20 because it is under my belt. What we plan to do is
21 during the conceptual design, we will involve the
22 cyber security, we call them cyber security Subject
23 Matter Expert.

24 MEMBER STETKAR: Okay, that's --

25 MR. AMIN: And we will write and you'll

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 see those words used in my slides.

2 MEMBER STETKAR: Okay.

3 MR. AMIN: And so we use them to perform
4 that activity, because they have that niche knowledge
5 that is not there. Ultimately our goal is to train
6 our Digital Engineers into some form of cyber
7 security.

8 But the fact remains that licensees will
9 end up with one or two experts at their sites.

10 MEMBER STETKAR: Do you have, I know we're
11 running long on time here and I know you have to get
12 to an airport, so I'll be careful.

13 MR. AMIN: That's all right.

14 MEMBER STETKAR: Have you developed any
15 guidance yet for that team or is this still pretty
16 well in the developmental process? In other words, do
17 you actually have guidance for what those cyber
18 security Subject Matter Experts do, what type of
19 evaluations they perform?

20 MR. AMIN: We have started thinking about
21 it and we're in the process of putting together the
22 updating of our procedures to address that.

23 We have already addressed many elements of
24 these Cyber requirements under the NEI protocol
25 program. We have already done that. So we are now

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 going to the next level, is what I characterized that
2 and going through a much more formal rigor within the
3 procedures also.

4 So you're looking at revamping of
5 procedures because consistency is what I worry about.

6 I lose sleep over consistency every day. That how do
7 we assure that one person to another person, they are
8 consistent in what they do.

9 MEMBER STETKAR: Okay, thanks.

10 MR. AMIN: Okay. The requirements phase.

11 The goal of this phase is to ensure that the security
12 requirements are clearly specified to ensure that the
13 vendors address them so that we have the confidence
14 that the upgrade will meet the Reg Guide 1.152,
15 requirements and pertinent 5.71 requirements of
16 security. So, hypothetically, assuming that the
17 safety project is underway, the focus is on two key
18 areas.

19 Site-specific requirements for cyber
20 security that were developed during the concept phase.

21 I think we discussed some of these in the morning.
22 These are like digital I&C upgrade-specific cyber
23 security architecture.

24 Communication, networking requirements
25 consistent with station cyber security defensive

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 strategy. That is very important. Because we want to
2 make sure that these requirements are clearly
3 specified so that vendors can understand them, so then
4 they can provide us a design that meets those
5 requirements.

6 So this up front work becomes very
7 critical for us. And these include things like, you
8 know, directing direct connectivities, ports and
9 services and modems, communication protocols. We
10 discussed those lessons learned this morning, also.

11 Chain of custody, how the transfers would
12 occur. And then the second key aspect is the vendor/
13 Integrator in-house cyber security secure process
14 level, I think we talked about it.

15 CHAIRMAN BROWN: vendor security, we
16 talked about that this morning. In other words, from
17 the secure development --

18 MR. AMIN: Environment.

19 CHAIRMAN BROWN: -- operating environment,
20 okay. And that you effectively have to have a similar
21 environment at the vendor for the development of this
22 software, hardware design, architecture, in place at
23 the vendor's facility, for the area, for your product.

24 For what you're ordering. And, how they
25 separate that off, that's something that you have 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 ensure, at least that's what I got out of reading of
2 the stuff and the conversation this morning.

3 MR. AMIN: That is correct.

4 CHAIRMAN BROWN: So you have to transfer
5 your requirements effectively that you have to run on
6 site. You have to transfer those to the vendor, at
7 least in some part of his facility and his design
8 capabilities. That's within, you're shaking your head
9 up and down and saying, I could have stopped a few
10 sentences ago, but I'm just making sure I covered it.

11 MR. AMIN: No.

12 CHAIRMAN BROWN: But that's what you would
13 be doing, is that correct?

14 MR. AMIN: That's correct. We would write
15 into the requirements, we would have, we would also
16 the audit the vendors to make sure that, you know,
17 they have that process.

18 CHAIRMAN BROWN: But want NRC to be
19 challenging that either, once you've got --

20 MR. AMIN: I mean NRC can challenge us on
21 anything, any time.

22 CHAIRMAN BROWN: Oh, I know. But you know
23 what?

24 MR. AMIN: That's always a given.

25 CHAIRMAN BROWN: But my point being is you

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 don't want that to come after the fact?

2 MR. AMIN: That is correct, that is
3 correct. That is correct, yes.

4 CHAIRMAN BROWN: And you want them in bed
5 with you, figuratively speaking?

6 MR. AMIN: Yes, absolutely.

7 CHAIRMAN BROWN: Excuse me, I'm sorry. A
8 colloquialism that I probably should not have used.
9 You want them agreeing with you that your approach is
10 satisfactory in that phase, again?

11 MR. AMIN: Yes, absolutely, yes.

12 CHAIRMAN BROWN: As part of the licensing
13 phase?

14 MR. AMIN: That is correct, because we
15 want certainty before we spend too much money on the
16 project. And I believe the ISG-06, correct me if I'm
17 wrong, Bill, but the ISG-06 has laid out a process and
18 this, requirement of this life cycle phases that I'm
19 discussing pretty soon, one of the STARS plants,
20 Diablo Canyon is going to cycle through as a pilot
21 project for this process.

22 CHAIRMAN BROWN: Okay.

23 MR. AMIN: So security will also be part
24 of what they're submitting, I know that.

25 CHAIRMAN BROWN: Okay, go ahead, thank

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 you.

2 MR. AMIN: So at this stage, we have a
3 clear idea as to what security requirements from Reg
4 Guide 5.71 or NEI 08-09, Rev 6, are being addressed as
5 part of the safety-related upgrade.

6 They are mostly in the technical controls
7 area. This information would also be addressed in
8 the ISG-06, related LAR submittal if the safety-
9 related upgrade required a preapproval from the NRC.

10 So I wanted to make that point. So, in
11 other words, we will have a clear nexus between the
12 Reg Guide requirements to the, yes, a clear nexus to
13 the Reg Guide requirements, so we know what we are
14 asking and the NRC would, in turn, know that okay
15 they're addressing this set of requirements within the
16 design of the product or the LAR that we are seeking.

17 DR. HECHT: Can I ask a question?

18 MR. AMIN: yes.

19 DR. HECHT: About the tradeoff between
20 controls, let's just say between an administrative
21 control and a technical control. Might define a
22 requirement which basically allows for an
23 administrative control in place of a technical
24 control, in order to reduce costs or increased
25 operational efficiency or something like 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 How will you assure that, or do you feel
2 that you're taking a risk by doing that, before
3 clearing it with the NRC, and if you do clear it with
4 the NRC, how will you be sure that your agreements are
5 in fact honored, particularly if there's a problem
6 later on?

7 MR. AMIN: That's a tough question. No,
8 but here, if I'm, see the process is laid out, okay,
9 we discussed this morning about the cyber security
10 assessment process. I think there was some questions
11 from the Subcommittee, that what process, how would
12 you do the assessment?

13 It's already laid out. There's a
14 deterministic process laid out under NEI 08-09, Rev 6,
15 with clear cut requirements as to how you go about
16 doing the assessment, cyber security assessment.

17 And same what we would, what that process
18 requires us that is we take a, say for example a
19 technical control, and I determined that I don't want
20 to implement it and it applies, and I'm going to do it
21 in an alternate manner, then I have to justify myself
22 that that alternate control is equal or better than
23 the control expectations that were there for that
24 original control.

25 And I think that is pretty much ingrained

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 within the licensee community that that's what will
2 have to do.

3 DR. HECHT: Don't you think that that
4 might change by level? For example, I might be
5 satisfied with an administrative control, even though
6 it's inferior to a technical control, but it might be
7 acceptable at Level 2, whereas it might not be at
8 Level 4?

9 MR. AMIN: That is possible, but typically
10 when we talk about the security controls, we are
11 talking about most assets in Level 3 and 4, so we're
12 not going into the Level 2.

13 Level 2 is the business LAN, which is out
14 of scope of 10 CFR 73.54. Unless I misunderstood your
15 question.

16 DR. HECHT: No, okay. What I really
17 should have said is higher level to lower level.
18 Let's just say, is there any difference in your mind
19 between Level 3 and Level 4?

20 MR. AMIN: For us at Comanche Peak, there
21 is very little difference between Level 3 and Level 4,
22 because remember my diodes are protecting Level 3 and
23 Level 4.

24 It's completely air gap, any asset in 3
25 and 4 is totally air gap through --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 DR. HECHT: Well, it's not totally, it's
2 one-way, right?

3 MR. AMIN: Yes, it is one-way. So what
4 I'm saying is that Level 3 and Level 4, more or less,
5 carry the same type of protections.

6 DR. HECHT: Okay, so basically you have
7 high security and low security?

8 MR. AMIN: Right.

9 MR. ERLANGER: I just want to clarify,
10 this is Craig Erlanger, that regardless of what level
11 we're in, every digital asset or critical system that
12 goes in gets the same 148 security controls and finds
13 them.

14 It doesn't, you're not putting a less, a
15 lower level of a security control implied here in
16 Level 2 versus Level 4. What Jay is laying out is
17 that there's a communication pathway in the separation
18 of systems.

19 They're still getting all the security
20 controls applied to them.

21 DR. HECHT: So, I'm confused. Does that
22 mean that your rigor at Level 2, would be the same as
23 it would be at Level 4?

24 MR. ERLANGER: What he's talking about is
25 the communication pathways, it's a different thing.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 They still have the same 148 security controls applied
2 to them in Level 2, 3 or 4. Whatever the architecture
3 they determine.

4 DR. HECHT: Okay, so let me ask it in a
5 specific sense. Level 2, might say administrative
6 control, only three people are allowed into the TSC at
7 one time.

8 And that could be implemented
9 administratively or you could have a man trap in
10 there which has double doors and says that, you know,
11 basically one person goes in and then, and you would
12 use that man trap at a Level 2 facility, at the, Level
13 2 part of the plant, the same way you would a Level 4?

14 MR. ERLANGER: So, and Jay I'm not going
15 to speak for Luminant. So Jay goes through a process,
16 the criteria, the process outline, and whether it's
17 08-09 or Reg Guide 5.71, he'll determine what scopes
18 into the rule for safety security emergency
19 preparedness in 2, based on the function, not the
20 system.

21 DR. HECHT: Okay.

22 MR. ERLANGER: He'll ID the systems based
23 upon the need, whether it's a technical support center
24 that has a need to not only talk to the Control Room,
25 but maybe push out information to the public.

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 He'll determine where it fits in the
2 architecture. In a perfect world, these could work
3 concurrently with physical protection boundaries.

4 Whether a location is the vital area, the
5 protected area or a controlled area. In some
6 instances it won't. The controls though, the 148
7 controls, the technical operational management ones,
8 they apply no matter what the level is.

9 Jay does have the latitude though to say I
10 will apply the control you've described, I won't
11 apply, I'll explain why it doesn't fit. Perhaps it's
12 a, and again, the analogy I used this morning was a
13 Control Room Operator might not put a password on his
14 work station because he could be prevented from
15 performing a safety function that's time sensitive and
16 lock himself out.

17 Or, he can come up with a third way, that
18 meets the same intent, the same level of protection
19 and control. If it is a, the example of adding that,
20 the extra heavy door or whatever, that's up to Jay, as
21 long as it meets the intent and fulfills what we're
22 trying to do with that control.

23 But I kind of felt, and this is my opinion
24 from just listening in the background. That there was
25 a bit of potential confusion that we do different

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 things at different levels for the application of
2 security controls.

3 DR. HECHT: I think you, would you
4 because, for example, not apply a control saying it's
5 not justified at Level 2? Because, basically, that
6 doesn't have too much of an impact on the plant.

7 MR. ERLANGER: You would go, but you have
8 to --

9 MR. LEE: No, because, this is Eric Lee.
10 Our rule requires that those systems that could
11 adversely impact, I think Mr. Erlanger defined it.
12 Rule only requires licensees to protect certain
13 systems, not all systems within the nuclear power
14 plant.

15 Those systems associated with the systems
16 that performs safety function, equipment to safety
17 function --

18 DR. HECHT: That's SSEP.

19 MR. LEE: Right, that's SSEP function
20 system. So if you're talking about those systems that
21 does not have anything to do with those systems, then
22 they are not required to protect under 10 CFR 73.54.

23 CHAIRMAN BROWN: That effectively says
24 that Level Zero doesn't have to have all 148, that's
25 the way I understand, that's the way I interpret your

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 words.

2 MR. LEE: Right, now if --

3 CHAIRMAN BROWN: If it's a non-safety
4 system --

5 MR. LEE: The rule only requires them to
6 protect only those systems that could cause --

7 CHAIRMAN BROWN: Potential --

8 MR. LEE: Radiological sabotage.

9 CHAIRMAN BROWN: Right.

10 MR. LEE: And of course I would like to
11 amplify that the, just like what Mr. Erlanger had just
12 stated, it doesn't really matter where you're located.

13 What you need to do is you need to
14 identify all the vulnerabilities, known
15 vulnerabilities associated with that particular system
16 and you need to protect it.

17 So what we did, I'm trying to go through
18 in my presentation is that one thing that we did do
19 through this process is that we leverage on all the
20 years of our research that done by NIST and also with
21 the experiment they did by NIST and DHS.

22 Then, from that, they came out with a list
23 of more than 200 security controls and these are
24 processed from defense audit calc and all this
25 different industry.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 And they collected the results, these
2 security controls and each of these security controls
3 address currently known vulnerabilities. So from
4 that, what we did was we got NRC industry experts and
5 also cyber security experts and we went through each
6 and every one of them and went through and see whether
7 that particular control applies to the nuclear power
8 plant or not.

9 Then after we determined that, and some of
10 these security controls, we had to modify a little
11 bit, and that process is exactly what is required or
12 recommended by NIST. I think that's Appendix I,
13 following that process.

14 So 148 security controls that we have
15 right now, those are the security controls.
16 Vulnerabilities associated with those 148 security
17 controls are currently known vulnerabilities that are
18 applicable to the nuclear power plant and also falls
19 within the scope of our regulation.

20 So, you know, 148, oh, there's 148, it's
21 not more than 148 vulnerabilities.

22 DR. HECHT: I should think that the HVAC
23 system and the administrative building of the nuclear
24 power plant, are you saying that that's going to be
25 received exactly the same scrutiny as the HVAC system

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 the containment?

2 MR. LEE: If they're identified as a
3 critical digital asset. These are potential
4 vulnerabilities that bad guys could exploit them. So
5 what we said was these are the potential
6 vulnerabilities, so you have to address them.

7 Not apply them, but address them. See
8 whether --

9 DR. HECHT: Will they be addressed
10 differently?

11 MR. ERLANGER: Sir, it will come out in
12 the scoping, whether the licensee or applicant
13 determines that if it's, this is in, I think, C.3.3.2.

14 In the Reg Guide it gives you a process to determine
15 what, and also in 08-09, what's within the scope and
16 what not.

17 If it does fall within the scope of the
18 rule, the 148 controls are applied against it.

19 MR. LEE: At the beginning.

20 MR. ERLANGER: At the beginning, no --

21 MR. LEE: Then if it comes out more --

22 CHAIRMAN BROWN: If it's not a critical
23 digital asset, you don't have to apply all the
24 controls. I'm simple-minded, okay? You've gone
25 through a lot of filler. I need a one sentence thing.

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 it's not a critical digital asset, if a guy brings
2 his calculator in, which is a digital asset, but it's
3 not a critical digital asset, you don't have to have
4 any controls on that.

5 You've got a stand-alone computer on a
6 desk in an office and it has no information, no
7 connection to the safety systems. It doesn't
8 consider, it doesn't have critical data that can be
9 used or manipulated that could cause a poor decision
10 to be made, it's not a critical digital asset and
11 would then not, therefore not fall within the purview
12 of the 148.

13 So it's within that assessment range. So
14 you're right, from the standpoint that you don't apply
15 to everything at every level, only if it's a
16 critical --

17 DR. HECHT: If it's above the threshold,
18 then they all apply?

19 CHAIRMAN BROWN: Yes, if it's a, if it's
20 defined, based on vulnerabilities, as a CDA, then they
21 get a flag, regardless of level, 0, 1, 2, 3 or 4.

22 DR. HECHT: Okay.

23 CHAIRMAN BROWN: And now we need to move
24 on.

25 DR. HECHT: I apologize.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 CHAIRMAN BROWN: No, no, no, that's just
2 fine. You clarified something for me, as well.

3 MR. AMIN: So, moving through the
4 requirement phase, you now have selected a vendor, you
5 have the specific requirements, so what do you do
6 next?

7 Well, part of the requirement phase is the
8 bid evaluation, purchase order and contracts. We
9 consider this as Luminant very important since this
10 will clearly spell out any and all cyber security
11 requirements in a contract.

12 And throughout the requirement phase, the
13 cyber security Subject Matter Expert input and review
14 of the requirements package and required element of
15 our program.

16 CHAIRMAN BROWN: Is it one guy?

17 MR. AMIN: It could be one or more.

18 CHAIRMAN BROWN: Okay.

19 MR. AMIN: It depends upon what it is.
20 Mostly, you know, it's not possible for one person to
21 do it all.

22 CHAIRMAN BROWN: Well, that's what I was
23 saying, John brought up this fact it's a CST, it's a
24 team. And then you said, well, that's our equivalent
25 to, it's a Subject Matter Expert.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. AMIN: See, the CSAT team is cyber
2 security Assessment Team. And what that happens is
3 when we go through this assessment process that I will
4 talk about, that's when the Team becomes active.

5 Because then the Team is comprised of
6 maintenance, design engineers, system engineers,
7 subject matter experts in design basis and that is all
8 the team, collectively. That's kind of a formation.

9 CHAIRMAN BROWN: Okay.

10 MEMBER STETKAR: And when is that CSAT --

11 MR. AMIN: You will see that, I'll cover
12 that.

13 CHAIRMAN BROWN: Not at the concept stage.

14 MR. AMIN: Not at the concept stage. At
15 the concept stage the cyber security Expert is there
16 now. There are system engineers involved of that same
17 asset. So he's going to be part of that assessment
18 team.

19 The Design Engineer is involved so the
20 cyber security Assessment Team is a little bit of a
21 different, it applies more to assets that are already
22 there and we are going to backfit the rule or you
23 know, address the assets that are already there.

24 Then we have to form a team. Then the
25 team will assess that particular asset. Here what 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 are talking about is developing a new asset and
2 putting it into the plant.

3 MEMBER STETKAR: Okay. I'm interested in
4 learning how you interpreted the guidance and how
5 you're implementing it.

6 MR. AMIN: Okay. So, the requirement
7 specification is updated to reflect the final cyber
8 security requirements based on the selected vendors.

9 Requirement specs become input into the
10 upgrade specific cyber security address ability matrix
11 that we would develop to track all these security
12 controls.

13 For us this phase directly determines the
14 amount of backfit and rework later on, since it forms
15 the basis for the rendered design for the upgrade.

16 So specificity and clarity of requirements
17 is very important. Next slide. So the goal of this
18 phase is to ensure, which is the design phase, the
19 goal in this phase is to ensure that all the
20 requirements specified in the requirement
21 specifications are correctly translated into the
22 vendor design, integrated correctly in the site-
23 specific product, which is the hardware and software.

24 And correctly reflected into the
25 documentation, because these form the core elements 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 configuration management. The cyber security Subject
2 Matter Experts are engaged in review and approval of
3 the cyber security aspects within this design phase.
4 At this, during this phase periodic Vender in-house
5 cyber security compliance reviews and independent QA
6 Audits, would also be conducted as part of the design
7 phases.

8 Many times we also put in quality controls
9 holds before the product moves from one phase to
10 another, to make sure that the critical
11 characteristics are addressed in the product.

12 Which is nothing new to the nuclear
13 industry, we do that today.

14 CHAIRMAN BROWN: Many of the design
15 aspects, as you're going through the development,
16 you've got a vendor but he subcontracts a lot of stuff
17 out, also.

18 So you've got subvendors to the vendor.
19 Is there --

20 MR. AMIN: Yes, the way we would address
21 that is that when we work up the contracts with the
22 vendor, then we would make sure that the elements of,
23 the security-related elements are addressed by the
24 vendor, which also applies to the subvendor under 10
25 CFR, what is that, Part 50, Appendix B?

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. CORREIA: B, quality assurance.

2 MR. AMIN: The quality assurance would
3 cover that. So it does apply to the subvendor.

4 CHAIRMAN BROWN: Okay, so necessary stuff
5 would have to be passed down maybe even another level,
6 depending on the nature of what you're subcontracting.

7 MR. AMIN: Yes, sir.

8 DR. HECHT: Do you have any practices on
9 assuring cost?

10 MR. AMIN: Pardon?

11 DR. HECHT: Do you have any practices for
12 assuring software and cost networking. Nearly all the
13 devices you're going to be using, particularly in new
14 plants are going to be, have intelligence associated
15 with them.

16 MR. AMIN: Yes and no. We have every
17 produced guidance on how to apply carts hardware
18 entered an application, I believe that has been
19 endorsed by the NRC.

20 What we have not addressed in that
21 guidance is how to address cyber security elements.
22 Which, I believe, the Reg Guide 5.71, NEI 08-09, does
23 provide enough guidance that we can use in making sure
24 that there is no gap.

25 DR. HECHT: So if I have a router, for

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 example, which has a web server in it so that it can
2 be configured or, and this is real, right?

3 MR. AMIN: Yes.

4 DR. HECHT: How do I know that that
5 router's underlying operating system and web server
6 are acceptable, or how would you know?

7 MR. AMIN: The way you would know that is
8 the carts guideline has a process. You determine
9 critical characteristics of what you are trying to do
10 with that particular asset and then you define those
11 critical characteristics and then you verify that
12 particular commercially available router that you are
13 using doesn't need those things.

14 In order to do that, you'll have to
15 understand what other functions does that router
16 perform? What other connectivities? Does it have
17 capabilities? Does it have, and how those
18 capabilities that are not used, would unintentionally
19 impact the functions that are or importance to you.

20 So you may end up like cutting, clipping
21 wings or clipping wires to make sure that the
22 functionality that you want is the only functionality
23 you get.

24 You have to prove it with some certainty,
25 so there is a process or there is a method to the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 madness within the guideline that you have to follow.

2 And it gets complex when you use like a
3 router example which has software in it and all kinds
4 of different software.

5 DR. HECHT: Connectivity.

6 MR. AMIN: And connectivity. So you have
7 to address all that.

8 DR. HECHT: And I suppose that one of the
9 requirements in that router is that it doesn't have
10 Stuxnet in it or another virus. But the only thing
11 you have is the firmware, object code. Do you have
12 guidelines for how you deal with that?

13 MR. AMIN: You said do we have guidelines?

14 DR. HECHT: Do you have guidelines as to
15 how you would accept that?

16 MR. AMIN: See, when we are in that stage,
17 we would be working with vendors like Westinghouse,
18 and I believe they do have guidance on how they handle
19 those kind of things.

20 As licensees, we don't have that. We
21 would always rely on some entity that has that
22 experience.

23 DR. HECHT: Well, I'm thinking not about
24 the course of things, but about those Sub, SSEP, more
25 like the E and P.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. AMIN: Right. For those, also, we
2 would rely on the experts that would do, there are
3 entities that perform commercial grade dedication and
4 we would go to them. We would have our Cyber Experts
5 also give it an independent look, if you're not
6 satisfied and it is too complicated, we can always get
7 some expertise in some niche areas to really make sure
8 that those things are looked at thoroughly.

9 Tested thoroughly, documented thoroughly,
10 analyzed. Failure mode for us. We want to make sure
11 that all failure modes are understood and addressed.

12 Because, otherwise it shows up at the
13 wrong time, when it is too late.

14 CHAIRMAN BROWN: Let's wrap this one up
15 and go on, okay.

16 MR. AMIN: Okay, during the design phase
17 it is three phases. The preliminary design review to
18 ensure that the vendor and the licensee are on the
19 same page as to the requirements.

20 Then the vendor will go and build some of
21 his design and we will conduct a critical design
22 review. And during this review we will focus on the
23 draft project-specific vendor cyber security Plan.

24 We will also look at the system and
25 software requirements, specifications and design

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 specifications, to ensure that cyber security is
2 properly addressed.

3 We will also look at the test plans that
4 the vendor develops. Next slide. And then during the
5 detailed design review, we will review and confirm the
6 vendor design meets the specified cyber security
7 requirements.

8 During this phase the cyber security
9 Subject Matter Experts prepare the preliminary cyber
10 security assessment for the upgrade.

11 So, John, this is where the formal process
12 is initiated for developing the cyber security
13 assessment for this particular upgrade. And it
14 continues until the asset is installed in the plant.

15 So that we have a clear nexus on each and
16 every requirement, how we are addressing it. So if
17 leverages on different phases.

18 MEMBER STETKAR: Jay, is that, I hear you
19 saying that the cyber security assessment, in one
20 sense I can think of it in a compliance sense. To
21 make sure that I've addressed all 140 whatever there
22 are, six or eight, I've lost track.

23 Some number of issues. But there's a
24 different context of that assessment, at least in the
25 way I understood Reg Guide 5.71, and NEI 08-09.

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 that is an independent assessment to
2 look for additional vulnerabilities and threats. In
3 other words, not just, there's words that says threat
4 and vulnerability assessment. That's not a compliance
5 role, to check off the boxes that in deed we've met
6 all of these identified things, based on some missed
7 assessment of things that have happened in the past.

8 It's looking at the actual design and
9 thinking carefully using, this is what I'm trying to
10 get out, is tools. Things like failure modes and
11 effects analyses or other types of assessment tools,
12 to see whether your particular design has any
13 vulnerabilities.

14 And from what I'm hearing you say, your
15 role is more of a compliance checklist.

16 MR. AMIN: No, not really. See, this
17 presentation is only for security related elements.

18 MEMBER STETKAR: That's what I'm talking
19 about, though.

20 MR. AMIN: Yes, but there is, during the
21 design phase one of the very important aspect that
22 occurs is that we expect the vendors to develop if
23 failure modes effects analysis document, that would
24 then provide the details on system level failure
25 modes, equipment failure modes and all those are

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 considered and then cyber security failure modes are
2 also considered with acceptance criteria, as to what
3 we expect.

4 For example, if somebody turned off some
5 port and say the system reboots and, again, activates
6 that port. How do we know that? So those are the
7 elements that would go into the failure modes effects
8 analysis, and many of these elements would be tested
9 out at the factory acceptance test.

10 MEMBER STETKAR: Let me stop you there.
11 Because what you said, I think, is where I've been
12 headed. What, make sure that I understand. You said
13 that you expect the vendor to perform a failure modes
14 and effects analysis that addresses both, if I can
15 characterize it as system safety function, does it do
16 what it's supposed to do?

17 And security, cyber security issues. IN
18 other words, is it vulnerable to malicious threats,
19 let's call it that. So your specifications require
20 the vendor to perform that.

21 MR. AMIN: The vendor will perform those
22 failure modes analysis in context of the cyber
23 security requirements that we have specified for that
24 upgrade.

25 Remember now, this is the, call it a black

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 box or, that you know we are, not, I shouldn't call it
2 a black box, but the safety-related upgrade that we
3 are specifying.

4 So it is limited to that. Now, failure
5 modes does, it affects analysis, it doesn't end there.

6 The vendor can tell us what those failure modes are,
7 but when we integrate the system, we can also
8 introduce new failure modes.

9 So when we put the design modification
10 package together, we do assess failure modes beyond
11 what the vendor did, to ensure that those other
12 failure modes do not compromise the already assessed
13 system.

14 So that is very important. That leads
15 into the, during the design, the design, that leads
16 into the next phase, which is the, next slide,
17 implementation, integration, test phase.

18 This is where we get heavily engaged wit
19 the vendor. Because this is where the vendor takes
20 the entire design, integrates into, onto the hardware
21 platform and software platform.

22 Performs all kinds of system integration
23 and system hardening. Verifies proper implementation
24 of cyber security requirements. Verifies that the
25 test plan also addresses all security requirements.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 And also verifies that all issues
2 discovered during the analysis, testing, and address
3 design is adjusted and system is retested, documented
4 and approvals are obtained. It is very important to
5 know, John, that during this process the licensee is
6 approving all the documents.

7 Reviewing and approving. And these review
8 and approvals are done by Subject Matter Experts.
9 It's not like this one design engineer disapproved of
10 everything.

