

Official Transcript of Proceedings

NUCLEAR REGULATORY COMMISSION

Title: Advisory Committee on Reactor Safeguards

Docket Number: (n/a)

Location: teleconference

Date: Tuesday, November 30, 2021

Work Order No.: NRC-1775

Pages 1-106

NEAL R. GROSS AND CO., INC.
Court Reporters and Transcribers
1716 14th Street, N.W., Suite 200
Washington, D.C. 20009
(202) 234-4433

DISCLAIMER

UNITED STATES NUCLEAR REGULATORY COMMISSION'S
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

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

This transcript has not been reviewed, corrected, and edited, and it may contain inaccuracies.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

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

UNITED STATES OF AMERICA
NUCLEAR REGULATORY COMMISSION

+ + + + +

691ST MEETING

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
(ACRS)

+ + + + +

TUESDAY

NOVEMBER 30, 2021

+ + + + +

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

COMMITTEE MEMBERS:

MATTHEW W. SUNSERI, Chairman

JOY L. REMPE, Vice Chairman

RONALD G. BALLINGER, Member

VICKI M. BIER, Member

DENNIS BLEY, Member

CHARLES H. BROWN, JR., Member

GREGORY H. HALNON, Member

VESNA B. DIMITRIJEVIC, Member*

DAVID PETTI, Member

1 ACRS CONSULTANT:

2 STEPHEN SCHULTZ

3

4 DESIGNATED FEDERAL OFFICIAL:

5 WEIDONG WANG

6 CHRISTOPHER BROWN

7 *Present via teleconference

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

P R O C E E D I N G S

1:00 p.m.

CHAIRMAN SUNSERI: Okay. It is 1:00 o'clock. We will reconvene the ACRS meeting for today. Our next topic on the agenda is Draft Guide 5061, Revision 1, cyber security programs for nuclear power reactors. At this point, I will turn it over to Member Brown for any comments before getting into presentations.

MEMBER BROWN: Okay. We have Jim Beardsley and Jeanne Johnston here with us in person to help answer questions. Kim, I'm going to get this right, Lawson --

MR. BEARDSLEY: Jenkins.

MEMBER BROWN: -- Jenkins. I'm sorry. Are you on?

MS. LAWSON-JENKINS: Yes, I am. I am on the call. Thank you.

MEMBER BROWN: I apologize for that. I'm going to let them make some introductory remarks. You may remember we have one subcommittee that all the people present here for this presentation are the same ones. So we'll have some continuity.

And I think everybody but Walt, you weren't at our October meeting, were you? Okay. So

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1716 14th STREET, N.W., SUITE 200
WASHINGTON, D.C. 20009-4309

(202) 234-4433

www.nealrgross.com

1 most of the slides, we asked them to pay attention to
2 the important slides, not just the little ones. And
3 so we cut the slide deck, I think, from 43 or 44 or
4 49, whatever it was, down to, what, 20?

5 MR. BEARDSLEY: Twenty-eight.

6 MEMBER BROWN: Twenty-eight. So we ought
7 to be able to fit in okay.

8 MEMBER BROWN: And Jim and Jeanne, I will
9 open it up to you for you to all to make opening
10 comments.

11 MR. BEARDSLEY: Thank you very much. And
12 thank you for the opportunity to brief the full
13 committee on our updates to Regulatory Guide 5.71 or
14 Draft Guide 5065 --

15 MEMBER BROWN: 5061, Rev. 1.

16 MR. BEARDSLEY: -- Rev. 1. The staff
17 recognizes that there have been concerns raised
18 relative to the safety and security regulation and the
19 coordination thereof. The staff does not believe that
20 there is a gap in this area. And we've invited a
21 colleague, Jeanne, from NRR, Division of Engineering,
22 to join us today and help describe how our two
23 organizations work together to ensure the safety and
24 security objectives are met.

25 In July 2021, the staff provided the

1 digital INC subcommittee and update brief on the
2 entire cyber security oversight program. In October,
3 we followed that brief with a detailed brief on
4 Revision 1, Regulatory Guide 5.71. And a shorter
5 version of that presentation will be used today.
6 Excuse me.

7 Since 2012, the operating nuclear power
8 reactor licensees have implemented their full cyber
9 security programs. The NRC has implemented an
10 oversight program of the licensees' cyber security
11 implementation. Each cyber security program has been
12 inspected at least two times since 2013 and found to
13 be effective.

14 Revision 1, Regulatory Guide 5.71 does not
15 change the staff's position on the cyber security
16 program implementation for nuclear power plants. The
17 revision includes guidance clarification based on
18 lessons learned from program implementation and our
19 oversight inspections, reference to updated
20 international and NIST standards -- National Institute
21 of Standards standards. And it reflects one new NRC
22 regulations, 10 Code of Federal Regulations 73.77,
23 cyber security event notification rule, which was
24 implemented following the initial publishing of
25 Regulatory Guide 5.71.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1716 14th STREET, N.W., SUITE 200
WASHINGTON, D.C. 20009-4309

(202) 234-4433

www.nealrgross.com

1 Following the Executive Director of
2 Operations direction to staff based on concerns raised
3 by the ACRS' March 2021 letter, cyber security staff
4 incorporated one change into Regulatory Guide 5.71
5 into one of the technical security controls. And Ms.
6 Lawson-Jenkins will address that change in her
7 presentation. As part of our coordination efforts,
8 the ancillary staff are -- excuse me, are
9 participating in pre-application discussions for
10 digital INC upgrades and pre-application discussions
11 with new licensees and also the ancillary staff,
12 support vendor and regional oversight inspections, or
13 digital INC upgrades, factory acceptance testing, and
14 site acceptance testing. At this point, I'll turn it
15 over to Jeanne to speak to NRR's perspective.

16 MEMBER HALNON: One quick question.

17 MR. BEARDSLEY: Oh, yes.

18 MEMBER HALNON: You mentioned that the
19 programs are found to be effective.

20 MR. BEARDSLEY: Yes.

21 MEMBER HALNON: When you say effective,
22 did you mean that you were able to inspect whether the
23 cyber program actually repelled an attack or something
24 to that effect? Or is it just in compliance?

25 MR. BEARDSLEY: So the cyber security plan

1 is a license condition for each licensee. So it's
2 part of their license requirement. And what we've
3 done is it's primarily compliance because we have not
4 had -- we don't have a method to test -- actually test
5 them.

6 But as part of the instructions, we do
7 look at the configurations they've used or the
8 hardware they use for protection. We've gone very
9 deep into those inspections. Between the two
10 inspections, there was over four weeks of actual
11 inspection activity, and so that's a lot of effort we
12 put in to verify that they understand the requirements
13 and they've implemented them.

14 MEMBER HALNON: No elevated findings or
15 did you have some?

16 MR. BEARDSLEY: At this time, we have no
17 findings greater than green.

18 MEMBER HALNON: No greater than --

19 MR. BEARDSLEY: There is one potential
20 finding that is being adjudicated and it has not been
21 closed out yet. But over the course of all those
22 years -- and I can't remember. There's something like
23 150 inspections. We have found nothing is greater
24 than green.

25 MEMBER HALNON: I just want to distinguish

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1716 14th STREET, N.W., SUITE 200
WASHINGTON, D.C. 20009-4309

1 between when you say the security, the physical
2 security is actually what's after force on force and
3 actually tested the defenses as opposed to cyber. You
4 don't really have testing, a way to test it at this
5 point.

6 MR. BEARDSLEY: We don't have a way to
7 test it similar to the force on force.

8 MEMBER HALNON: Okay. Thanks.

9 MEMBER BLEY: I'm just a little curious.
10 When we first started looking at this with you, we had
11 a lot of discussion about how one defines -- is the
12 right term essential cyber assets or it's a different
13 --

14 MR. BEARDSLEY: Critical digital assets.

15 MEMBER BLEY: Critical digital assets.

16 MR. BEARDSLEY: Yes.

17 MEMBER BLEY: And it was -- looked like a
18 massive job. And I know you made changes to make that
19 more directly useable. When you do those inspections,
20 is a lot of that inspection time aimed at seeing how
21 well defined those critical digital assets are?

22 MR. BEARDSLEY: So one of the things we
23 looked at very closely in the first inspection program
24 between 2013 and 2015 was the process the licensee
25 used for defining which digital assets were critical

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1716 14th STREET, N.W., SUITE 200
WASHINGTON, D.C. 20009-4309

1 digital assets. Once we inspected that, we had a
2 level of assurance -- reasonable assurance that they
3 had a process in place that was effective. Then we
4 went in for a second set of inspections between 2017
5 to 2021. We actually looked at the change control
6 process they use for adding or deleting critical
7 digital assets or reclassifying them and found that to
8 be within reasonable assurance to be adequate as well.

9 MEMBER BLEY: I'm just curious. Did a lot
10 of people make changes?

11 MR. BEARDSLEY: Many of them did make
12 changes, and they were primarily to be -- so what we
13 did was we approved guidance for them to use a graded
14 approach to those digital assets that were less -- had
15 less of a risk. And so yes, we did look at that, and
16 many of them did make changes. And we believe that
17 there'll be further changes made prior to our new
18 inspection program that'll start next year.

19 MEMBER BLEY: Next year? Okay. Thank
20 you.

21 MEMBER BALLINGER: You said that you had
22 over, what, 150 inspections?

23 MR. BEARDSLEY: It's more than that.

24 MEMBER BALLINGER: Okay. More than that.

25 A lot?

1 MR. BEARDSLEY: Yeah, yeah, yeah. But
2 that's --

3 (Simultaneous speaking.)

4 MEMBER BALLINGER: No higher than green?

5 MR. BEARDSLEY: No findings greater than
6 green at this time. As I said, there is one finding
7 that is currently under adjudication by one of the
8 regions that could be greater than green. But other
9 than that, no.

10 MEMBER BALLINGER: But how many greens?

11 MR. BEARDSLEY: There were a number of
12 greens.

13 MEMBER BALLINGER: Was there a pattern in
14 the number of greens? In other words, this particular
15 issue was common among the green findings.

16 MR. BEARDSLEY: So what we found was over
17 time there were some repeat findings. But industry
18 using their operating experience program had to
19 educate themselves. And we, through public meetings,
20 had to explain, hey, this is an area that we think
21 industry needs to work on.

22 And so they would correct those. And we
23 don't want to look at the same thing in every
24 inspection. So we would change our focus as we went
25 through. But industry did learn and did improve

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1716 14th STREET, N.W., SUITE 200
WASHINGTON, D.C. 20009-4309

1 performance over the course of the inspection program.

2 MEMBER BLEY: Correct me. But I think
3 what Ron was getting at is, did you see not at one
4 plant the same things repeating but was some area that
5 repeated a lot across --

6 (Simultaneous speaking.)

7 MR. BEARDSLEY: We did. We did see areas
8 that were repeated across multiple inspections. But
9 industry learned those lessons and put the corrections
10 in place. So latter inspections, to a great extent,
11 they had made corrections. And we did not find those
12 same --

13 (Simultaneous speaking.)

14 MEMBER BALLINGER: Multiple inspections at
15 multiple plants?

16 MR. BEARDSLEY: Correct, yes.

17 (Simultaneous speaking.)

18 MR. BEARDSLEY: Multiple inspections at
19 multiple plants.

20 MR. BEARDSLEY: Correct, yes.

21 (Simultaneous speaking.)

22 MR. BEARDSLEY: Multiple inspections at
23 multiple plants.

24 MEMBER HALNON: -- kiosk were common for
25 a while. And so --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1716 14th STREET, N.W., SUITE 200
WASHINGTON, D.C. 20009-4309

1 MR. BEARDSLEY: Right.

2 MEMBER HALNON: -- that issue got
3 resolved.

4 MR. BEARDSLEY: Yeah.

5 MEMBER HALNON: And a couple of other
6 issues --

7 MR. BEARDSLEY: Correct.

8 MEMBER HALNON: -- stayed -- until NEI
9 engaged and there was a meeting of the minds. And so
10 there were some things. But like, you're right. They
11 kind of decreased as time went on.

12 MR. BEARDSLEY: Right. For the kiosk, we
13 actually had a series of meetings with industry to
14 come to terms with what the requirements were. The
15 majority of those issues that you identified is
16 corrected through industry operating experience. They
17 would just share the experience across industry and
18 make the appropriate corrections. And we would not
19 find those same issues.

20 MEMBER BALLINGER: So you really don't
21 have any repeat offenders?

22 MR. BEARDSLEY: It's hard to characterize
23 industry as a whole. Some licensees would pick up on
24 operating experience. Some of them might now. So a
25 year later, we'd see something we saw before and we'd

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1716 14th STREET, N.W., SUITE 200
WASHINGTON, D.C. 20009-4309

(202) 234-4433

www.nealrgross.com

1 a new finding. So I can't speak to industry as
2 overall. But in general, the trend we saw was
3 improvement over the course of the inspection. Okay?
4 Jeanne?

5 MS. JOHNSTON: Okay. Thanks, Jim.

6 (Simultaneous speaking.)

7 MS. JOHNSTON: Thank you. Thank you, Jim.
8 My name is Jeanne Johnston. I'm the Branch Chief of
9 the Long-term Operations and Modernization branch at
10 NRR. My branch has responsibility for guidance
11 development, for instrumentation controls, and
12 electrical areas that support modernization. So
13 primarily, this includes the increase of digital
14 modernization projects that we expect for control and
15 protection systems at nuclear power plants.

16 As Jim mentioned, headquarters staff from
17 NRR and NSIR continue to closely coordinate on issues
18 that are related to safety and security. And we do
19 this coordination with the regions. So examples
20 include our implementation of an alternate review
21 process for digital modernization license amendments
22 and implementing that and licensing and inspection
23 activities for digital modifications.

24 We understand the concerns that were
25 previously conveyed by the ACRS regarding

1 unidirectional communications from higher to lower
2 safety systems. And we plan to communicate
3 expectations and best practices to our stakeholders in
4 upcoming public interactions. To mention, there is a
5 public meeting that will likely be held in the January
6 time frame on our guidance development where we will
7 seek stakeholder input on prioritization.

8 There's also -- we're planning also on
9 having a lessons learned workshop in the March time
10 frame to discuss lessons learned from digital
11 modernization and applying the alternate review
12 process in licensing and in section activities. You
13 may know that the NRC recently approved a digital
14 modification at Waterford to updated their core
15 protection calculator. That is the first use of the
16 alternate review process for digital modification.

17 And we expect more applications next year
18 to use that process. The clarifications that we
19 expect to convey will emphasize the design option that
20 is available to vendors and applications to implement
21 a hardware-based unidirectional communication between
22 systems of different safety significance. The staff
23 recently updated the ACRS subcommittee on --

24 (Simultaneous speaking.)

25 MEMBER BROWN: Could you back and repeat

1 that again?

2 MS. JOHNSTON: Sure. So -- okay.

3 MEMBER BROWN: Just pick it up. Pick it
4 up.

5 MS. JOHNSTON: Okay, okay. I'll try to
6 project.

7 MEMBER BROWN: That's it.

8 MS. JOHNSTON: Okay.

9 MEMBER BROWN: Thank you.

10 MS. JOHNSTON: So we were given direction
11 from the EDO that stemmed from the ACRS feedback that
12 we got from the March letter from Chairman Sunseri.
13 And as you know, the Chairman tasked the EEO to create
14 a task force to look into the concerns that were
15 raised regarding unidirectional communications when
16 they go from higher safety significance to then lower
17 safety significance systems. The independent task
18 force recommendations were given to the staff as the
19 direction from the EEO to implement clarifications.