11 So this is normally a reiterative process.
12 Next slide. Now that the design is complete, we
13 enter into what we characterize as a factory
14 acceptance test.

15 So here's where we will make sure that we
16 have a traceability matrix and this is our last line
17 of defense, where we have to make sure that all the
18 requirements are verified to be functioning properly,
19 have been tested properly, includes cyber security.

20 And this is the report that the NRC is
21 always eagerly waiting for before they issue the SER,
22 right?

23 And so what happens at this stage? As
24 this stage if the FAT is successful, that means that
25 we now have a system that is under full configuration

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 management.

2 In other words, we have established
3 systems of very specific configuration controlled
4 baseline, as well as security-specific configuration
5 baseline.

6 Very important to note that. And this
7 successful completion of this phase, results now
8 becomes the starting point for the transition to the
9 10 CFR 73.54 program.

10 Remember I said at a certain point there
11 is a transition? So this is where the big handoff
12 occurs. Where now the system is going to be shipped
13 to the site, and the Site Acceptance process and all
14 other processes keeping with the licensee. I hope
15 this is making sense?

16 MEMBER STETKAR: It is, you can ask any
17 questions.

18 MR. AMIN: So what happens during the site
19 installation and site acceptance phase? In this
20 phase, the cyber security Subject Matter Experts
21 review and approve the site installation plans for the
22 cyber security requirements.

23 Ensure that all necessary procedures, test
24 reports, back up software, disaster-recovery
25 procedures are in place for the modification, prior to

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 turnover of the system to the operations.

2 So here we are validating that all the
3 configuration control elements are in place. And then
4 the Team also reviews the Site Acceptance Test Plan
5 and Procedure for cyber security. It includes
6 verification that the site plans address any of the
7 security controls that are functions that could not be
8 tested in the factory.

9 That is possible. It is sometimes humanly
10 impossible to replicate the configuration of the plant
11 into the factory environment.

12 So we capture those kind of things to make
13 sure that those are tested when we install the system
14 at site. So the site acceptance activities include
15 verification and validation of the final, as built,
16 CDA security configuration, very important.

17 Also, verification that all required
18 surveillance is per the cyber security assessment
19 execute properly. Why do we want to do this? Because
20 this surveillance has become --

21 CHAIRMAN BROWN: Can you hold on a minute?
22 Can we get Slide 14, up, which is what you are doing
23 right now?

24 MR. AMIN: Thank you, I'm sorry. I'm
25 sorry for that, I wasn't paying attention.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 CHAIRMAN BROWN: Well, I kind of lost
2 track.

3 MR. AMIN: So during the site acceptance
4 test activities, I'll just repeat that.

5 CHAIRMAN BROWN: Oh, you don't have to,
6 I'm with you. Maybe nobody else is.

7 (Laughter.)

8 MEMBER SIEBER: I'm reading this, not
9 that.

10 CHAIRMAN BROWN: I was reading here, so I
11 knew where you were.

12 MR. AMIN: So here we verify that all the
13 required surveillance is, all the cyber security
14 assessment execute properly. What happens, John, is
15 when we're doing this cyber security assessment, the
16 Assessment Team does that, the CSAT Team that you
17 mentioned.

18 That Team will then determine that these
19 are the surveillance that need to be conducted when
20 the asset is commissioned, during it's operation and
21 maintenance phase.

22 So we will make sure that those
23 surveillance execute properly, so that when we are in
24 the operations and maintenance phase, we know that,
25 you know, we can perform that activity.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 And then verification of proper operation
2 of the security technical controls that are in place
3 is also necessary. So, in other words, we will make
4 sure that all our specs of the cyber security plan
5 commitment, which is part of Operating License, are
6 addressed in this phase.

7 And at this phase, the cyber security SME,
8 will update the cyber security assessment and obtain
9 final approval of this particular assessment and this
10 becomes the baseline for the operations and
11 maintenance phase. Next slide.

12 So now we have transitioned into the
13 operation and maintenance phase of the upgrade. So
14 the CDA is under our, we now call it a critical
15 digital asset.

16 It's under full configuration, management
17 program. This also includes specific security posture
18 for the CDA, which is a baseline of record, for the
19 life of the CDA.

20 So no it's a given that time to time we
21 will have the CDA interval changes. So any changes to
22 the CDA, the word is any changes to the CDA or their
23 supporting environment, like HVAC that, you know was
24 mentioned. Myron, you talked about it.

25 That rely on for performing their security

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 function, then those changes are handled under the
2 station change management program, or the
3 modification process program.

4 Which requires us to perform 5059
5 evaluation before, I should say 5059 reviews, before
6 we implement that change.

7 And so, again, just like change, when you
8 make any change, you have to recycle yourself through
9 the cyber security assessment process, make sure that
10 all the security controls are still in tact and that
11 the new baseline is established and documented.

12 So you go through again. A factory
13 acceptance test, if it's a big change, if it's a small
14 change, then you still do that test. There is no
15 option or any other alternative, that's the process.

16 In addition, any changes to the station's
17 cyber security defensive strategy, is also assessed
18 for impact to the planned critical digital asset,
19 because that maybe taking credit in a defensive, that
20 model for that particular defense.

21 So we want to make sure that things are
22 not compromised and we look at it holistically. At
23 this point the Rev Guide 5.71, NEI 08-09, Rev 6, also
24 required addressing several cyber security controls to
25 protect against malicious Cyber attacks.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 So many of these controls are independent
2 of the security controls that are established as part
3 of the upgrade under Reg Guide 1.152. Those have to
4 be managed and maintained during the operation and
5 maintenance phase.

6 So, in short, the current station
7 surveillance program, corrective action program,
8 maintenance program, work control program,
9 configuration management program, audits and
10 assessment programs, all play a key role in providing
11 the high assurance of adequate protection for the
12 critical digital assets to ensure consistency and
13 provides opportunities for continuous improvement in
14 the station cyber security program.

15 So that's what happens during this phase.

16 The next phase, the retirement phase. Eventually,
17 the CDA is retired. When that happens, the law
18 requires producing a CDS specific retirement plan.

19 That would then ensure that we verified,
20 that we identified critical security-related
21 information for proper disposal. We verified that the
22 security-related records are retained for records
23 retention requirements for historical use.

24 And we verified the proper sanitization,
25 disposal of media and security-related information

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 occurs. So at this point, you know, the life cycle
2 comes to an end. Next slide.

3 I'll quickly go over the slide. These are
4 initiatives already in progress to address several of
5 the challenges. We, as licensees, face as we move
6 forward into the program implementation phase.

7 NEI, Nuclear Energy Institute, is
8 basically the primary driver of the Task Force. They
9 are the ones that predominantly interface with the
10 regulator on cyber security.

11 And under, in NEI we have a cyber security
12 Task Force. The Task Force then relies on NITSL,
13 which is the Nuclear Information Technology Strategic
14 Leadership.

15 It's another industry group that is
16 sponsored by INPO, and this group provides the
17 community or provides the technical expertise and it
18 also is community of best practices in cyber security
19 for the industry.

20 So the industry relies on NITSL guidance
21 in many ways for consistency. EPRI, Electric Power
22 Research Institute, also comes into play. A good
23 example is in conjunction with NEI and NITSL, EPRI
24 developed the Technical Guidance for cyber security
25 Requirements and Life Cycle Implementation Guidelines

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 Nuclear Plant Digital Systems.

2 Basically, in this guidance, we have
3 broken down the security controls and put them in
4 different buckets of system development life cycle.
5 And the targeted audience again here was the Plant
6 Digital Engineers and other staff responsible for
7 addressing cyber security requirements throughout the
8 system developing life cycle. So there's, there were
9 some questions in the morning, John, that you know
10 were directed at operations phase and how would we do
11 that.

12 So this is how the process would play in.
13 Next slide. Challenges, there are four challenges
14 that we see. Application of security controls to
15 legacy systems, our plan to address this is going to
16 be keep it simple.

17 Lock your cabinets and alarm your cabinet
18 doors when somebody opens it, and use common sense.
19 Because we cannot make these systems do what they
20 cannot do.

21 These are systems with five and three inch
22 quarter floppy discs, that you know I'll have to even
23 find. They don't even have any passwords.

24 So we would alarm the physical location
25 and prudent things. And the Reg Guide or NEI 08-09,

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 allows us that flexibility, like you know we have to
2 address the controls, so it does allow us that
3 flexibility.

4 The challenge is the vendor In-House cyber
5 security programs and processes that secure
6 development environment. I worry about what is
7 threshold for this particular requirement. Do we even
8 have a common understanding of these requirements?
9 What constitutes an acceptable secure development
10 environment?

11 How are we mitigating this? We are
12 working with the vendor community through the
13 industry, through NEI, NITSL, EPRI, to see if we can
14 double up some kind of a procurement, requirement,
15 specification that addresses some of these
16 requirements on the vendors.

17 Because this is where I believe we can go
18 all over the map, assuming many things. The third
19 item is nuances associated with cyber security
20 knowledge and its expertise.

21 Through these years I found out that our
22 best Network Engineer may be our weakest link when it
23 comes to cyber security, just because we never send
24 him for any training.

25 So, this is, we are very sensitive to 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 as an industry and we are working on training plans on
2 that. And then the last one is the security controls
3 evolution.

4 The fact remains that facts will change,
5 security controls will change. So how do we ensure
6 that the, that we keep up with the security controls
7 and similar to what we do in the ASME Code arena,
8 where I believe the last Reg Guide Revision, was the
9 Revision 23, by the NRC, issues this Reg Guide every
10 two years.

11 Something similar has to be done to make
12 sure that we have consistency, as to what security
13 controls apply. When the evolve. So that's an
14 opportunity there.

15 Oh, last slide. So, in conclusion, I
16 won't bore you with that, but basically we believe
17 that there is sufficient regulatory clarity exists for
18 cyber security in the digital upgrades.

19 The new LAR process and the pilot project,
20 will provide insights and opportunities for
21 improvement in the security arena. And that the
22 system development life cycle approach will evolve as
23 we integrate cyber security into the plan process,
24 programs and procedures.

25 And, I'll take any more questions that 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 all might have.

2 CHAIRMAN BROWN: Jack.

3 MEMBER SIEBER: I just like the wording of
4 sufficient regulatory clarity exists. In other words,
5 we just make it.

6 MR. AMIN: No, and I'll tell you why I
7 chose that word. When I say sufficient, it's an
8 evolving area. It is new to everybody. I don't think
9 even NIST can tell us with a straight face that they
10 have control over this.

11 MEMBER SIEBER: Well what I mean by my
12 comment is the staff has made a great effort to
13 separate cyber security from other assets. Whereas
14 the licensee, when he gets the job and decides he
15 wants to do something, puts it all back together
16 again.

17 Now, I understand the legally reason for
18 why the staff does that, I also understand the
19 practical reasons why licensees do that. And that's
20 why your statement, sufficient regulatory clarity
21 exists, impresses me. Just sufficiently.

22 CHAIRMAN BROWN: The same, similar
23 observation and I peaked, so I'm going to steal Matt's
24 comment, because one of his slides, which is
25 unnumbered here, you said you support the Reg Guide

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 1.152, Rev 3, you very clearly stated that.

2 You sort of stated earlier that 5.71 works
3 with it, it's not explicitly stated. But yet you're
4 bringing it up forward to ensure you cover the
5 waterfront and up front, as opposed to getting hit and
6 the tail end.

7 MR. AMIN: That is correct.

8 CHAIRMAN BROWN: And if you don't mind me
9 stealing one of your boards, okay?

10 MR. GIBSON: Certainly not.

11 CHAIRMAN BROWN: One of your conclusions
12 that you feel that the safety security interface is
13 well served by a functional division between the two
14 regulations.

15 And so we've been talking about that he
16 whole time. And I get both of you are sort of saying,
17 yes, we can --

18 MR. GIBSON: We can deal with it.

19 CHAIRMAN BROWN: -- you can deal with it.

20 MEMBER SIEBER: And that's comforting.

21 CHAIRMAN BROWN: So, I'm, you didn't shake
22 your head up and down, he did.

23 (Laughter.)

24 CHAIRMAN BROWN: I'm going to let go on,
25 you're complete? I'm going to, so that you all can be

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 finished, I'm not going to take a break right now,
2 we'll wait until Matt finishes his, if that's
3 acceptable, we'll move on. You want a slide show,
4 right?

5 MR. GIBSON: There is numbers on these
6 slides, they're little teeny white numbers down in the
7 corner. Just so we know.

8 CHAIRMAN BROWN: Got it, got it, yes, I
9 had my thumb on that part of the page.

10 (Laughter.)

11 MR. GIBSON: And you guys will have to
12 bear with me, because I'm reaching that age where I
13 can't see the screen and my notes at the same time.

14 With that, I want to thank the staff for
15 inviting me, and the Committee for letting me speak.
16 And, with that, I'm going to introduce our company,
17 Progress Energy.

18 Fortune 500 Company, we have a service
19 area in the Carolinas and Florida, 3.1 million
20 customers, approximately 22,000 megawatts. A lot of
21 employees, 11,000 of us.

22 Of that capacity we have four nuclear
23 sites, and you can see those there. Plus two COL
24 applications in flight for two AP1000 sites at Harris
25 and Levy County.

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, as I talk today, I'll try to give you
2 all the perspective on both existing plant activities
3 and new plant activities.

4 As for me, I'm Matt Gibson, I have 29
5 years of experience in the industry. I've been
6 everything from an I&C technician to a Nuclear IT
7 Manager, in those 29 years.

8 Right now I'm a Process Systems Architect
9 in the Design Engineering Department, our Fleet Design
10 Engineering Department. The last four years I've been
11 the NuStart I&C Committee Lead for AP1000.

12 I don't do that lead role anymore, I'm not
13 dividing my time between new plants and our existing
14 fleet.

15 I'm going to try to talk with three points
16 today. One is how we understand the regulation, how
17 we implement or will implement the regulation and a
18 couple of case studies.

19 We understand the requirements of Part 73
20 and Part 50, including the associated regulatory
21 guidance and licensee commitments as two parts of the
22 cyber security puzzle.

23 These regulatory structures work together
24 to protect the public by allocating the elements of
25 cyber security to the licensing and program oversight

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 process, where it can be the most effective.

2 By placing overall cyber security in Part
3 73, it allows for a performance-based cyber security
4 program that can accommodate a wide variety of plant
5 designs, technology and equipment inventories.

6 It's real important thing, too, because
7 we're not all created equal. We could address the
8 cyber security controls and program requirements in
9 flexible ways to accommodate the capabilities, the
10 legacy and new industrial automation equipment apply
11 the safety related applications, that may not directly
12 support every Cyber good practice.

13 And we've touched on some of those, the
14 tradeoffs. In any case, we can achieve the
15 performance objectives from establishing adequate
16 cyber security protections for these systems and with
17 a high level of assurance that the objective is being
18 met using the Part 73 Requirements and ensure that we
19 have safety-related systems that protect the public by
20 addressing the Part 50 Requirements.

21 The function division between these to
22 regulations allow the predominantly deterministic
23 safety question to be addressed by the NRC I&C during
24 licensing review, without conflict with the
25 predominantly performance-based security requirements.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 It then allows the licensee to implement
2 the performance-based cyber security program with the
3 full knowledge of the safety -related systems,
4 licensing and design basis.

5 That allows us to craft an effective
6 protection scheme, and this regulatory structure
7 answers to safety and security questions in an
8 effective.

9 I go a little bit more than that, because
10 I think there's a natural, you know, there's a tension
11 between safety and security. And I think, at least,
12 you know, I'll give you my opinion.

13 I'll be brave there, safety comes first,
14 security second, if you had to make a choice. I think
15 you can have both and I think we meet both regulations
16 by first addressing the safety question and having
17 that done.

18 Because that's in our design basis, that's
19 in our licensing basis. And you're wrapping around
20 that the security issues, and making sure that we
21 adequately protect our important safety-related assets
22 in a way that, you know, that continues to protect the
23 public.

24 I think it's close, from a regulatory
25 point of view, to combine those two into one review.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 It's also going to be difficult to have a single
2 Reviewer or a group of Reviewers try to resolve that
3 question in the same sequence of reviews.

4 You guys asked a lot of questions today.
5 And I'd like to answer a couple of them. I better
6 make slides so you have something pretty to look at,
7 before I answer that.

8 This I believe is a graph illustration of
9 the interface between the two, Regulation 73 and 50.
10 And it has a functional handoff here in the middle.
11 And when I speak of Appendix E-11 and C-12, I'm
12 talking about sections of NEI 08-09 and Reg Guide
13 5.71.

14 The positions there are from the proposed
15 Reg Guide 1.152, Revision 3. Now these functional
16 handoffs are important because you, I know some of you
17 guys on the Committee have some ideas about how maybe
18 you'd like to see this actually work.

19 When prepare, say an LAR for a safety-
20 related I&C modification, we're assuming that
21 requires, something that requires prior NRC review.
22 What we're going to be looking for is to use the ISG-
23 06 process and we're going to package that up in a way
24 that can be reviewed by the I&C staff to make a safety
25 finding.

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 Parallel to that and in conjunction with
2 that, there has to be additional cyber security
3 considerations addressed, that will not get prior NRC
4 review at all.

5 The licensee will make good on their
6 commitment in their cyber security plans to implement
7 or address the 148 controls. And by doing that, two
8 of those six, there's a whole six, and they're not
9 just individual requirements.

10 Those two sections in both of those
11 guidance documents provide information for the
12 procurement or supply chain phase, when you're buying
13 something, when it's in the vendor's hands.

14 So we have to deal with that, that's the
15 licensee's responsibility, under the Part 73 Rule, it
16 is something that we can be inspected to and that's a
17 performance-based requirement.

18 CHAIRMAN BROWN: So you would do it
19 differently than Luminant is doing?

20 MR. GIBSON: Hard to say.

21 CHAIRMAN BROWN: No, I just said it for
22 you.

23 (Laughter.)

24 MR. GIBSON: Then I'll leave you with that
25 opinion.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 CHAIRMAN BROWN: It's okay, it doesn't say
2 you have to them the same. There's nothing in there
3 that says you have to do them the same. You have to
4 meet the requirements.

5 So I wasn't saying that negatively. All
6 we've done was try to articulate some potential
7 problems that have to be addressed on how you do it.
8 Because you've got to think about the business aspects
9 of how you do it, as well as the technical and, you
10 know, performance and safety aspects that, cyber
11 security and safety aspects.

12 So, we're not trying to dictate, don't
13 take our comments to dictate one or the other, we're
14 not. We're just trying to get the perspective, our
15 perspective.

16 It's interesting to hear your comment
17 relative to that and I'm glad we had divergent thought
18 processes here. So I'm interested in hearing, you can
19 go ahead now, I just had to throw in my two cents
20 worth, as usual.

21 MR. GIBSON: Let me build on that a bit.
22 We do not think that if we try to get the staff to
23 review a cyber security design, apart from the safety
24 determinations, that they would actually do it?

25 CHAIRMAN BROWN: During the licensing

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 process.

2 MR. GIBSON: During the licensing process.

3 And you don't think they would do it.

4 CHAIRMAN BROWN: They'd say no.

5 MR. GIBSON: They'd say no to that. I'm
6 just being frank with you. And regardless what people
7 think might happen that, I think, is how it would turn
8 out.

9 They would tell us that it's our
10 responsibility and not going to be our Sea Daddy and
11 tell us how to do it. And they'll come later and
12 check us out. And we better have it --

13 CHAIRMAN BROWN: Right.

14 MR. GIBSON: -- a reasonable approach to
15 it, you know, one that they can buy off onto, in a
16 performance-based approach.

17 CHAIRMAN BROWN: Right.

18 MR. ERLANGER: Matt, can I ask a question,
19 it's Craig Erlanger. Do you agree with that, though,
20 what we look at in design, are we at an adequate level
21 for what we, you know, from where we look at cyber
22 security as an operational firm ground.

23 MR. GIBSON: Well, you know, I'm like a
24 lot of utility guys. When we first started this, and
25 I'll be frank with you, I was like everybody else.

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 Well, I want to know exactly what the
2 Regulator wants so I can bring him the correct rock
3 and everybody would be happy, right? I mean, you
4 know, who wouldn't want that.

5 I think as you learn more about cyber
6 security an security in general, you understand that
7 that's for, or that has a lot of merit over in the
8 safety question determination.

9 It doesn't have the same level of merit in
10 a security situation. Because you've got to remember
11 all your Part 73 mods going all over the industry,
12 none of those, to my knowledge, have prior NRC review.

13 They have set criteria. We're busily building new
14 security computers and stuff, you know.

15 And they're going to come in, the security
16 Branch is going to come in and check those out. And
17 we have some leeway from a performance-base, to meet
18 those performance objectives in ways that are unique
19 to our facility.

20 And I think that's a real, that's a real
21 dichotomy between safety and security that we have to
22 recognize. And it is better, and I do agree, Craig,
23 that in going forward we're better off sticking with
24 our performance-based security plans, being able to
25 have some flexibility to tailor our cyber security

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 programs to the actual, you know, our ground truth, as
2 they call it.

3 Meeting the performance requirements and
4 having, and you're just being subject to their
5 reviews. That was the long answer to your question.

6 CHAIRMAN BROWN: Yes, but there's, you
7 also phrased it slightly differently. You've got an
8 operating plant today that you now have to execute
9 73.54 requirements in and you've already got a plan,
10 you've got a design.

11 You have to do it in a manner that
12 somebody comes in and looks at what you're going to
13 do, and you then have to put in, implement, execute,
14 whatever needs to be done.

15 There's no opportunity to catch on the
16 front end. Whereas if you've got, if you're doing an
17 upgrade on your systems, you have the opportunity
18 under the LAR process, the licensing process to bring
19 those forward and get them understood.

20 Or at least get enough hooks to have it
21 understood, so that you're not caught later. It's not
22 a dictate, I'm saying there's two different scenarios
23 in my mind as how you, some of things get executed.

24 Whether it's an already existing operating
25 plant with no changes or no upgrades, or one in which

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 you're making upgrades.

2 I don't disagree with what you said, it's
3 just, it's a matter of what you want to do.

4 MR. GIBSON: I'm not trying to change your
5 mind either, but I think that it's, and you'll see in
6 a moment, when I get to our case studies, that by
7 doing performance-based during the procurement
8 process, we are able to do the same thing for our
9 vendors that security branch does to or for us,
10 depending on how you look at it.

11 And that is we can provide them with
12 performance-based criteria for their secure
13 development, from a cyber security point of view, from
14 a malicious intent point of view.

15 And we can evaluate what they do, based on
16 the effectiveness of it. A performance-based review,
17 and we'll be doing it to the vendor in this case,
18 versus the staff doing it for us.

19 And why is that important? Because the
20 results of that performance-based process to a vendor,
21 it allows us to roll the documentation of that,
22 configuration control, will practically pass up the
23 supply chain line, and also the documentation will
24 pass up the line.

25 So in future times, when we have

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 performance-based reviews, we can show that we did
2 these things. And we did them in a prudent manner in
3 the proper order.

4 And that's when they would get looked at.

5 They wouldn't get looked at, necessarily, if you're
6 in the actual LAR process.

7 To move on to my next slide, you know, I
8 guess what we, we're comfortable with this allocation
9 of malicious and non-malicious. And that's the way we
10 look at it in the field.

11 You know, the staff has chosen the, you
12 know, create a definition for cyber security like I
13 think Deanna said earlier. The lawyers told her how
14 to do that.

15 But you've got to remember that the non-
16 malicious criteria that's in the proposed Revision 3,
17 are the same kind of cyber security criteria you'd
18 find in any mainstream cyber security plan in a non-
19 nuclear industry.

20 I mean they're going to worry about fires,
21 they're going to worry about water damage. They're
22 going to worry about unintentional, you know, operator
23 actions.

24 They're going to worry about this things.

25 And they'll be called in the academic sense, all that

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 cyber security. But for the sense it is, it's
2 valuable to separate them, malicious and non-malicious
3 for a lot of good reasons.

4 Reportability is one of them. You know, a
5 malicious thing, it's like the difference between if
6 you get home and you don't have your key and you've
7 got to get in the house, and you kick your backdoor
8 in, well, that's just your problems, you've got a door
9 to fix.

10 If your neighbor kicks your backdoor in,
11 that's a problem for the cops. The same exact thing,
12 the same exact thing happened. One is a malicious
13 thing and one is not a malicious thing. So we
14 generally will like that.

15 And also, in the Part 50 area, too, you're
16 able to evaluate the changes you make to the safety-
17 related digital system through your 59 process. That
18 is going to address the safety issue.

19 It's going to address the design basis
20 issue. So there's a value in separating the design
21 basis that's part of the safety determination, from
22 any additional design that you do to meet a cyber
23 security problem, a malicious cyber security Problem.

24 DR. HECHT: Jay, I meant to make this
25 point earlier and he mentioned 5059 within the context

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 an HVAC system, and I've been waiting to ask this
2 question.

3 Is there an equivalent to 7359? And, if
4 not, should there be?

5 MR. GIBSON: Well, I'll tell you how it
6 works. When you do a 5059, you're trying to answer
7 basically a regulatory question whether your change is
8 going to affect your, if you're doing anything that
9 will affect your licensing and design basis, and
10 decrease your safety.

11 I mean, in a nutshell, that's what the
12 5059 does. When you do a change to a system that's
13 under the 73.54 Rule, you have to do an impact
14 evaluation on that change, to determine whether or not
15 it impacts your commitments under 73.54 and impacts
16 the plant.

17 Because that could trigger a 5054P change,
18 I mean, you got that? You got that? They're
19 different processes but they do very similar things.

20 But, again, because the security and the
21 safety process are different, they have slightly
22 different, you know, criteria for how it works, I
23 guess, is the best way to describe it.

24 But in both cases, you will always review
25 a change for both the design and safety impacts and

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 the cyber security impacts. And to the extent that a
2 cyber security feature of a system, is also embedded
3 in its basis design, then you'll evaluate the changes
4 to that, in the 5059 process.

5 So if you had a security feature, for
6 instance, and a safety system that had been, you know,
7 evaluate by the staff and approved for use. And you
8 wanted to change that.

9 And it was part of the safety scope, so to
10 speak, part of the design basis of the safety system.

11 You'd have to do a 5059, you know, safety evaluation
12 of those security changes, because they have impact to
13 safety. If they were outside of that, then it would
14 just be a cyber security program review. Does that
15 make sense?

16 DR. HECHT: Yes. So what you're saying is
17 you go from this change evaluation 5054, for cyber
18 security?

19 MR. GIBSON: 5054 has, no, you still do
20 the evaluation, 54, you know, has a different kind of
21 threshold, but 5054P would be where you would have to
22 change your cyber security plan.

23 And you're evaluating it for any changes.

24 Now the threshold for that gets set by the procedures
25 in the programs you develop to meet your plan.

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 Like do you have a cyber security plan
2 which we've all submitted and just for everybody's
3 benefit, you so level set this, to my knowledge no one
4 has an implemented 73.54 cyber security Program, as of
5 today.

6 We're all still running off of 0404, just
7 so everybody realizes that. You know, we have a
8 schedule to do that, we brought forward, we've
9 preemptively done some things and we're doing all
10 that, but from a pure licensing point of view, we're
11 still under 0404.

12 So as we get ready for that and we
13 implement our 5054 plans, life is good. We've
14 assessed all our systems, we've implemented all our
15 controls. We're sitting there and we want to make a
16 change.

17 Well, those changes we make to our
18 controls and to our systems, should be bounded by the
19 security procedures and processes that we've developed
20 for our program.

21 Because we will have bounded those under
22 our plan. You plan the programs, you're getting them
23 confused. The plan drives the program. You set up
24 the program, you do things, as long as the changes you
25 make generally, you know, are bounded by your program,

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 you probably won't trigger a 5054P change.

2 But say you want to get rid of your CSAT
3 or change your defensive architecture, those things
4 would trigger 54P changes, because they would be of a
5 magnitude to require that.

6 Now, when we get into implementing these
7 guys, and I've talked about some of this already,
8 about your Cyber-aware, 5059 reviews and evaluations
9 and your, how your Cyber, how your changes to the plan
10 or evaluated for cyber security change.

11 You know, like we talked about, you know,
12 previously, in order to implement these, and we're
13 talking about safety-related system, new digital
14 systems. We take the elements from Part 70 and Part,
15 73 and Part 50, and we do combined procurement
16 requirements.

17 We follow the ISG-06 process. Now, for
18 those up, you know, I know some of you are familiar
19 with ISG-06, because you reviewed, I think. But ISG-
20 06, invokes the SDOE, and I think even today it
21 invokes the SDOE.

22 It talks about doing all that. So we
23 combine the Part 73 requirements, out of Appendices 11
24 or C-12, depending on which guidance document you're
25 using.

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 you merge those with the ISG-06 phased
2 approach. Now, ultimately, we also integrate the
3 requirements of 73.54 and, depending on which document
4 your plan is written to, either 08-09 or 5.71.

5 You integrate the cyber security
6 requirements and your work management configuration
7 control and document management processes, your
8 engineering processes.

9 All those have, the word Cyber can be
10 found in all of them where there's criteria in there
11 to review changes or activities, it has, you know, 74
12 related, 73.54 related activities.

13 So, if you can view that, we integrate the
14 73 and Part 50 processes, 73 and Part 50 processes,
15 for procurement and functional requirements. And then
16 we also have, in our processes, Part 73, you know,
17 trigger points, to help us continue to meet our
18 program requirements.

19 And this diagram, I'm just trying to give
20 you a visual. Your Part 50 requirements, which in
21 this case, you know, we're narrowly talking about the
22 Reg Guide 1.152 Revision, there's a lot of Part 50
23 requirements.

24 But 1.152, Rev 3, pulls through your, IEEE
25 603 and IEEE 7-4.3.2, pulls those through into the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 review process. Now, when you talk about the Part 73,
2 stuff, again we have the cyber security controls that
3 we're required to address in our guidance documents.
4 Either E-11 or C-12.

5 So we take those two and we integrate them
6 into our procurement and functional specifications,
7 and that's how we, that's our, that's how we interface
8 with the vendors.

9 We provided that information to them and
10 functional requirements for the actual system. And
11 then for SDOE, those are requirements we provide in
12 our procurement contracts.

13 That establishes the SDOE during the
14 creation of the system, I'll make it real simple. You
15 create the system under an SDOE. When it's delivered
16 to us, we have a secure system.

17 Our cyber security program informs that as
18 well, because we have all our processes that are cyber
19 security aware, that also apply, and that's your
20 maintenance activities, your testing and whatever else
21 goes a long with that, that are apart from the SDOE,
22 get addressed through our site process.

23 Which all has to deal with the same, Part
24 50, Appendix B things that we've always had to deal
25 with. So we have all those. Questions? I've got a

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 couple of case studies for you.

2 First is an existing project we have
3 underway right now, the ICCMS Project at Crystal
4 River. ICCMS stands for Inadequate Core Cooling
5 Mitigation System.

6 We developed an integrated SDOE in 08-09
7 based security requirement. So, basically, I'll give
8 you the narrative of this.

9 In our procurement requirements, we are
10 requiring the vendors to do an independent assessment
11 of their development environment. That means
12 independent of them, they got to hire somebody to do
13 this.

14 An independent assessment of their
15 environment. They've got to provide us the report,
16 along with the corrective actions. And the assessment
17 methodology or the assessment objective is to assess
18 their SDOE against 08-09, because that's the one that
19 we're using for this particular project.

20 And that happened way at the front end.
21 That's what you would call the conceptual phase. Also
22 at that time, we put in whatever functional
23 requirements we need the system itself to have, for
24 the fact of whether it has to have a password or not.

25 Or whether it has to have closed ports or

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 not. I give you the example you used earlier. Those
2 kinds of requirements, the functional requirements for
3 that system that impacted safety. So they have to go
4 in to functional requirement up front, so they can
5 pass through the process, you know.

6 Down they go to ISG process. And they're
7 integrated up front, and they pass on through. SDOE
8 requirements which are just related to that vendor's
9 environment where they do work at, that's in the
10 procurement process.

11 And finally, at the end of this top line,
12 the ISG-06 top line, we're requiring the vendor to do
13 another independent assessment of the target system,
14 and again provide us with the report of corrective
15 actions. And that's what we're doing today, because
16 we don't have, we're just basically doing what 73.54
17 does.

18 We're giving the vendor a performance-
19 based type opportunity to meet the requirements for
20 the SDOE, and for the target system. Jack.

21 MEMBER STETKAR: Does your process call
22 for any static analysis of the code to check for known
23 vulnerabilities or to check for viruses or things like
24 that?

25 MR. GIBSON: It does not. And here's why,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 performance based. So there's, dependent on the brand
2 and the different circumstances, that would be
3 considered potentially a control, all right.

4 Just like we do in the other one. So if
5 you ask the vendor, you know, you know that the
6 performance objective is this piece of, from a
7 malicious cyber security objective is it, does it
8 contain any malicious code. That's the performance
9 objective.

10 So we let them tell us how they're going
11 to figure out that it doesn't have any malicious code
12 in it. Because it varies with technology, it varies
13 with the tools that are available on the market.

14 It varies with a lot of things. Now over
15 in the 1.152 arena, they're going to have to make sure
16 that they meet those requirements as well. And
17 they're also being imposed on us, contractually.

18 Because, remember, the utilities own the
19 whole thing, contrary to popular belief. We have to
20 make the vendor do stuff. They don't do stuff on
21 their own.

22 So the, you know, in that it's going to
23 say, you've got to meet the requirements of Reg Guide
24 1.152, Revisions 2 or 3, whatever current one is. So
25 we see all this and we have the responsibility 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 making sure our quality assurance programs are met.

2 That they meet the requirements of both
3 the non-malicious and the malicious. We've reviewed
4 our outputs. We don't have, we, and I don't agree
5 that we probably should try to have those kind of
6 deterministic things at this point in the technology,
7 because it can't be consistently applied to every
8 technology platform as a deterministic measure.

9 DR. HECHT: Let me just say that, you
10 know, Stuxnet was installed in a Siemens, I think
11 System 7 type of control system, and it would seem to
12 me that that's something that you might want to check
13 for, not only in Siemens, but also in Foxboro,
14 Westinghouse or whomever else is left.

15 MR. GIBSON: Let's speak about Stuxnet for
16 a minute. The 148 controls, is that right, 148? And
17 the people who got affected by that, addressed all
18 those controls effectively. They could not have been
19 affected by Stuxnet.

20 DR. HECHT: You think so?

21 MR. GIBSON: Because Stuxnet was a
22 configuration control problem, period. The people
23 that built that, didn't use, they just collected a lot
24 of different vulnerabilities and packaged them in a
25 way to get their object achieved. They didn't use

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 anything special.

2 DR. HECHT: Okay, let me put it this way.

3 If it was introduced through the, after it was built,
4 that's one thing. But what I'm saying is that it
5 could have also been introduced in the supply chain.

6 MR. GIBSON: That's where the performance-
7 based approach to the supply chain, I think is a
8 failure, because we're asking the vendors to assess
9 their development environment using the same controls
10 that we've been ask to address by a Regulator, in a
11 performance-based approach.

12 So we'll get to inspect that. And we'll
13 say, well how are you doing this? I mean are you
14 checking, are you tagging, for instance, are you
15 tagging all your software objects when they're made?

16 What validation are you doing? How do you
17 know where you got this stuff? We'll ask them all
18 those questions. Because that's the same kind of
19 questions them guys will ask us when they show up here
20 to inspect us. We passed it down, that's how it
21 works.

22 DR. HECHT: If you're not smart enough to
23 ask the right question in that performance-based
24 approach, you won't see it because this is, it's very
25 difficult to establish a performance-based requirement

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 if you don't know whether something exists.

2 MR. GIBSON: Well, I mean, I guess that
3 can be a bit of a professional debate. But if the
4 controls were addressed, if you address all those
5 controls, and they all require configuration control.

6 Making sure you know, you vet, you know,
7 changes. That you know where things come from, that
8 you do tests and you do vulnerability scans. You do,
9 which would detect, you know, configuration that could
10 detect known, you patch, all of those things.

11 If you look at Stuxnet, Stuxnet used the
12 whole sequence of, you know, bad patch management,
13 bad configuration control, blah, blah, blah.
14 Together, those controls, together, address it.

15 DR. HECHT: But a scan, I'm just asking
16 you whether you require a scan, and you're saying no,
17 this is all performance-based and then I understand
18 the reason for performance-based, because you don't
19 want to constrain people and you don't want to add
20 expense and you don't want to exclude people who might
21 otherwise be very good suppliers.

22 On the other hand, this is, you know, the
23 tradeoff is, is that when you have a performance-based
24 approach, flexibility allows you the opportunity to
25 miss 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 MR. GIBSON: It also works the other
2 direction.

3 CHAIRMAN BROWN: Let me interrupt. We're
4 getting a little bit too far down in the weeds at this
5 point. So let's move on.

6 DR. HECHT: I apologize.

7 CHAIRMAN BROWN: No.

8 MR. GIBSON: That's okay. So, I think you
9 see the picture on the Crystal River Project is, you
10 do stuff in the, what would be the conceptual phase,
11 procurement phase in the practical way of talking
12 about it.

13 Functionally, and from a procurement point
14 of view and it comes through all the way to when the
15 system goes to FAT, it gets assessed again. You know,
16 you put it in a box, you lock the doors on it, and you
17 get ready to ship it to the site.

18 Now, the things we'll share with you is
19 our AP1000 experience. You guys have looked at that
20 extensively, so I won't try to rehash that with you.

21 We followed a similar approach with
22 Westinghouse, as far as being engaged with them early
23 on. You know, five years ago, doing these same
24 things, forming cyber security Teams.

25 Shaping, engaging them and shaping them on

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 their DCD and involved in their initial submittal,
2 their ultimate SDOE environment, you know.

3 And they're not necessarily taking their
4 orders from us directly, but we have a say and we're
5 real interested in, you know, what kind of findings
6 and approvals that they get from you guys.

7 So, I think at this point, you know,
8 they've had a finding of an SDOE for the AP1000, so
9 they got a SCR on that.

10 CHAIRMAN BROWN: I'm thinking we said that
11 they will comply with 5.71.

12 MR. GIBSON: That's right.

13 CHAIRMAN BROWN: That was the cyber
14 security plan.

15 MR. GIBSON: Abbreviated.

16 CHAIRMAN BROWN: In the DCD.

17 MR. GIBSON: And we'll continue to engage
18 them through our contract and project management
19 interfaces as we go forward, to achieve the same thing
20 we're talking about with this Crystal River project.

21 Turnover, we expect to have the
22 documentation and assurance that we've had good
23 functional cyber security design. Did they protect
24 the development environment adequately? And they got
25 documentation to show for it.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 CHAIRMAN BROWN: And that's when you
2 expect NRC now to come in and take a look and see that
3 you really did comply?

4 MR. GIBSON: And we expect them to do
5 that.

6 CHAIRMAN BROWN: I think the difference in
7 approaches is very clear from the thought process in
8 your explanations. It's good to hear a couple of
9 different viewpoints.

10 CHAIRMAN BROWN: John, Jack, anything
11 else?

12 MEMBER SIEBER: I don't have any
13 questions, but I can give you a comment. It was
14 pretty clear what the staff was trying to do in the
15 development of the changes to the Reg Guide and the
16 separation of cyber security from operational issues.

17 I thought the process was complicated. I
18 worried about whether the staff had dropped some
19 pieces that were requirements, and it appears that it
20 is complicated, but they hadn't dropped pieces.

21 And I also conclude that you aren't
22 finished. And that there are things that need to be
23 done in the future. And when I thought about that, I
24 thought about do you ever do a job where you're
25 absolutely satisfied that you're going to finished,

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 then how long does it take, to be absolutely
2 certain that you've covered every base and every
3 conceivable issue.

4 In the amount of time that it takes to get
5 there, is probably infinite. And so to be practical,
6 you have to make changes in order because the
7 situation is not going to stay still.

8 And I worried about the complexity and
9 whether there were missing pieces or pieces that were
10 not easy to understand. But my opinion changed with
11 licensee presentations this afternoon.

12 It seems to me the licensees fully
13 understand it and in particular for the change control
14 process. Where you have 5059 plus cyber security
15 requirements. The separation actually makes that
16 process easier to understand and easier to implement.

17 And so, from that standpoint, even though
18 it's complex, it does have, it has the advantages of
19 being structured the way the regulations are
20 structured and also understood by licensees as to how
21 they should perform.

22 So, I come away with it with the whole
23 review, from my viewpoint, as the staff has perhaps,
24 not perhaps, but assuredly done the right thing to get
25 the regulations in the positions, in the position 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 it's in at this level.

2 And that were are critical pieces that are
3 missing or misconstrued, and that licensees understand
4 it and can work with it. So, I guess my opinion is
5 that it's basically okay.

6 CHAIRMAN BROWN: By and large you ought to
7 understand that the Subcommittee does not speak for
8 the Committee.

9 MEMBER SIEBER: Or for each other.

10 CHAIRMAN BROWN: Or for each other.

11 (Laughter.)

12 CHAIRMAN BROWN: In all circumstances.
13 There will be, I'm sure, interesting discussion when
14 we get around to presenting this at the full Committee
15 for final adjudication and however it comes out.

16 But it is important to get the very
17 viewpoints out on the table, with their considerations
18 and the bases for the consideration. So, I think, I
19 want to thank you all for you all coming in here and
20 doing this, and providing your all's insight.

21 I think getting the insight from two
22 people who actually have to do the work, even though
23 they diverge in their approach, is valuable.

24 I'm never quite so sure from listening
25 whether they will be as divergent as they sound, once

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 you get into full-bore execution, but that's a thing
2 for the future.

3 So, anyway, we thank you very much for
4 your all's presentations and the time you took to come
5 here and listen to us pontificate and ask questions
6 and everything else.

7 I'm going to propose we take a ten or 15
8 minutes break, if that's acceptable. Let's make it 15
9 minutes, we'll convene back here at 3:35, and we'll
10 finish off with Eric Lee and the cyber security
11 presentation from NSIR.

12 (Whereupon, the proceedings went off the record at
13 3:19 p.m. and came back on at
14 3:34 p.m.)

15 CHAIRMAN BROWN: The meeting is back in
16 session and we will now proceed with NSIR's
17 presentation with Mr. Eric Lee leading us off, I
18 guess.

19 MR. LEE: Yes, thank you.

20 CHAIRMAN BROWN: Thank you very much, and
21 for your patience.

22 MR. LEE: Thank you. Good afternoon, my
23 name is Eric Lee and I'm a Senior cyber security
24 Specialist with the Integrated security Coordination
25 and Policy Branch within the Office of Nuclear

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 security and Instant Response.

2 Here with me are Dr. Shinn, and he's a
3 Senior cyber security Consultant, and George Simonds,
4 he's also Senior cyber security Specialist and Ralph
5 Costello who is from Division of security Operations.

6 Next slide. The previous presenters have
7 covered the overview of digital system safety and
8 cyber security and the differences between Revision 2
9 and Revision 3, of Regulatory Guide 1.152.

10 And in my presentation, I would like to
11 make, or I would like to emphasize the following two
12 important points, made by the earlier presenters.

13 One, once the NRC reviews and accepts
14 licensee's and applicant's cyber security Plans, the
15 cyber security program criteria described in their
16 cyber security plan becomes condition of their
17 license.

18 In other words, they become the Regulatory
19 requirements. In their plan, the licensees and
20 applicants have committed to follow guidance provided
21 in Regulatory Guide 5.71, or equivalent, in their
22 plan.

23 CHAIRMAN BROWN: So the CSP becomes part
24 of the licensing basis?

25 MR. LEE: Yes, sir.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 CHAIRMAN BROWN: Okay, just to summarize
2 that.

3 MR. LEE: And we are currently doing the
4 review right now. Second point that I would like to
5 make is that the main differences between Revision 2
6 and Revision 3, of Regulatory Guide 1.152, is that in
7 Revision 3, cyber security guidance provided in
8 Revision 2, is moved to Part 73 requirement, Part 73
9 Programs including Regulatory Guide 5.71, and also
10 into the cyber security plans that submitted by
11 licensees and applicants.

12 The second point naturally leads to the
13 question of what, to what extent the security guidance
14 provided in Regulatory Guide 1.152, is covered by
15 Regulatory Guide 5.71, or I guess security
16 requirements inherent in Regulatory Guide 5.71.

17 Therefore, a goal of this presentation is
18 to answer that particular question. I'll briefly go
19 over the overview of the security Life Cycle within
20 the Regulatory Guide 5.71. And I will also explain
21 each phases, each phase of security Life Cycle in
22 Regulatory Guide 5.71, from the perspective of Life
23 Cycle phase contained in Regulatory Guide 5.71.

24 Then I'll conclude my presentation by
25 taking a few moments to summarize my presentation,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 before leading into a presentation on inspection and
2 oversight activities.

3 Let me begin by stating that Regulatory
4 Guide 5.71, provides full system security life cycle.

5 Additionally, it provides comprehensive requirements
6 for each phase of security life cycle.

7 However, this is often overlooked in
8 Regulatory Guide 5.71, because security life cycle and
9 its prospective phases are not discussed in the same
10 manner or the logical sequence, as provided in
11 Regulatory Guide 1.152.

12 Instead, these phases are provided
13 Regulatory Guide 5.71, as security measures and
14 activities that licensees and applicants have
15 committed to perform as element of their cyber
16 security program.

17 And compounding this issue, is that 10 CFR
18 73.54, is a programmatic, performance-based as
19 previous presenters have stated. Because of that, we
20 seem to put a lot focus on the Reg Guide 5.71, seem to
21 put a lot of focus on operational and maintenance
22 phase.

23 This overview diagram shows, at a high
24 level, what main cyber security activities takes place
25 in each phase of life cycle.

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 I will walk through each phase in
2 detail to explain how Reg Guide 5.71, rather how
3 security activities and the measures that a licensee
4 have committed in Reg Guide 5.71, cover them.

5 Next slide. Actually, at this concept and
6 requirement phase, phases are a good example of how
7 security activities and measures provided in Reg
8 Guide 5.71, are covered by the life cycle phases
9 described in Reg Guide 1.152.

10 Specifically, the concept and requirement
11 phases are covered by security controls, security
12 impact analysis and the system and service
13 acquisitions requirements sections of Reg Guide 5.71.

14 Let me explain how they are alike. Let me
15 first begin by asking question. What is that
16 licensees are required to defend against? 10 CFR
17 73.54, requires each licensee to provide high
18 assurance that those systems, within the scope of the
19 rule, from cyber attack, up to and including a design
20 based threat. A design based threat which is
21 described in 10 CFR 73.1 or DBT. DBT describes
22 characteristics of adversaries, whose object is to
23 cause radiological sabotage or theft and diversion of
24 a nuclear material.

25 And the Cyber is a, one method that DBT

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 adversaries can use to achieve their goal. Now, given
2 this, how do we provide high assurance that these
3 systems are protected from Cyber attacks?

4 Well, the DBT adversary will seek out and
5 search out a vulnerabilities and weaknesses and try to
6 exploit them to achieve their goal. So, to provide
7 high assurance from Cyber attack, licensees --

8 CHAIRMAN BROWN: What was the acronym
9 again?

10 MR. LEE: Designed-base threat, DBT.

11 CHAIRMAN BROWN: Design-based threat,
12 okay, all right. I just couldn't connect those
13 letters.

14 MR. LEE: So to provide high assurance, a
15 licensee needs to identify all the currently known
16 vulnerabilities and then to implement security
17 measures to protect against adversaries from using
18 those vulnerabilities to achieve that.

19 And that was our philosophy behind this,
20 applying these 148 security controls. Up until
21 development of Reg Guide 5.71, NRC relies upon the
22 risk assessment and the vulnerability assessments that
23 we developed for pilot study at four nuclear power
24 plants. And the result of this is provided in NUREG -
25 6847.

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, based on this study, industry
2 published NEI-0404, which is a cyber security program
3 guidance document and also NRC updated Reg Guide
4 1.152, Rev 2.

5 On paper, developed risk assessment and
6 vulnerability assessment appears to be logical and
7 appropriate, to find the problems and fix the
8 problems.

9 But, in reality, it poses a lot of
10 challenges, because it's limited by the amount of
11 knowledge and the imagination of people who are
12 performing the assessments.

13 After the result of this risk analysis is
14 dependent, are dependent on the knowledge and
15 experiences of those people who are going to perform
16 the assessment and also their willingness to look at
17 it from the adversaries point of view.

18 And, therefore, if the knowledge and the
19 experience of the Assessor is limited, and if they
20 have a limited willingness to look at it from the
21 adversaries point of view, the result they're going to
22 get is going to be very limited.

23 In other words, vulnerability they're
24 going to identify is going to be very limited.
25 However, the people who are going to perform this

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 assessment, they are going to feel very comfortable,
2 confident that they've addressed all the issues.

3 But, in reality, what they did was they
4 only addressed those vulnerabilities or weakness they
5 know. Not all the vulnerabilities that have been
6 documented and published.

7 And this is, this also poses a challenge
8 to the staff, because when we --

9 CHAIRMAN BROWN: Hold on a minute, Eric,
10 please.

11 MR. ERLANGER: I apologize for the
12 interruption. We were just informed that there is one
13 piece of information in a latter slide related to the
14 architecture discussion related to TSC, that we've got
15 to sabotage one sentence in the slide, otherwise it
16 becomes proprietary and we have to change.

17 So, I apologize for the interruption, sir,
18 if we could just spend one second on the screen.

19 CHAIRMAN BROWN: Have at it.

20 (Asides.)

21 CHAIRMAN BROWN: We're going to go off the
22 record for this.

23 (Whereupon, the proceedings
24 went off the record at 3:46
25 p.m. and came back on at 3:53

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 p.m.)

2 CHAIRMAN BROWN: We're back on the record
3 now. Slide 3. I was trying to, when I first started
4 looking at this, it says digital safety system life
5 cycle, Reg Guide 5.71, and it shows five phases.

6 Okay and I'm sitting here, I didn't see
7 any of that, I'm looking at the four column headers,
8 the five column headers. So, because I don't remember
9 seeing those terms in 5.71.

10 That's what I saw in 1.152. So I was
11 trying to figure out what point you were trying to
12 make, relative to concepts and requirements. It
13 looked like the first two blocks are Sections,
14 equivalent to 2. positions, 2.1 through 2.5 in 1.152,
15 and the last three columns fall under the 2.6 through
16 2.9.

17 Except the words under them are different.

18 Well, let me finish, because concepts and
19 requirements doesn't have anything to do with security
20 planning and requirements analysis in 1.152. So, I
21 had a disconnect on what we're doing with this
22 particular picture.

23 MR. SIMONDS: As Eric Lee had mentioned
24 before, sir, the 1.152 Revision 2 and Revision 3, both
25 are laid out from a life cycle perspective --

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 CHAIRMAN BROWN: Oh, nine phase life
2 cycle.

3 MR. SIMONDS: The Regulatory Guide 5.71,
4 doesn't walk linearly in the same manner. It just
5 refers to the life cycle phases as you've read in your
6 own review.

7 So what we did is we pulled the 5.71
8 requirements and this particular slide, it's high
9 level activities, and then tie them back and link them
10 back to the 1.152 waterfall life cycle phases.

11 So that you, as we're moving through the
12 presentation we can get a link or a connection between
13 the requirements that are in the 5.71, and tie them
14 back to the phases as they're described in 1.152.

15 CHAIRMAN BROWN: However, I was told that
16 you don't do things during the first five phases of
17 the concepts, requirements, design implementation and
18 test in the factory.

19 You don't do security planning, you don't
20 do supply chain security, you don't do functional
21 security design. It's all safety-related not
22 security-related. Well, yes, that's what it says.

23 They don't, they don't do cyber security
24 under the first five positions.

25 MR. LEE: What we tried to do was that

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 the, at the beginning of my presentation, what I said
2 was that the differences between Revision 2 and
3 Revision 3, was that in Revision 3, they took all the
4 security out of, removed, excuse me.

5 They migrated those security guidance,
6 provided in Revision 2, into Part 73 programs. And
7 this diagram, what I'm trying to do, as one of the
8 goal of my presentation is to inform you that the
9 security requirements or security activities and the
10 measures that licensee have committed to perform,
11 actually covers those items that move out of Revision
12 2 of --

13 CHAIRMAN BROWN: So all you're trying to
14 say is those items that would have been in positions 1
15 through 5, they were removed and moved into these
16 other categories?

17 MR. SIMONDS: Or that they're covered
18 under Regulatory Guide 5.71.

19 CHAIRMAN BROWN: Okay, I was trying to
20 read more into this figure than what was really there,
21 in terms of equivalency. You can go on.

22 MR. LEE: Thank you, sir.

23 CHAIRMAN BROWN: Have you learned once
24 you've said that you just keep on bogeying. Back to
25 Page 4.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. LEE: The, as I have just mentioned
2 that the, because of the limited capability of people
3 who are doing the, these assessments, risk assessments
4 and vulnerability assessments, that there is a reason
5 for that.

6 Because of that, NRC needs to review the
7 adequacy of how well licensees perform this analysis
8 during the concept and requirement phase provided in
9 Reg Guide 1.152.

10 In other words, the reason that we had to
11 look at it was because their limited knowledge, so
12 somebody has to check how well they have covered
13 these, identified these vulnerabilities.

14 However, again, because when NRC reviews
15 these assessments, it's also going to limited by their
16 knowledge and their experience and their willingness
17 to look at it.

18 So this could also provide some challenges
19 as to how well we do this. And this also provides,
20 could lead to a false sense of security that, since
21 the NRC looked at it everything is secure.

22 So, our objective to ensure that we are,
23 high assurance that protect against this DBT
24 adversaries, we need to identify all the
25 vulnerabilities that are applicable to the nuclear

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 power plants and address them.

2 So, to solve this problem, what we decide
3 to do for the development of Reg Guide 5.71, was that
4 to leverage years of research and a trial conducted by
5 NIST and DHS on the vulnerabilities associated with,
6 and not only the digital systems, but also with the
7 digital control systems.

8 And the results are provided in NIST
9 Special Publication 800-53, and 82. And these
10 standards provide more than 200 security controls.

11 And the source of these security controls
12 are from, as I mentioned earlier, like a defense
13 audit, financial, healthcare, intelligence community,
14 as well as the controls defined by the National and
15 International Standard organizations.

16 So what we did was joined team of NRC,
17 industry and cyber security experts and we tailored
18 those security controls to, for a nuclear power plant
19 and to fit within the Regulatory framework of NRC.

20 And they have tailored them to about 148
21 security controls. And this is equivalent to
22 performing a vulnerability assessment and the risk
23 analysis, and identifying more than 148 security, I
24 mean vulnerabilities and weaknesses.

25 Because security control can provide more

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 than one vulnerability of weaknesses.

2 MEMBER STETKAR: Eric, why do you say
3 that's equivalent to performing a risk assessment?
4 Because there's, in this publication, 800- I think
5 it's 30, that strongly recommends a plant-specific
6 integrated risk assessment.

7 Just this list of 148 generic things that
8 somebody thought about, looking at a bunch of generic
9 stuff, doesn't tell me anything about my nuclear
10 plant.

11 I think what we've learned from more than
12 30 years of doing risk assessments on nuclear plants,
13 is that until you do an integrated, plant-specific
14 risk assessment, you don't understand vulnerabilities
15 and risks.

16 So it's not clear to me why this list,
17 other than it's a convenient checklist, is equivalent
18 to doing an integrated risk assessment. I'd like to
19 understand your statement that it is equivalent. It's
20 a checklist.

21 DR. SHINN: Yes, Mike Shinn, yes, I can
22 answer your question for you, sir. So we actually did
23 follow the same process that NIST uses. So the
24 process of performing the risk assessment, is to first
25 do an impact analysis, which we did.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 The systems that are under the scope of
2 the Rule are the high impact systems. So following
3 the NIST process, that means that those high impact
4 controls are applied, period.

5 So then what you do, is you do additional
6 assessments, vulnerability assessments and
7 effectiveness analyses, to determine that those
8 measures are effective against the threat and the
9 vulnerabilities that you have.

10 And you also do the vulnerability
11 assessment to determine whether or not you need to do
12 additional things. So we actually took the formula
13 apart, all the elements that make it up, and it's
14 actually built into 5.71. So there is a risk
15 assessment in there.

16 MEMBER STETKAR: When you say you do it,
17 do you mean I as in --

18 DR. SHINN: The licensee.

19 MEMBER STETKAR: Okay.

20 DR. SHINN: Right. Part of it is
21 prepopulated due to the nature and the scope of the
22 system. Because we're only concerned with the
23 radiological sabotage system, so there are things in
24 the plant that don't fall under the scope of the Rule,
25 and potentially could need less security.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 So, in that case, they don't really count.
2 The systems that count to us are the high impact
3 systems. So following the NIST approach, that's why
4 that baseline set of controls is there.