20 So one clarification, as Jim mentioned, is
21 included in Reg Guide 5.71 which you're going to hear
22 about today. The other clarifications are going to be
23 in other guidance documents which my branch would have
24 responsibility over, and primarily Reg Guide 1.152,
25 which will be updated not for another year or so, and

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1716 14th STREET, N.W., SUITE 200
WASHINGTON, D.C. 20009-4309

(202) 234-4433

www.nealrgross.com

1 Branch Technical Position BTP 7-19. So the BTP 7-19
2 guidance is for the SRP. It's staff guidance.
3 Revision 8 was completed earlier this year. So due to
4 resources and prioritization, we aren't planning on
5 updating those documents in the near term.

6 But before we memorialize the guidance
7 updates, we are going to communicate our expectations
8 during public workshops, public meetings where we
9 engage stakeholders and talk about expectations for
10 licensing amendments for additional modification
11 projects. And the two workshops that I mentioned, one
12 would be in the January time frame to talk about our
13 guidance development infrastructure improvements. And
14 the other one is a lessons learned workshop for
15 digital modification, licensing, and inspection items.
16 And that would be in the March time frame.

17 MEMBER BLEY: Thanks. It might not be
18 fair to put you on the spot.

19 MS. JOHNSTON: Sure.

20 MEMBER BLEY: But to the best of my
21 knowledge, the staff hasn't sent a response back to us
22 on that letter. Do you have any --

23 MS. JOHNSTON: Yes. Okay, that --

24 MEMBER BLEY: -- knowledge about that?

25 MS. JOHNSTON: That is correct. So the

1 letter was not addressed to us. Are you referring to
2 the Chairman's letter, the ACRS --

3 (Simultaneous speaking.)

4 MEMBER BLEY: I am.

5 MS. JOHNSTON: -- letter to the Chairman?
6 Okay. That was addressed to the Chairman. So it
7 never came down to the staff to get a response.

8 MEMBER BLEY: Okay. We often get
9 responses from the staff on letters we write to the
10 Chairman. But that's all right.

11 MS. JOHNSTON: Oh, okay. Well, we can
12 certainly -- if that is what is expected, we can
13 certainly do that. It just was never --

14 MEMBER BLEY: We'd like -- we've been
15 looking for something clear that says where you're
16 headed.

17 MS. JOHNSTON: Okay.

18 MEMBER BLEY: We've looked at the things
19 you've sent back to the Commission and EDOs
20 promulgated. But --

21 MS. JOHNSTON: Sure.

22 MEMBER BLEY: -- something directed at us,
23 I think, Charlie, don't you? We'd like to --

24 (Simultaneous speaking.)

25 MEMBER BROWN: The issue is coming down to

1 the point where BTP 7-19 was kind of the kickoff. If
2 you go back to about two years, one of the earlier
3 reviews of 7-19 and then November of '19 --

4 MS. JOHNSTON: Sure.

5 MEMBER BROWN: -- when we commented. And
6 then we had the follow-up. We requested something.
7 And then you all didn't agree with us with that. So
8 you went ahead and issued Revision 8 --

9 MS. JOHNSTON: Right.

10 MEMBER BROWN: -- without anything at all.
11 So right now, there are no technical documents at all,
12 neither the standard review plan, 7-19, defense-in-
13 depth, which is a pretty critical review document for
14 all the new applications. And Reg Guide 1.152 is not
15 specific on this area at all.

16 I'm not being critical. I'm just stating,
17 even rev 3 which you have incorporated into the new
18 Reg Guide. It doesn't have any particular direction
19 relative to this.

20 And so right now, the only document that's
21 anywhere to provide what I call NRC documented
22 comments, not public workshops, not notes, lessons
23 learned, conferences, all that kind of stuff, that's
24 nice which it's a good thing to do. But it doesn't
25 provide what is expected. And just talking about it

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1716 14th STREET, N.W., SUITE 200
WASHINGTON, D.C. 20009-4309

(202) 234-4433

www.nealrgross.com

1 in a public meeting or in a -- I mean, it's a personal
2 opinion.

3 MS. JOHNSTON: Sure.

4 MEMBER BROWN: Okay. It's good. At least
5 the applicants and the licensees know what you guys
6 are thinking, but yet it's not written down formally.
7 So I mean, it's -- we've managed at least in the new
8 advanced reactor -- advanced reactor design review
9 guide actually addresses this issue very pointedly
10 with the exact kind of similar type words we would
11 have liked to have seen in 7-19. We would have liked
12 to have had a nice new design review guide as part of
13 the standard review plan development. But that's a
14 big conflagration of the whole thing being looked at.
15 So it's going to be quite a while.

16 MS. JOHNSTON: Right.

17 MEMBER BROWN: So the difficulty is
18 there's no -- nothing written down that says, hey,
19 this is really what our expectations are via either a
20 regulatory guide or a branch technical position or
21 even an ISG. ISG-6 talks about architectures, even in
22 the alternate review process. You've got to develop
23 an architecture similar to what we did for the new
24 plant designs.

25 And then it's got a bunch of other stuff

1 that makes a little bit easier for them to get through
2 the alternate review process. So that, to me -- and
3 this is, again, my personal opinion. You've heard it
4 from me before is there's a gap in my own mind at
5 ensuring that in the design space five or six years
6 separated from a COL type space when you all do the
7 cyber or when Jim does the cyber stuff. What do the
8 designers do when we're doing a design review? For
9 instance, we've got Limerick and Turkey Point --

10 MS. JOHNSTON: That's right.

11 MEMBER BROWN: -- coming up. And as you
12 might expect based on at least from my view point
13 we're going to look at those what they propose. And
14 if we don't see a unidirectional hardware-based not
15 configured by software, in other words, a data diode,
16 if you call those synonymous, we'll be making a
17 comment. Or at least I will be recommending that we
18 make a comment.

19 Excuse me. I want to make sure I phrase
20 this properly. So that's not the right way to do it.
21 I mean, it ought to be recognized that there's a
22 difference between when we had the analog world all
23 you needed was the physical access security.

24 But once you introduce the new path,
25 control of access or electronic access and what you

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1716 14th STREET, N.W., SUITE 200
WASHINGTON, D.C. 20009-4309

1 call an attack path I guess was what the NSER
2 (phonetic) calls it. Did I get that right, attack
3 pathway? Now you had to have some electronic.

4 Designers have to do something. They've
5 got to send data out because you got to go tell the
6 pumps to start and the valves to open and send data
7 off to the control room. How do they do that? You
8 can't wait five years.

9 Having a little bit of humor in this
10 thing, you can't deliver a set of cabinets with
11 fiberoptic cables hanging out the bottom. They got to
12 have a transmission device hooked up to them
13 someplace. And when we make comments to do that, you
14 get pushback because that's cyber.

15 And I think that's not the right way to do
16 it. That's a personal opinion. The designers have to
17 -- in the design space, they have to be able to do
18 that. And it's not in any of the design documents
19 other than the advanced lightwater design review guide
20 right now.

21 But that's the fundamental for us. I went
22 back through rev 0 that we did. I wrote the letter on
23 that ten years ago and also reviewed it line by line.
24 And I compared it to the new rev 1.

25 And fundamentally, that's all the changes

1 you made, highlighted them. I don't have any real
2 disagreements with what you all did with a few
3 exceptions. Those exceptions revolve around how do we
4 differentiate the cyber world from those systems that
5 can't have any -- they can't have virus systems.

6 They can't have detection mitigation
7 systems in them. We can't do that. It'll destroy the
8 control functions if you do that. It just doesn't
9 work. So they're sitting there naked.

10 So the only way you can protect them from
11 other than the implant, the insider threat is via the
12 unidirectional device. And there's no place else and
13 it's not separated, even in the one section that you
14 all address. And I don't have the paragraph in here.

15 You made the comment that if the
16 application or the licensees decide to review -- to
17 use -- to do a cyber review during -- and I'm getting
18 the words a little bit. But it talks about a cyber
19 review during the design process to implement those.
20 That implies they're doing a cyber review.

21 They're not. They're doing a design
22 review. And they're not to commit to doing a cyber
23 review as part of the design process. So there's a
24 little disconnect on how that's worded.

25 So that's a separation of how do you get

1 the design people freed up to do the design as they
2 ought to be able to do. And if they don't do it right
3 when they get to cyber end of the business, fine. But
4 we know it's not going to happen that way if you
5 implement these.

6 So that's -- from my standpoint, that's
7 what I've been trying to get discussed and get some
8 action taken. This is the only document going out in
9 the next few years frankly. And all I was looking for
10 was something more than the one sentence in Section
11 331 which talked about technical security controls.

12 You did a good job on some others. You
13 talked about when you wanted unidirectional, it ought
14 to be hardware-based, et cetera. That's up ahead of
15 the big -- the defensive architecture diagram. That
16 was expanded, and that was good.

17 So there's a couple more changes like that
18 that you all introduced. But we don't get to the
19 point where we say, there's a world that has no virus
20 detection and mitigation systems. And those methods
21 we use here in 527-1 are suitable because I think they
22 are for application in their design world.

23 And then they can be reviewed later if
24 there's some other aspects that come up. That's the
25 disconnect I see. And other than that, I was pretty

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1716 14th STREET, N.W., SUITE 200
WASHINGTON, D.C. 20009-4309

(202) 234-4433

www.nealrgross.com

1 satisfied with rev 1.

2 You can argue about the length of the
3 appendices and ginormous amount of paperwork that goes
4 along with it. But I think Appendix B is the primary
5 technical part of it. A and C are more management.

6 And I had another word and I promptly --
7 my 80-year-old brain just forgot it. Administrative,
8 tells you how to lay out the paperwork process and
9 programming and teams to review and all that, but not
10 the technical aspects. Yeah, thank you. Very good.
11 Yeah, Appendix B.

12 But you don't want to put this other
13 information about separation of stuff that doesn't
14 have any capability to put cyber detection, virus
15 detection and mitigation software in. That's the
16 wrong place. That's where you're actually doing
17 stuff.

18 It's put in the applicability paragraph.
19 And there's another paragraph a little bit later where
20 the allowance for -- or recognition, excuse me. That
21 the methods that you use here, you don't have to be in
22 a cyber review.

23 You can use them and not complete a cyber
24 review. Use them as necessary to make your design
25 work. And that's where the disconnect is because

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1716 14th STREET, N.W., SUITE 200
WASHINGTON, D.C. 20009-4309

(202) 234-4433

www.nealrgross.com

1 right now the applicability says when you're doing a
2 7354, bang, and everything else follows. There is no
3 differentiation.

4 So a second paragraph that says, hey,
5 there are systems -- safety systems and others,
6 control systems where you can't have the virus
7 protection and mitigation systems. And those have to
8 be accounted for during the design process, not wait
9 for the COL cyber review process years later. So all
10 I've been trying to drive for is trying to get that
11 recognition up in the front of these and the
12 applicability and down in part of the discussion
13 section.

14 And there's a few other pieces. Like,
15 there's no data diode to find. You talk about a data
16 diode, but you don't really say it's a unidirectional
17 hardware-based not configured by software. It's a
18 definition issue. Those are small potatoes.

19 MS. JOHNSTON: Right. So --

20 MEMBER BROWN: And you use one way then.
21 So anyway, the point being is that's what I've been
22 trying to emphasize in our meetings.

23 MS. JOHNSTON: Understood.

24 CHAIRMAN SUNSERI: And we recognize that
25 you may not be in a position to address this right

1 now. We wrote to the Commission. They passed it to
2 the EDO. We need to hear back from the EDO's office
3 really.

4 MS. JOHNSTON: Okay.

5 CHAIRMAN SUNSERI: But you have influence
6 on that. So thank you for being a good listener. And
7 the messenger here, we don't intend to shoot you.

8 MEMBER BROWN: Oh, no.

9 (Simultaneous speaking.)

10 CHAIRMAN SUNSERI: No, no. I know. It
11 didn't come out that way. But I want ask --

12 MS. JOHNSTON: No, no, no.

13 CHAIRMAN SUNSERI: -- do you have a --

14 MEMBER BROWN: Start shooting those
15 arrows.

16 CHAIRMAN SUNSERI: -- do you have a
17 presentation?

18 MR. BEARDSLEY: We do.

19 CHAIRMAN SUNSERI: Okay. Well, maybe we
20 can get into the presentation and some of this will
21 all weave in. Okay?

22 MS. JOHNSTON: Okay. If I could, though,
23 just to respond briefly to your concerns, Member
24 Brown, I don't disagree with the underlying concern
25 that you're raising that unidirectional hardware-based

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1716 14th STREET, N.W., SUITE 200
WASHINGTON, D.C. 20009-4309

(202) 234-4433

www.nealrgross.com

1 is a good thing to implement. The problem that we
2 came up with was we didn't see a clear regulatory
3 requirement to dictate that as a need. It is a good
4 practice and --

5 MEMBER BROWN: Well, let me interrupt you
6 then.

7 MS. JOHNSTON: Okay.

8 MEMBER BROWN: How can you live with a
9 bidirectional software controlled data transmission
10 device out of a protection system out to the rest of
11 the systems if there's not a safety need? That's
12 hackable right away.

13 MS. JOHNSTON: Well, what's on the other
14 side, though? Is it --

15 MEMBER BROWN: What do you mean on the
16 other side?

17 MS. JOHNSTON: What's on the other side of
18 that connection? Like, it could be another secure
19 computer or --

20 (Simultaneous speaking.)

21 MEMBER BROWN: Let me answer. I agree
22 with you. However, it goes to a control system for
23 starting a pump. Sometimes hacks into the starting of
24 the pump and it has a virus in it. Now it's got a
25 direct path into the reactor.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1716 14th STREET, N.W., SUITE 200
WASHINGTON, D.C. 20009-4309

(202) 234-4433

www.nealrgross.com

1 MS. JOHNSTON: Okay. So --

2 MEMBER BROWN: So you can't -- every
3 system is within that boundary.

4 MS. JOHNSTON: Right. So --

5 MEMBER BROWN: It's affected. When you
6 send it out of the reactor protection system to a
7 control system, it starts safeguards, rods in, scram
8 them, whatever. If that is insecure --

9 MS. JOHNSTON: Right.

10 MEMBER BROWN: -- then you've got to
11 direct that. That's why --

12 MS. JOHNSTON: Agree that there's a
13 vulnerability there in that case. What I was trying
14 to convey was we couldn't tie that -- what you were
15 suggesting to a regulatory requirement and make it a
16 clear design requirement. However, it is a best
17 practice and it would help eliminate potential
18 failures.

19 And we would review upcoming applications
20 to make sure that they meet the single failure
21 criterion. In addition, I understand -- I'm not an
22 authority on this at all. But I understand industry
23 is standardizing their design process, using an EPRI
24 document called the digital engineering guide.

25 And that process, as I understand it,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1716 14th STREET, N.W., SUITE 200
WASHINGTON, D.C. 20009-4309

1 would take all of the requirements. So our safety
2 requirements and cyber security requirements at the
3 forefront of the design process and take that into
4 consideration. So really the onus is on the industry
5 to design and vendors to design secure systems. We
6 are seeking to clarify our guidance, clarify our
7 expectations, and memorialized the lessons learned and
8 improvements over time. So that's what we are
9 planning on doing with the planned revisions to Reg
10 Guide 1.152, the BTP 7-19, and 5.71 which is today's
11 meeting.