5 Because we know the capability of the DBT,
6 that's another variable that we feed into this. And
7 the process of tailoring the controls, was that risk
8 assessment that we're talking about.

9 Once you develop that minimum baseline set
10 of things that we knew collectively, us and the
11 industry, that we were going to need to address for
12 those high impact systems of the plant.

13 MEMBER STETKAR: Well, you're saying that
14 in addition to that, I, as an applicant or a licensee,
15 also need to do an additional assessment?

16 DR. SHINN: Yes.

17 MEMBER STETKAR: Okay.

18 DR. SHINN: Yes, because this is baseline.

19 MEMBER STETKAR: That was my understanding
20 of 5.71, by the way.

21 DR. SHINN: Yes, it's not a checklist, I
22 mean it's a very valid observation, because that's not
23 what we want, you know. That's that minimum set of
24 controls and you're doing this analysis to make sure
25 that they're effective, that they're actually

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 addressing the capabilities of the threat.

2 And then for the unique circumstances of
3 your plan, which is why we made the program flexible,
4 you have to, how you're going to do that is going to
5 be unique at each plant.

6 MEMBER STETKAR: Okay, that helps.
7 Because I was looking at a section of the Reg Guide
8 and my reading of that section is more intuned from
9 what you just said, so thanks, that helps.

10 MR. LEE: Actually that answers all --

11 DR. SHINN: That's the rest of the slide.

12 MR. LEE: So, one thing, in the interest
13 of time, there's one thing that I'll repeat what Mr.
14 Erlanger said earlier, is that this is the reason why
15 we said that we took fun out of the risk analysis and
16 we also refer this as the NIST standard for nuclear
17 power plants.

18 One thing that I would like to point out
19 is that in addition to this, licensees also have
20 committed to follow vulnerabilities, new
21 vulnerabilities and also they have committed to
22 perform the risk, I mean a vulnerability assessment
23 prior to implementing their system, turning the system
24 operational.

25 Another point, one point that I would like

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 to make is that the, as I said before and as what Dr.
2 Shinn has stated, that the, these are like 148
3 security controls that, you know, when you apply,
4 minimum set that you apply, when you first establish
5 your program.

6 And also, as you do that, you also,
7 licensees and applicants have committed to, you know,
8 cognizant of all the vulnerabilities that are
9 appropriate to them.

10 Also they are committed to track all the
11 security measures to address those. So that means
12 that the, when they do the next modification, after
13 they establish a cyber security program and when they
14 try to do the modification, that means that they have
15 to address new vulnerabilities they have collected,
16 from the time they have established their program.

17 So, only point that I'm saying all this is
18 to make a point that under Reg Guide 1.152, concept
19 and the requirement phase is a discrete stuff. But
20 under Reg Guide 5.71, you could say that this is like
21 continuous, because you continue to track, not only
22 the 148 security controls, but you also have to track
23 all the new vulnerabilities and the new threats.

24 So when the acquire a new system they have
25 to consider how they're going to address that and see

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 whether those vulnerabilities apply to them. So
2 that's why in 5.71, it's continuous rather than
3 discrete. Next slide, please.

4 This diagram summarizes what I just talked
5 about. What's reflected in this diagram is that on
6 the, is that the amount of knowledge, put into a place
7 to identify the security controls associated with a
8 system, the left is 1.152 process where you do
9 assessment to see what vulnerabilities or weakness
10 apply.

11 But if on the right-hand side, because
12 you are looking at 148 security controls, you see all
13 those red dots, and plus you also see the below the
14 box there, those are the new vulnerabilities that you
15 collected since you've established your program.

16 CHAIRMAN BROWN: Okay, I want to make sure
17 I understand something, because I'm not sure I quite
18 grasp this. You say I've got five systems, I'm using
19 the right-hand side of your viewgraph.

20 And you've got 148 baseline controls,
21 security controls?

22 MR. LEE: Yes, sir.

23 CHAIRMAN BROWN: That means that I take
24 each system and I evaluate each of those 148 for their
25 applicability to that each system?

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. LEE: Yes, sir. Yes, sir.

2 CHAIRMAN BROWN: And then, because those
3 are controls now?

4 MR. LEE: Yes, sir.

5 CHAIRMAN BROWN: Those are not
6 vulnerabilities, those are controls?

7 DR. SHINN: Correct.

8 CHAIRMAN BROWN: That address, to use to
9 address other already known vulnerabilities?

10 DR. SHINN: Yes, sir.

11 CHAIRMAN BROWN: Now you come up with, in
12 some interim period, a new set of vulnerabilities?

13 DR. SHINN: Yes, sir.

14 CHAIRMAN BROWN: That's your little
15 bubbles down at the bottom there?

16 DR. SHINN: Yes, sir.

17 CHAIRMAN BROWN: And you identify controls
18 for each of those vulnerabilities and then those, and
19 you show nine of them, you then have to address those
20 controls that meet, against each of the five systems,
21 as well?

22 Is that the concept?

23 DR. SHINN: Yes.

24 CHAIRMAN BROWN: As opposed to a more
25 limited, that's what I would call it based on the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 1.152.

2 DR. SHINN: Yes, sir.

3 MR. LEE: Because if you really look at it
4 on the, I guess, lefthand side, it's done by a handful
5 of people. But if you look at it on the right-hand
6 side, it's actually done by, not only the NRC Industry
7 Experts, but also cyber security Experts and also it
8 has the knowledge of all those people that
9 participated in developing that NIST standard.

10 So that's what's shown in the right-hand
11 side.

12 CHAIRMAN BROWN: You're just saying the
13 folks that you're going to, to design the stuff, won't
14 have the knowledge of this combined knowledge over a
15 wider world than you're pulling all those together and
16 saying take all of those, we're not going to depend,
17 you may find some others yourself, but we're not going
18 to depend on you to figure out what controls you need
19 against what vulnerabilities.

20 We're going to tell you, and then anything
21 else, either we come up with or you come up with, you
22 have to factor in, in terms of your assessment.

23 And the stuff you show on the right, I
24 want to make sure I understand that you're explaining
25 your assessment type thing.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. LEE: Yes, sir.

2 CHAIRMAN BROWN: The vendor, the licensee
3 is still doing a threat, is he doing a threat
4 assessment or is he doing a, it seems to me he's doing
5 an assessment of controlled application. In other
6 words, here's a set of controls that bind you, that do
7 something to a system and we're looking, can you even
8 apply them to the system.

9 You may not be able to apply them, just
10 because of the nature of the system. But they may not
11 be necessary.

12 MR. LEE: Correct.

13 CHAIRMAN BROWN: How do they get the
14 necessary in with the control? Your vulnerability
15 that goes with it, in other words, with that control.
16 Go ahead.

17 MR. LEE: For each of these security
18 controls in the Reg Guide 5.71, I believe it's Section
19 3.1.6, specifically tell you how you're supposed to
20 apply these security controls, or address these
21 security controls.

22 You either address the security control or
23 you may apply alternative security controls or you do
24 not apply the security controls because these security
25 controls does not apply to you.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 And they do that for every single system,
2 and --

3 CHAIRMAN BROWN: Don't they have to know
4 the vulnerability that they're addressing, though, at
5 the same time? I mean I could apply some controls,
6 but I don't have a vulnerability that requires that
7 control.

8 DR. SHINN: Yes, there is a level of
9 expertise certainly necessary, because there's a step
10 in there called the effectiveness analysis which is
11 ensuring that the control adequately meets the
12 capabilities of the threat.

13 Whether or not it actually works for the
14 system and so on. That's why, for us, it's dynamic
15 programmatic process. Because we know that's going to
16 change on an ongoing basis Because the bad guys learn
17 how to do new things.

18 You may have to go back and change those
19 controls around, you may have to add controls. You
20 may have to change the system, potentially. So, yes,
21 there's certainly a level of expertise necessary to
22 assess whether or not a control, as applied, is
23 effective, based on the capabilities of the threat,
24 what the system will do and so on, certainly, yes.

25 MR. SIMONDS: But real quick, is the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 question, sir, whether or not more defining new
2 controls that tie back to vulnerabilities that we've
3 identified through analysis?

4 CHAIRMAN BROWN: I'm looking at the 148,
5 I'm just trying to get a handle on the 148. Somebody
6 has done a vulnerability assessment, cyber security
7 vulnerability assessment of bunches of systems,
8 somewhere.

9 And they have found, these are the
10 controls that are effective against these
11 vulnerabilities. So you've identified those up front.

12 So you've got to assess your systems for
13 those --

14 MEMBER SIEBER: To see which
15 vulnerabilities you have.

16 CHAIRMAN BROWN: Well, they're getting the
17 controls. My point is, is the vulnerability
18 identified along with the control, or just the
19 control, wherever that list is?

20 Because I can go and I could look at a
21 particular system and say, well that system doesn't,
22 if you know what the vulnerability is, you can apply
23 the control, but there's no vulnerability.

24 So I don't connect that really to the
25 effectiveness. I look at the, here's a vulnerability,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 yes my system is susceptible to it, but that control
2 you've defined for that, won't work very well for this
3 system.

4 That's the one thought process. Or it
5 could be, oh, it will work just fine for this one.

6 DR. SHINN: I hope this answers your
7 questions, sir. I mean we are developing a NUREG that
8 explains these controls in more detail, to address
9 just that.

10 CHAIRMAN BROWN: I'm not disagreeing with
11 your approach, don't understand. I'm just trying to
12 understand the application, that's all. Maybe I've
13 missed something.

14 MR. LEE: One thing we did do when we were
15 developing this security control, is that the, with
16 each and every one of these security controls, we sat
17 down with the industry folks, people who are experts
18 in the plant system and cyber security from the
19 industry.

20 We sat down with them and we asked them,
21 did this particular security control, I mean we think
22 that this particular security control applies, is that
23 applies to you?

24 So we have discussion on every single one
25 of them, and see whether applies or not applies, and

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 what are we worrying about.

2 So we were looking at the, I guess, in a
3 way doing the vulnerability assessment or the threat
4 assessment on each one of the security controls, and
5 that's how we got to this list of 148 security
6 controls, out of well over 200 security controls.

7 So what we are saying is that these
8 security controls effectively address all the
9 currently known vulnerabilities that are applicable to
10 the nuclear power plants, at this time.

11 And in, also to address the, which I'll
12 discuss more in my slides is that also we know that
13 these threats and vulnerabilities are evolving.

14 So what licensees have committed to do is
15 that, yes, of these, we'll see, because the objective
16 is to make sure that we plug all the known
17 vulnerability to provide this high assurance against
18 DBT adversaries.

19 So, after that, what we're going to do is
20 we're going to do, right before I turn my system
21 operational, I'm going to do effective analysis to
22 make sure that the oldest security controls are
23 properly configured and performs as it's supposed to
24 perform and it address vulnerabilities it's supposed
25 to address and also they're going to perform a

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 vulnerability assessment and see whether there are any
2 other vulnerabilities that's not covered by 148
3 security controls.

4 So that in case, while the, during the
5 development process, it might take a year or two
6 years, during that time, they may have more
7 vulnerabilities. So by the time they need to
8 configure it, it may be necessary for them to
9 reconfigure their security controls.

10 Or the security control may cover that
11 particular vulnerability or it may be necessary for
12 them to think about other ways to address that
13 particular vulnerability.

14 MR. SIMONDS: If I could say it maybe in a
15 different way. When we went through the process of
16 tailoring the baseline controls that are outlined in
17 NIST-853, which of course there were in excess of 200
18 some odd controls.

19 We often refer to it as a nuclear, we
20 nuclearized that baseline. And what that essentially
21 entailed, as a collaborative effort with industry and
22 with staff consultants and so on and so forth, experts
23 in the private sector.

24 We basically walked through each of those
25 controls and we asked ourselves about its

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 applicability within the target environment. Which,
2 again, was a discussion based upon what vulnerability
3 are we really looking to address by implementing this
4 control or putting it as a part of a nuclearized
5 baseline.

6 So, to answer your question, sir, if I
7 believe I'm understanding it correctly, is that yes
8 there was a discussion up front as to what is the
9 vulnerability that each of these controls tie back
10 too.

11 But understanding that, because we're
12 dealing with an emergent threat or these emerging
13 vulnerabilities, we recognize that as we performed
14 vulnerability analysis from the onset, and as we
15 continue to perform that sort of analyses throughout
16 the process, or throughout the life cycle, there may
17 be new vulnerabilities that we identified that we're
18 not sure at the onset whether or not there is one of
19 the existing controls addresses it or does not address
20 it.

21 So that process then comes back to, is
22 There an existing control which satisfies or mitigates
23 or eliminates that particular vulnerability.

24 Or, at this stage, are we required to
25 basically build a new control, that we would then have

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 articulate, put into practice and implement it so
2 that it addressed whatever new vulnerability we've
3 discovered.

4 But it all comes back at some point to an
5 analysis of the root cause or the vulnerability
6 itself.

7 DR. HECHT: Can I ask, are you done,
8 Charlie?

9 CHAIRMAN BROWN: I'm cooked.

10 (Laughter.)

11 DR. HECHT: Ask a related question which
12 is not determining which applies to which, but let's,
13 well maybe it is related. But how these apply is also
14 extremely difficult to fathom and to verify.

15 I'll give you an example. I happen to
16 turn to Page B-13 of 5.71, and I was lucky, I guess.
17 But C-311, unauthorized remote activation of services.

18 And basically says configuring CDAs to prevent remote
19 activation of collaborative computing mechanisms.

20 And configuring CDAs to provide physical
21 disconnection of cameras and microphones. And under
22 the first one, I was thinking, well, gee, why do I
23 have a plant knowledge repository, something like
24 LiveLink or eRooms or something like that?

25 That's certainly a critical digital asset.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 And I'm not sure I want to prohibit activation of
2 that, I think I want people to be using that common
3 knowledge repository.

4 Then I looked at D-3.13, public, PKI
5 certificates. Well, what if, why would, I'm not ever
6 sure why a plant would want to use public
7 certificates, why not use another form of
8 authentication specifically badges?

9 And so these are not, and then I look at
10 B-3.14, mobile code. It basically says establish
11 usage restrictions and implementation for guidance and
12 mobile code technologies based on their potential to
13 cause damage. Wow. That's a tall order.

14 That's really difficult. I mean that's
15 basically what's going on, on the Internet today. So,
16 I guess the, we call about design criteria in the
17 safety world, but these are not simple.

18 CHAIRMAN BROWN: Mobile code means cell
19 phones?

20 DR. HECHT: No mobile code means basically
21 when you download, when you're getting a file and all
22 of a sudden you see an advertisement playing on your
23 newspaper app, that's mobile code.

24 CHAIRMAN BROWN: I hate that.

25 MR. ERLANGER: So, Mr. Hecht, if I can try

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 and then you all can correct what I misstate here.
2 They'll do just what you said there. They will go
3 through those controls and figure out if they apply to
4 a critical digit asset, if that particular system
5 screens in as an asset.

6 So, an example being, does that safety
7 security EP function, in that system you described,
8 does that take you to a radiological core damage type
9 scenario?

10 If it does, perhaps it screens in. They
11 will then go through the security controls and see if
12 they apply. Maybe you're right. Maybe they do need
13 a, you know, some access to an e-library, maybe they
14 don't.

15 But they'll ask themselves that battery of
16 questions and then they'll, they can simply say this
17 control doesn't apply because, or yes I do need this
18 control.

19 It has the flexibility. What the staff is
20 trying to do in the guidance document is force the
21 licensee and the applicant to ask themselves those
22 questions for that particular digital asset.

23 So you're 100 percent correct. Depending
24 on what the asset is, it may or not apply. But these
25 are known things that they need to consider as they 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 their thought process.

2 DR. HECHT: That was certainly one part of
3 it, but the other part of it is, how do I do this.
4 And particularly with respect to the vulnerabilities
5 of mobile code is an example.

6 CHAIRMAN BROWN: Let me, I'm trying to use
7 your example here. If I've got a system that can,
8 within the plan and it's a Level 3 or Level 4 system,
9 I guess I would look at the mobile code thing and say,
10 I don't have to apply that control.

11 DR. SHINN: You may not. That is
12 absolutely correct.

13 CHAIRMAN BROWN: The fact is I would
14 almost say, why would I ever have to apply it. Not
15 may, you wouldn't.

16 DR. SHINN: You're absolutely correct,
17 sir.

18 CHAIRMAN BROWN: But now if I'm talking
19 about something up in the Level 0 for Level 1, where I
20 have the potential for an off-site or wireless, for
21 some reason, coupling into my, some network that I've
22 got, you know, I don't want to call it explicitly a
23 business network, but some other kind of auxiliary
24 network, regardless of whether it's, I guess maybe, I
25 don't know, maybe I'm not saying this 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 But if there's a place where I'd have to
2 say it could be vulnerable. Because if you're
3 accessing sites or off-sites or some places where that
4 type of stuff could get on the line and come in to
5 you, just like it does on our PCs.

6 Then you would have to think about how do
7 I block those things, which is, it sounds to me like
8 pop-up control. And that doesn't work all the time,
9 that's all I know.

10 Even when you enable it. So am I thinking
11 in the right ballpark?

12 DR. SHINN: Yes, sir.

13 DR. HECHT: So what you really mean in
14 this case would be like what plug-ins you allow and
15 what plug-ins you don't allow?

16 DR. SHINN: That certainly may be one way
17 to solve the problem. Or, you may simply say, there's
18 no need for there to be mobile code on this thing. It
19 supports it, I'm going to disable it.

20 Or, as Charlie said, I don't have to worry
21 about this, because this vector doesn't exist in this
22 environment, and the justify that accordingly.

23 Or, there may be another solution that we
24 haven't thought of, to the problem.

25 CHAIRMAN BROWN: Okay, let's move on.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 John, go ahead, I'm sorry.

2 MEMBER STETKAR: Yes, move on for the next
3 slide, because I can ask --

4 MR. LEE: I think I've covered most of
5 that last, the only thing that I would like to say is
6 the last bullet item, which says that the Reg Guide
7 1.152 and Reg Guide 5.71, requires that if
8 implementing security controls could adversely impact
9 the functioning of the safety system, then don't apply
10 that security control.

11 However, under Reg Guide 5.71, that
12 doesn't mean that that particularly vulnerability does
13 not exist. You have to apply alternate security
14 control to address that vulnerability. If that
15 vulnerability exists.

16 CHAIRMAN BROWN: If you can find a control
17 that will not affect reactor safety. You're saying a
18 security control should not be applied if the control
19 adversely impacts reactor safety, or safety systems.

20 MR. LEE: Yes, sir.

21 CHAIRMAN BROWN: And if you went through
22 your whole list of controls and any other controls and
23 you find out I can't find one that will do that, then
24 you have to make a judgement that my, I don't, I hate
25 to hesitate to use this word, risk is small enough

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 that I will live without a control.

2 But it has to be acknowledged and
3 accepted, you know, by the regulatory environment.
4 Have I got --

5 MR. SIMONDS: Or another option would be
6 to find an alternative approach that would provide
7 equal protection --

8 CHAIRMAN BROWN: If I just said you
9 couldn't find, the circumstance where none of the
10 identified controls nor any other controls seem to
11 meet it without it impacting, then you're forced,
12 that's got to be within the purview I would think, of
13 making that decision. You just can't be, hopefully
14 the risk would be small.

15 Okay, I'm finished with it. John, did
16 they get you, or do you have some more on that?

17 MEMBER STETKAR: No, what I've been
18 struggling with is I hear all the words. I read the
19 words and I hear people's interpretations of what the
20 words might mean.

21 I'm still left questioning how this
22 process is implemented throughout the complete life
23 cycle of the digital systems.

24 From what I hear you folks saying is that
25 someone performs an evaluation of those 148, whatever

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 they're called.

2 DR. SHINN: security controls.

3 MEMBER STETKAR: Thanks, security
4 controls. And confirms that in deed they're relevant
5 to my system. And then the Reg Guide and what you've
6 said also says that I need to also perform an
7 evaluation of my system to verify that no other
8 vulnerabilities exist, that aren't covered by these
9 148 or whatever subset I've decided apply, and figure
10 out what to do with those.

11 Fine, I get that. When is that assessment
12 performed? According to this it's performed long
13 after the conceptual design, requirements phase. It's
14 when the system is already there, is that correct?

15 MR. SIMONDS: Yes, sir.

16 DR. SHINN: Not necessarily.

17 MEMBER STETKAR: I hear yes and a no.

18 DR. SHINN: Not necessarily, sir.

19 MEMBER STETKAR: Not necessarily, that's
20 where I'm hung up. So I want to know when it's
21 performed and by who?

22 DR. SHINN: So, at the end of the day,
23 what matters is whether or not they address the
24 vulnerability. It could occur now or in the future.

25 The licensee may choose to do that earlier

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 the process and work with the vendor to address
2 those early on problems.

3 MEMBER STETKAR: The Luminant approach to
4 doing --

5 DR. SHINN: It certainly may be more
6 advantageous to do it that way. But from a security
7 perspective, as long as the vulnerabilities are
8 addressed, as to when that occurs in the process is
9 ultimately immaterial to that result, that it is
10 secure.

11 MEMBER STETKAR: I understand that, from a
12 security perspective. And I understand, from the
13 safety perspective, as long as some security thing
14 that I know about when I'm licensing this system,
15 which only goes up through prior to installation, some
16 security protection does not interfere with safety, I
17 can make a licensing determination that in deed my
18 system is acceptable.

19 Now, somebody later comes in and says, oh,
20 I identified a vulnerability that I need an additional
21 protection. I have to install that and, in a safety
22 licensing space, that is now left up to the inspection
23 process.

24 That's not part of the licensing process
25 is my understanding of what I heard this morning. My

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 question is why, why don't we, why doesn't the
2 guidance require this integrated assessment from Day
3 One?

4 DR. SHINN: And if I understood your
5 question correctly, sir, from whom did you want the
6 integrated assessment?

7 MEMBER STETKAR: With that's --

8 DR. SHINN: It does require it from the
9 licensee. There is an integrated assessment that the
10 licensee does.

11 MEMBER STETKAR: Well, when I say
12 integrated assessment, I mean that decision that if I
13 have specific encryption set of software to satisfy a
14 security issue, if that doesn't affect a safety
15 function then, okay, I can make a determination that
16 in deed I can license this system, that it's safe. On
17 the other hand, if there's a vulnerability that
18 doesn't necessarily affect safety, that I should know
19 about on Day One, I'm not, I don't want to use the
20 term required because Reg Guides don't require
21 anything.

22 But the guidance doesn't tell me to go
23 look for those things. I later identify them and
24 figure out some way to deal with them later, post-
25 design.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 DR. SHINN: The, actually --

2 CHAIRMAN BROWN: To identify them, but it
3 doesn't require them to identify them during the
4 design phase.

5 MEMBER STETKAR: During the, that's right.

6 MR. LEE: Actually this slide kind of
7 discussed that, sir. The licensees have committed to
8 be cognizant of evolving threats and vulnerabilities.

9 And cognizant of our latest protective
10 strategies to address that. Meaning that the, not
11 only the 148 security controls. You know, when they
12 first establish their program, they need to
13 continuously track that.

14 Meaning that whenever they find something
15 or apply to that particular system they have or apply
16 to their nuclear power plant, and they need to look at
17 it and say, does this apply to me or not? And if it
18 is, then what is the solution for resolving that
19 particular vulnerability?

20 Then you keep that and put it someplace,
21 or put it in a database. Then when you acquire new
22 system, go to the previous slide.

23 That when you provide, try to obtain new
24 system, see those, I guess, red dots under the box of
25 the, right-hand side? Those are the vulnerabilities

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 they captured since they have established their
2 programs.

3 And after, I mean this design process
4 could take years. So while they're doing, developing
5 this process, if they don't capture it and if right
6 before they turn the system on, they'll also going to
7 perform the vulnerability assessment and to make sure
8 that they capture everything.

9 So, that's where they capture it. So they
10 capture it a number of different ways, and that is why
11 I said, that unlike the Reg Guide 1.152, 5.71 is
12 continuous.

13 MEMBER STETKAR: I understand that and in
14 some sense my concern is more focused on the 1.152
15 part of this, is if by doing that process, they
16 identify a new vulnerability, just before they flip
17 the switch.

18 And say, oh, I need to install a security
19 protection to address that security vulnerability. If
20 that security protection now introduces a potential
21 conflict with the safety function of that system, that
22 system is already licensed at that time.

23 MR. JACKSON: This is Terry Jackson. I
24 understand, I think I understand your question. That
25 if they identify a new vulnerability, after a system

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 is designed and installed, let's say, and then they
2 need to make a modification to the safety system
3 itself.

4 And the system is already licensed, how is
5 that taken care of. And really it's taken care of the
6 same way as if they wanted to make a modification
7 irrelevant, if it were secured, involved in security
8 vulnerability.

9 It would be under the 5059 process.

10 MEMBER STETKAR: I understand that. I'm
11 just questioning whether or not the guidance should be
12 written that way.

13 Well, let's, we've had this, we need to
14 keep going on, Charlie, I think --

15 CHAIRMAN BROWN: I'd like to make a very
16 clear cut example. I mean the way I, and we're going
17 to rehash a little bit at this point.

18 There's 148 security controls based on
19 some threat of vulnerabilities. If I, when I looked
20 at this initially, and before I heard all the
21 discussion today, I would have said nobody has to even
22 look at those, until the license got to them. That's
23 my opinion, okay, based on the way, I may have misread
24 it, but the licencing goes on and you all look at it
25 from a safety standpoint meeting the requirements,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 from a safety viewpoint.

2 It's handed over. The system is designed,
3 it's licensed and now you start the cyber security
4 program. And that's when you go look and you say,
5 okay.

6 Now people walk in and they look at it
7 from the 148 security controls, to see those have been
8 adequately addressed or assessed or whatever.

9 Now that's not necessarily what I've heard
10 today. At least from the Luminant guy who says, no,
11 we're going to do this up front and the Progress
12 Energy Representative said, I'm not quite sure.

13 He obviously didn't, I'm not going to put
14 words in his mouth, but it was a different perception
15 as to how far you went one way, in one phase, as to
16 how far you went in the other phase.

17 So, instead of looking at a new one, I'm
18 just trying, I was trying to look back at the initial
19 ones and how did they get captured early, and it was,
20 in my reading of the thing was that, no, you start
21 this phase after the stuff is finished and you've got
22 licensing done.

23 And you don't even have to look at these
24 before then. Other than from whatever is encompassed
25 in those with your normal safety.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. ERLANGER: And I think some of these
2 are licensee decisions, because at the end of the day,
3 we're always going to have new requirements, new
4 regulations. And in the totality, the licensees and
5 applicants need to meet those regulations.

6 My observation of what I heard from
7 Luminant, as well as Progress, was that they need to
8 think through their business plan, their strategy on
9 one level, how they're going to do this.

10 And obviously it behooves them to start
11 thinking about this early in the process. But the
12 reality of the program approach that is if they do get
13 that far down the road, you know, taking the operating
14 fleet example, is the application of security controls
15 can occur.

16 And some things will be considered, some
17 things, you know, Mr. Hecht's point, you know it might
18 apply, it might not apply. But you're going to go
19 through the process to consider all these things.

20 CHAIRMAN BROWN: Yes, and I'm not going to
21 beat this horse anymore right now, other than I think
22 it's almost, if the licensees have not addressed all
23 of these 148 vulnerabilities, during their design,
24 building up to their final licensing, if they haven't
25 done that, that's their problem.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 Because it's going to be very difficult
2 afterwards for them. And I'm not trying to dictate
3 anything, that's, I just share the concern that all of
4 a sudden things are, they get very, very difficult at
5 the 11th hour and 59th minute and there's no clue.

6 There's nothing that urges them or there's
7 nothing in the Reg Guide that says these really need
8 to be considered throughout the design process leading
9 up to the licensing and giving licensing basis.

10 They're left just, they're two separate
11 phases.

12 MR. ERLANGER: And what I can tell you,
13 sir, because obviously this is a new requirement and
14 we've been living it from Day One, is we are seeing
15 the vendors and the applicants working together from
16 the staff.

17 I can say that comfortably and confident
18 and Westinghouse is here today. They are very
19 involved from Day One, knowing what, and again you go
20 back to that business model, that business decision.