12 MEMBER BLEY: Well, I hope the industry
13 guidance makes this very clear. I think where we're
14 coming from is you step outside of the nuclear
15 business and you look across business applications,
16 other engineering applications, automobile, trucks,
17 ship vendors, railroads, and look at the incidents
18 that have occurred. You don't have to be very
19 creative to see that no matter how good you think
20 software control is, somebody can break through it.
21 And it's happened over and over and over again.
22 That's kind of what's driving some of us anyway.

23 MEMBER BROWN: I would amplify that a
24 little bit. Wouldn't you say there's no regulatory
25 guidance because we've asked for it.

1 (Simultaneous speaking.)

2 MEMBER BROWN: And you said no. I'm
3 saying that with a whole heart.

4 MS. JOHNSTON: Understood. Feedback
5 received. Understood.

6 MEMBER BROWN: I mean, at the starting
7 point of all this -- so I'm going to give another
8 little soliloquy here before you get to your
9 presentation. I apologize, Matt. But it's important
10 to get the information out.

11 The whole architecture approach for
12 reviewing the reactor safeguards, reactor protection
13 systems, and associated safety-related systems that we
14 started ten years ago starting with an architecture,
15 that's your focal point for defense-in-depth and
16 independence, thus the four standards that we keep
17 espousing, at least since I've been here anyway. And
18 now they're embodied in ISG, those four frameworks.
19 Control of access has been the one we have not been
20 able to get our fingers wrapped around.

21 And the object here is we're not
22 mandating. The point being was if you differentiate
23 the only cyber 7354 in your applicability and one of
24 the other paragraphs and don't separate out the stuff
25 that you can't put mitigation software in and allow

1 people -- and just you don't have dictate anything.
2 You just say if you need it one way, this is the way
3 to do it.

4 But right now, they consider they're
5 precluded. I mean, the staff seems, if we make a
6 comment, they feel it's precluded because it's not a
7 regulatory requirement to look at it. And we're not
8 trying to dictate every place that one goes. It's
9 where super safe critical systems, safeguards, and
10 reactors --

11 (Simultaneous speaking.)

12 MEMBER BLEY: I think this Reg Guide has
13 the structure to make that clear. I mean, you use the
14 word, architecture, over and over again and in ways we
15 would very much agree with. And I think within that
16 framework, this falls very neatly. We ought to let
17 them go ahead.

18 MEMBER BROWN: No, I'm going to let them
19 go ahead. I mean, however this comes out, we will be
20 writing a letter to you. Hopefully, I will be able to
21 convince my compatriots to provide some suggestions
22 that you all may accept or reject. Hopefully, you
23 will -- but they're not meant to be dictatorial.

24 They're meant to identify within the cyber
25 world that there are systems that don't have software

1 that can detect and mitigate but you can't put it in.
2 And therefore, other methods may be necessary to
3 protect those from outside sources. And this document
4 provides ways to do that. That's the thought. Okay?

5 Not trying to dictate, but this document
6 -- because it's the only one that's going to be out
7 there for a good -- you say one or two -- it's really
8 going to be four or five years. I'll make sure. I
9 will certainly make this happen in my lifetime. I
10 hope that was taken facetiously. And now I will defer
11 to my Chairman.

12 MEMBER BLEY: I'm going to do one more.

13 MEMBER BROWN: Oh, go ahead. Have at it.

14 MEMBER BLEY: Charlie's used these words
15 many times, and I don't quite see the link back in
16 here is that the Reg Guide, you just said it a second
17 ago, doesn't recognize that you can't build in virus
18 detection and mitigation within these systems. And --

19 MEMBER BROWN: Oh, no. It's not in there.

20 MEMBER BLEY: No, you've said it. You've
21 said it many times. But you were looking for that, I
22 take it.

23 MEMBER BROWN: That's what I was -- my
24 drive on this is not to dictate. My whole drive and
25 my suggestions to my -- which they're helping me, by

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1716 14th STREET, N.W., SUITE 200
WASHINGTON, D.C. 20009-4309

(202) 234-4433

www.nealrgross.com

1 the way. I come from the naval nuclear program. I
2 know how to write very specific stuff.

3 So they help me put it in a little bit
4 different framework, the commercial world. The idea
5 is to identify where, as Dennis said, what is this
6 differentiation? And it does not exist.

7 The cyber document says everything cyber
8 or nothing. It just stops right there. That's what
9 the applicability says. And there's a paragraph in
10 the discussion that says the same thing. You say that
11 people may use these processes during -- if they want
12 to do a cyber review during the design process.

13 Well, that sounds like they're doing a
14 cyber review during the design process which they're
15 not doing. At this point, that's not what they do.
16 They design a system. So thank you for illuminating
17 that, Dennis. That's what I'm -- and that's the
18 suggestions I'm going to be hoping for --

19 (Simultaneous speaking.)

20 CHAIRMAN SUNSERI: Well, I'm going to
21 interject here, though. I think it's been clear
22 guidance provided that a physical security designer
23 should take in their design considerations and build
24 security into the designs. I doubt that they are
25 ignoring that kind of philosophy here.

1 MEMBER BROWN: Oh, no. That's in there,
2 the physical security part. And --

3 (Simultaneous speaking.)

4 CHAIRMAN SUNSERI: So they're not
5 completely separate. You can do a cyber review when
6 you're doing the design.

7 MEMBER BROWN: The physical part is
8 physical. That's insider threat. And we're talking
9 about outsider threat stuff, the electric pathway.
10 You're right, 603, 1993 actually addresses control of
11 access. And it focuses on administrative controls,
12 but that's all.

13 And they focus -- they've got the
14 administrative stuff in here which is good. They talk
15 about it in both of them., but they don't do the
16 recognition of the other side of it. That's just the
17 only point I'm trying to get across.

18 MS. JOHNSTON: Understood.

19 (Simultaneous speaking.)

20 MR. BEARDSLEY: So why don't we bring up
21 the slides. I just wanted to address two points: one
22 that Member Brown made and one that Member Bley made.
23 So when he used the example of controls to pumps,
24 right now in the current fleet the system that would
25 send the controls, the pumps, the valves, all of that

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1716 14th STREET, N.W., SUITE 200
WASHINGTON, D.C. 20009-4309

(202) 234-4433

www.nealrgross.com

1 is protected by the data diode.

2 So as a collective set of systems,
3 everything is protected by the data diode from the
4 internet today. And then the point about systems that
5 you couldn't do virus protection or couldn't do those,
6 there are controls requiring those protections in the
7 cyber security requirements. If the licensee can't do
8 it, they have to analyze the control and identify in
9 their assessment how they would -- what alternates
10 they would use for protection.

11 So they have to apply protection to higher
12 systems or networks. So it's not like they don't do
13 anything. They have to do an analysis. And that's
14 one of the things that we looked at in inspection is
15 those analyses to see how they've done the protection.
16 So I just want to make sure that the public doesn't
17 think that there's nothing being done because there is
18 definitely something being done.

19 MEMBER BLEY: There is and I think we're
20 affected by things that happened 10, 12 years ago --

21 MR. BEARDSLEY: Without a doubt.

22 MEMBER BLEY: -- when we had some vendors
23 claiming they didn't need a hardware block, that they
24 could write software and nobody could get through.
25 And we had a lot of discussion. And in the end, the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1716 14th STREET, N.W., SUITE 200
WASHINGTON, D.C. 20009-4309

(202) 234-4433

www.nealrgross.com

1 put them in because that was the only way to really
2 resolve it. And we would just like to see that in
3 your language memorialized.

4 MS. JOHNSTON: Okay.

5 MEMBER BLEY: Everybody does it.

6 MS. JOHNSTON: We would certainly question
7 why a computer system -- why it wouldn't introduce
8 failures that would impact the safety function from
9 being performed. And if it had a one-way diode, that
10 would be a really simple answer. If they don't, then
11 it's opening up for a lot more questions on the
12 reliability of that design.

13 MEMBER BROWN: I can give you one example
14 in one of the last designs we looked at. There was an
15 output from the reactor protection systems and
16 safeguard controls. Both of them had a
17 unidirectional. Of course, we kind of suggested that,
18 and they agreed to do it. But then they also had it
19 feeding a network which went out to the world. And
20 that was bidirectional.

21 MS. JOHNSTON: One other --

22 MEMBER BROWN: And we -- let me just
23 finish the thought here real quick. Okay? I'm not
24 criticizing.

25 MS. JOHNSTON: No, it's okay. Go ahead.

1 MEMBER BROWN: We dug in our heels. And
2 the applicant decided that the input into the network
3 also ought to be unidirectional, hardware-based which
4 was the right way to do it just to provide that second
5 barrier. But when you're doing it without some
6 mention of this differentiation between the types of
7 systems, what you can do and can't do, I understand
8 your point about everybody is protecting their control
9 systems.

10 Nothing can come in to them. They've got
11 a data diode there so it can do it. But a lot of
12 those vendors think it'd be great to sit back in their
13 place and send new software updates to their control
14 system because they found an error and they can send
15 it via the internet and all the way down into the
16 system and right into the -- that's just great, isn't
17 it? You really ought to be coming in and opening up
18 your cabinet and downloading it.

19 MR. BEARDSLEY: And they wouldn't be able
20 to do that with the current regulations in there.

21 MEMBER BROWN: Anyway, go ahead. Let's go
22 ahead --

23 (Simultaneous speaking.)

24 MR. BEARDSLEY: One other question.

25 MEMBER BROWN: -- do her thing.

1 MEMBER BIER: Yeah, I guess the one other
2 --

3 MEMBER BROWN: I'm sorry, Vicky.

4 MEMBER BIER: -- comment that I would add
5 that's come up in some of the previous discussions is
6 that handling at the inspection stage is kind of late
7 if a plant has already has been built, assuming a
8 different solution. So --

9 MEMBER BROWN: That's correct. We had
10 made that point before.

11 MR. BEARDSLEY: Okay, okay. At this
12 point, we'll turn it over to Kim Lawson-Jenkins who
13 will provide the update on Regulatory Guide 5.71,
14 Revision 1.

15 MEMBER BROWN: We have time, right? If
16 we're quiet during the slide presentations. That's
17 probably wishful thinking. Kim, go ahead.

18 MS. LAWSON-JENKINS: Yes, thank you.

19 MEMBER BROWN: Thank you.

20 MS. LAWSON-JENKINS: My colleague, Michael
21 Brown, will be advancing the slide for me. Thank you
22 very much for this opportunity to present on
23 Regulatory Guide 5.71, Revision 1, the draft guidance
24 that we're hoping to get out for public comment soon.
25 The Regulatory Guide is an acceptable implementation

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1716 14th STREET, N.W., SUITE 200
WASHINGTON, D.C. 20009-4309

(202) 234-4433

www.nealrgross.com

1 of Title 10, Code of Federal Regulation Part 7354.
2 That regulation was made effective in 2009, and the
3 original version of Regulatory Guide 5.71 was
4 introduced -- issued in 2010.

5 The cyber security rule which is what we
6 call -- generically call 7354 protects computers,
7 equipment, and systems that affects safety, important
8 to safety, security, and emergency preparedness
9 functions. That's what the rule says. So this is one
10 implementation that we found acceptable for
11 implementing that rule. Next slide, please.

12 Okay. When I was asked to give this
13 presentation today, there were three things that I was
14 directed to doing this. Number one was discuss the
15 summary of the changes in Reg Guide 5.71 over the last
16 ten years. Number two was to discuss any changes to
17 the guide based on the EDO direction earlier this
18 year. And number three, any changes that we made
19 since the subcommittee meeting just this past October.

20 The first two items with what I presented
21 in October, just a subset of the slides. And we'll
22 talk about number three. Some of these things you've
23 actually discussed already before the presentation.
24 But we can still elaborate on them. Okay.

25 There was an -- the draft guidance was

1 originally revised in 2018. And we actually issued
2 that, put that out for public comment. The main
3 purposes of that was to clarify the regulations based
4 on lessons learned through the first set of
5 inspections we -- cyber security inspections we did
6 from 2013 to 2015.

7 As Jim mentioned, we only had one new
8 regulation which had to do with cyber security event
9 notification. Between the original version of 5.71
10 and the draft version we put out, NIST Special Product
11 853, had a new revision of the security controls for
12 federal systems. So we updated the slides based on
13 some of the changes in there.

14 And shortly after, the cyber security rule
15 was issued and also the guidance was issued. The
16 Commission gave direction on how to handle balance of
17 plant equipment at nuclear facilities. And that
18 version of the draft guidance updated content based on
19 that.

20 Also, yes, I want to mention that there
21 was IAEA security guidance that was issued in 2011.
22 So we noted that also and picked up a few of the best
23 practices that was in the IAEA document. The work on
24 the draft guidance was delayed for two years because
25 we were approaching the new set of inspections that we

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1716 14th STREET, N.W., SUITE 200
WASHINGTON, D.C. 20009-4309

(202) 234-4433

www.nealrgross.com

1 were going to implement.

2 So there was a decision made to wait until
3 we completed those new set of cyber inspections. The
4 post-assessment work we did on how we did the program
5 in general and also industry as Jim mentioned had a
6 lot of lessons learned from their implementation of
7 their program and the inspections that they wanted to
8 get done. So everyone thought it was desirable to
9 wait for issuing this guidance. Next slide, please.
10 Mike, next slide. Okay, thank you.

11 So once we made the decision to delay
12 issuing this guide, we actually started on some new
13 updates. That gave us more time to do more things.
14 At that point, a lot of the guidance for cyber
15 security -- not just international guidance -- but if
16 you look at the NIST guidance, it's definitely focused
17 more on risk informed cyber security. And we picked
18 up that information.

19 There was some discussion earlier about
20 some things that we've seen. I think someone else has
21 to go on mute. Thank you. There was, what areas did
22 we see multiple findings? Okay. And one was the need
23 to have more accurate information about the equipment
24 that the licensees have at their plant, specifically
25 the critical digital assets that as we said could

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1716 14th STREET, N.W., SUITE 200
WASHINGTON, D.C. 20009-4309

(202) 234-4433

www.nealrgross.com

1 affect safety, importance of safety, security, and
2 emergency preparedness functions.

3 New international standards and guidance
4 were issued. And also another version of a NIST cyber
5 security document was issued. So we picked up any
6 applicable changes for that.

7 And of course we addressed any public
8 comments that we received in the -- when we issued the
9 document for public comment in 2010. I would like to
10 say I shared those public comments with -- as a
11 package with the subcommittee. And as I mentioned
12 then in the presentation, a lot of the really useful
13 information that we received was from vendors who had
14 questions about how to implement things in their
15 design. Okay.

16 So they are very much interested in this
17 document. Even though the regulation and it's based
18 on operating plants, the bottom line is that the
19 licensees rely on technical requirements that are
20 implemented by the equipment. Okay. So people who
21 manufacture security equipment, people who manufacture
22 safety equipment but they want it to be secure,
23 they're looking at that information that comes in the
24 guidance.

25 And the licensees and the applicants are

1 going to rely on the equipment to implement some of
2 these requirements. There's two ways when you're
3 doing cyber security or any kind of security. Either
4 the equipment itself can have security functions which
5 you just turn on and start using, or you're going to
6 have to put something in the environment where the
7 equipment is operating to give you that security that
8 you need.

9 So just because the guidance is for
10 operating plants, the safety functions don't just
11 happen in a vacuum. They rely on this information
12 that's coming out of the guidance. And that's why we
13 really want to get this out in the public sphere very
14 soon.