21 They want to sell a product that a
22 licensee or an applicant can use. So everyone is
23 paying attention. But what we go back to, what is the
24 requirement, what is our guidance based on, tying
25 everything to the requirement.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 Where, you did make the point it's the
2 licensee, I won't say the licensee's problem, but it's
3 their, you know something they need to consider. But
4 they are working, you know, what we are observing, at
5 least, as the Regulator, is we are seeing licensees
6 and applicants, excuse me, applicants and vendors
7 communicating on these issues.

8 So, they are considering, you know, the
9 requirement, there's, I think what the experts and Dr.
10 Shinn and Mr. Simonds can speak to, is there are
11 things that should be considered in the design, but
12 the totality of the program is very much, in our
13 opinion, well placed as an operational program.

14 So we're trying to balance what can be
15 done on the front end, to where the preponderance of
16 the program rests. And it is challenge, and I think
17 we heard throughout the day, the threat keeps
18 changing.

19 CHAIRMAN BROWN: I understand the threat
20 changing aspect, you can never avoid that. That's,
21 I'm not, I'm not, there's no certainty that you've
22 caught everything.

23 It's just, I'm going to stop right here on
24 this particular subject.

25 MR. LEE: Chairman Brown, actually

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 Sections C-12.4, actually the whole section requires
2 licensees and the licensees have committed to work
3 with their vendors from the very beginning.

4 What they have required, committed to do
5 is that they are going to develop a Policies and
6 Procedures about how they're going to purchase these
7 equipment.

8 So, from the very beginning, they're going
9 to establish the process for testing these equipment.

10 And throughout the whole process, it discusses how
11 they need to get involved and the kind of requirements
12 that they are going to impose on their Developers.

13 DR. SHINN: Yes, specifically, sir, I
14 bring to you attention C-12.4, which is what you were
15 talking about.

16 CHAIRMAN BROWN: C-12.4.

17 DR. SHINN: C-12.4, integration of
18 security capabilities. Because we recognize that.

19 CHAIRMAN BROWN: Is that Appendix C?

20 DR. SHINN: Yes, sir. Sorry, there's a
21 body C and there's Appendix C.

22 CHAIRMAN BROWN: Somebody said --

23 DR. SHINN: 12.4, yes, sir. And so that
24 talks about the new acquisitions and building security
25 into these systems.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 CHAIRMAN BROWN: What C again? Management
2 control?

3 DR. SHINN: Yes, sir.

4 MR. LEE: Actually the whole Chapter is C-
5 12.

6 DR. SHINN: There are more in Section 12
7 that I wanted --

8 MR. LEE: Whole Section 12, covers the
9 purchasing, acquiring of products and --

10 CHAIRMAN BROWN: C-12.4?

11 DR. SHINN: Yes, sir.

12 CHAIRMAN BROWN: Integration and security
13 capabilities?

14 DR. SHINN: Yes, sir.

15 CHAIRMAN BROWN: Yes.

16 DR. SHINN: So that talks about what we
17 were just discussing here, the value of, there is
18 value in building security in. It's a nice to have,
19 but not a must have thing, from a security
20 perspective.

21 As long as those vulnerabilities are
22 addressed, we solve the security problem. But you're
23 correct, there is value in doing these things earlier.

24 It certainly makes it easier to address the problem
25 later on, but it may present other problems.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 You may not be able to build security into
2 something, it may complicate it, and may be better to
3 address the security external to that device, as
4 opposed to building it into that device.

5 CHAIRMAN BROWN: I agree with both of
6 those thoughts. All right, let's go ahead and get on.
7 John, did you want anymore?

8 MEMBER STETKAR: No.

9 MR. LEE: Slide 7. In the interest of
10 time, I'll just make quick points on these slides.
11 The point here I'm trying to make is that they, not
12 all 148 security controls can be translated into
13 security features or the functional capability within
14 the systems.

15 Usually those secure controls associated
16 with technical nature, technical security controls are
17 those security controls that does not require human to
18 activate, and those are the type of a secured control
19 that could translate into security features or the
20 functional capability within the system. Next slide.

21 So, actually, another point that I would
22 like make from there is that the, that means that only
23 like one-third out of 148 security controls, only
24 about one-third technical security controls and two-
25 thirds are managerial in nature.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 That means that the other two-thirds of
2 the security controls can be addressed, cannot be
3 addressed in the product or through the features or
4 function or capability within the system. Next slide.

5 The main objective of the implementation
6 phase are to ensure that the system developer employs
7 software quality assurance method or the program to
8 ensure that developed security features or
9 capabilities within the systems are correct, accurate
10 and complete and they will implement security,
11 implement security or mitigate any tampering of the
12 developed system.

13 And security requirement inherent in the
14 Reg Guide 5.71, states that specifically, I think
15 that's coming out of C-12. States that the licensees
16 and applicants are, applicants require their system
17 developer to implement protective measures to ensure
18 that the integrity of the system being developed is
19 protected until that delivered to the site.

20 And this also includes just what Jay Amin
21 and Matt Gibson have stated, that the, requiring their
22 offenders to implement security control data similar
23 to that provided in Reg Guide 5.71.

24 CHAIRMAN BROWN: That's the SDOE concept.

25 MR. LEE: Yes, sir. Additionally, in

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 Section 12, requires licensees and applicant to
2 require their system developer to employ software
3 quality and validation method to minimize flow or
4 malformation of software.

5 That means that the licensees and
6 applicants have committed in the cyber security plan,
7 that they will require their system developer to
8 employ software quality assurance methods or programs
9 to ensure that developed security features or
10 capabilities in the systems are correct, accurate and
11 complete.

12 DR. HECHT: But this wouldn't necessarily
13 help if you have a Linux-based, I don't know,
14 database, a plant management system for collecting
15 parameters, for example, at Level 2?

16 I mean if you have a lot of large scale
17 COTS software, your SQA process for example, isn't
18 going to give you terribly much inside into those very
19 large, you know, something built on Linux, my sequel
20 and PHP.

21 DR. SHINN: That's a great question, sir,
22 Because that's actually sort of the beauty of the
23 process. We recognize that there are going to be
24 controls, but you can't be, you can't implement,
25 because of what you just said.

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 that demonstrates you have a
2 vulnerability now. You've got a system that's in a
3 state that's essentially unknown. So you're going to
4 have to implement other things to compensate for that.

5 Because that is, in fact, the case. A lot
6 of commercial software out there, you're not going to
7 be able to get into the weeds and look at the source
8 code for, you know, let's say Oracle for example or
9 Microsoft operating system or, well, Linux, because
10 you can look at the source code if you wanted to.

11 But you probably wouldn't, right? So we
12 recognize that. I mean there are definitely
13 challenges with this. Certainly the more complex a
14 system gets, it becomes more difficult to analyze
15 that.

16 And there are going to be cases where that
17 can't occur, and you're going to have compensate for
18 that via other means. It's just the nature of cyber
19 security.

20 There's not anything you can do about that
21 other than compensate for it.

22 DR. HECHT: So what you're saying is that,
23 in these cases, I guess these are in Section C-12?

24 DR. SHINN: Yes, sir.

25 DR. HECHT: Those, those, what you're

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 going to be saying is that your, there's something
2 else in the technical controls that you're going to be
3 doing basically to put that suspect item, to contain
4 it some how or other.

5 DR. SHINN: You may have. I can give you
6 a simple technical example. Let's say we had a piece
7 of software that took an input and we didn't know what
8 the pedigree of that software was.

9 We didn't know how robust it was and
10 whether or not it had a buffer overflow or something
11 in it. So we could put some sort of input validation
12 control in place, same as a web application.

13 So we could put a web application firewall
14 in front of it, specifically defined, we allowed input
15 to that device and we could take credit for that. We
16 could say, I know, that this thing can only accept
17 this input, which I know isn't going to overrun a
18 potential buffer overrun that that could have.

19 And I accept the fact that that thing may
20 have a buffer overrun and say I lack the means
21 dynamically or whatever to test for that.

22 And I could address that vulnerability in
23 that way. And that's why we built the program this
24 way. COTS is a particular reason why we had to do it
25 this 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 Because we know there's going to be cases
2 of technology where the pedigree is largely an
3 unknown. Does that answer your question, sir?

4 CHAIRMAN BROWN: Go on.

5 MR. LEE: Design, implementation and test
6 phases. The main objective of test phase are to
7 verify that security features and capabilities,
8 incorporated into the developed systems are
9 functioning as required and does not cause more
10 vulnerability into the system or do not adversely
11 impact the level of operation of safety functions.

12 CHAIRMAN BROWN: Are you going to hire some
13 hackers? Smart hackers?

14 (Laughter.)

15 (Asides.)

16 CHAIRMAN BROWN: That's just a thought
17 process. I'm curious as to how you test these
18 security features, if you don't have somebody
19 challenging you that's good at it.

20 DR. SHINN: Yes, that certainly is one
21 way. There are actually packaged tools that actually
22 automate a lot of this stuff now.

23 CHAIRMAN BROWN: Yes, I know, but packaged
24 tools can be known --

25 DR. SHINN: Certainly.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 CHAIRMAN BROWN: -- by the guys who want
2 to circumvent the systems.

3 DR. SHINN: Certainly.

4 CHAIRMAN BROWN: And so they take the
5 tool, they learn it and they figure out a way around
6 it.

7 DR. SHINN: Certainly.

8 CHAIRMAN BROWN: So that doesn't give me
9 any warm feeling at all, on the packaged tools.
10 Although, you grab a guy that does one of these whiz
11 bang games, who can get into the Defense Department.
12 That's the guy you want to go test this stuff.

13 DR. SHINN: It's certainly our expectation
14 that the individuals doing that testing at the sites,
15 have the requisite expertise to arrive at those
16 conclusions.

17 CHAIRMAN BROWN: Do you all validate that?

18 DR. SHINN: That is an inspectible item,
19 we will look at that. That is part of their
20 commitment in the cyber security plan, as well, the
21 make up of the cyber security Team.

22 CHAIRMAN BROWN: Okay, all right. I was
23 not really being facetious when I brought up the
24 point. Because that is a --

25 DR. HECHT: And Charlie, be aware that

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 that would only work for the technical controls.

2 CHAIRMAN BROWN: I understand that.

3 DR. HECHT: So if people are sharing
4 passwords or --

5 CHAIRMAN BROWN: I totally agree. You are
6 absolutely right. Or they make copies of keys.

7 MR. COSTELLO: Chairman Brown, I think
8 I'll be able to address that thought when we talk
9 about inspections.

10 CHAIRMAN BROWN: Okay, thank you.

11 MR. LEE: Other than saying that the Reg
12 Guide 5.71, covers these aspects, not much to say
13 here. Actually, what it says is that the, it requires
14 applicants and the licensees to require their system
15 developer to create, implement, document a security
16 testing evaluation plan to ensure that the acquired
17 product or developed system meets all the specified
18 security requirements.

19 This includes making sure that it doesn't
20 have, you know, cause more vulnerabilities, and make
21 sure that, make sure that the system perform as,
22 doesn't adversely impact the level of operation of the
23 system.

24 And this is also where Reg Guide 5.71,
25 provides a list, a laundry list of testing, to 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 they test for all the known vulnerabilities and
2 things of that nature.

3 And we have a pretty lengthy list of --

4 DR. SHINN: Appendix C-12.5, has the list.

5 MR. LEE: I think that's where they
6 address--

7 DR. SHINN: Buffer overflows.

8 MR. LEE: And the ultra static and dynamic
9 --

10 DR. SHINN: Analysis.

11 MR. LEE: -- analysis. The main objective
12 of the installation, checkout and acceptance test
13 phase are to verify and validate the correctness of
14 security features and capabilities incorporated into
15 the systems in the target environment.

16 Here licensees and applicants are required
17 and are committed to and verified and validate the
18 results of the vendor, the test at the factory.

19 And also they're going to test to ensure
20 that the security features and functional capabilities
21 are incorporated properly.

22 And they're going to test to make sure
23 that they are operated as intended and producing
24 desired outcome of eliminating all the known
25 vulnerabilities.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 And at this phase, they're also required
2 to perform the effective analysis, and at this stage
3 they're also required to perform a vulnerability
4 analysis to make sure that they cover, your systems
5 are going to -- put it in the nuclear power plant,
6 address all the vulnerabilities currently known. Next
7 slide.

8 (Asides.)

9 DR. HECHT: While we're waiting, you said
10 that Reg Guide 5.71, has an extensive list of test
11 requirements. Where are they?

12 DR. SHINN: C-12.5, Appendix C. That's the
13 Developers security testing controls. And that is a
14 list of different types of code vulnerabilities that
15 we're interested in.

16 CHAIRMAN BROWN: I don't recognize this
17 one. No, what happened to Slide 11, modified.

18 DR. SHINN: We're going to do that one,
19 once we get through this, sir.

20 CHAIRMAN BROWN: All right, that's fine.

21 DR. SHINN: It's on his computer, if
22 that's okay with you.

23 CHAIRMAN BROWN: I'm sorry, go ahead.

24 MR. LEE: The main objective of the
25 operation and maintenance phase is to maintain the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 established security system until they are retired.
2 And basically, under Reg Guide, under Revision 2, Reg
3 Guide 1.152, licensee may provide their commitment to
4 follow guidance provided in Revision 2, and the cyber
5 security guidance provided in Revision 2, is a high
6 level framework for the operational and maintenance
7 phase.

8 But under the cyber security requirement,
9 inherent in Reg Guide 5.71, licensees already have
10 committed them in their cyber security plan.

11 And currently we are reviewing that. And
12 basically, a couple of pages worth of guidance
13 provided in Reg Guide 1.152, is about 105 pages, but
14 that spells out into about 90 pages of detailed
15 criteria provided in Reg Guide 5.71. Next.

16 CHAIRMAN BROWN: How many pages in 5.71?

17 MR. LEE: I think it's 105, but I think.

18 CHAIRMAN BROWN: That's including all the
19 Appendices?

20 MR. LEE: Right, about 90 pages or so is -
21 -

22 CHAIRMAN BROWN: Yes, yes, I was focusing
23 on main text, I apologize for that interruption, go
24 ahead.

25 MR. LEE: Retirement phase is the, another

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 example of how life cycle phase is covered by security
2 activities and measures provided in Reg Guide 5.71.

3 Specifically, the retirement phase is
4 covered by cyber security requirement inherent in the
5 media control, configuration management and security
6 impact analysis section of Reg Guide 5.71.

7 Under these sections, licensees and
8 applicants are required to provide adequate
9 documentation to verify that these important
10 activities are carried out to ensure information is
11 properly disposed by using method that would preclude
12 reconstruction by means available to the DBT
13 adversaries and changes to a system or component
14 authorized beforehand and the disposal of a system or
15 component will not adversely impact the effectiveness
16 of established security.

17 In conclusion, as I have explained,
18 although the Reg Guide 5.71, is not organized or
19 outlined according to the life cycle phase in the same
20 way as Reg Guide 1.152, Reg Guide 5.71, does provide
21 full system security life cycle and comprehensive
22 requirements for each security life cycle phase.

23 And life cycle phases are provided as
24 cyber security measures and activities that licensees
25 have committed to perform, as an element of their

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 cyber security programs.

2 Also, another important point I would like
3 to make is that guidance provided in Revision 2 of Reg
4 Guide 1.152, is that guidance. But because licensees
5 have a committed to follow guidance provided in Reg
6 Guide 5.71, guidance provided in Reg Guide 5.71, are
7 requirements.

8 And also Reg Guide 1.152 guidance is a
9 high level framework, but the Reg Guide 5.71, provides
10 detail, provides all the elements making that
11 framework and the guidance requirements for each of
12 these elements. And that concludes.

13 CHAIRMAN BROWN: That's the first time
14 I've heard a Reg Guide turned into requirements.

15 DR. HECHT: It's because the plant is
16 incorporated into the license basis.

17 MR. LEE: Because the license --

18 CHAIRMAN BROWN: Okay.

19 MEMBER STETKAR: If the licensee commits
20 to it it's not a requirement.

21 CHAIRMAN BROWN: I've got it, thank you.

22 DR. HECHT: If they don't, they don't get
23 a license.

24 CHAIRMAN BROWN: I got that. I like the
25 thought process.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 (Asides.)

2 MR. ERLANGER: In the interest of time,
3 Michael you can speak to the elements on the side,
4 right, and we can obviously --

5 CHAIRMAN BROWN: We've got the slides.

6 DR. SHINN: We can bring it up if you want
7 to.

8 Go ahead, Eric.

9 MR. LEE: One of the items that ACRS
10 expressed interest in discussing today, revolved
11 around Vogtle cyber security plan concerning the
12 location of technical support centers.

13 The plant space that the technical support
14 center will be located at the lower level of the
15 applicant's defensive architecture. And this raised
16 some concern of whether there is high assurance that
17 technical support center adequately protected from
18 Cyber attack.

19 I think we discussed this point earlier by
20 Mr. Erlanger and during the Q and A Session. What we
21 said earlier was that it does not really matter where
22 the system is located.

23 Because the approach that we took was that
24 once a system is identified as a critical system or
25 those systems within the scope of the rule, they must

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 address all the known vulnerabilities.

2 Because, as I have explained earlier, at
3 the beginning of my presentation, DBT Adversary will
4 actively search for weaknesses and vulnerabilities.

5 So, if there's a known vulnerability then we need to
6 address them to provide higher assurance. So, whether
7 it's at the high level or low level, it does not
8 really matter.

9 Because you have to address all the
10 vulnerabilities and therefore, one thing I'd like to
11 say is that the level does not really dictate the
12 level of security that you're going to apply to a
13 system.

14 CHAIRMAN BROWN: Well, with that thought
15 in mind that means why bother putting the other ones
16 in a higher level, because they have to meet the same
17 148 things, so who cares about the two high levels,
18 just stick them all up in here, where I've got fewer
19 definitive levels to have to deal with.

20 DR. SHINN: Great question.

21 CHAIRMAN BROWN: You can answer the
22 question, I'm just hypothetically making that point
23 that --

24 MR. ERLANGER: And I'm actually going to
25 phrase the question slightly different. When I

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 reread, I just reread the Reg Guide to prep for this
2 meeting, like a lot of us did to make it was fresh in
3 our mind.

4 What I'm thinking of is the dialogue on
5 the defensive architecture. What we tried to do with
6 mapping it to physical locations, logical
7 communication pathways.

8 So it might be helpful on a very high
9 level if you speak through why we put certain, we'll
10 say safety significant, imported systems with one-way
11 communications flows by systems.

12 Or if it screens in using TSC, because
13 actually the applicant tipped a hand saying that,
14 going through their criteria, that was a system that
15 made it as a, whether a critical system or a digital
16 asset, they presented that.

17 So what some did a little bit to
18 generalize what their logic was, I can tell you right
19 away they had to talk to Wiz (phonetic).

20 Where they put them in their architecture
21 in that lower level, was they recognized they'd be
22 getting information from the control room. They would
23 also need to push information out to external bodies.

24 CHAIRMAN BROWN: Well, you can always push
25 it out, one way. You don't have to accept it back

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 from the external bodies, it doesn't have to be
2 bidirectional.

3 So that thing could be in a higher level
4 and still be receiving from the main control room and
5 pushing out to the other levels.

6 MR. ERLANGER: So what I think would be
7 helpful, if you can just talk through on a high level
8 what the architecture looks like and what's some of
9 the decision processes about where you should think
10 about putting a system or an asset.

11 CHAIRMAN BROWN: And one the Luminant
12 today made it very clear that they thought about it in
13 this way, like a high level manner and yet when we
14 listened in on the licensing, the new design, the new
15 reactor designs and that one in the applicant's COL
16 did not look at it that way.

17 DR. SHINN: I think it's important, sir,
18 to recognize what Eric brought up earlier, which was
19 that the defensive architecture level is not a level
20 of security.

21 All CDAs have to be protected equally.
22 The architectures are very different. We use, between
23 the two licensees, because I've seen both of their
24 architecture, the nomenclatures are the same, but the
25 architectures are actually very different between

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 them.

2 CHAIRMAN BROWN: You're talking about the
3 two new?

4 DR. SHINN: Yes, the AP1000 and Luminant's
5 Comanche Peak architecture. They're actually very
6 different. They use the same words but they actually
7 mean very different things.

8 At Jay Amin's plant, well since he
9 mentioned it. Sorry, go ahead, Bill.

10 MR. GROSS: We need to be off the record
11 if we're going to talk about --

12 DR. SHINN: That's true.

13 MR. GROSS: -- existing --

14 DR. SHINN: The architectures, they use
15 the same words, but they are very different things.
16 So when they say level blah, that means something
17 different in the AP1000 design.

18 So even though they use the same words,
19 their architectures are very, very different. So you
20 can't, you can't compare them. I would have to get
21 proprietary to be specific.

22 CHAIRMAN BROWN: Well, we asked them, we
23 tried to get clarification on that relevant to 5.71,
24 but, because I actually had the picture with me and
25 said what do you mean?

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 they were very clear, as to what they
2 meant. So, I don't know if that meant what they other
3 guy said or not, and I don't want to get into that
4 discussion.

5 The point being is if somebody recommended
6 putting the critical reactor safety systems at a
7 higher level, I think they'd have an adverse response.

8 MR. SIMONDS: But, Mike, correct me if I'm
9 wrong. One of the benefits of utilizing the
10 architecture as it exists in 5.71, and granted we have
11 to apply the controls to every CDA equally, which
12 means equal protection regardless of where it sits in
13 that architecture.

14 One of the benefits of it, of having the
15 higher levels, Level 4 and Level 3, has to, and not to
16 get into a technical discussion but time back to
17 inheritance.

18 Being able to take advantage for the
19 controls, the environments, the protections that are
20 inherent to those areas, those environments.

21 And so whenever these, some of these CDAs
22 can basically, in terms of satisfying this body of
23 requirements that we have for each CDA itself, many of
24 those may be already satisfied by virtue of --

25 CHAIRMAN BROWN: I understand, exactly

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 right. I understand that it makes it easier, and I'm,
2 when you're talking about communications though, where
3 you're going to have to be making decisions on a, in a
4 TFC and/or an EOF type, I don't want to say decisions
5 but consulting, in some circumstance.

6 It would be nice to know that you have not
7 got corrupted, mildly different information where one
8 guy could be providing you consulting advice based on
9 altered data due to some embedded, I don't want to
10 call it a worm, or something similar to whatever it
11 was that hit the Stuxnet thing. And guys are
12 sophisticated these days.

13 DR. SHINN: And we have controls in there
14 for just what you were talking about. You know, we
15 have transmission integrity controls in there, for
16 example, that specifically deal with the scenario that
17 we're talking about.

18 Because we've, we recognize that, you
19 know, in a modern, digital environment that they're
20 even in an area where we might have something behind a
21 data diode, for example, that there are going to be
22 things talking to each other.

23 And we recognize that a threat can be
24 introduced into that environment. So we expect there
25 to be some way to protect the integrity of that, as

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 well.

2 That applies across all of the CDAs, so I
3 don't want you to get a false sense of security that
4 just because it's behind a diode that essentially
5 these issues go away.

6 You know, we still have to address them up
7 here. And just because it's down here, it doesn't
8 mean that it's unnecessarily exposed in a way that
9 this asset isn't.

10 MR. SIMONDS: And at the same time may
11 there not be, especially in the case of an applicant
12 or a licensee, a false expectation that because, you
13 know, a TSC, let's say, or what have you can be
14 located in the lower level of the architecture.

15 And by virtue of the fact that has fewer
16 protections that they might enjoy at a higher level,
17 that doesn't negate the requirement for them to walk
18 through the 148 control baseline, plus whatever other
19 controls are out there. And they addressed those as
20 well.

21 DR. SHINN: Which includes boundary
22 controls. I want to make sure that's important. That
23 when you're analyzing a CDA, you still have to address
24 that boundary control.

25 How am I going to prevent bad guys from

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 getting to this particular CDA.

2 DR. HECHT: Can I just make the
3 observation though that what it really comes down to,
4 is that although you have to look at all 148 controls,
5 you in fact would apply them differently at different
6 layers, I mean you've said that.

7 DR. SHINN: Potentially. I can't say that
8 for sure, but potentially.

9 DR. HECHT: You've said it. Because when
10 you're talking --

11 DR. SHINN: Well, if I said it, then we
12 didn't, that's, we can't speculate on how they're
13 going to apply. Potentially.

14 DR. HECHT: We were talking before about
15 the COTS database for the plant historian data. And
16 that was a situation where we can't get into the code
17 and be sure that there's no badness there.

18 And that badness could be exactly what we
19 were talking about, where what's in the database isn't
20 necessarily what's out.

21 So, in fact, that flexibility that was
22 also mentioned, the word flexibility in terms of
23 applying these controls, does differ by security layer
24 and differs by apparently other characteristics.

25 I just want to make the point that even

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 though you say, you have to apply the filter, if you
2 will, or the sieve, where the methodology equally to
3 all CDAs, you don't necessarily get the same outcome.

4 DR. SHINN: I think I would professionally
5 disagree with that.

6 MR. GROSS: To try to boil it down into a
7 nutshell --

8 COURT REPORTER: Mention your name,
9 please.

10 MR. GROSS: Hi, this is Bill Gross from
11 Nuclear Energy Institute. We don't protect every CDA
12 the same way, but they all receive the equivalent
13 level of protection.

14 Every CDA must be protected with high
15 assurance of adequate protection that it can withstand
16 a Cyber attack and perform its design function.

17 DR. HECHT: Well, aren't you really saying
18 that if you're going to apply containment, rather than
19 doing something internally to a component, I don't see
20 that as being equivalent.

21 I see that as being a substitute, but I
22 would always prefer to have a white box than a black
23 box, when I'm worried about assuring that component.

24 MR. GROSS: Well, there's a difference
25 between what you can get and what you have to do. 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 we can't rebuild the plants. We've got to protect
2 what we've got.

3 DR. HECHT: I think we're in violent
4 agreement in that case. That the outcomes are going
5 to be different, and you can say that the containment
6 is an equivalent level of assurance or safety or
7 security, but we don't really know.

8 MR. GROSS: I think you can test it. And
9 there are cases to ensure, to be able to ensure that
10 we have that, have met the high assurance requirement.

11 So if we have to use a comp measure because we can't
12 build it in, then we test the comp measure to make
13 sure we've at least mitigated the same threat factor
14 that the security control addresses.

15 And that's the essence. If you can't
16 build it in, we test and make sure that we've
17 adequately mitigated the threat.

18 MR. LEE: And then another item that I'd
19 like to mention is that the, as we have mentioned
20 earlier, not only the 148 security controls, but all
21 the other vulnerabilities that applicable to that
22 particular CDA or system.

23 So if system is exposed to much larger, a
24 group of threat factors that it may be, then they have
25 more security controls. Because they have to address

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 all the known vulnerabilities.

2 CHAIRMAN BROWN: Well, that's if they get
3 known.

4 MR. LEE: Yes.

5 CHAIRMAN BROWN: Right now you've only got
6 148.

7 DR. HECHT: What you're saying is, for
8 example, level, Zone 2 contain, what is it, Level 2
9 area Because it has both input and output, might be
10 subject to more controls than a Level 4, because it
11 has only output?

12 MR. LEE: Could be because if they, when
13 they performed the --

14 DR. SHINN: Hang on, let me just make sure
15 I'm clear. Remember, if I understood you correctly,
16 you still have to address them all. But you may not
17 have to apply them all, because that vector may not
18 exist.

19 As to whether or not that vector wouldn't
20 exist at 2 or 4, couldn't say it at this point.

21 CHAIRMAN BROWN: Okay, let's go on, Mr.
22 Costello.

23 MR. COSTELLO: Thank you for inviting me
24 to speak. And the rest of the Committee also.

25 DR. SHINN: Do you have slides, Ralph?

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MR. COSTELLO: I think I do.

2 (Asides.)

3 MR. COSTELLO: As Eric mentioned, my name
4 is Ralph Costello, I'm with the Office of Nuclear
5 security Instant Response, Division of security
6 Operations. And I will be providing a very concise
7 presentation on the early stages of our inspection
8 oversight program development, and then also give you
9 an overview of the NRC's Cyber Assessment Team. Next
10 slide, please.

11 As I mentioned, with the very early stages
12 of developing an inspection procedure, temporary
13 instructions inspection procedure, we've identified
14 internal stakeholders to participate and help us in
15 that effort. And we intend to work with external
16 stakeholders in industry and some of our federal
17 partners to make sure we develop a good product.

18 We've very recently worked on and
19 developed an Inspection Training Course and we held a
20 pilot course relative that.

21 We will be, during this coming year, 2011,
22 developing a significance determination process
23 relative to the Reactor Oversight Process.

24 CHAIRMAN BROWN: Is this just for Cyber?

25 MR. COSTELLO: Yes, sir.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 CHAIRMAN BROWN: And this is for --

2 MR. COSTELLO: cyber security relative to
3 73.54.

4 CHAIRMAN BROWN: And Inspectors at the
5 sites?

6 MR. COSTELLO: Regional Inspectors.

7 CHAIRMAN BROWN: Regional Inspectors.

8 MR. COSTELLO: And I'm going to go into
9 your concern that you mentioned a couple of times and
10 I think it's a very, very astute comment you made.

11 I'm going to go down my laundry list here
12 and then go back to your comment.

13 CHAIRMAN BROWN: Oh, no, that's fine. I
14 just wanted to make sure I knew --

15 MR. COSTELLO: Because I think it was a
16 very good one. We intend to, prior to inspections,
17 conduct pilot inspections to work the procedure and
18 make sure the process and protocols work efficient
19 for us, and industry.

20 We plan on doing workshops. And I caveat
21 this, we plan, providing we have the resources.
22 Again, in this day and age, when members of Congress
23 say we might be closing government, that's always an
24 option.

25 We're looking at our first inspection

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 based on one licensee's implementation schedule,
2 roughly late 2011. That's where we're at in
3 development.

4 Very early stages and we'd be more than
5 glad to provide this Committee an update at a later
6 date, if so desired. Chairman Brown had mentioned do
7 we have Inspectors in the Regions or in NRC anywhere,
8 that have the technical skill set needed.

9 I don't think there's many folks in the
10 whole United States that have the skill sets we really
11 need for cyber security. So our approach is a team
12 approach.

13 We're going to collect a group of very
14 intelligent, skilled people together and we're going
15 to get some of the hacker, cracker types like Dr.
16 Shinn here, and other Contractors, maybe from some
17 colleagues in Department of Energy Labs, who are in
18 fact Cyber warriors to assist our Inspectors.

19 They do it on a daily basis, both attack
20 and defend. So we'll understand a lot of these
21 concepts that I think Mr. Hecht was concerned about.

22 I think Chairman Brown was concerned that
23 we had the skill sets out there on inspections. I
24 don't want to belittle the fact that our NRC
25 Inspectors are extremely knowledgeable and they bring

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 another core group of skill sets that's going to
2 complement this team effort.

3 And we have folks in our Agency that are,
4 have PhDs in digital control systems and
5 instrumentation control. So we have some pretty
6 talented folks in NRC space and I'd just like to say,
7 I don't happen to be one, but knowing and working with
8 these folks for roughly the last ten years, NRC
9 Inspectors are very good at what they do in terms of
10 getting to the truth and I think their skill sets
11 combined with our Contractor's skill sets will answer
12 some of the concerns that Chairman Brown mentioned and
13 Mr. Hecht had addressed.

14 I'm going to move on to the next topic
15 real fast because I know it's been a long day and I
16 want to give the Committee the opportunity to ask some
17 questions, before the sun goes down. And that topic
18 is the Cyber Assessment Team. In April of 2009, the
19 Executive Director for Operations formed the NRC Cyber
20 Assessment Team.

21 And we took the team approach there as we
22 are doing in the inspections phase. We have
23 approximately 25 very talented individuals that bring
24 digital I&C, plant operations, materials operations,
25 IT network security, digital control systems,

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 security, forensics and many, many, many other skill
2 sets together.

3 And the tasks and the mission of the Cyber
4 Assessment Team is to evaluate any potential cyber
5 security issues. And then document those issues and
6 feed them into our operating experience program.

7 Which, through the course of the day, I
8 think we touched around that, but that feeds into
9 changes we would make in our inspection procedures,
10 data points from both operating experienced and threat
11 vectors that we learn about that's new.

12 And also changes that Mr. Erlanger
13 mentioned that are a learning organization, we're
14 constantly trying to approve our requirements. Which
15 would be in the form of the Reg Guide which, of
16 course, is a license condition.

17 So we're not just sitting on our 148
18 control laurels, we're constantly looking at the
19 things that are going on out there and the inspection
20 effort and the operating experience that we're getting
21 on a daily basis, as feeding into that.

22 The last requirement of the Cyber
23 Assessment Team is communicate, coordinate and provide
24 recommendations to management here, and that can work,
25 coordination and communication is between ourselves

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 and our licensees, and also with our federal partners,
2 in particular Department of Homeland security in
3 accordance with the National Cyber Instant Response
4 Plan.

5 And we have constant communications and
6 coordination with them. As a matter of fact, they in
7 turn work with our licensees on a regular basis on
8 various issues that come up.

9 Our licensees are getting daily data feeds
10 from U.S. CERT, which stands for the United States
11 Computer Emergency Response Team, and also the
12 industrial control systems computer emergency response
13 team.

14 And again, daily they're giving me data
15 feeds in terms threat, vulnerability analysis. And
16 we've confirmed with them through generic
17 communications and also interactions that every one of
18 them are getting these feeds and using these feeds.

19 These efforts, as I mentioned, feed our
20 operating experience program and that's an ongoing
21 effort that we continually loop back into our
22 inspection program and our overall regulatory
23 requirement program, relative to updating new
24 vulnerabilities or new issues that come about. That
25 concludes my short presentation.

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 CHAIRMAN BROWN: Okay, thanks. I
2 appreciate that, it's nice to see the planning going
3 in up front in terms of how these, what these folks
4 are going to have to be faced with.

5 And I understand the team concept and I
6 think most of the rest of us do also. I don't think
7 any of us expected any one guy to be able to handle
8 all of this.

9 So it's really got to be a team effort to
10 have all those various disciplines. Before we adjourn
11 here, are there any questions, John?

12 MEMBER STETKAR: Yes, let me just ask
13 Mike Shinn a question. Mike, the stuff that you
14 emphasized in Appendix C.12.4 of the Reg Guide 5.71,
15 got me thinking an awful lot.

16 And I want to understand, and if it takes
17 too long, you can just leave it. I think I see what
18 that section is telling me as an applicant or a
19 licensee that I need to do.

20 Except that it seems to say that for newly
21 acquired systems, I need to be aware of advancements
22 in protection strategies and protection controls,
23 above and beyond those that are enumerated in Appendix
24 B.

25 And make sure that I address those. It

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 doesn't seem to tell me that I need to be aware of
2 additional vulnerabilities in that newly acquired
3 system or am I not reading that correctly.

4 And that's sort of, eventually gets to the
5 crux of what I've been struggling with.

6 DR. SHINN: It's an excellent question,
7 sir, I mean it's sort of the nature of the beast the
8 way 5.71 is organized. It's not, it's not in that
9 linear format, if you will, that 1.152 is.

10 What I can tell you is that it's there in
11 a number of different places in the document.

12 MEMBER STETKAR: It is.

13 DR. SHINN: 12.4 talks about trying to
14 integrate the technical security controls in Appendix
15 B, into a product, and being cognizant of these new
16 threats and vulnerabilities.

17 We have a phrase in cyber security.
18 Security is a process not a state. The biggest
19 problem we have in Cyber is that when we build
20 security into stuff, it ends up essentially going out
21 of date.

22 So a more significant emphasis, if you'll
23 pardon the phrase, in the way that the document is
24 organized, is around that evolving threat issue.
25 Particularly because of the operating plants, we have

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 technology where we just can't go back.

2 MEMBER STETKAR: Sure, right, sure, I
3 understand that.

4 DR. SHINN: And, as Mr. Hecht said, we're
5 going to have cases where we just can't, we, everybody
6 in the world, can't really do anything about the
7 product, it's just built that way.

8 So, 12.4, is one of these sort of ideal
9 cases, if you will. It would be great if we could get
10 a product that had all the security we could need
11 built into it.

12 The practical matter is that, as Eric
13 mentioned before, two-thirds of the problems we have
14 to address, we can't do in the design of the product
15 anyway.

16 So the gist of the approach in 5.71,
17 philosophically is defensive in death to all of these
18 things. We certainly want them to try and make more
19 robust, more security products, but we recognize that
20 we can't always get that, as Bill Gross said, you
21 know, there's a difference between what we want and
22 what we can get.

23 So we definitely want to do all the things
24 that you said. We talk about that in a number of
25 different places. And in many cases, we may not be

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1 able to do anything about the product itself.

2 You know, there's a vulnerability and
3 we're going to have to address that via other means.
4 In practical terms, from my experience, most of the
5 security problems that we deal with, the emergent
6 ones, you have to deal with them outside of the
7 product.

8 MEMBER STETKAR: Sure, sure, yes.

9 DR. SHINN: That's just the nature of the
10 beast, yes.

11 MEMBER STETKAR: I certainly understand
12 that, the dynamic nature.

13 DR. SHINN: I hope I answered your
14 question.

15 MEMBER STETKAR: You've helped, thanks.

16 DR. SHINN: Okay, well if there's some
17 other place I can maybe point you to in the document,
18 I'd be delighted to do so.

19 MEMBER STETKAR: Well, you pointed me to
20 this place and it was a good place to be pointed to,
21 so that helped.

22 DR. SHINN: Yes, I would say in Appendix
23 A, if you look at the vulnerability assessment, I want
24 to say 4.1, I forget off the top of my head. That's
25 where we're talking about that ongoing process 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 reevaluating it.

2 It's also at the end of 12, I want to say
3 12.6 or is it 13.

4 MEMBER STETKAR: Again, that's more
5 philosophically --

6 DR. SHINN: That's right, 13.1, I
7 apologize. Because we have a real complex problem that
8 we have to address here. WE have a lot of challenges,
9 you know, even if we can't build security into the
10 product, we still have two-thirds of the problem that
11 we can't address in the products.

12 So we have to come at this from a lot of
13 difference angles to be able to provide adequate
14 protection. And certainly we want better products.

15 We asked for that. But we're also
16 cognizant of the fact that, in many cases, you're just
17 going to get whatever the vendor sells.

18 MEMBER STETKAR: Okay, thanks.

19 CHAIRMAN BROWN: Jack.

20 MEMBER SIEBER: No questions.

21 CHAIRMAN BROWN: I wanted to just make one
22 observation. We talked about the 148, got to cover
23 them all, it doesn't matter where you are, what you
24 are, whatever, you've got to cover them all.

25 But right up in the front of 5.71, in

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 Section 3.2, C-3.2, 3.2.1, you talk about defense and
2 depth protective strategies and security defensive
3 architecture.

4 And in there you're fairly clear when you
5 talk about by operating with, at a higher level,
6 you're actually putting yourself in a higher secure
7 environment.

8 And therefore, it says CDAs associated
9 with safety, important to safety, as well as supports,
10 as well as, I want to emphasize that, support systems
11 and equipment which, if compromised, could adversely
12 affect, impact safety important to safety and security
13 functions are allocated to Level 4, and are protected
14 from all lower levels.

15 And a similar, although slightly watered
16 down thought process applies to Level 3, as well, in
17 the next bullet.

18 So, to make it sound like it doesn't
19 matter where you are, because you have to do the 148,
20 I just, I don't think that's good advertising. That's
21 the only point I would like to make.

22 And if I was looking at those critical
23 systems, and I throw, personal opinion, this is not a
24 Committee opinion, this is just a personal opinion.

25 That the technical support center of all

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 the other stuff I see outside that boundary, when
2 you're doing a design certification or whatever, LAR,
3 whatever it is, and you're looking for, how are they
4 going to do it now that they're converting over to
5 digital type systems.

6 That's a critical support system. It's
7 not a command center, theoretically, different
8 argument. But it's a critical support system in terms
9 of other information that can be fed to the main
10 control room of technical details based on information
11 and data.

12 And yet it's potentially, it's made harder
13 to protect potentially, by putting it into the lower
14 security levels, than 3 and 4.

15 So that's just something, when I look at
16 it from a top level, intuitive, engineering protective
17 standpoint, that's the way I look at it. You're
18 probably going to have to address this question again,
19 I think in the full Committee meeting, so you probably
20 ought to figure out a way to explain this one in a
21 little more crisp, clear manner than it's a little
22 cleaner.

23 I'm just giving you that recommendation,
24 trying to smooth the road when you get to the full
25 Committee 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 Other than that, that was all I had. I
2 wanted to thank you all for being patient with my time
3 management, which, since we had it, this is, like you
4 say, this is an extremely complex, evolving area and
5 our understanding of the cyber security world is
6 evolving at the same time, although considerably
7 behind your all's understanding.

8 And so the purpose of allowing a little
9 bit more free flow discussion and interaction, I
10 wanted to do that to make sure we had as best a feel
11 we could, when we're then trying to communicate this
12 stuff to our fellow members and at least coming to an
13 understanding of how we think about it and what we
14 think is acceptable, from whatever standpoint you want
15 to look at it.

16 So, John or Jack, did you all want to
17 amplify my comment? If you want to disagree with me,
18 you can, that's also within our purview.

19 MEMBER SIEBER: I'll think about it.

20 CHAIRMAN BROWN: Other than that, I want
21 to thank you all. It was a very good set of
22 presentations today, I thought it was a very good set
23 of free back and forth discussions.

24 Very open, very candid, at which is the
25 only way to do it. And I very much appreciate the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 quality of the discussions and presentations. Okay,
2 with that -- oh, I now see that he's moved up.

3 MR. ARNDT: A couple of things, before the
4 Subcommittee, whatever the right terms is, dismisses.
5 We're scheduled for full Committee. Obviously the
6 staff's most important issue associated with that is a
7 discussion of 152 Rev 3 and how would you like us to
8 prepare to represent at the full Committee?

9 CHAIRMAN BROWN: I've given that some
10 thought during the meeting. There, the overview part
11 that we did at first, which was relative to why we're
12 going the way we're going.

13 And I'll also ask John and Jack, I don't
14 know how much we have to, we obviously can't take two
15 hours on that alone, but why you went this direction
16 and the split and then the question is how do you
17 bring these, which we didn't, how do you bring the
18 apparent split, how you wanted to separate the two.

19 You go out and you start doing stuff and
20 how do you bring it back together. From a, abbreviated
21 a little bit from what you did today.

22 I think that's an important component of
23 what we ought to present. I think you can condense
24 the 1.152 discussion, because you really kind of
25 deleted stuff and you moved it, well you state 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 you captured it in 5.71, although stated and phrased
2 differently under different headings and stuff like
3 that.

4 I personally wouldn't disagree with that.

5 I think 5.71, is more comprehensive than what was in
6 the more limited scope of 1.152, Rev 2. So, I mean I
7 like the additional detail because I think it gives
8 more information to licensees, as to what they're
9 supposed to do and what matrix they have to make.

10 And I think I made that statement back
11 when we did the 5.71, when I really knew absolutely
12 nothing about it, I had only been on the Committee for
13 about three months or something like that.

14 So I think you have, that's the, condense
15 that a little bit, but, you know, I think that's what
16 you covered. The TSC issue is probably going to come
17 up because there's a couple of other members that
18 aren't here today.

19 It was actually addressed in one of our
20 Certification letters. So that point I think is, and
21 Summer, by the way, I think answered the question when
22 we asked them.

23 They said they had a land line telephone
24 or a walkie-talkie where they could talk to the main
25 control room which was totally independent of all 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 other systems, and say what are you reading on that
2 meter?

3 Which is kind of an interesting backup
4 system.

5 MEMBER SIEBER: We had close-circuit TV so
6 you could actually look. Or you can ask the Operator.
7 I see this, what do you see?

8 CHAIRMAN BROWN: Some way to make sure. I
9 mean if they're going to do it, what they're going to
10 do. The question is going to be how do you assure
11 that they're both talking from the same sets of data,
12 and how do they confirm with each other that they're
13 doing that.

14 You know, we're not going to sit here and
15 tell you where to put it, I don't think. It's not my
16 ballpark. And then I, I don't know how to capture the
17 industry part.

18 I can't take two hours to get two
19 different perspectives. Is there a way to get a
20 summary of the two different perspectives? Any
21 suggestions, John? Jack? I mean we've got two
22 different outlooks from the industry. One, they both
23 agreed that they could live within the guidelines of
24 the two separate Reg Guides.

25 MEMBER SIEBER: I think you can generalize

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 that part of it.

2 CHAIRMAN BROWN: If you all think you can
3 cover that, as opposed to having them do that.

4 MR. ARNDT: We're always hesitant to speak
5 for the industry, for obvious reasons.

6 MEMBER SIEBER: You may want to ask one of
7 them to come to the meeting.

8 CHAIRMAN BROWN: Well, but there's two
9 different, how do you capture two different thought
10 processes? The Luminant thought process was different
11 from the Progress Energy thought process, in terms of
12 when you have to capture --

13 MR. ARNDT: Well, there were similarities
14 and there were differences.

15 CHAIRMAN BROWN: I understand, but they
16 were, one guy was hard left and that's the way he was
17 going to do it to make sure he didn't sandbagged.

18 And the other guys said, oh, you know, we
19 understand --

20 MEMBER STETKAR: Charlie, before, you
21 know, Steve has a point. The meeting is on Reg Guide
22 1.152. It's not on Reg Guide 5.71.

23 CHAIRMAN BROWN: Exactly.

24 MEMBER STETKAR: Okay, now, that being
25 said, they're related sort of somehow to one another.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MEMBER SIEBER: That's actually good.

2 MEMBER STETKAR: So I think going into
3 details of how the industry might figure out how to
4 comply with Reg Guide 5.71, is kind of off the table
5 for the full Committee meeting.

6 On the other hand, but I do agree that
7 that introductory, you know, perspective is important.

8 A couple of other things that, so I'm trying to kind
9 of tone down how do we get the industry in, because
10 they were all security related issues.

11 CHAIRMAN BROWN: Well, no, I hadn't
12 thought about it from --

13 MEMBER STETKAR: I think, from my
14 perspective, not only the basic introduction, the
15 split, the notes I was taking and the questions I was
16 asking about update to the Rule, 10 CFR 5055, update
17 to Reg Guide 5.71.

18 Update to Reg Guide 1.152. I think it's
19 worth the Committee hearing about that in a bit of a
20 more coherent fashion.

21 So there's some sense of, you know, in
22 effect we're taking a snapshot of things, the way they
23 are in, you know, right now, February of 2011, given
24 where we are.

25 The question is what direction are we

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 headed from here and over what time frame? So I think
2 that is worthwhile for the Committee to hear.

3 CHAIRMAN BROWN: I totally agree. And I'd
4 throw one of the right, go ahead and finish your
5 thought, sorry.

6 MEMBER STETKAR: And the only thing I had
7 within the specific context of 1.152, forget about the
8 cyber security stuff. Is the questions that I raised
9 regarding the guidance 1.152, either implicitly or
10 explicitly requiring some type of an assessment of the
11 digital safety system.

12 Purely from the perspective of its
13 performing its inherent safety function. And I don't
14 know whether you want to call that a fault tree
15 assessment or FMEA or that whole discussion.

16 The current guidance, as it's being
17 published, seems to require that, and yet does not
18 have any guidance to either the industry or the
19 Reviewers in terms of what is an acceptable
20 assessment.

21 So if you can somehow address that, that
22 is a, you know, it doesn't have anything to do with
23 the cyber security.

24 MEMBER SIEBER: Yes, but that assessment,
25 they call it a risk assessment, because it's not a

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 PRA type thing.

2 MEMBER STETKAR: No they don't call it a
3 risk, I was careful about not calling it a risk
4 assessment, that's why I didn't call it -- they call
5 it, they say fault tree analysis or FMEA are very
6 useful tools, but it explicitly does not endorse --

7 MR. ARNDT: Exactly.

8 MEMBER STETKAR: -- the IEEE guidance, but
9 it still says that those assessments implicitly need
10 to be done. So the question is, well, if they need to
11 be done and a Staff Reviewer or the industry knows
12 what they can't use, how do we know what they can use?

13 At least in an interim, you know, in an
14 interim and what is that interim process.

15 MEMBER SIEBER: It's almost like an ISA.

16 MEMBER STETKAR: Sort of. From keeping it
17 focused within the context specifically of the Reg
18 Guide and I'm done, thanks.

19 CHAIRMAN BROWN: The one other thing I'd
20 like to toss into that list was the idea of the a more
21 formal method of communication between NSIR and NRO
22 and NRR.

23 MEMBER STETKAR: I'm hoping that that, you
24 know, where are we headed going forward discussion
25 would do that.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 CHAIRMAN BROWN: Well, I've listed three
2 specific, and that they didn't, this is an internal
3 coordination, integration thought that I wanted to
4 make sure.

5 So somebody is looking at it along with
6 licensing at the same, in some manner or some aspect.

7 But there's got to be some touching as opposed to
8 just having this wall between.

9 MEMBER STETKAR: I was hoping that the
10 different sections of the SRP would essentially do
11 that.

12 CHAIRMAN BROWN: I took a quick look at
13 13.6.6.

14 MEMBER STETKAR: They don't now.

15 CHAIRMAN BROWN: Yes, well it's devoid.

16 MEMBER STETKAR: And you don't know.

17 CHAIRMAN BROWN: So that's the other thing
18 I put into that list of, you know, 7.4.3.2 and Rev 4,
19 and whatever, and Rev 2 or whatever it is of 5.71, if
20 there's one of those in the works somewhere.

21 I have no idea, well what's the plan --

22 MR. ARNDT: We'll put together a couple of
23 slides that lays out --

24 CHAIRMAN BROWN: What's the plan?

25 MR. ARNDT: What's the plan and where,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 we're going to try and address these various issues.

2 CHAIRMAN BROWN: And where you want to end
3 up.

4 MR. ARNDT: Right.

5 CHAIRMAN BROWN: Okay, now, time? A
6 couple of hours, two and a half hours.

7 MS. ANTONESCU: Well, usually for
8 Committee meetings we have two hours to two and a half
9 hours. But maybe two and a half hours.

10 MR. ARNDT: Given the interest --

11 MEMBER STETKAR: It depends on, we can't
12 do that at this meeting because we do that during our
13 --

14 CHAIRMAN BROWN: P&P?

15 MEMBER STETKAR: -- P&P, when we look at
16 all of the topics for particular Committee meetings.

17 CHAIRMAN BROWN: Oh, okay, all right.

18 MEMBER STETKAR: So we can't, in this
19 Subcommittee session, we can't make that.

20 CHAIRMAN BROWN: Well, we've probably got
21 at least an hour and a half.

22 MEMBER STETKAR: I mean typically you get
23 at least an hour and a half.

24 MR. ARNDT: Well, it's up to you guys, but
25 we'll adjust to fit the schedule.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 MS. ANTONESCU: So they know how to
2 prepare for it.

3 MR. ARNDT: And we're looking a April?

4 MS. ANTONESCU: April.

5 MEMBER STETKAR: See, in our March P&P
6 we'll look about going ahead and you'll know. You'll
7 know in the next two weeks.

8 MEMBER SIEBER: I think the members would
9 be interested in knowing, having a list of the 148
10 vulnerabilities.

11 CHAIRMAN BROWN: How much time do you want
12 --

13 MEMBER SIEBER: Not a slide, not a slide,
14 just --

15 CHAIRMAN BROWN: How many slides, we can
16 put --

17 MEMBER SIEBER: You just hand it out and
18 say here are the lists, because they will say, there
19 aren't 148 vulnerabilities, and if you say they are,
20 what are they?

21 MR. ARNDT: We can provide whatever
22 background material you need.

23 CHAIRMAN BROWN: I'm not sure I'd put any
24 of that on a slide, but maybe --

25 MEMBER SIEBER: No, I said not a slide.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 CHAIRMAN BROWN: Maybe just a --

2 MEMBER SIEBER: Maybe it's something
3 Christina would put in her status report as an
4 attachment.

5 CHAIRMAN BROWN: Make it 32 pages.

6 MEMBER STETKAR: Anything that's handed
7 out is subject to discussion. I mean whether it's on
8 the board or handed out.

9 CHAIRMAN BROWN: Well, but if you 148, it
10 begs the question of what do they look like? The
11 only, okay, let me take, if you're going to talk 148,
12 you ought to just make two points.

13 Number 1, they're divided into roughly a
14 third of them, but make it what the number is that are
15 technical and the rest are management.

16 Here's an example of a technical one,
17 here's an example of a management one, and leave it go
18 at that. I'm even, but that, and make it the last
19 slide and we're running out of time, so I can
20 terminate the discussion.

21 You never terminate a discussion at a full
22 Committee meeting, if a member wants to have a
23 discussion. So that's, that doesn't work either.

24 (Asides.)

25 CHAIRMAN BROWN: Unless there's something,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

1 did we give you enough?

2 MR. ARNDT: More than enough.

3 CHAIRMAN BROWN: More than enough, okay.

4 MS. ZHANG: Is there a date for this?

5 CHAIRMAN BROWN: Yes, it's the April full
6 Committee meeting.

7 MS. ANTONESCU: The first week of April.

8 MR. ARNDT: It will be Thursday or Friday.

9 MS. ANTONESCU: Thursday or Friday, we
10 haven't decided.

11 CHAIRMAN BROWN: Excuse me?

12 MR. ARNDT: The question was, was there a
13 specific date.

14 MEMBER STETKAR: And also, identify
15 yourself. You really do need to do this, for the
16 record.

17 CHAIRMAN BROWN: That was Deanna Zhang.
18 All right, with that, I will thank you all again and
19 the meeting is adjourned.

20 (Whereupon, the proceedings in the above-entitled
21 matter were concluded at 5:42
22 p.m.)