15 MEMBER HALNON: So Kim, this is Greg
16 Halnon. The licensees will rely on the equipment to
17 do the job. But if it's found that they don't do the
18 job, the violation goes to the licensee, not --

19 MS. LAWSON-JENKINS: Absolutely.

20 MEMBER HALNON: Unless it's a Part 21
21 issue. So this is subject to Part 21 too. And so the
22 licensee still -- I mean, I just want to make a point.
23 They need --

24 MS. LAWSON-JENKINS: That is true.

25 MEMBER HALNON: -- to understand it, need

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1716 14th STREET, N.W., SUITE 200
WASHINGTON, D.C. 20009-4309

1 to make sure and do the validation and require the
2 vendors do the equipment --

3 MS. LAWSON-JENKINS: Right. Which is
4 absolutely --

5 MEMBER HALNON: -- in the right way.

6 (Simultaneous speaking.)

7 MS. LAWSON-JENKINS: We put this
8 information in the guidance that the licensees have to
9 understand the functions, not just actually the safety
10 functions but the security functions and to use those
11 appropriately. And my colleague, Mike Brown, who's
12 advancing the slide, one of the areas that he's
13 working in is supply chain because no one knows the
14 equipment like the company that manufactures it. They
15 will know the vulnerabilities if there are any there,
16 even though you have researchers always trying to find
17 that too. Okay.

18 They will know the best way to fix those
19 vulnerabilities. Okay. And they are the best people
20 to know how to secure the device. So the licensees
21 and the applicants must, must have a lot of
22 communication with the vendors to adequately protect
23 their plant and equipment. And the guidance does
24 encourage that communication that it's clear now that
25 they have to communicate and know what's in their

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1716 14th STREET, N.W., SUITE 200
WASHINGTON, D.C. 20009-4309

(202) 234-4433

www.nealrgross.com

1 plant. Next slide. Thank you. Next slide, Mike.

2 Okay. So as you can imagine after ten
3 years for cyber security, there were quite a few
4 changes in the Reg Guide. And this page I'll mention
5 very briefly one and then we'll go into more detail
6 about each section. Please again if someone else is
7 not on -- on speaking, please go on mute. Thank you.

8 Okay. So Section C is the staff
9 regulatory position. Okay. So some of the
10 information that we gave for clarifying is to add text
11 for risk informed cyber security. We added the
12 information that I spoke to earlier about balance of
13 plant identification of those assets.

14 We added decision points in the text --
15 diagrams and text for identifying CDAs as was
16 mentioned before the presentation that the licensees
17 and the NRC got a lot more experience in identifying
18 which assets really do affect safety and security and
19 emergency preparedness functions. We updated text on
20 defense-in-depth protective strategies. This is
21 really important because there definitely has been
22 some confusion on what defense-in-depth is, and we'll
23 talk about that as we move along in the slides. But
24 to clarify -- yes?

25 MEMBER BROWN: Without -- you don't have

1 to change the slides. Just the first item on there,
2 just -- and I don't remember clearly. I thought I
3 looked for this when I was muted. You added -- I
4 remember reading the risk informed cyber security text
5 that you went through.

6 And I don't disagree that there's a wide
7 range of stuff. Some things you add that I really
8 don't care. Some stuff, yeah, a little bit but not as
9 much. You think a risk not doing any, that's fine.

10 But there's a category of stuff like
11 reactor safety stuff that's really not amendable to a
12 risk assessment. It has to work. You don't kind of
13 -- it can't kind of work. It can't kind of trip the
14 reactor. It can't sort of start a pump. It's got to
15 start all of it or the required amount of it.

16 I would suggest that you think about
17 identifying there's classes of equipment where risk
18 doesn't really work toward. And I'm not quite -- I'm
19 not trying how to tell you how to do that. But there
20 certainly are.

21 I would hate to see the reactor scram
22 system say, we're going to do a risk assessment of
23 that, whether -- how do you do that? And if you got
24 a better answer than I do, fine.. I just didn't
25 understand how we apply that.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1716 14th STREET, N.W., SUITE 200
WASHINGTON, D.C. 20009-4309

(202) 234-4433

www.nealrgross.com

1 MEMBER BLEY: Yeah, I'm a little concerned

2 --

3 (Simultaneous speaking.)

4 MEMBER BLEY: -- that you're giving such
5 advice to this staff --

6 (Laughter.)

7 MEMBER BROWN: That's all right.

8 MEMBER BLEY: -- because you do a risk
9 assessment isn't the reason why reactor scram should
10 sometime fail. It might. Risk assessments try to
11 acknowledge that and understand the impacts of it.
12 It's designed to work. It ought to work. But the
13 risk assessment has nothing to do with building
14 something into a system that lets it fail. That's a
15 bad concept.

16 MEMBER BROWN: But that wasn't the way I
17 read the stuff that I read.

18 MEMBER BLEY: That's what it sounded like.

19 MEMBER BROWN: But that's -- I'm
20 remembering -- again, it's been two months since I
21 read this. So --

22 MS. LAWSON-JENKINS: We're actually going
23 to have a slide on this informed security.

24 (Simultaneous speaking.)

25 MEMBER BROWN: Okay. All right. That's

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1716 14th STREET, N.W., SUITE 200
WASHINGTON, D.C. 20009-4309

1 good. Go ahead, Kim. Thank you.

2 MEMBER BLEY: Hey, Kim. Let me ask you a
3 quick question. And this is for my own edification
4 and you didn't do it. It seems as if the staff has
5 changed the structure of the Reg Guides.

6 And now C-3 are the regulatory positions.
7 But as in your guide, you never use that phrase. And
8 somebody else's guide that we got recently, they did
9 the same thing except they kept referring to
10 Regulatory Position No. 1 and No. 2 which got very
11 confusing because they weren't defining the section.
12 If anybody knows what's going on, I'd just be
13 interested in why we've changed the format.

14 MR. BEARDSLEY: Well, I think one of the
15 big points with the Regulatory Guide 5.71 is it
16 provides a template for a cyber security plan which is
17 where the meat of the licensee's commitment comes.
18 And so when we say regulatory position, those are the
19 requirements the licensee has to meet in their cyber
20 security plans. There's another Reg Guide that
21 doesn't provide that same structure, may put them in
22 a different place. I can't answer your question
23 explicitly. But that is why we did it this way in our
24 Reg Guide.

25 MEMBER BLEY: Okay. But you don't call

1 them regulatory positions in this Reg Guide. You
2 never mentioned that --

3 (Simultaneous speaking.)

4 MR. BEARDSLEY: We do not. We call them
5 licensee requirements.

6 MEMBER BLEY: Yeah, but it's perfectly
7 clear. Okay. There's no real answer.

8 MS. LAWSON-JENKINS: And I have to admit
9 I did not change the structure of the original
10 guidance because I didn't want to get to the space of
11 backfit. Okay. So there might've been some better
12 way of restructuring the guide. But especially on a
13 topic as expansive and comprehensive as cyber
14 security, I really didn't want -- I wanted to be clear
15 what we changed and why rather than restructure --

16 MEMBER BROWN: This is the same as --

17 MS. LAWSON-JENKINS: -- the whole
18 document.

19 MEMBER BROWN: -- rev 0 is what you're
20 saying --

21 (Simultaneous speaking.)

22 MS. LAWSON-JENKINS: Yes, compared to rev
23 0.

24 MEMBER BROWN: -- which was a good idea.

25 MS. LAWSON-JENKINS: So it made clear what

1 we --

2 MEMBER BROWN: I understand that.

3 MS. LAWSON-JENKINS: -- change and why.
4 But I did not restructure. If any of the guys changed
5 in the future, that was fine. But I really want to be
6 clear on what we did and why.

7 MEMBER BLEY: Okay. I wasn't implying
8 that. I was just curious about what was going on
9 across this. It's irrelevant to your presentation.
10 Your structure is great.

11 MS. LAWSON-JENKINS: Okay. Thank you.
12 We'll talk again about defensive architecture and why
13 we have what we have in there. And like I said, we'll
14 have more details about that when we get to the slide.
15 We updated text regarding the use of alternate
16 controls because, as I said, the guidance we have in
17 here is one acceptable way of doing it.

18 Many times, licensees decided not to use
19 certain controls that we suggested. And we wanted to
20 clarify when that was appropriate, what kind of
21 evidence they needed to show that what they did was
22 sufficient. We updated text to clarify the use of a
23 consequence-based graded approach in applying security
24 controls.

25 And I think this is tied to that first

1 point that everyone was worried about risk informed
2 cyber security. I guess the best way to try to
3 explain this is that people do have to understand what
4 they're doing and why and what risk is associated with
5 it. If you need something that want to have very
6 little or no risk, you will just find that
7 accordingly. You will.

8 But you have to look at the problem. A
9 lot of times, people have no idea of the unknown or
10 what they don't cover and things like that. And part
11 of this risk informed cyber security is acknowledging
12 what you're doing, why you're doing, saying what you
13 do know, and how you're going to adjust when new
14 things come along and on things you don't know. Okay.

15 So just because you're doing cyber
16 informed -- risk informed cyber security, I'm saying
17 you apply risk to everything. And in actuality, in a
18 way, you do. You're just saying, we aren't going to
19 accept any risk on certain areas. And you have to
20 protect those things accordingly. Okay.

21 And that's what we're doing here when we
22 say what controls you apply. But the first step is to
23 identify what's important and why you can or cannot
24 tolerate a certain amount of risk. And that is
25 absolutely critical.

1 And the last point on this slide is to
2 talk about the technical controls that can be
3 incorporated using the design certification. And also
4 the updates we did based on the cyber event
5 notification rule. Okay. So we'll talk about, like
6 I said, a lot of these things in detail. We have
7 slides for every one of these items. Next slide,
8 Mike. Thank you.

9 Okay. So we added a reference which is
10 actually based on some of the comments we had to the
11 sections of Reg Guide 1.152. Like I said, we'll have
12 a slide on that, Revision 3. We added many more
13 examples of continuance monitoring which is really one
14 of those lessons learned that's crucial over the past
15 ten years.

16 You don't implement controls, you don't
17 implement a plan and say I'm good. I don't have to
18 worrying about it anymore. You have to make sure
19 those controls are in place and they are working as
20 intended. And you have to understand in your system
21 when you start seeing new things. We gave a proposal,
22 introduce text to say how and the way of licensees
23 using metrics to measure how effective their analysis
24 of this system is.

25 As I said, we added a lot of text

1 regarding how licensees could have quality CDA
2 assessments. We'll talk a bit more about that when we
3 get to the slide. One of the reasons we had more
4 pages in the updates -- the updated document for 5.71
5 is we added clarification for every security control
6 in Appendix B and C saying why these controls are
7 needed, the purpose of them so then the licensees
8 could understand if they wanted to substitute, use a
9 different control, how those new controls were meeting
10 the intent of the original control that we
11 recommended.

12 We added new terms and definitions in the
13 glossary. Like I said, we learned a lot over the last
14 ten years, not just the Nuclear Regulatory Commission
15 by cyber security professionals in general. We
16 clearly updated the references. And throughout the
17 document, we had lots of editorial changes based on
18 public comments, OGC comments, and peer reviews.

19 MEMBER BLEY: Kim?

20 MS. LAWSON-JENKINS: Yes.

21 MEMBER BLEY: It's Dennis Bley. I'm
22 curious as to what kind of response you've gotten back
23 from the licensees. Are they appreciating the added
24 detail you've provided?

25 MS. LAWSON-JENKINS: I think it's going to

1 be one of those it depends. Well, first of all, we
2 haven't gotten this out for public comment yet. So
3 once we get it out for public comment -- once we get
4 it out for public comment, the industry will have an
5 opportunity to give input officially.

6 The input we got when we tried to put it
7 two years ago in 2018 was that you need to wait. So
8 we finished the assessments. And then also we wanted
9 to finish the inspections and it would be a better
10 time to do this. So it was more, we need to wait.
11 That was the main input and plus risk informed
12 security. Okay. But mainly to wait.

13 MR. BEARDSLEY: Industry has seen the
14 document, both in 2018 and after release of last
15 summer. But there has not been a formal public
16 comment process for them to provide us feedback.

17 MS. LAWSON-JENKINS: Right. But they will
18 have an opportunity. We will have -- we hope to have
19 two public meetings on this document when we do issue
20 it for public comment. Okay. Next slide, Mike.
21 Thank you.

22 Okay. So this was the slide that I had on
23 risk informed cyber security. And as I said, it's a
24 way of categorizing and to understand what is
25 important -- what is important at the plant as far as

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1716 14th STREET, N.W., SUITE 200
WASHINGTON, D.C. 20009-4309

1 facility functions including the identification of
2 SSEP functions, threats to the facility, the
3 specification of requirements which will include the
4 cyber security program. The program usually consists
5 of a plan.

6 That's what we implement -- they usually
7 implement based on a plan and the defensive
8 architecture and the defense-in-depth methodology that
9 they use. They will use -- if they want to use a
10 graded approach, they could look at seeing where in
11 the security architecture they put the most
12 protections and place those devices in that logical
13 boundary where those devices are protected. And this
14 is what was relatively new that we wanted to clarify
15 for risk informed security. There has to be some kind
16 of validation and verification of the implementation
17 of that program.

18 Okay. Like I said, it isn't just a matter
19 of implementing it, thinking everything is working or
20 saying the first time it worked and never doing
21 anything else with it. You have to show that you are
22 protecting the right things, that you can react if
23 something changes, that when new threats come along to
24 be able to say based on your program how you're going
25 to deal with that. It's really ongoing, continuous

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1716 14th STREET, N.W., SUITE 200
WASHINGTON, D.C. 20009-4309

(202) 234-4433

www.nealrgross.com

1 monitoring of your system so that it is not a one
2 time done thing, after inspections, we don't have to
3 worry about it.

4 MEMBER HALNON: So Kim, back to a question
5 I had earlier, how do you physically do that? Do you
6 have the ability to -- or do licensees have the
7 ability to inject a cyber threat and watch their
8 systems defend against it? Or --

9 (Simultaneous speaking.)

10 MS. LAWSON-JENKINS: They can use -- they
11 can -- there's several things, first of all. Right
12 now, they do have outages when they do bring down
13 equipment to make updates and changes to the system.
14 So there is some testing.

15 If they wanted to, they could -- this is
16 an example. It isn't a requirement, but it's an
17 example, okay, that they can do things that way. They
18 can have simulations of those systems because they
19 have to verify it when they make certain changes to
20 the systems that they aren't changing the security
21 posture of it. Okay.

22 So many more licensees are moving to being
23 able to model the effect of their systems. And that's
24 one area that I know I've been working on lately in
25 some of the standards groups to understand what goes

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1716 14th STREET, N.W., SUITE 200
WASHINGTON, D.C. 20009-4309

1 into a very good security model, okay, things like
2 that. But the main issue -- the main -- the important
3 points, I think, to understand this is that they
4 really must understand what they have at their plant
5 because in a way you have to think the best analogy is
6 that they have to think like attackers these days.
7 Okay.

8 The attacker when you get malware, it'll
9 come on to your system and it'll see what's there.
10 That's the way malware works. It sees what's there.
11 Okay. And then once it sees what's there, it sees
12 what it can speak to, talk to, what it can do. And
13 then it may propagate itself through the network.
14 That's a very simple over-generalization of what
15 malware can do. Okay.

16 (Simultaneous speaking.)

17 MEMBER HALNON: And I guess I'm just
18 curious --

19 MS. LAWSON-JENKINS: No, let me make this
20 -- this is an important point. I always tell the
21 licensees that the malware, a potential malware should
22 not ever, ever know more about your system than you
23 know about it. Okay. So if they understand their
24 system well, they can pretty much start modeling and
25 explaining why their system will operate and be able

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1716 14th STREET, N.W., SUITE 200
WASHINGTON, D.C. 20009-4309

(202) 234-4433

www.nealrgross.com

1 to respond adequately to any kind of problems.

2 MEMBER HALNON: Well, just the validation
3 and verification, and maybe it's something for future
4 research to figure out benign -- being able to inject
5 a benign malware or something and see how far it gets
6 or something to that effect.

7 (Simultaneous speaking.)

8 MS. LAWSON-JENKINS: Okay. Please don't
9 confuse those two things. I did not say inject
10 malware in your system to figure out that it works.
11 That is not what I said.

12 MEMBER HALNON: It comes down to is it
13 just a paper exercise or is it something that you're
14 -- a validation and verification makes it feels like
15 there's something physically you're going after and
16 trying to do.

17 MS. LAWSON-JENKINS: But you have to do
18 this all the time in network development where you
19 develop systems. You have to -- you cannot always
20 test -- especially you cannot always physically test
21 what you're using. Times have really changed.

22 You have to be able to model and simulate
23 and test input and output before you actually build
24 the devices. That's how -- I've been in development.
25 That's how you have to do it if you want to get things

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1716 14th STREET, N.W., SUITE 200
WASHINGTON, D.C. 20009-4309

(202) 234-4433

www.nealrgross.com

1 in a timely manner and still have a secure and
2 efficient system.

3 MEMBER HALNON: I agree. But the design
4 is static. I mean, it's done. Go install it in the
5 plant, then it becomes a head exercise after that.
6 But we can move on. Just --

7 (Simultaneous speaking.)

8 MS. LAWSON-JENKINS: Okay. But you can
9 use -- if something is not operational, you can use a
10 scan to verify what's going -- how your system -- your
11 equipment is operating before you restore it to in
12 use. So there are ways of testing and making sure
13 that the configuration hasn't changed, that nothing is
14 there that shouldn't be there. So as I said, when you
15 have outages, those are the perfect times to do some
16 of this verification and validation that you cannot do
17 when the system is online.

18 MEMBER HALNON: On some systems. There's
19 a lot of systems that we're talking about here.

20 MS. LAWSON-JENKINS: I know.

21 MEMBER HALNON: It's a tremendous amount
22 of work to add to an outage.

23 MS. LAWSON-JENKINS: Which is why you need
24 to know what's important and do the consequence-based
25 analysis on it. You can't look at everything. You

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1716 14th STREET, N.W., SUITE 200
WASHINGTON, D.C. 20009-4309

(202) 234-4433

www.nealrgross.com

1 can't. So you have to focus on what's important and
2 know why it's important and --

3 (Simultaneous speaking.)

4 MEMBER HALNON: It feels like the design
5 organization would be bigger than the regular physical
6 security organization.

7 MS. LAWSON-JENKINS: Next slide, please.

8 MEMBER BLEY: Well, it's got its finger
9 ins everything. So maybe that's not the wrong
10 approach.

11 MS. LAWSON-JENKINS: I will get to talking
12 about our resources, things at the end. I am going to
13 briefly mention that. But I'll go on with this next
14 slide, though, balance of plant. Okay. So we did
15 introduce information about balance of plant
16 equipment.

17 There's going to be updated guidance from
18 the industry on how they're classifying --
19 identifying, classifying, and protecting balance of
20 plant equipment. Okay. But in our guidance, we
21 mention an identification function for the equipment.
22 The balance of plant equipment has to be listed there
23 when you're deciding on what to protect.

24 Now keep in mind this is not an either/or.
25 Okay. Because if you look earlier in number 3, if the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1716 14th STREET, N.W., SUITE 200
WASHINGTON, D.C. 20009-4309

(202) 234-4433

www.nealrgross.com

1 equipment provides a pathway to a critical digital
2 system or a Critical Digital Asset, then it's a CDA.
3 Okay. It really doesn't matter what else you do.

4 If you keep going, it's going to be a CDA
5 if it provides a pathway. Okay. But they have to --
6 you have to look at all these things at some point,
7 not just one. So you don't just say balance of plant
8 and we don't care what it does in the system and what
9 it speaks to and things like that. It's one of the
10 considerations but not everything. Next slide,
11 please.

12 Okay. For the identification of Critical
13 Digital Assets, we made a few changes to this slide.
14 Number one is, does the system contain any digital
15 components from the software? That wasn't in the
16 original slide.

17 We, again, added information about BOP.
18 And then the text, we talked more about whether this
19 device protects other critical groups of assets. The
20 diamond was there before. But we actually explain in
21 a lot of text that spoke on that point.

22 Because as I mentioned earlier in the
23 presentation that either the device itself can have
24 security functions or you can add a device to the
25 system in the environment where the equipment is

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1716 14th STREET, N.W., SUITE 200
WASHINGTON, D.C. 20009-4309

(202) 234-4433

www.nealrgross.com

1 operating and have it protect the device. And there
2 was some debate or discussion with industry. And it
3 was a little too early when we spoke about the kiosk,
4 okay, whether or not that was a Critical Digital
5 Asset.

6 From my point of view, it would've been.
7 But industry elected a lot to do that in the way they
8 implemented their program. That's fine, well, and
9 good. But I remember we had the discussion that it
10 had to be protected at the same level as the device is
11 protecting.

12 It made no sense to have it provide a
13 protective function and it's not the same level that
14 totally invalidates your defense of architecture,
15 where you have the most critical things being
16 protected. And also I raise the point and industry
17 understands that if that device is protecting multiple
18 Critical Digital Assets, it's actually a higher value
19 asset because the impact if something happens to it is
20 greater than if only one device fails. So like I
21 said, there's been a lot of discussion with industry
22 and going back and forth on what is a Critical Digital
23 Asset.

24 And regardless of what you call it, we do
25 this because we're humans. Okay? We can write

1 programs. We can write procedures that say if
2 something is a Critical Digital Asset, this is how you
3 treat it.

4 At the end of the day, the attacker
5 doesn't care. They really don't care how we label
6 these devices. They're going to only go about what it
7 does, okay, and how they can affect it.

8 So we have to use this information wisely.
9 Okay. And I saw, well, because it's not a CDA, we
10 don't have to protect it. It's what it does and what
11 its communication that it's supporting. And that's
12 what's reflected in this new text. Next slide,
13 please. Okay.

14 Defense-in-depth protective strategies,
15 that the strategies should employ multiple, diverse,
16 and mutually supported tools, technologies, and
17 processes to effectively perform timely detection of,
18 protection against, and response to a cyber attack.
19 That is a lot in one sentence. It is a lot. But
20 that's why defense-in-depth for security, especially
21 cyber security, is not one or two things that they
22 must do to meet that defense-in-depth requirement.
23 Okay.

24 MEMBER BLEY: I'm just curious if you
25 played your definition of defense-in-depth against the

1 NUREG. I forgot what they called that new set of
2 general ones. I think it's No. 5 or 9 on defense-in-
3 depth.

4 MS. LAWSON-JENKINS: Oh, is this physical
5 security? Or what are we referring to here?

6 MEMBER BLEY: The term, defense-in-depth,
7 and what it means.

8 MS. LAWSON-JENKINS: No, no. I mean, what
9 document are you citing?

10 MEMBER BLEY: I'll tell your colleagues
11 here before they leave.

12 MS. LAWSON-JENKINS: Okay, okay.

13 MEMBER BLEY: I just have to look up the
14 title.

15 MS. LAWSON-JENKINS: Okay. Well, for --
16 (Simultaneous speaking.)

17 MEMBER BLEY: No, it's just one of the
18 general NUREGs.

19 MS. LAWSON-JENKINS: Okay. For Reg Guide
20 5.71, to meet the cyber security rule, when someone
21 receives a violation of defense-in -- based on
22 implementing defense-in-depth, this is what we mean
23 because it's really important. And I could give
24 multiple examples of this as we go through the
25 presentation. Clearly for software, you can't have

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1716 14th STREET, N.W., SUITE 200
WASHINGTON, D.C. 20009-4309

(202) 234-4433

www.nealrgross.com

1 the same software everywhere. Okay.

2 If you have on vulnerability, and you just
3 mentioned that on some systems you may not want to be
4 updating all the time. That's going to play into the
5 decision, well, maybe you need to use a different type
6 of software or technology there. That's something
7 they -- and that's why, yes, the decision needs to be
8 made before you install the equipment.

9 Sometimes we say, as you've seen in
10 Appendix B and C, there's lots of cyber security
11 controls that you can install. And sometimes a
12 licensee will say, we'll need to install of these. We
13 can do a few.

14 And maybe based on the analysis they can.
15 But as I said, we add lots of information about why a
16 control is there. Okay. And a lot of times, you have
17 these overlapping things to protect if one of the
18 controls fails. So there's a lot involved in this.

19 But like I said, and this is just one
20 sentence. We didn't include all of the text. But
21 clearly, we have a lot of information about what
22 defense-in-depth means as far as the cyber security
23 requirement. Next slide, please.

24 Okay. Protecting SSEP function, that
25 comes straight from the cyber security rule, 10 CFR

1 73.54. The rule says to protect the function. So
2 once again, if someone could go on mute, that would
3 help a lot.

4 The functions that are the most important
5 are the safety and security functions. And that
6 clearly if you're placing those in the defense of
7 architecture where you have more security as you go
8 into the architecture, you're going to place those at
9 the highest level. So the point being made before
10 where you want to have very little risk -- very little
11 interaction with outside systems where you're going to
12 care about those things, you're going to place those
13 devices at the highest security level in your
14 architecture.

15 A function can be implemented by one or
16 more systems. And as I said, the system allocation to
17 a security level is dependent on the safety or
18 security significance of that function. So using risk
19 informed doesn't mean you're allowed to introduce more
20 risk into the system.

21 At least it just makes sure that you
22 actually looked at it. And you're making decisions
23 based on knowledge of your equipment, knowledge of the
24 plant functions. And you're placing them at the
25 appropriate part in your defense of architecture.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1716 14th STREET, N.W., SUITE 200
WASHINGTON, D.C. 20009-4309

(202) 234-4433

www.nealrgross.com

1 Next slide, please.

2 Initiation of communication from access
3 from a lower security level to a higher security
4 level, if you have that communication, to be done on
5 a deny all and permit by exception basis with the
6 exceptions supported complete justification and
7 security risk analysis. I can't speak to plants. I'm
8 not going to speak specifically to plants that have
9 been built 30 years ago.

10 And there's some systems in those plants
11 that are never touched. There are a few of those that
12 are never touched. All you do is just received
13 information from it. You don't even do configuration
14 changes. Okay.

15 Most systems now have software running in
16 it. It may be a little bit, they have software
17 running. And you have to be able to make changes to
18 that software.

19 Sometimes they're configuration changes.
20 Sometimes it's a vulnerability that's there. And
21 based on how you designed your system, you may
22 decided, I don't need to address that vulnerability,
23 if you don't have any kind of connections to it.

24 But by being in a system -- in the
25 communication systems, it's communicating. And this

1 is where Member Brown and we are in agreement that you
2 have to tightly control the communication. So it has
3 to be decided if there's no communication coming in at
4 all ever, okay, then you don't have to have that
5 exception.

6 But on things -- if you have several
7 security levels and all your security vulnerability
8 updates come from a different system that will not be
9 at that same level, you have to have some way of
10 performing those updates. I mean, that's a
11 requirement of your cyber security plan. And this was
12 a mechanism to let them do that. Do we have any
13 questions on this one, because we had quite a bit of
14 discussion on this at the subcommittee meeting?

15 MEMBER BLEY: No, but I want to go back
16 and remind you that the document I was talking about
17 is NUREG/KM, that's Knowledge Management, 0009, which
18 is a historical review and observations of defense-in-
19 depth. It was done several years ago because almost
20 everything around NRC had a different definition of
21 defense-in-depth. And they were trying to pull it all
22 together. So I hope you can fit yours within this or
23 get somebody to reconcile things because it's been so
24 confusing over the years. It's good to have it
25 clarified.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1716 14th STREET, N.W., SUITE 200
WASHINGTON, D.C. 20009-4309

1 MS. LAWSON-JENKINS: Okay. I will look at
2 that document. If it hasn't been updated for several
3 years, I won't claim that this -- the definition we
4 currently have now is going to be in there. But I
5 know the definition we have now is very similar if not
6 the same as what defense-in-depth is for the NIST 882
7 which is for industrial control systems. Okay.

8 So they do the same thing saying you have
9 multiple overlapping controls so that if one control
10 fails, you won't have a problem. If you have a
11 vulnerability that has to be addresses in one area,
12 you have diversity that will help with that. So I
13 will look at that.

14 But for the cyber security plan -- and I
15 can understand wanting to have a one size fit all or
16 an inclusive definition. And we can see if the other
17 document possibly could be updated. Be we are in
18 alignment with what NIST says. We're in alignment
19 with the international standards on this also for
20 security.

21 MEMBER BLEY: I guess if it ends up
22 they're separate, I hope you would call it cyber
23 security defense-in-depth to clarify --

24 MS. LAWSON-JENKINS: Okay. That's --

25 (Simultaneous speaking.)

1 MEMBER BLEY: -- because the rest of this
2 agency tried to pull all of their definitions together
3 through this document.

4 MS. LAWSON-JENKINS: Fair enough. I
5 understand the comment. Can you, one more time -- I'm
6 sorry. I know there'll be a transcript of this. Can
7 you repeat the document number again for me, please?

8 MR. BEARDSLEY: I have it, Kim. I'm
9 sending it to you in a message.

10 MS. LAWSON-JENKINS: Okay. Thank you.
11 Okay. Next slide, please.

12 MEMBER BROWN: Nope, nope, nope, nope.
13 You said we had considerable discussion on this issue
14 before in the last meeting. We made the comment in
15 rev 0, this bullet completely prohibited communication
16 from assets at lower to higher levels. And so we made
17 the comment this would require basic communication
18 therefore to be bidirectional and software configured
19 so that you could permission by exception and then
20 execute whatever you wanted to with software commands.

21 And the way it was written could be to
22 apply protection, safeguard controls. And so you
23 could have access to anything with this deny all,
24 permit by exception communication from lower to
25 higher. I believe it was you, or maybe it was one of

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1716 14th STREET, N.W., SUITE 200
WASHINGTON, D.C. 20009-4309

(202) 234-4433

www.nealrgross.com

1 the other people talking, went through a considerable
2 discussion about kiosks and other type set ups that
3 you had.

4 And I don't remember all the details. It
5 wasn't elaborated. But you all commented that no, no,
6 no, no, it was not meant to apply, and that you all
7 were going to clarify -- it was only supposed to apply
8 to some specific circumstances and not as we had
9 perceived. I wasn't the only one that made this
10 comment. I think Dave --

11 MS. LAWSON-JENKINS: We haven't gotten to
12 that discussion point yet.

13 MEMBER BROWN: Oh, we haven't? Okay.

14 MS. LAWSON-JENKINS: No.

15 MEMBER BROWN: I just saw it, so --

16 MS. LAWSON-JENKINS: I know. Two more
17 slides, okay? Because I'm --

18 (Simultaneous speaking.)

19 MS. LAWSON-JENKINS: -- going through the
20 slides.

21 MEMBER BROWN: Are you going to do
22 something about that? Is that the point? Okay. All
23 right. Oh, okay. Got it. All right. Thank you. Go
24 ahead, Kim. I'm sorry.

25 MS. LAWSON-JENKINS: No, no, it's fine.

1 I want to make sure we address every issue. Honestly,
2 I really want to do that. Minimizing the attack
3 surfaces and pathways, that for defense of
4 architecture, this is -- I only want to say this is a
5 best practice.