23

24

25

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com



Overview of Digital System Safety and Cyber Security

Terry Jackson, Chief, NRO/DE/ICE1

William Kemper, Senior I&C Engineer, NRR/DE/EICB

Craig Erlanger, Chief, NSIR/DSP/ISCPB

February 23, 2011

Purpose

- Present the modifications to Regulatory Guide 1.152 regarding a Secure Development and Operational Environment (SDOE)
- Provide an overview of digital system safety and cyber security licensing and oversight
- Address ACRS questions regarding digital system safety and cyber security reviews and inspections

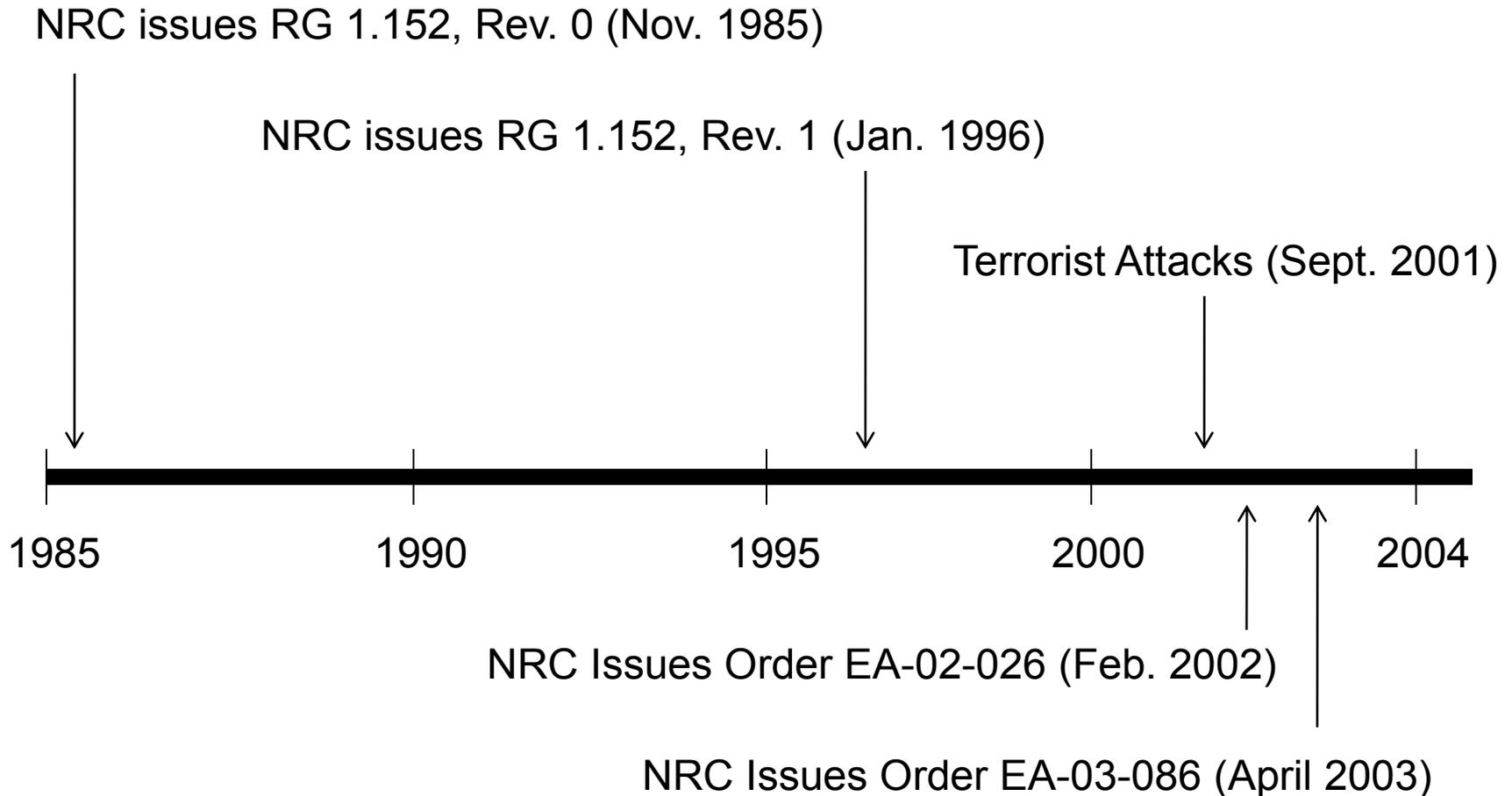
Desired Outcomes

- Address all ACRS questions
- Common understanding of the NRC's licensing and oversight process for digital system safety and cyber security
- ACRS recommendation to issue Regulatory Guide 1.152, Revision 3

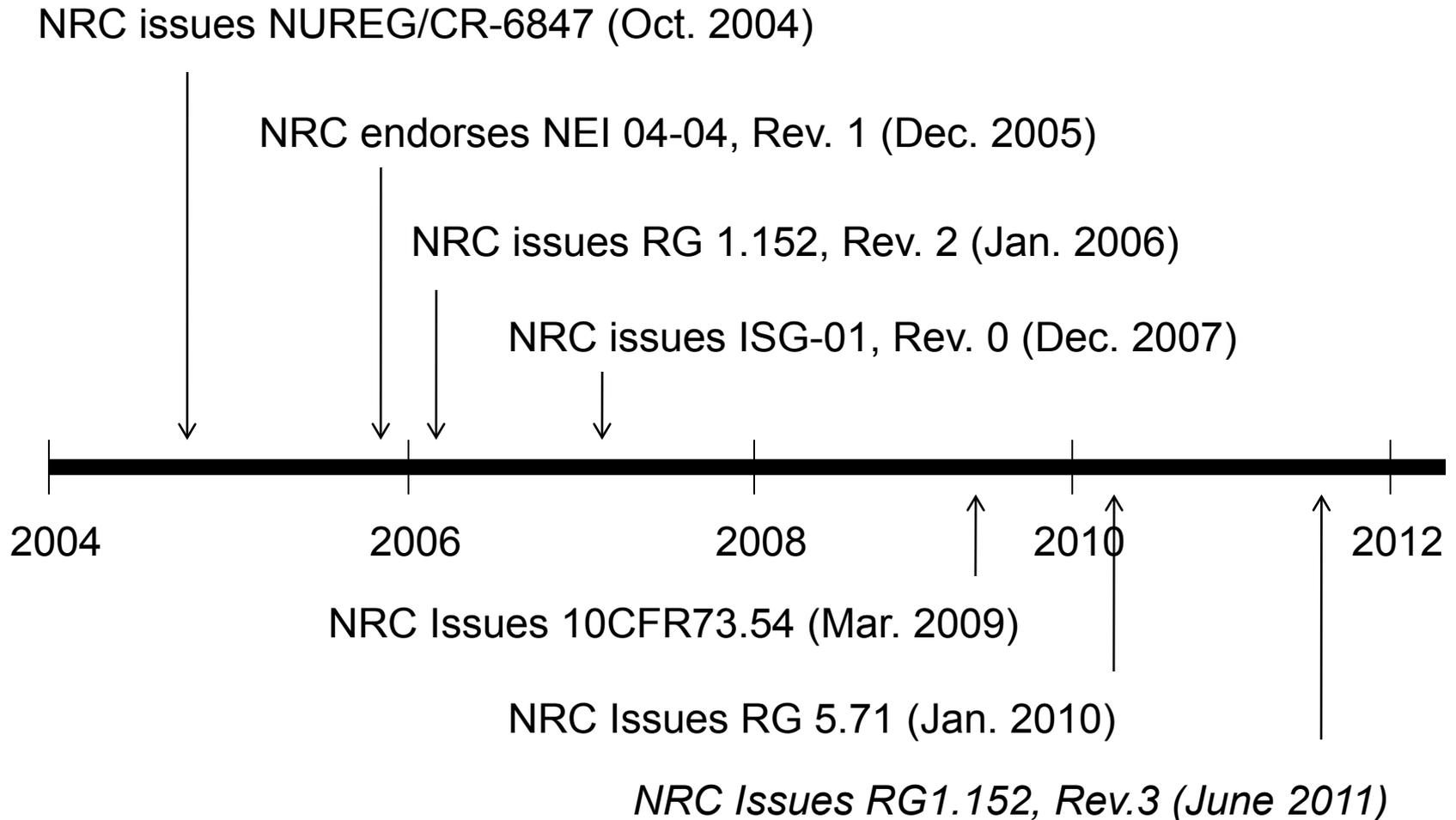
Topics

- History of digital system safety and cyber security
- Overview of the current cyber security program and digital system safety review
- Modifications to Regulatory Guide 1.152
- Regulatory developments regarding cyber security

Timeline



Timeline



Cyber Security Framework

- **10 CFR 73.54**
 - Program focused
 - Performance-Based
- **Cyber Security Licensing Process**
 - Cyber Security Plans
 - One of Four Security Plans
 - Templates
 - Appendix A of RG 5.71 and NEI 08-09, Revision 6
 - Minimizes Licensing Review Period

Cyber Security Framework

- **Use of Chapter 13.6.6 NUREG 0800
Cyber Security SRP**
 - Deviations or Alternate Methods Submitted by Licensees / Applicants Undergo In-Depth Review Against SRP and RG 5.71
- **Status of Cyber Security Licensing
Reviews**
 - Operating Reactors
 - New Reactor Applicants

Cyber Security Framework

- Recent Policy Developments
- Planned Updates to RG 5.71 and SRP 13.6.6
- Status of endorsement of NEI 08-09, Revision 6
- Cyber Security Oversight / Inspection

Digital System Safety Framework

- Goal: Ensure digital safety system reliability, availability, and integrity for non-malicious events.
- Part 73 review – determines adequacy of cyber security protection.
- Part 50/52 review – ensures protective feature does not impact safety.
- RG 1.152, Revision 3, supports these concepts.

Digital System Safety Framework

- RG 1.152 was revised to:
 - Eliminate reference to cyber-security
 - Eliminate direction to evaluate systems against malicious actions or attacks
- RG 1.152 is clarifying its focus on:
 - Controls to prevent inadvertent access to systems
 - Protection against undesirable behavior of connected systems
 - Protection of the development environment from inclusion of undocumented, unneeded, and unwanted code

Technical Aspects of Digital System Security

- Design practices addressing non-malicious events could be used for malicious events
- Little technical change in the RG 1.152 regulatory positions
- Licensees and vendors are addressing cyber security up-front in the development stage

Summary

- NRC's framework for addressing digital system security has evolved over the years.
- Digital systems must have sufficient reliability, availability, and integrity in the face of non-malicious events.
- There is technical overlap in addressing malicious and non-malicious events.
- RG 1.152 modifications are necessary to maintain consistency with the NRC's cyber security position
- NRC has a robust framework to address digital system safety and security

Background Slides

IEEE 603-1991

- Clause 5.6.3 (5.6 Independence) Between Safety Systems and Other Systems. The safety system design shall be such that credible failures in and consequential actions by other system, as documented in 4.8 of the design basis, shall not prevent the safety systems from meeting the requirements of this standard.
 - Clause 4.8 Design basis shall document conditions having the potential for functional degradation and for which provisions shall be incorporated to retain the capability for performing the safety functions (e.g., operator error, failure in nonsafety-related systems)
 - Clause 5.6.3.1(1) Interconnected Equipment Classification. Equipment used for safety and non-safety . . . Isolation devices used to effect a safety system boundary shall be classified as part of the safety system.
 - Clause 5.6.3.1(2) Interconnected Equipment Isolation. No credible failure on the non-safety side of an isolation device . . . A failure in the isolation device shall be evaluated in the same manner as a failure of other equipment in a safety system.

IEEE 603-1991

- Clause 5.9 Control of Access. The design shall permit the administrative control of access to safety system equipment. These administrative controls shall be supported by provisions within the safety systems, by provision in the generating station design, or by a combination thereof.



U.S. NRC

UNITED STATES NUCLEAR REGULATORY COMMISSION

Protecting People and the Environment

Regulatory Guide 1.152, Rev 3

Tim Mossman, NRR / DE / EICB

Deanna Zhang, NRO / DE / ICE1

February 23, 2011

Content

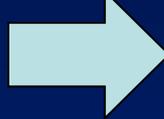
- Modification to address predictable challenges to digital safety system development and operation
- Enhanced focus on Part 50/52 reliability requirements
- Planned enhancements to the existing guidance

Mapping of Security/ Reliability Guidance

RG 1.152
Rev. 2

Sections 2.1 -2.2
Security
Requirements

Concept &
Requirements



RG 5.71

Security Controls
Section C.12.2

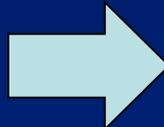


RG 1.152
Rev. 3

Sections 2.1 -2.2
SDOE requirements

Development

Sections 2.3-2.5
Q/A, CM



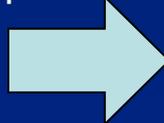
Sections C12.3 -
12.5



Sections 2.3-2.5
Q/A, CM

Operation

Section 2.6-2.9
Implementation
Operational
Maintenance
Retirement



Section C12.6 &
Cyber security
Program
Implementation
Operational
Maintenance

Reliability & Cyber

Cyber

Reliability

RG 1.152, Revision 3

- Revision 3 is ready for release
- Since 10 CFR 73.54 has been codified and RG 5.71 has been issued, RG 1.152 is being revised to:
 - Remove references to the term “cyber-security”
 - Remove direction to evaluate systems against malicious actions or attacks under Part 50
 - Remove guidance pertaining to life-cycle phases beyond what is credited in Part 50 / 52 licensing reviews

Reliability and Cyber Security

- The Part 50 / 52 licensing evaluation will focus on ensuring the reliable operation of the digital safety system
 - The NRR / NRO staff will evaluate protective actions taken against a predictable set of non-malicious events that could challenge the integrity, reliability, or functionality of a digital safety system
- To promote clarity between Part 50 / 52 and Part 73 “security”, Regulatory Guide 1.152, Revision 3 adopted the use of the term “secure development and operational environment” in its place

RG 1.152, Revision 3

- RG 1.152, Revision 3 is clarifying its focus on:
 - Protection of the development environment from inclusion of undocumented, unneeded, and unwanted code (Criterion III, “Design Control,” of 10 CFR Part 50, Appendix B)
 - Controls to prevent inadvertent access to systems (IEEE Std. 603-1991, Clause 5.9)
 - Protection against undesirable behavior of connected system (IEEE Std. 603-1991, Clause 5.6.3)

“Secure Development Environment”

- Applicants should protect their development environments such that unwanted, unneeded and undocumented code is not included in safety systems
 - These types of code increase the potential for a system to exhibit unpredictable and undesirable behavior

Secure Development Guidance

- Each phase of the development process has unique characteristics
- As part of their Concepts phase assessment, an applicant should identify opportunities where superfluous requirements, features or code could be introduced into the system
- The adequacy of appropriate development phase controls adopted will be dependant on the results of the assessment

Platform versus Application

- Applicants should be prepared to describe the secure environment controls that will be applied to both the platform software and the application software
 - It is anticipated that these two software products may be developed at different times
 - These software products could also be developed at different locations by different personnel under different development processes

“Secure Operational Environment”

- Applicants should provide design features and/or protective measures to ensure that the reliability of the digital safety system is not compromised by:
 - Undesirable behavior by connected systems (per Clause 5.6.3 of IEEE Std. 603-1991)
 - Inadvertent access to the safety system (per Clause 5.9 of IEEE Std. 603-1991)

Independence from Other Systems

- Undesirable behavior of connected digital systems includes consideration of failures, as well as other off-nominal behaviors, such as:
 - Excessive data transmission
 - Corrupted data transmission
 - “Missing” or out-of-sequence messages
 - Transmission of out-of-range data
- Applicants should consider these types of occurrences for digital safety systems and have features provided to ensure that the safety function will be unaffected

Example Operational Events

- Examples of non-malicious, undesirable behavior of connected systems impacting other plant (non-safety) systems
 - Browns Ferry, Unit 3 – August 2006 event
 - Failure of a system – resulting in excessive network traffic – on a shared integrated computer system network caused unexpected behavior of unrelated, but connected, digital systems
 - Oconee, Unit 3 – November 2008 event
 - A transmitted time signal message with out-of-range data resulted in the failure of a digital system that had not anticipated receiving a time message flawed in that manner

Access Control

- For digital systems, access controls must consider physical, as well as logical, points of access
 - Digital systems often feature points of access (e.g., USB ports) in their design
 - Systems residing on networks may be accessed from other connected systems on the same network
 - Applicants should provide, via plant controls enabled by system and facility design features, reasonable assurance that only authorized personnel will be able to access the system

Example Operational Event

- Example of non-malicious, inadvertent access event that impacted a (non-safety) digital plant system
 - Hatch, Unit 2 - March 2008 event
 - Inadvertent (i.e., *non-malicious*) access by plant personnel to a digital system via a two-way LAN connection caused the system to behave unexpectedly

Cyber Security Features

- Digital safety systems may include features that serve a cyber security purpose
- Those features should be described in a Part 50 / 52 application such that:
 - NRC staff can evaluate whether the cyber feature will degrade reliable system function
- The cyber function adequacy will be addressed under Part 73

Public Comments Summary

- 38 comments received
- Incorporated:
 - Several language / editorial changes to the document that improved the RG's background and regulatory positions
 - Clarifying scope of Part 50 versus Part 73
- Not incorporated:
 - Requests to delete secure operational environment provisions in favor of programmatic coverage per RG 5.71 and NEI 08-09
 - Requests to reference ISG-04
 - Several out-of-scope requests
- Deferred
 - Requests for additional guidance pertaining to Concept phase assessments and use of pre-developed systems

Future RG 1.152 Activities

- IEEE 7-4.3.2 – 2010
 - IEEE 7-4.3.2-2010 was very recently issued by IEEE and will be evaluated for NRC endorsement
 - RG 1.152 will be updated, as applicable
- Both staff and industry (per public comments received) would like to see more guidance published regarding:
 - Format and content of concept phase assessments
 - Treatment of pre-developed systems

Regulatory Guide 1.152, Rev. 3

- Addresses predictable challenges to the safety system development and operation
- Focuses on Part 50/52 reliability requirements
- Staff will continue to work to enhance the existing guidance

RG 1.152, Rev. 3 provides an acceptable method to ensure integrity, reliability and dependability of digital safety systems during design and development activities



Back-up Slides

Changes to Reg. Position 2.1

- Concepts phase system “assessment” refocused on:
 - identification of challenges related to inadvertent access and undesired behavior of connected systems
 - events leading to inclusion of superfluous code during development
- Guidance on prohibiting remote access expanded
- Sentence on data transfer reworded to reference other staff positions on communication between safety and non-safety systems

Changes to Reg. Position 2.2

- New terminology adopted to speak to focus on reliable operation rather than security
- Development activity guidance reworded to focus on requirements phase-specific challenges (per public comment)

Changes to Reg. Position 2.3

- New terminology adopted to focus on reliable operation rather than security
- Development activity guidance reworded to focus on design phase-specific challenges (per public comment)
- References to cyber security removed

Changes to Reg. Position 2.4

- New terminology adopted to focus on reliable operation rather than security
- Paragraph on scanning (which did not contain any guidance) was removed

Changes to Reg. Position 2.5

- New terminology adopted to focus on reliable operation rather than security

Regulations

- 10 CFR 50.55a (h)
 - 10 CFR 50.55a (h) approved IEEE 603-1991 for incorporation for the design of protection and safety systems
 - Secure software is an essential part of IEEE-603 to ensure safe and reliable software
- GDC 21
 - Criterion for protection system reliability and testability
 - Ensure secure software through all phases of design, development, implementation, and testing phases regardless of the source of vulnerability or threat
- GDC 22
 - Criteria for protection system independence
- 10 CFR 50, Appendix B
 - Provides quality assurance criteria

IEEE 603-1991 Language

IEEE-603-1991:

- Clause 5.6.3 (5.6 Independence) Between Safety Systems and Other Systems. The safety system design shall be such that credible failures in and consequential actions by other system, as documented in 4.8 of the design basis, shall not prevent the safety systems from meeting the requirements of this standard.
 - Clause 4.8 Design basis shall document conditions having the potential for functional degradation and for which provisions shall be incorporated to retain the capability for performing the safety functions (e.g., operator error, failure in non-safety related systems)
 - Clause 5.6.3.1(1) Interconnected Equipment Classification. Equipment used for safety and non-safety . . . Isolation devices used to effect a safety system boundary shall be classified as part of the safety system.
 - Clause 5.6.3.1(2) Interconnected Equipment Isolation. No credible failure on the non-safety side of an isolation device . . . A failure in the isolation device shall be evaluated in the same manner as a failure of other equipment in a safety system.

IEEE 603-1991 Language (continued)

IEEE-603-1991:

- Clause 5.9 Control of Access. The design shall permit the administrative control of access to safety system equipment. These administrative controls shall be supported by provisions within the safety systems, by provision in the generating station design, or by a combination thereof.



Luminant

SR Digital Upgrades and Cyber Security- An Integrated Approach

ACRS Subcommittee Meeting

February 23, 2011

Jay Amin

Manager: Digital Programs & Cyber Security Program

Proposed Regulatory Guide 1.152, Rev. 3

We support the proposed revisions

- Keeping the focus of Regulatory Guide 1.152 on security from a safety design stand point ensures protection of digital safety systems against non-malicious events
- The licensee's cyber security programs will address malicious actions or attacks while ensuring preservation of the safety functions associated with the SR CDAs to meet the requirements of 10 CFR 73.54
- The combination of proposed RG 1.152, Rev. 3 and the programmatic provisions under 10 CFR 73.54 {RG 5.71 or NEI 08-09 R6} seamlessly address the secure design, development, and operation of digital safety systems

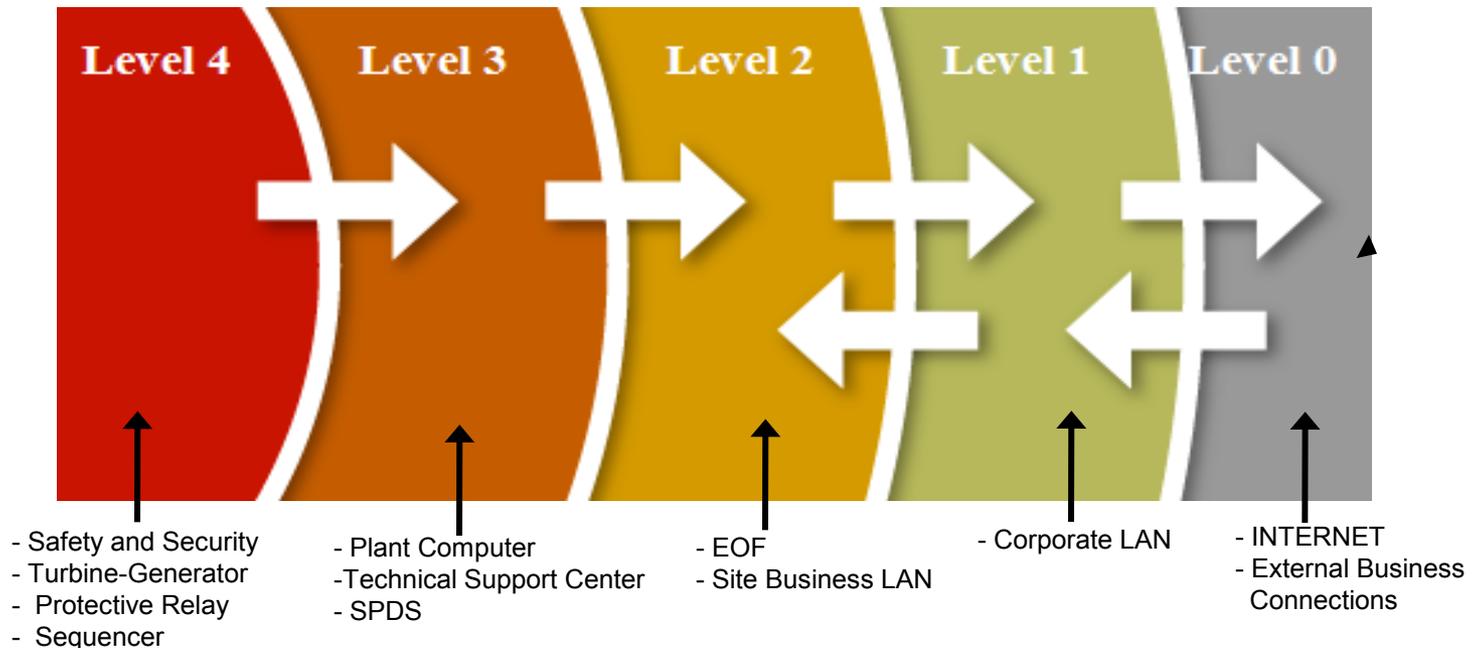
Cyber Security (CS): Key Elements

- **Station Cyber Security Plan- Part of Plant Operating License**
- **Cyber Security Policy, Program & Implementing Procedures**
- **Station Cyber Security Defensive Strategy**
- **Security Controls**
 - **Technical Security Controls**
 - Direct / Indirect Pathways
 - Access Controls / Password Controls
 - Communications Controls
 - System Hardening
 - **Operational & Management Cyber Security Controls**
 - System and Services Acquisition
 - Configuration Management / Media Control
 - Contingency Planning / Disaster Recovery
 - Maintenance/ System Integrity / Training
 - Attack Mitigation and Incident Response

Example: Cyber Security Defensive Strategy

Four defensive levels with Level 4 having the greatest level of protection

- Defensive levels separated by security boundary devices
- Logical Levels



D I&C Cyber Security Integrated Life Cycle Management (LCM) Process

Procedures being updated to address NEI 08-09, Rev. 6 in:

- DI&C Upgrade /Modification Process & Procedure
- Procurement /Contract Process & Procedures
- QA & SQA Program and Procedures
- Other Station Policies, Programs, & Procedures for Operational LCM considerations
 - Corrective Action Program
 - **Work Control Program**
 - Ongoing Program Assessment for effectiveness
 - Configuration Management Program
 - Records Management Program
 - Security Program
 - Regulatory Reporting Program
 - Emergency Response Program
 - Incident Handling & Attack Mitigation

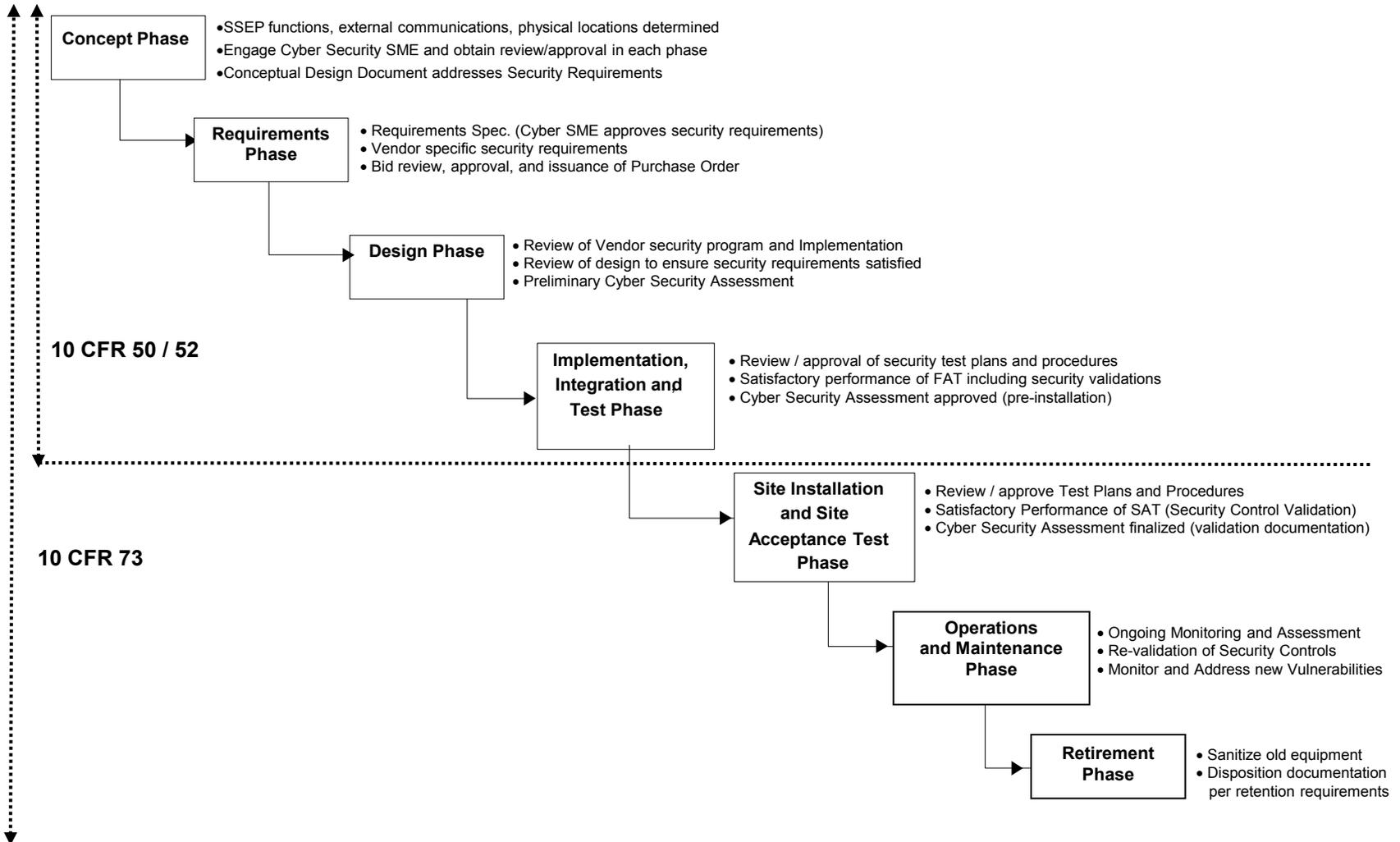


Luminant

How is Cyber Security Addressed in System Development Life Cycle (SDLC)?