6 This is almost a requirement because it
7 goes into understanding what you have on that system
8 and understanding why it's there and so that services
9 and protocols cannot be used against you as an attack
10 factor or some vulnerability. So the licensees and
11 applicants should remove applications, services,
12 protocols that are not necessary to support the design
13 basis functions and for the CDA. Basically, you
14 eliminate things. You reduce the attack surface.

15 And as I kind of mentioned before, you use
16 implementation of multiple diverse technologies so
17 that it will address the attack surfaces for the
18 environment. And -- okay, we'll talk about this in
19 the next slide too -- that the protections of a
20 defensive architecture are not bypassed or
21 circumvented. Okay. So I'm going through these
22 slides based on the changes we actually made in the
23 document.

24 So the next slide, Mike, okay, is going to
25 address, I believe, the concern or discussion we had.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1716 14th STREET, N.W., SUITE 200
WASHINGTON, D.C. 20009-4309

1 Next slide, Mike. Yes, this was the information we
2 added after the meeting in October. Okay. For
3 necessary and required -- and this is the exact text
4 -- necessary and required firmware, software, and/or
5 data updates for a digital device, digital asset
6 protected behind the data diode. An acceptable way to
7 implement the update that does not circumvent the data
8 diode protection for wired connections in the
9 architecture is by implementing whatever measures you
10 want to do that does not -- that the update is not
11 verifying and assuring that the update does not
12 contain no malware and the integrity of the update is
13 maintained during transport.

14 Okay. So this is why -- this text would
15 be why no one can just -- first of all, the data diode
16 is there for protecting wired connections, okay,
17 physical wired connections. So no one can say, I want
18 to do a remote update by attaching -- making the
19 connection remotely based on that. You cannot do that
20 because the integrity of the update can't be
21 maintained. And your bypass is -- you're
22 circumventing and bypassing the diode detection for
23 wired connections.

24 Okay. The acceptable way that licensees
25 have implemented this is if they've implemented this.

1 It's if they've implemented the kiosk. They've
2 implemented processes to get the information from a
3 vendor with digital signatures and verifying that
4 there's no malware there and it can be only
5 transported on secure USB devices or DVDs. So they
6 have a process to do this that does not circumvent
7 that wired connection of that data diode.

8 MEMBER BROWN: Kim, I don't disagree with
9 what you said here. What you're effectively talking
10 about, you're now back in the physical access of
11 control. You make sure that anybody that wants to
12 come in on the backside --

13 (Simultaneous speaking.)

14 MS. LAWSON-JENKINS: Physical --

15 MEMBER BROWN: -- coming in through the
16 backside. You want to do --

17 (Simultaneous speaking.)

18 MEMBER BROWN: -- software update and
19 design and change the software. You've got to protect
20 it in transport. You've got to protect it when it's
21 developed at the vendor, and you've got to protect it
22 in a manner how you introduce it into the equipment.

23 MS. LAWSON-JENKINS: Yes.

24 MEMBER BROWN: Very common sense. And
25 that's what that says to me. Is that --

1 MR. BEARDSLEY: That is correct.

2 MEMBER BROWN: Am I reading that
3 correctly?

4 MR. BEARDSLEY: That is correct.

5 MEMBER BLEY: And I want to go back to one
6 of Charlie's first comments. I'll just point out to
7 you that in your glossary, you don't have data diode.
8 You've got to have data diode in the glossary and
9 explain what it is.

10 MEMBER BROWN: And I want to give you a
11 help on that letter.

12 MS. LAWSON-JENKINS: Okay, okay.

13 MEMBER BROWN: The data diode is
14 effectively a unidirectional, hardware-based, not
15 configured by software data transmission device.
16 Really easy.

17 MS. LAWSON-JENKINS: Okay.

18 MEMBER BROWN: I mean, if the Committee
19 agrees, that's just -- and you also use the word, one
20 way, in a bunch of places. I don't disagree with
21 that. But it's really synonymous with data diode.
22 And you might want to somehow --

23 (Simultaneous speaking.)

24 MS. LAWSON-JENKINS: Usually why I say one
25 way in the text is usually with one way. And I say

1 it's implemented using hardware mechanisms.

2 MEMBER BROWN: If you've got the
3 extensions on there, that's fine. I thought I saw --
4 but I'm just pointing out is that they're really
5 synonymous.

6 MR. BEARDSLEY: So I think for history's
7 sake when the document was originally developed, it
8 was unclear whether there'll be other technologies
9 that could perform the same task as the data diode.
10 So we define it as a one way deterministic device.
11 Left it to the licensees to figure out how to meet
12 that requirement.

13 They all chose a data diode. So I don't
14 disagree with your point. And defining a data diode,
15 we have the comment. But that's the reason we are
16 where we are today.

17 MEMBER BROWN: Okay.

18 MEMBER BLEY: And that's a very good
19 definition. I don't think anybody would --

20 MEMBER BROWN: No.

21 MEMBER BLEY: -- object to that.

22 MEMBER HALNON: I'm curious about this
23 known malware. I mean, is that a list of stuff that
24 you compare? Or it seems like you wouldn't want any
25 malware much less the known stuff.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1716 14th STREET, N.W., SUITE 200
WASHINGTON, D.C. 20009-4309

1 MS. LAWSON-JENKINS: This is a common term
2 in cyber security. This is not an NRC term. Okay.
3 There's, in general, two types of malware. Malware
4 that has been identified, there's a signature for it.
5 Security devices can find it, can identify to find it.
6 And then there's clearly what they call the zero day
7 exploits.

8 MEMBER HALNON: Okay. So this is --

9 MS. LAWSON-JENKINS: Things you don't know
10 about.

11 MEMBER HALNON: -- what's physically
12 tossed.

13 MR. BEARDSLEY: So right, remember these
14 words are going to be a license requirement to the
15 licensee. So if we said no malware and the licensee
16 had a zero day that no one knew about and got through,
17 we could theoretically write a violation. And so we
18 termed it this way because we didn't think that was
19 fair. You've got to have other problems than that if
20 it's a zero day.

21 MS. LAWSON-JENKINS: If it's a zero day,
22 that's why they need to minimize the attack surface so
23 that there's less things that the attacker can exploit
24 if they get on your network, if they get on there.

25 MEMBER BROWN: But fundamentally, it comes

1 down to all virus detection software is fundamentally.
2 In general, it's reactive.

3 MS. LAWSON-JENKINS: It is reactive.
4 (Simultaneous speaking.)

5 MEMBER BROWN: -- know about it. You
6 store all this stuff in your detection software. But
7 it's reactive. If something new comes up and you see
8 it happening, every day in the newspaper some days,
9 that's the -- what do you call it, a zero day? It's
10 a zero day thing.

11 MS. LAWSON-JENKINS: Yes.

12 MEMBER BROWN: It's a new one. Now oh,
13 now it's caused a problem. Now we're going to put
14 that into our database so that we can protect it.

15 MS. LAWSON-JENKINS: Exactly.

16 MEMBER BROWN: That's why I'm so hard over
17 on this stuff in reality. And I apologize for milking
18 these cow many, many times.

19 MS. LAWSON-JENKINS: If wired connections
20 were the only way malware could get on the network, I
21 would --

22 (Simultaneous speaking.)

23 MEMBER BROWN: Oh, no. Absolutely.

24 (Simultaneous speaking.)

25 MS. LAWSON-JENKINS: Okay, okay.

1 MEMBER BROWN: If you've got a hardware
2 diode there, it can come in via somebody, bringing in
3 a new software upgrade. That's where the physical
4 protection -- they have to work just like in the old
5 days, physical access, changing set points, doing
6 something to cards. Now you got to make sure the
7 software -- it's like changing out a part. So you've
8 got to make sure that part is a good part. And it's
9 hard to do.

10 MS. LAWSON-JENKINS: So using --

11 MEMBER BROWN: It's very hard.

12 MS. LAWSON-JENKINS: -- a data diode will
13 absolutely reduce the risk as far as licensees are
14 concerned. They rely heavily, heavily on use of a
15 data diode. So from the licensees' point of view, I
16 don't think you'll have a real problem with that.
17 It's more of a design issue. Okay?

18 And I understand this, where you're
19 looking at it from -- especially from the safety point
20 of view. But I know from experience licensees
21 leverage safety requirements. If they did something
22 for safety, they say, well, we take credit for this
23 for security also.

24 That may or may not work depending on the
25 site and the design and things like that. But use of

1 one way information flow control, it is vital for
2 protecting systems. There's no doubt about it. We
3 really don't have any disagreement on that. And if
4 you can introduce it effectively in a way early in the
5 process, that is the better way to do it obviously.
6 But it really is going to depend on the design.

7 MEMBER BLEY: On some of these other
8 attacks, I spent some time working with the railroads.
9 And they had a very difficult time when they moved
10 over to digital control of their trains. They were
11 bringing in approved software and apparently by
12 approved vendors.

13 And it was -- had stuff loaded in it. It
14 came in with the upgrades and caused them all kind of
15 problems for a while. I've had it explained to me how
16 our QA is so perfect, that can't happen. It's one I
17 worry about.

18 MS. LAWSON-JENKINS: It is a challenge.
19 It's a challenging problem. Okay. It is challenging
20 because the adversaries change their techniques all
21 the time.

22 MEMBER BROWN: Can I hold --

23 MS. LAWSON-JENKINS: We were talking about

24 --

25 MEMBER BROWN: Can I hold you up for a

1 minute? We're at two hours and 38 minutes into --

2 MS. LAWSON-JENKINS: Oh, sorry, sorry.

3 MEMBER BROWN: -- our 3:00 o'clock time.

4 And it's our fault. It's not your fault. It's not
5 your fault. Do we have a little extra time coming up
6 after this?

7 (Simultaneous speaking.)

8 CHAIRMAN SUNSERI: How much time do you
9 need?

10 MEMBER BROWN: Well, we're at slide 13 of
11 28. But I think the last one says questions.

12 MS. LAWSON-JENKINS: No, actually, I left
13 the questions out because I figured you'd be asking
14 all the way through.

15 MEMBER BROWN: If Dennis and I will shut
16 up, we might make it. Really me. I'm going to try to
17 restrain myself from now on. So Kim --

18 MS. LAWSON-JENKINS: I think we --

19 MEMBER BROWN: -- go ahead and --

20 MS. LAWSON-JENKINS: I think we've talked
21 about a lot of these. We will save -- I will breeze
22 through the other ones unless -- I will --

23 MEMBER BROWN: Okay.

24 MS. LAWSON-JENKINS: -- explain them.

25 I'll ask for each one, any questions. And I'll keep

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1716 14th STREET, N.W., SUITE 200
WASHINGTON, D.C. 20009-4309

(202) 234-4433

www.nealrgross.com

1 going.

2 MEMBER BROWN: I'll try to restrain
3 myself.

4 MR. BEARDSLEY: We'll make sure we
5 highlight the ones that reflect the changes.

6 MEMBER BROWN: Exactly. Okay. Go ahead,
7 Kim. Thank you.

8 MS. LAWSON-JENKINS: Next slide, please,
9 Mike. Okay. The use of alternate controls, as I
10 said, that's why we introduce what the intent of the
11 controls were, if the control cannot be implemented.
12 As Jim mentioned earlier, they have to have
13 countermeasures to make sure to be able to detect if
14 there's any problem because just because you didn't
15 think there was going to be a problem doesn't mean an
16 attack can't happen. Next slide, please, Mike. Thank
17 you.

18 Use of consequence-based graded approach,
19 this was just repeating what I said earlier, that the
20 most important devices are at the highest security
21 level. And you should be able to reproduce all the
22 time how you made these decisions. There should be a
23 real process to this and consistency to this applying
24 this approach. In the I-1310, there's some guidance
25 that the industry has put out has been decided as an

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1716 14th STREET, N.W., SUITE 200
WASHINGTON, D.C. 20009-4309

(202) 234-4433

www.nealrgross.com

1 acceptable way of doing this. Next slide, Mike.

2 Okay. You've alluded to this earlier in
3 some of the discussion that we added for technical
4 security controls that we added this text that they
5 can -- during this design certification that the
6 applicants or licensees can incorporate the technical
7 security controls as a part of the nuclear power
8 reactor. The best way to put this is that very
9 rarely, rarely will equipment manufacturers just put
10 in something. They usually do that because it's
11 requested by a customer or they know they need it to
12 be sold to a customer, whatever.

13 So yes, as we mentioned earlier, it's the
14 licensee or the applicant that will receive -- the
15 licensee that will receive the violation. So they
16 need to send the security requirements to the
17 equipment if they're expecting the equipment to
18 perform certain security functions. So that's clear.

19 And for a lot of the technical security
20 controls when we talk about the classes of them, we
21 added information regarding access control, audit and
22 accountability, system and communication protection,
23 authentication identification, and system hardening.
24 Okay, especially the audit. Anyone who knows me in
25 cyber security, I'm a big hawk on being able trace

1 what happened with that device from a security point
2 of view.

3 Okay. So we added more explanation about
4 what that's really needed. Okay. But like I said, a
5 lot of that information won't get in unless the
6 guidance is out there, whether the equipment
7 manufacturers can read the information or that if
8 information is given to them directly by the
9 licensees. Any questions on this slide?

10 MEMBER BROWN: I'm not going to restrain
11 myself again. It's not a problem except it's somewhat
12 vague. And they're good generalized words, but it's
13 somewhat vague in that the context of -- within the
14 context rather of systems where you can use the
15 conventional cyber protection mode as opposed to those
16 who can't use them.

17 So how you balance, how you apply that,
18 it's not in the context of the old analog to now
19 digital controls. And then some of the digital
20 controls can't have software that does anything other
21 than through the controls. Not quite -- just I don't
22 disagree with the sentence. It's just pops in and
23 it's somewhere in the document there ought to be a
24 differentiation again like I said earlier.

25 Some stuff like safety systems can't have

1 it. And other stuff, you can have the traditional
2 mitigation and identification. Then it has more
3 meaning if you have that up front. This is up in the
4 early parts. We'll see what pops out, if anything --

5 MS. LAWSON-JENKINS: Okay. If you --

6 MEMBER BROWN: -- in our report.

7 MS. LAWSON-JENKINS: I was getting ready
8 to say if you have any specific suggestions --

9 (Simultaneous speaking.)

10 MEMBER BROWN: It's not mine. The
11 Committee has to agree.

12 MS. LAWSON-JENKINS: I understand. But
13 like I said, if you look --

14 MEMBER BROWN: I'm just a Lone Ranger down
15 here. Okay. Go on to your slide.

16 MS. LAWSON-JENKINS: Very quickly, the
17 issue, like I said, for the data diode is one control.
18 It's information flow control. Okay? I care about
19 access control in general. I care about auditing. I
20 care about the communication, the type of
21 communication, the encryption if you're going to have
22 any on there, system hardening.

23 There's lots of things in the technical
24 controls I would like to see actually on the device if
25 possible rather than knowing after the fact there's a

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1716 14th STREET, N.W., SUITE 200
WASHINGTON, D.C. 20009-4309

(202) 234-4433

www.nealrgross.com

1 report somewhere that, oh, we may have a problem.
2 Okay. And like I said, the manufacturer is the best
3 entity to do these things correctly and well. So if
4 in the future -- like I said, we'll see what comes out
5 in the next month if you have any specific
6 suggestions.

7 But really I understand the importance of
8 the data diode. And it is important. And we will
9 continue to have it as a part of it. But the
10 sophistication of the equipment, we need to broaden
11 what we think of as technical controls and things that
12 really are important in this --

13 MEMBER BROWN: My point is not a data
14 diode issue. It's more of a functionality issue of
15 the different types of systems you have to deal with.
16 Some you can use software controls. Some you can't
17 introduce because of their safety function. It's not
18 saying what. It's saying you got to differentiate the
19 world. That's all.

20 MS. LAWSON-JENKINS: Okay.

21 MEMBER BROWN: Okay. Go ahead to your
22 next slide. I'll help you move on.

23 MS. LAWSON-JENKINS: Okay. Next slide,
24 Mike. Okay. Incident response, there was a new
25 regulation which is reflected in the guidance. And we

1 updated the references for NIST and DHS for incident
2 response. Next slide, Mike. Systems and services
3 acquisitions, these is the Reg Guide 1.152, Revision
4 3. The original text said Section 1.2 -- sorry,
5 Section 2.1 to Section 2.6. It should've been to
6 Section 2.5. So that was -- it was a typing error
7 that was corrected.

8 MEMBER BROWN: We can handle that one.

9 (Laughter.)

10 MEMBER BROWN: You can go on. You can go
11 on.

12 MS. LAWSON-JENKINS: Next slide, please,
13 Mike. Okay. It's continuous monitoring. I'm not
14 going to spend a lot of time on this because it's self
15 explanatory in the text. But one of the issues --
16 we're in the maintenance mode phase now for the
17 operating plants.

18 They've all implemented cyber security
19 plants. They have been inspected at least two times.
20 And they've had a lot of information from us. Now
21 they're maintaining their plant. Okay. And they have
22 to make sure it stays effective.

23 And that's what this new text gets to.
24 And it's like I said, I added text -- we added text.
25 They had to do with anomaly detection. And that's

1 hard to do if you don't harden the devices. If you
2 have everything on there, you don't know what's new
3 and what's bad.

4 So it really is just to continuously
5 educate the equipment manufacturers and licensees that
6 focus on what you really need on there and then
7 protect accordingly. If you don't want to worry about
8 new vulnerabilities on something that you don't really
9 need, don't have it on the device. Next slide, Mike.

10 Okay. Effectiveness analysis for security
11 controls, this is where we introduce information about
12 metrics because, like I said, we're running out of
13 time. We added a whole new section on metrics. It's
14 optional. Licensees may determine that in a different
15 way, that they want to demonstrate the effectiveness
16 of their program.

17 They may do it as we had in the earlier
18 discussion by saying, okay, we want to do it. We have
19 a model that very closely simulates this. And we can
20 run a test on it to show how we would react to a cyber
21 attack.

22 They can come up with any method they want
23 to do. Okay. But they already have auditing
24 requirements. If you have auditing requirements to
25 get logs, you need to know what those logs mean and

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1716 14th STREET, N.W., SUITE 200
WASHINGTON, D.C. 20009-4309

(202) 234-4433

www.nealrgross.com

1 you come up with metrics that can show how effective
2 your program is. Next slide, Mike.

3 Okay. Maintenance of CDA security
4 assessments. This was a major issue for the plants,
5 and it's paperwork. It is. But they have to
6 understand, as I keep harping on, you have to know
7 what's in your system. You have to know what's in
8 your system is secure.

9 Okay. So therefore, the only thing you
10 have to go by is the assessments of this equipment you
11 have. And it has to reflect what is reality, not what
12 you did ten years ago, not what you did five years
13 ago. It needs to reflect what is there today.

14 So we added information all through the
15 document when any changes were made to the systems.
16 And you have the validations, whatever, that that
17 information is reflected in a security assessment.
18 And it's really important, like I said. The licensee
19 and the regulator needs to understand how these
20 devices are protected and that their controls are
21 still effective. This is one way of doing it, that an
22 objective person could look at this and understand it.

23 MEMBER HALNON: Is this simply, we made a
24 change, we do an assessment? Or is this a full
25 assessment on everything again, over and over again?

1 MS. LAWSON-JENKINS: If you make a change,
2 you want to know your change worked, right?

3 MEMBER HALNON: Right. I get that.

4 MS. LAWSON-JENKINS: You want to make sure
5 that you didn't introduce something that --

6 MEMBER HALNON: I'm just saying if you
7 have a system that hasn't been change, do you have to
8 go through an assessment?

9 MS. LAWSON-JENKINS: No, no. If you --
10 there has been no communication with that system.
11 This goes back to the graded approach, okay, and using
12 risk informed security. If you --

13 MEMBER HALNON: That's fine. I got it.
14 I just want to make sure that we weren't asking for a
15 reassessment of --

16 MS. LAWSON-JENKINS: No, no, no. I mean,
17 like I said --

18 (Simultaneous speaking.)

19 MS. LAWSON-JENKINS: -- like I said, this
20 is risk informed security. You have to -- if you have
21 tested and there's nothing there, then why would you
22 need to go back there? This is -- okay.

23 (Simultaneous speaking.)

24 MEMBER HALNON: All right. We're on the
25 same page. We're good.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1716 14th STREET, N.W., SUITE 200
WASHINGTON, D.C. 20009-4309

1 MS. LAWSON-JENKINS: Okay. Next slide,
2 Mike. Okay. As I said, we added the intent of every
3 control. We added text about reducing or eliminating
4 tech pathways and surfaces. And we aligned with the
5 NIST SP 853, Revision 5. So NIST has had two
6 revisions of their security controls since we've been
7 doing this. Next slide, Mike.

8 Okay. Very briefly, the Reg Guide 5.71,
9 the revision, it's close but not exactly the same as
10 the NEI version. It's like a version of what we have.
11 And some things, actually, we took out. We saw no
12 real need for.

13 Other things, we were in alignment in.
14 We're removed controls. And a few things we left --
15 that we left in our document. And they came up with
16 alternate ways of doing it. And we'll see on
17 inspections whether that really plays out.

18 But the issue is that safety and security,
19 they do have synergy. They work together. But they
20 are different things. They are different. You can
21 have something in for a safety reason and then not
22 meet the need for security. And that's what has to be
23 looked at each time, especially when you're claiming
24 credit for it.

25 MEMBER BLEY: And I guess the key thing

1 here is from both sides, we have to make sure the
2 things we do for security don't have a negative impact
3 on safety and vice versa.

4 MS. LAWSON-JENKINS: Well, really, no,
5 it's one way there. The things we do for security to
6 never have a negative impact on safety. Okay.

7 MEMBER BLEY: Well, I suspect it's not one
8 way because some of the safety systems are tied into
9 -- on the cyber side, things are kind of -- in any
10 case, they don't want either one to degrade.

11 MR. BEARDSLEY: There was a safety
12 security interface requirement in the regulations that
13 the licensees have to maintain.

14 MS. LAWSON-JENKINS: Yes.

15 MEMBER BLEY: I wanted to ask about NIST.
16 We keep referring to NIST. Do they have some
17 hierarchical rule over us? Or do we think they're
18 just really good and we want to follow them? Or
19 what's the relationship?

20 MS. LAWSON-JENKINS: Well, one thing is
21 they've been working in this area for quite a while.
22 And the original version of 5.71 was a tailored
23 version of one of the NIST documents. Two of them
24 really.

25 MEMBER BLEY: So it's directly derivative

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1716 14th STREET, N.W., SUITE 200
WASHINGTON, D.C. 20009-4309

1 from it, yeah.

2 MS. LAWSON-JENKINS: Right, right. So
3 anytime they change the corresponding controls, we
4 look at it to see, do we need to pick up this change?
5 And if not, why? Okay. Sometimes we did. But
6 sometimes we didn't and we had justification on why we
7 decided to change things or not.

8 MEMBER HALNON: Looking at the joint task
9 force, the NRC is not on that joint task force. Are
10 you all planning on becoming a member of that joint
11 task force?

12 MS. LAWSON-JENKINS: For?

13 MEMBER HALNON: For the NIST document.
14 I'm looking at the --

15 MR. BEARDSLEY: We're not on the joint
16 task force. We do review all the NIST changes. We
17 were provided the opportunity to review and comment.
18 And so the level to which those changes are made and
19 the broad breadth in the government, it wouldn't
20 behoove us to give out resources to that.

21 MEMBER HALNON: I mean, you're on the ASME
22 committees and ANS committees and whatnot. This seems
23 pretty impactful to the nuclear industry. It seems
24 like you'd want to be --

25 MR. BEARDSLEY: The changes they make to

1 the controls, so those documents have hundreds of
2 controls. We selected maybe 130, 140 of them. So I
3 mean, the chances of them significantly impacting our
4 regulation or our plan are pretty low.

5 MEMBER BLEY: Are there any areas where
6 you've departed from NIST --

7 MR. BEARDSLEY: Yes.

8 MEMBER BLEY: -- intentionally?

9 MR. BEARDSLEY: Yes, we tailored the NIST
10 requirements in Reg Guide 5.71 to meet the industrial
11 control systems. Now industrial control systems,
12 there are NIST standards for industrial control
13 systems now that didn't exist in 2009 when we wrote
14 the Regulatory Guide. But we're not going to go
15 rewrite the Regulatory Guide at this point. That
16 doesn't make sense. We are looking at that level in
17 advanced reactor guidance for the future.

18 MEMBER BLEY: Okay.

19 MS. LAWSON-JENKINS: I just want to make
20 a quick clarification there, 850 -- so 882 did exist.
21 It was a very early version. So we have been tying --
22 if you look at the revisions, we have been tying 853
23 which is the security controls and 882 which are for
24 an industrial control system. We monitor those for
25 revision. Okay.

1 We don't give input. As Jim said, we give
2 comments if we see anything. But the changes that
3 were made, they haven't really changed them
4 significantly. Next slide, please. I think I'll be
5 close to getting towards the end of this. Thank you.

6 Supply chain, for supply chain, we had a
7 lot of -- especially for the developer, a lot of
8 prescriptive controls. I know as a software developer
9 that a lot of integrated design environments where you
10 use -- you don't make those coding mistakes anymore.
11 They won't let you do it.

12 So we clarify. We got rid a lot of the
13 prescriptive language in 12.5 for security testing and
14 then some of the licensee applicant testing. And as
15 I said, we keep adding more text about the attack
16 surfaces and pathways.

17 We updated the glossary. If you have more
18 definitions you would like us to add, please give us
19 that information. And references, we updated those
20 and obviously, like I said, made numerous editorial
21 changes. Next slide, Mike. Okay, next, one more. I
22 should've dropped this one.

23 So like I said, we've had a team working
24 on this draft guidance since 2016. And so we know
25 every sentence, every punctuation. Everything in this

1 document, we could defend everything in there.

2 We've had a lot of good people working on
3 this. We put -- like I said, we put it off because
4 public comment in 2018, got a lot of good feedback.
5 We resumed the work in 2020. We finished the two
6 rounds of inspections, and now we're getting close to
7 2022. So next slide, Mike.

8 So what we were like to do is after
9 receiving the feedback to make any last changes, look
10 at your input, and if necessary, make any last changes
11 and issue this draft guidance in January and have a
12 two-month public comment period. Like I said, I
13 anticipate having two public meetings on this, one
14 where we just give out for information and give people
15 time to digest it and then for stakeholders to come in
16 and make comments on it. To use most of 2022 getting
17 it through the NRC process.

18 And then hopefully in the fall, have
19 another brief with ACRS subcommittee and full
20 committee to get this guide ready for publication. So
21 that is the plan. I think that's the last slide,
22 Mike. Oh, one more, one more. Yes.

23 So as Jim as said, the licensees have
24 implemented their programs, and we've provided
25 oversight of those programs. There's no changes in

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1716 14th STREET, N.W., SUITE 200
WASHINGTON, D.C. 20009-4309

(202) 234-4433

www.nealrgross.com

1 the staff position, just clarifications and one new
2 regulations. And as we've been speaking all through
3 this, the world has changed a lot.

4 Ten, twelve years is two lifetimes in
5 cyber security. It's a long time. But the attacks
6 have changed. There are hardware attacks now. We've
7 been talking about software. There are actually
8 hardware attacks now and clearly firmware attacks. We
9 have those.

10 So there's lots of things going on. So we
11 have to adapt with that. We are not just sitting and
12 looking at what was done. We are monitoring the
13 changes that are coming up in the industry. We're
14 looking at -- there are public meetings on these new
15 technologies that are coming in. We are there.

16 I'm really wrapping it up really quickly.
17 I'll be finished in a moment. So if we have anymore
18 questions on that, we can see what we are actively
19 doing. But right now on a lot of the technology, I
20 think it's Reg Guide 1.152, you talk about the concept
21 phase.

22 And a lot of these designs right now are
23 in the concept phase. And we are listening and
24 understanding the functions they must perform and try
25 to understand how cyber attacks could affect those

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1716 14th STREET, N.W., SUITE 200
WASHINGTON, D.C. 20009-4309

(202) 234-4433

www.nealrgross.com

1 function. So now we're listening and being a part of
2 those discussions.

3 So I know Jim will probably speak on this
4 maybe and if you have a few more questions. But we
5 are not just looking back at what we did, but we are
6 forward looking. And we are busy, not just with the
7 inspections but, as I said, any of the new designs
8 that come up to make sure we have a subject matter
9 expert from cyber who would listen to what's going on
10 so they can understand those designs and understand
11 the impacts on there for cyber.

12 So we're doing our job. I guess the point
13 I want to make here. This isn't just Kim Lawson
14 speaking. It's really Mike Brown and Jim Beardsley
15 and Eric Lee who wrote the original version of 5.71
16 and a lot of people who continue to put a lot of time
17 and effort in this. And like I said, we appreciate
18 the comments. We appreciate the input. And I look
19 forward to receiving them, so --

20 MEMBER BLEY: I have a couple quick
21 questions and a comment. I went back and looked at
22 that Knowledge Management document that I cited. And
23 it appears they try to pick up some cyber security.

24 But I'm not sure if they did much more
25 than read the older version of 5.71. I don't know if

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1716 14th STREET, N.W., SUITE 200
WASHINGTON, D.C. 20009-4309

1 any of your folks were involved with them. So here's
2 some sections. But they're probably not thorough
3 enough. But it's worth a look.

4 And in Section A-2 which describes the
5 cyber security plan, there's a very clear sentence
6 about achieving high assurance that cite digital
7 assets are computer and communication systems and
8 networks associates with SSEP functions, hereafter
9 defined as Critical Digital Assets, are adequately
10 protected against cyber attacks up to and including
11 the design basis threat. I'm not sure when you talked
12 about risk informing, did you talk at all about risk
13 inform the design basis threat? I hope you do.

14 MR. BEARDSLEY: Okay. Let me just address
15 that for a second because this is actually a major
16 discussion, not only here in the U.S. but across the
17 world. We have elected not to modify the design basis
18 threat on a routine basis based on cyber threats. So
19 the design basis threat in general has a
20 characterization of what a DBT cyber adversary.

21 And we evaluate just like all DBT aspects
22 on an annual basis. And we'll make a recommendation
23 to the Commission. But we have not provided
24 significant definition to that threat or that
25 adversary because it changes so often.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1716 14th STREET, N.W., SUITE 200
WASHINGTON, D.C. 20009-4309

1 It would become untenable from an
2 administrative point of view. The licensees
3 understand what the threat it, and they know what they
4 have to meet. But we're not risk informing or
5 managing it.

6 MEMBER BLEY: Okay. But it's defined in
7 a function. I know you can't go into detail. But
8 it's defined in a functional way, I assume.