- **How do we assure that DI&C Upgrades satisfy both regulations (10 CFR 50/52 & 10 CFR 73)?**
- **How are hand-offs accomplished during the SDLC phases?**

System Development Life Cycle (SDLC) Phases



Concept Phase

Overall Goal: Ensure Security Controls are addressed consistent with the station CS defensive strategy and to establish a foundation for success in more detailed phases of the project

- Determine if the Digital Upgrade affects an SSEP function
- Information compiled on:
 - CDA locations & all required external communications
 - Defensive Strategy the CDA will leverage/inherit
 - CS roles and responsibilities, including vendor/integrator
 - **Vendor /integrator in-house secure development practices**
 - Expected CDA maintenance strategies
 - Transient media, maintenance tools
 - Operator Interfaces, physical locations
- **Cyber Security SME (Subject Matter Expert) input and review / approval of the Conceptual Design**
- High level DI&C architecture & cyber security requirements are captured to ensure that the cyber strategy is robust and does not have gaps that may affect system reliability down the road
- **Review potential vendor in-house CS programs and in-house practices**

Conceptual Design lays the foundation for CS requirements and becomes a starting point for the Requirements Phase

Requirements Phase

- Information compiled from the conceptual design phase is used to develop CS requirements for the requirements specification
- DI&C Upgrade specific cyber security architecture/communications/networking requirements consistent with the station CS defensive strategy
 - Direct/Indirect connectivity (e.g. open ports & services; media storage devices - thumb drives, CDs)
 - Communications & Protocols (e.g. LAN, Modems, Data Links)
 - Physical/Logical access controls needed
- Vendor /integrator specific cyber security requirements
 - Requirements for each Development Life Cycle Phase
 - System hardening requirements
 - Chain of custody requirements
 - System/software integrity certification

Requirements Phase (cont)

- CS SME input and review /approval of the requirements specification
- Bid Review, approval and Purchase Order / Contract Issuance
 - CS SME engaged
 - Requirements Specification updated to reflect the final requirements based on selected vendor
 - Requirements Specification becomes input into DI&C Upgrade specific Cyber Security Traceability Matrix
- This phase directly determines amount of back-fit and rework
 - Specificity and clarity of requirements is important

Design Phase

CS SME engaged in review and approval during this phase

Establish periodic vendor in-house cyber security compliance reviews/audits

- **Preliminary Design Review**

- Develop a common understanding of all CS Requirements
- Review vendor/integrator plans for addressing CS Requirements
 - Secure development environment
 - In-house process

- **Critical Design Review**

- Draft project specific Vendor Cyber Security Plan
- Draft vendor/integrator Requirements Specifications for cyber security
 - System/software requirements specifications
 - System/software design specifications
- Draft Cyber Security Architecture Plan
 - Communication/access controls
 - System hardening
- Software integrity checks
- Test plans (FAT)

Design Phase (cont)

- **Detailed Design Review**

- Review/confirm vendor design meets the specified cyber security requirements
- Review design to ensure security requirements are satisfied
- Verify that all vendor deviations/exceptions are addressed for security impact and alternate controls

- **Cyber Security SME- Prepares preliminary cyber security assessment**

- **Draft Verification & Validation (V&V) Plan**

- Must address cyber security

Implementation, Integration & Test Phase

Vendor/Integrator:

- Performs system integration/system hardening
- Verifies proper implementation of CS requirements
- Verifies security configuration baselines against design configuration
- Verifies that all issues discovered during security analysis/testing are addressed, design adjusted, system retested, documents updated and approvals obtained
- Verifies system disaster recovery process using approved procedure
- Verifies test plans address all CS requirements

Implementation, Integration & Test Phase (cont)

- Conduct factory acceptance test for all cyber security requirements
 - Design implementation, integration, and factory acceptance test documentation
- CS SME participates in all CS related activities
 - Verifies that all required surveillances can be run successfully
 - CS SME prepares draft CS Assessment
 - Cyber Security Assessment approved (pre-installation)
- Successful completion of FAT establishes DI&C Upgrade specific baseline and Security baseline
 - System is under FULL CM Program
- Transition point to 10 CFR 73.54

Site Installation & Site Acceptance Test Phase

- **CSAT and the CS SME**

- Review and approval of the DI&C Upgrade Installation Plan
- Ensure that all procedures, test reports, back-up software is approved and in place for the modification at turnover of the system to Operations
- Review and approval of the SAT Plan/Procedure
 - **Verify site test plans address any security functions that were not testable in the factory testing**

- **Site Acceptance Testing activities**

- **Verification and/or validation of final CDA security configuration**
 - **Additional security posture information captured based on as-built**
- **Verification that all required surveillances execute properly**
- **Final CDA Integrity checks performed for compliance**
- **Ensure all pertinent requirements of the Cyber Security Plan are satisfied prior to system turn over to operations**

• **Cyber security SME - Updates and obtains approval of final CDA cyber security assessment**

Operations & Maintenance Phase

O&M Phase requirements are carried out in accordance with the roles and responsibilities defined in the Station Cyber Security Program

Ongoing monitoring program includes:

- Configuration management and change control of CDAs
- Cyber security impact analyses of changes to the CDAs or their environment(s) to ensure that implemented cyber security controls are performing their functions effectively
- Verification that the cyber security controls implemented for CDAs remain in place throughout the life cycle of the CDA
 - Required surveillances are carried out in accordance with CDA assessment.
- Verification that rogue assets are not connected to the CDA
- Periodic cyber security program review to evaluate and improve the effectiveness of the program

Retirement Phase

CDA specific Retirement Plan is prepared that

- Identifies critical security related information for proper disposal
- Records the necessary actions
- Performs a review of the potential security impact from removal of the system
- Verifies that security-related records are retained per records retention requirements and historical use
- Verifies proper sanitization/disposal of media and security related information
- Documents actions and completion dates in specific report prepared for CDA
- Requires obtaining approval of retirement report from cyber security SME
- Requires the submission of the retirement documentation into records

Industry Initiatives

NEI

- NEI Cyber security Task Force
 - NEI 10-04- Systems in Scope – Issued
 - NEI 10-09- Security Controls Inheritance- In Progress
 - NEI 10-08- Inspection Review Program- In Progress

NITSL

- Community of Best Practices in Cyber Security

EPRI

- **EPRI TR- 1019187- Issued October 2010**
 - Technical Guideline for Cyber Security Requirements and Life-Cycle Implementation Guidelines for Nuclear Plant Digital Systems
 - Guidance based on NEI 08-09 R6 for addressing cyber security in all system development life cycle (SDLC) phases
 - **Target Audience:** Plant digital design engineers and other staff responsible for addressing cyber security requirements throughout the SDLC
- Other Key EPRI initiatives under consideration:
 - Procurement/Contracts guidance for Cyber Security

Challenges & Plans to Address Them

1. **Application of Security Controls to Legacy Systems**

- Keep it simple and use simple solutions
 - Alarm cabinet door
 - Lock cabinets/ manual logs

2. **Vendor In-house Cyber Security Program/Process**

- Secure Development Environment- Common understanding of requirements
 - What constitutes an acceptable Secure Development Environment?
- Working with vendor/integrator community thru industry organizations to ensure consistency in requirements specification

3. **Nuances associated with Cyber Security knowledge and Expertise**

- Developing training plans and will train staff on required competencies

4. **Security Controls Evolution**

- Regulatory alternatives for scheduled periodic update of RG with industry input

Summary Conclusion

- We support proposed Regulatory Guide 1.152, Rev. 3
- SDLC approach to digital design will evolve as we integrate cyber security into the plant process, programs and procedures
- Sufficient regulatory clarity exists for Cyber Security for Digital Upgrades
- The new ISG No. 6 LAR Process, and the pilot project will provide insights and opportunities for improvements



Luminant

Questions ?

Integrating Cyber Security Requirements

ACRS Subcommittee Meeting

February 23, 2011

Matt Gibson- Process Systems Architect

Progress Energy



Company Introduction- Progress Energy

Fortune 500

Service Area in the Carolinas and Florida

3.1 Million customers

21,800 owned megawatts of capacity

11,000 employees

Four Nuclear Sites

- Brunswick- 2 Unit BWR
- Harris- Single Unit PWR
- Robinson- Single Unit PWR
- Crystal River- Single Unit PWR

Two COL Applications

- Harris- 2 Unit AP1000
- Levy Co.- 2 Unit AP1000

Presenter Introduction- Matt Gibson

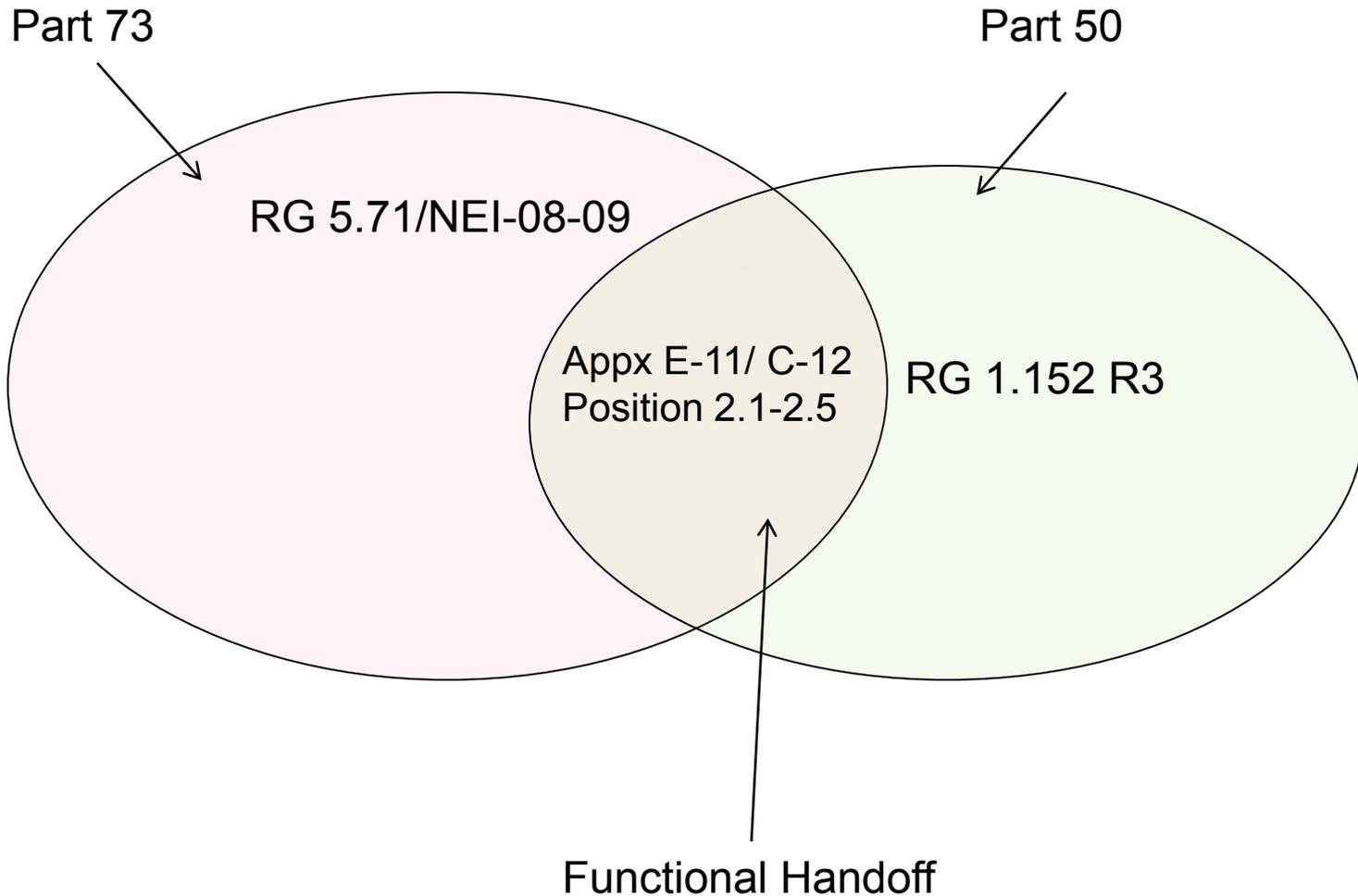
- Twenty Nine Years Nuclear Industry Experience
- Ranging from I&C Technician to Nuclear IT Manager
- Currently: Process Systems Architect
- Past 4 years- NuStart I&C Committee Lead- AP1000
- Currently dividing my duties between New Plant and the existing Progress Energy Fleet in the areas of Digital I&C , Cyber Security, SQA, and HFE.

Integrating Cyber Security- Safety Related

● How we understand the regulations...

- ▶ The Part 73 and Part 50 regulation and guidance(as proposed) are two parts of the Cyber Security puzzle.
- ▶ We have to address both to establish a Secure Development and Operational Environment(SDOE) and fully secure safety related systems.
- ▶ We feel that the Safety /Security interface is well served by a functional division between the two regulations.
- ▶ These regulations provide the public adequate protection.

Part 73 vs. Part 50



Integrating Cyber Security- Safety Related

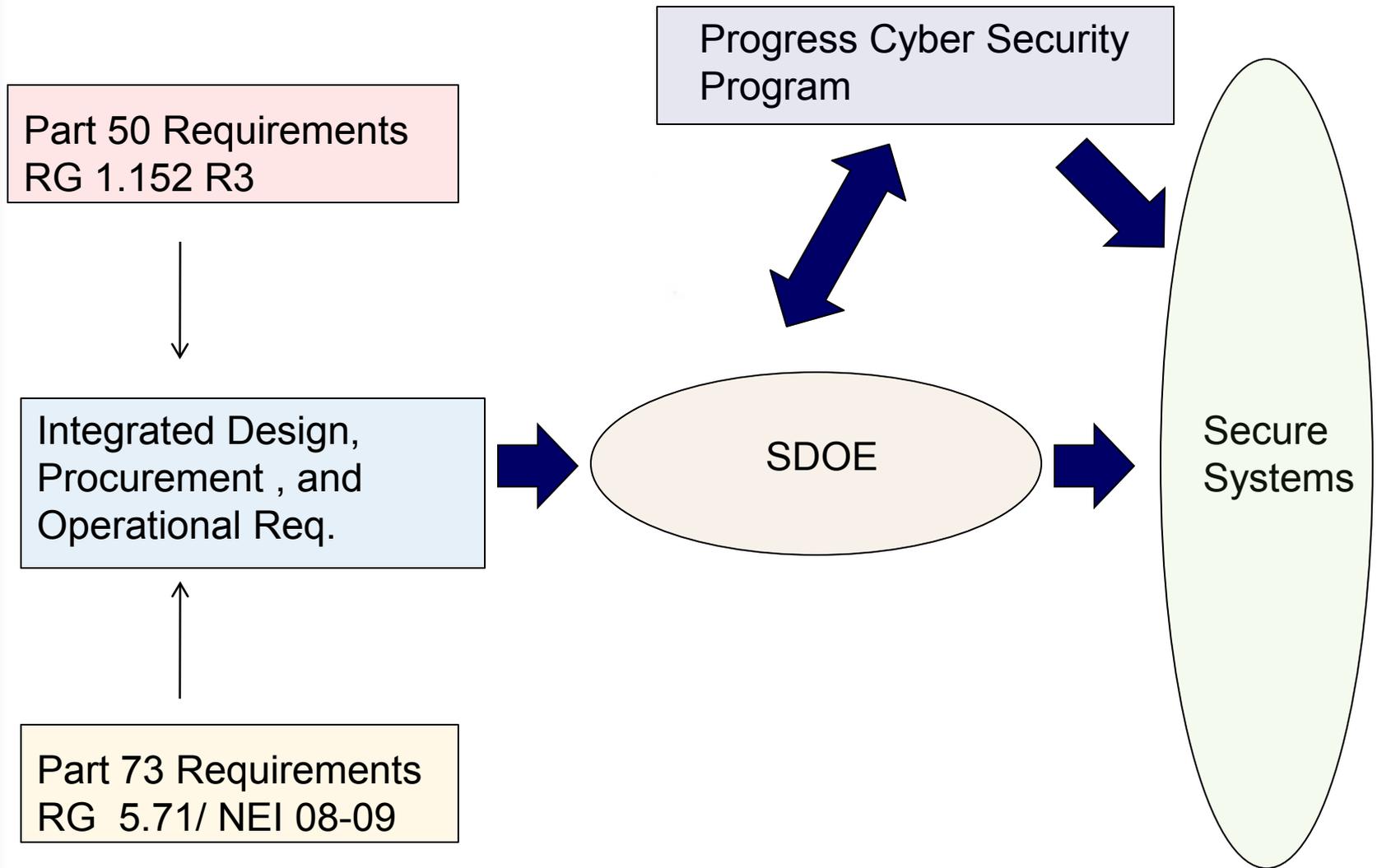
- Section E-11 of NEI 08-09 and C-12 of RG 5.71 provide supply chain requirements to address Intelligent malicious adversaries.
- Regulatory Positions 2.1- 2.5 of the proposed RG 1.152 Revision 3 provide protection from unintentional and undesirable non-malicious events.
- RG 1.152 effectively establishes that part of Cyber Security subject to prior NRC approval or 50.59 evaluation.
- RG 5.71/NEI 08-09 effectively establishes that part of Cyber Security that will be performance based.

Integrating Cyber Security – Safety Related

- **How we implement the requirements...**

- ▶ By implementing Cyber Security Programs in accordance with our approved Plans.
- ▶ Conducting cyber aware 10CFR50.59 reviews and evaluations.
- ▶ Implementing Combined Safety Related Procurement Requirements.
- ▶ Following the ISG-06 Process
- ▶ Integration of requirements into our site processes (work management, configuration control, document control, etc.).

Integrating Cyber Security – Safety Related



Integrating Cyber Security- Safety Related

● ICCMS Project at Crystal River Unit 3

- ▶ Developed Integrated SDOE and NEI 08-09 based security requirements.
- ▶ Required independent assessment of the vendor development environment with Progress review including corrective action resolution- Based on NEI 08-09 controls.
- ▶ Aligned output of assessment/corrective action with ISG-06 process.
- ▶ Required independent assessment of the vendor supplied target system with utility review including corrective actions.

Integrating Cyber Security- Safety Related

- **AP1000 (Harris 2&3 and Levy 1&2)**
 - ▶ Provided input to Westinghouse on SDOE and System Security features.
 - ▶ Continued engagement during DCD development and approval with a Staff finding of an adequate SDOE.
 - ▶ Continuing engagement via contract and project management interfaces with Westinghouse to ensure our RG 5.71 based Cyber Security Plan requirements are met.
 - ▶ Ensure RG 5.71 controls are addressed.

Integrating Cyber Security- Safety Related

- Questions???

Integrating Cyber Security Requirements

ACRS Subcommittee Meeting

February 23, 2011

Matt Gibson- Process Systems Architect

Progress Energy



Company Introduction- Progress Energy

Fortune 500

Service Area in the Carolinas and Florida

3.1 Million customers

21,800 owned megawatts of capacity

11,000 employees

Four Nuclear Sites

- Brunswick- 2 Unit BWR
- Harris- Single Unit PWR
- Robinson- Single Unit PWR
- Crystal River- Single Unit PWR

Two COL Applications

- Harris- 2 Unit AP1000
- Levy Co.- 2 Unit AP1000

Presenter Introduction- Matt Gibson

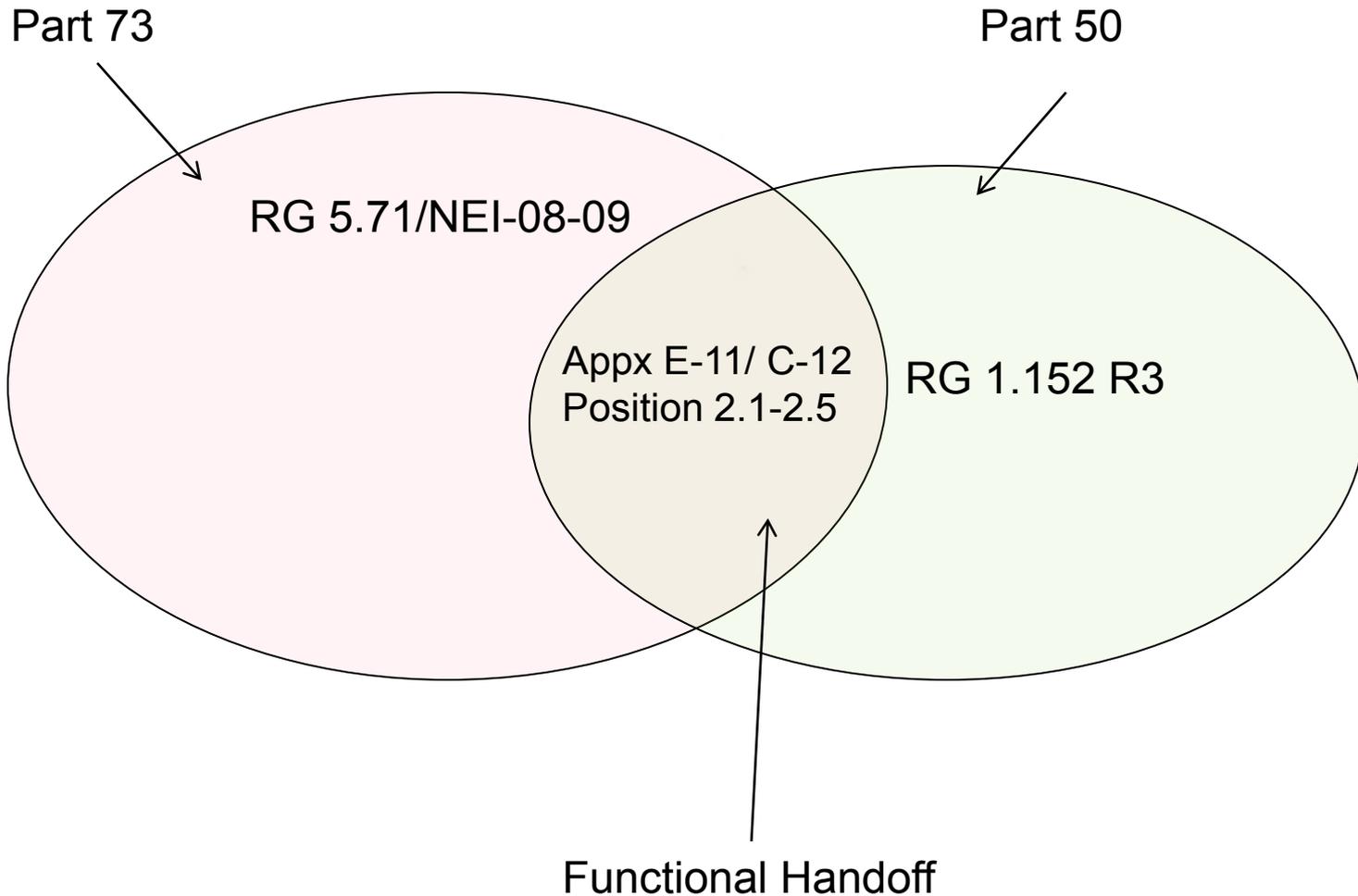
- Twenty Nine Years Nuclear Industry Experience
- Ranging from I&C Technician to Nuclear IT Manager
- Currently: Process Systems Architect
- Past 4 years- NuStart I&C Committee Lead- AP1000
- Currently dividing my duties between New Plant and the existing Progress Energy Fleet in the areas of Digital I&C , Cyber Security, SQA, and HFE.

Integrating Cyber Security- Safety Related

● How we understand the regulations...

- ▶ The Part 73 and Part 50 regulation and guidance(as proposed) are two parts of the Cyber Security puzzle.
- ▶ We have to address both to establish a Secure Development and Operational Environment(SDOE) and fully secure safety related systems.
- ▶ We feel that the Safety /Security interface is well served by a functional division between the two regulations.
- ▶ These regulations provide the public adequate protection.

Part 73 vs. Part 50



Integrating Cyber Security- Safety Related

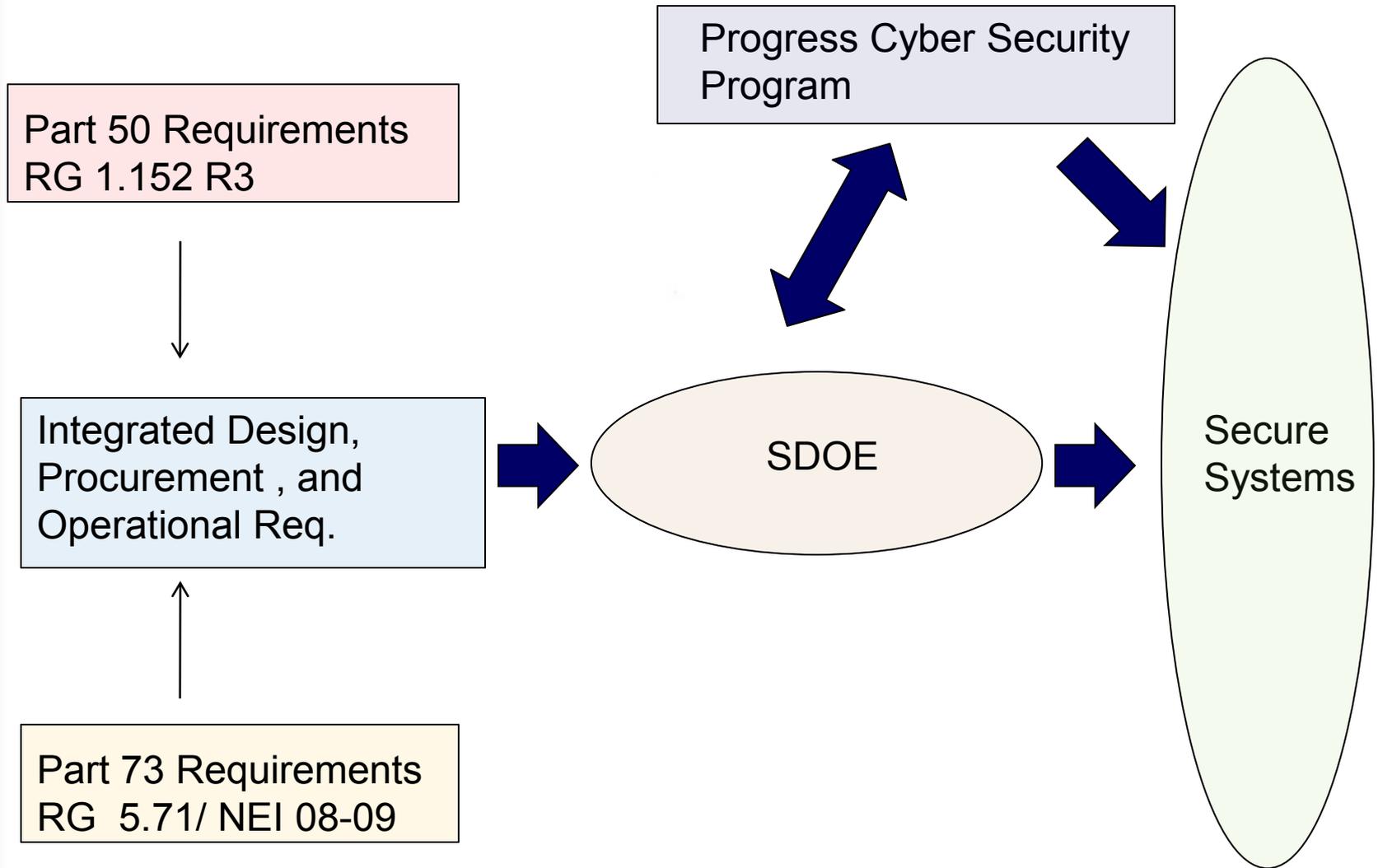
- Section E-11 of NEI 08-09 and C-12 of RG 5.71 provide supply chain requirements to address Intelligent malicious adversaries.
- Regulatory Positions 2.1- 2.5 of the proposed RG 1.152 Revision 3 provide protection from unintentional and undesirable non-malicious events.
- RG 1.152 effectively establishes that part of Cyber Security subject to prior NRC approval or 50.59 evaluation.
- RG 5.71/NEI 08-09 effectively establishes that part of Cyber Security that will be performance based.

Integrating Cyber Security – Safety Related

- **How we implement the requirements...**

- ▶ By implementing Cyber Security Programs in accordance with our approved Plans.
- ▶ Conducting cyber aware 10CFR50.59 reviews and evaluations.
- ▶ Implementing Combined Safety Related Procurement Requirements.
- ▶ Following the ISG-06 Process
- ▶ Integration of requirements into our site processes (work management, configuration control, document control, etc.).

Integrating Cyber Security – Safety Related



Integrating Cyber Security- Safety Related

● ICCMS Project at Crystal River Unit 3

- ▶ Developed Integrated SDOE and NEI 08-09 based security requirements.
- ▶ Required independent assessment of the vendor development environment with Progress review including corrective action resolution- Based on NEI 08-09 controls.
- ▶ Aligned output of assessment/corrective action with ISG-06 process.
- ▶ Required independent assessment of the vendor supplied target system with utility review including corrective actions.

Integrating Cyber Security- Safety Related

- **AP1000 (Harris 2&3 and Levy 1&2)**
 - ▶ Provided input to Westinghouse on SDOE and System Security features.
 - ▶ Continued engagement during DCD development and approval with a Staff finding of an adequate SDOE.
 - ▶ Continuing engagement via contract and project management interfaces with Westinghouse to ensure our RG 5.71 based Cyber Security Plan requirements are met.
 - ▶ Ensure RG 5.71 controls are addressed.

Integrating Cyber Security- Safety Related

- Questions???