9 MR. BEARDSLEY: It is defined at a very
10 high level and a functional --

11 (Simultaneous speaking.)

12 MEMBER BLEY: Okay. And I guess I
13 would've hoped there was a risk informing thought to
14 setting as functional criteria. And if not, I wonder
15 why not. We don't have to go into detail.

16 MR. BEARDSLEY: The challenge you have is
17 that the nation state cyber security today is someone
18 in their garage 18 months from now or 3 months from
19 now or 6 months. And trying to define it would be an
20 ongoing administrative burden that not only here in
21 the U.S. but across the world most regulators have
22 found is almost untenable.

23 MEMBER BLEY: So it's more of an umbrella
24 approach. We protect inside by having a good enough
25 umbrella that we're hoping however they come in, we

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1716 14th STREET, N.W., SUITE 200
WASHINGTON, D.C. 20009-4309

(202) 234-4433

www.nealrgross.com

1 catch them.

2 MR. BEARDSLEY: That's a fair
3 characterization.

4 MEMBER BLEY: Okay.

5 MS. LAWSON-JENKINS: While keeping an eye
6 on what's going on inside. You don't assume that only
7 good people are on the inside. And I don't mean
8 inside the threat. I mean that you don't have any
9 malware just because you haven't seen anything bad
10 yet. But you have to keep monitoring.

11 MEMBER BROWN: I just wanted to clarify
12 because I read this thing on design basis threat. And
13 I want to make sure I understand this. A plant has a
14 design basis threat it's supposed to be protected
15 against. Are we saying there's not a cyber threat
16 that's going to affect that and make it worse?

17 MR. BEARDSLEY: We are not saying that,
18 no. What we are saying --

19 MEMBER BROWN: You're not -- okay. Maybe
20 I said that the wrong way.

21 MR. BEARDSLEY: So the design basis threat
22 is defined in the regulation, then we have safeguards
23 level documents that provide more definition to the
24 physical design basis threat.

25 MEMBER BROWN: Exactly.

1 MR. BEARDSLEY: We have elected not to
2 provide in more significant detail --

3 (Simultaneous speaking.)

4 MEMBER BROWN: That's where I was trying
5 to get to. That's where I was trying to get to.
6 You're not saying there's something out there that
7 could compromise our design -- we're leaving it the
8 way it is.

9 MR. BEARDSLEY: Absolutely.

10 MEMBER BROWN: We're not trying to -- and
11 I'm not saying -- I just wanted to understand it, make
12 sure I got it clearly. Thank you. Kim, you're done?

13 MS. LAWSON-JENKINS: I am done, unless you
14 have anymore --

15 MEMBER BROWN: Okay. Well, thank you very
16 much, young lady. You did a fine job, very patient.
17 That's always appreciated. Let me --

18 MS. LAWSON-JENKINS: And honestly, we
19 appreciate your comments. I mean, every time we have
20 to --

21 (Laughter.)

22 MS. LAWSON-JENKINS: No, no. Seriously,
23 every time we have to discuss how it work, we should
24 defend it. And we're wrong, we need to fix something.
25 So thank you very much for the feedback. Thank you.

1 MEMBER BROWN: Hopefully, my intent is to
2 provide feedback that doesn't say, take another six
3 months to resolve our concerns.

4 MS. LAWSON-JENKINS: Hopefully, no.

5 MEMBER BROWN: Hopefully, we can be
6 specific enough that if you agree with them, you can
7 just do them. And then you go get your think out in
8 January. That's my goal. Whether I'm successful or
9 not, that depends on my colleagues here somewhat. Any
10 member comments starting on the other side? Dave?
11 Ron? Greg? Joy? Matt?

12 CHAIRMAN SUNSERI: That was a very
13 comprehensive presentation. They did a good job.

14 MEMBER BROWN: Yeah. Vicki? I'm done.
15 Do we go to the phones now during the full committee
16 meeting? I've forgotten.

17 CHAIRMAN SUNSERI: Yes, we do.

18 MEMBER BROWN: I presume the line is open.
19 Is that correct?

20 CHAIRMAN SUNSERI: So yes, if there's any
21 members of the public that wish to make a comment, you
22 can unmute yourself. You can *6, provide your name
23 and your comment.

24 MEMBER BROWN: Hearing none.

25 CHAIRMAN SUNSERI: Yeah, and then I guess

1 I would offer the same courtesy to any members on the
2 Teams chat that would like to make a comment. Not the
3 chat, the Teams session.

4 (No audible response.)

5 CHAIRMAN SUNSERI: Okay, nothing. All
6 right.

7 MEMBER BROWN: I got -- can I finish up?

8 CHAIRMAN SUNSERI: Go ahead.

9 MEMBER BROWN: Number one, I want to -- I
10 just want to thank you all. We've had three what I
11 thought very illuminating, providing a lot of
12 information between the September 22nd digital ANC
13 overview where we had extensive discussion, in general
14 on this general subject as well as the October session
15 and again a follow-up today with Kim. And you all did
16 a -- in my own personal opinion, did an excellent job
17 of trying to or even answering our questions.

18 I'm hoping that we -- I have a letter
19 prepared. And it's -- hopefully, I can get through it
20 without asking for the world to be reexamined and have
21 only specific suggestions of which hopefully you will
22 accept. Other than that, if you all have nothing else
23 to add, you have any final thoughts you'd like to say,
24 Jim?

25 MR. BEARDSLEY: Just thank you very much

1 for the opportunity.

2 MEMBER BROWN: Okay. Thank you all. It
3 was a good presentation. I really enjoy the back and
4 forth. They're very good for both of us.

5 CHAIRMAN SUNSERI: Yeah.

6 MEMBER BROWN: I'll turn it over to you,
7 Matt.

8 CHAIRMAN SUNSERI: Yeah, I agree, Charlie.
9 I think this session demonstrated the true value of
10 the in-person presentations and interactiveness. The
11 meeting was much more robust than I think I've seen on
12 nearly two years' worth of virtual ones. So thank you
13 all for that.

14 Okay. So at this point then, we're going
15 to take a break. We're going to take a break till
16 let's call it 3:30. At that time, we will complete
17 the day on deliberations by delivering two reports.

18 We're going to start with the Kairos
19 report because it's very near being done. I want to
20 get that one up and down before we get into a longer
21 one, right? And then we'll get into the -- Charlie,
22 you can be prepared to do your read-in. Hopefully,
23 we'll get through major comments and get pretty far
24 along on that one. Yes, Dennis?

25 MEMBER BLEY: Is staff going to provide us

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1716 14th STREET, N.W., SUITE 200
WASHINGTON, D.C. 20009-4309

(202) 234-4433

www.nealrgross.com

1 with hard copies or should I go print my own?

2 CHAIRMAN SUNSERI: Well, I'll take care of
3 that during the break, yeah. All right.

4 MEMBER BROWN: I have a hard copy. The
5 one I sent out to everybody, I printed out.

6 CHAIRMAN SUNSERI: Okay. All right.
7 Thank you. All right then. So we are now in recess
8 until 3:30. Thank you.

9 (Whereupon, the above-entitled matter went
10 off the record at 3:09 p.m.)
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

November 29, 2021

Project No. 99902069

US Nuclear Regulatory Commission
ATTN: Document Control Desk
Washington, DC 20555-0001

Subject: Kairos Power LLC
Presentation Materials for Kairos Power Briefing to the Advisory Committee on Reactor Safeguards (Full Committee) on KP-FHR Mechanistic Source Term Methodology Topical Report

References: Letter, Kairos Power LLC to Document Control Desk, "KP-FHR Mechanistic Source Term Methodology Topical Report, Revision 1," August 19, 2021, ML21231A290

This letter transmits presentation slides for the November 30, 2021, briefing for the Advisory Committee for Reactor Safeguards (ACRS). At the meeting, participants will discuss the KP-FHR Mechanistic Source Term Methodology Topical Report (KP-TR-012-P) Revision 1, which was submitted via the referenced letter to the Nuclear Regulatory Commission for review and approval.

The content of this information is non-proprietary; Kairos Power authorizes the Nuclear Regulatory Commission to reproduce and distribute the submitted content, as necessary, to support the conduct of their regulatory responsibilities.

If you have any questions or need additional information, please contact Drew Peebles at peebles@kairospower.com or (704) 275-5388, or Darrell Gardner at gardner@kairospower.com or (704) 769-1226.

Sincerely,



Peter Hastings, PE
Vice President, Regulatory Affairs and Quality

Enclosure: Presentation Slides for the November 30, 2021, ACRS Kairos Power Subcommittee Briefing

xc (w/enclosure):

William Kennedy, Acting Chief, NRR Advanced Reactor Licensing Branch
Benjamin Beasley, Project Manager, NRR Advanced Reactor and Licensing Branch
Weidong Wang, Senior Staff Engineer, Advisory Committee for Reactor Safeguards

Kairos Power LLC

www.kairospower.com

707 W Tower Ave, Suite A
Alameda, CA 94501

5201 Hawking Dr SE, Unit A
Albuquerque, NM 87106

2115 Rexford Rd, Suite 325
Charlotte, NC 28211

Enclosure 1


**Presentation Slides for the November 30, 2021
ACRS Kairos Power Subcommittee Briefing**



Kairos Power

KP-FHR Mechanistic Source Term Methodology Topical Report

ACRS Meeting, November 30, 2021



Kairos Power's mission is to enable the world's transition to clean energy, with the ultimate goal of dramatically improving people's quality of life while protecting the environment.

In order to achieve this mission, we must prioritize our efforts to focus on a clean energy technology that is *affordable* and *safe*.

KP-FHR Specifications

Uniquely Large Margins Between Operational and Failure Temperatures

Parameter	Value/Description
Reactor Type	Fluoride-salt cooled, high temperature reactor (FHR)
Core Configuration	Pebble bed core, graphite moderator/reflector, and enriched Flibe molten salt coolant
Core Inlet and Exit Temperature	550°C / 600-650°C

Design Temperature Limits	Value
Primary Salt (Flibe) Freezing and Boiling Temperatures	459°C / 1430°C
Maximum ASME Section III, Division 5, SS316 Temperature	816°C
Peak Fuel Temperature Limit	1600°C

Our combination of fuel and coolant provides a uniquely large safety margin.

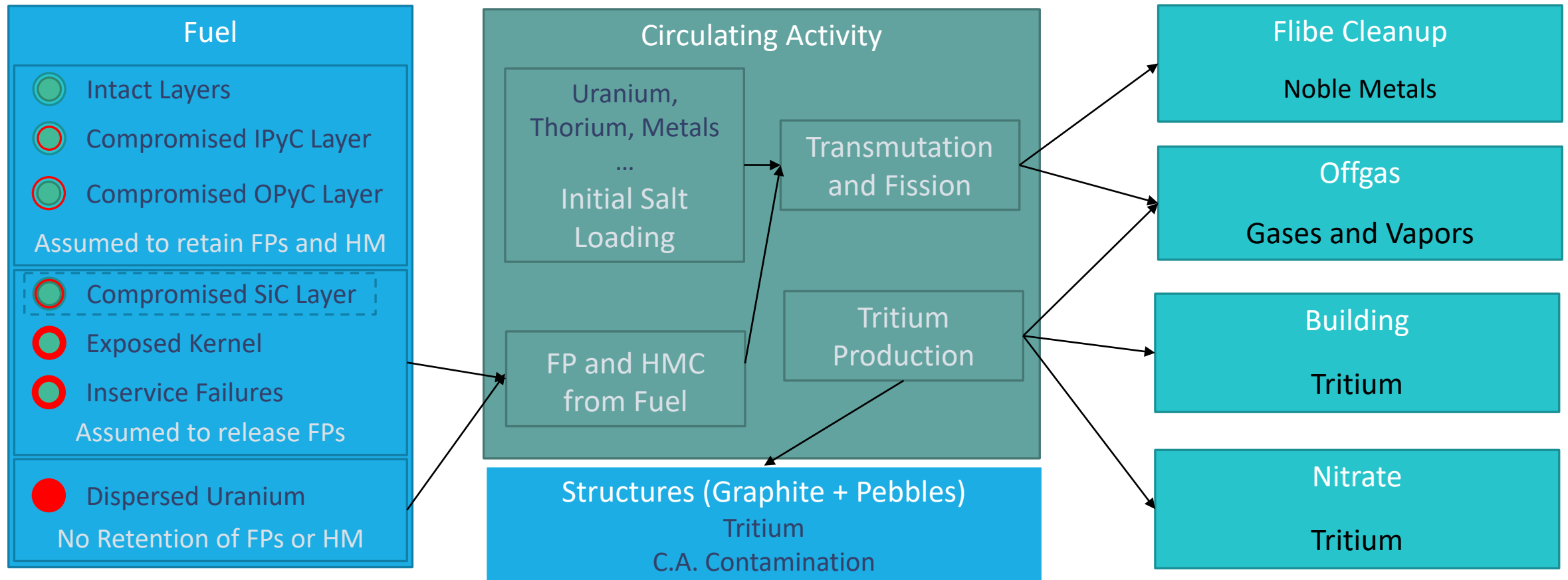
High Level Approach

Source Term Methodology

- Decompose the problem into a series of Material at Risk (MAR) and barrier Release Fractions (RFs) that separate that MAR from a receptor at the site boundary.
- For each barrier, group radionuclides into and model release through that barrier using a representative element for that group.
 - The barriers for radionuclide release are the TRISO fuel and the Flibe coolant (i.e., functional containment).
 - Radionuclide groups are used to facilitate transport through barriers.
 - Unique grouping structures exist for specific release modes (e.g., mechanical grinding of fuel in the PHSS vs diffusion through TRISO barriers).

$$ST^i(t) = \sum_{j=1}^J MAR_j^i(t) \prod_j RF_j^i(t)$$

Sources of Steady State Material at Risk (MAR)



MAR Mobilization in AOOs, DBEs, and DBAs

Only minor fractions of the total MAR can be mobilized in AOOs, DBEs, or DBAs

- The vast majority of MAR is safely protected in the fuel during AOOs, DBEs, and DBAs.
 - No incremental fuel failure is expected at temperatures $<1600^{\circ}\text{C}$.
 - Multiple inherent safety features protect the fuel from achieving high temperatures.
- MAR circulating in the reactor coolant as well as MAR present in other locations (cover gas, intermediate loop, etc) can be mobilized in AOOs, DBEs, and DBAs.
 - Aerosolization of Flibe – Hypothetical guillotine pipe break or primary pump operations
 - Vaporization– chemical specific evaporation is evaluated across accident temperature profiles
 - Limited release rates are expected from evaporation of soluble radionuclides from Flibe for temperatures below 816°C .
- Tritium stored in graphite, pebbles, and structures can be desorbed at elevated temperatures.

AOO, DBE, & DBA Source Term Methodology

- DBA site boundary dose to demonstrate KP-FHR meets dose limits in 10 CFR 50.34, 10 CFR 52.79, and 10 CFR 100.11.
- A technical specification (tech spec) limit will be set on activity in the Flibe, cover gas, and other systems.
 - The system is designed to preclude incremental fuel failures due to the DBA conditions as evaluated by KP-BISON.
- AOO and DBE source term analyses similar to DBAs, but a more realistic assessment of barriers, mitigation strategies, and initial conditions may be assumed.
- The circulating activity technical specification will be used to inform an operational limit on circulating activity. This operational limit can be used as a more realistic initial condition for normal operation effluent calculations as well as certain AOOs and DBEs.

Radionuclide Grouping and Transport Approach

- Transport of radionuclides through each medium is evaluated on an RN group basis using the following steps:
 - Individual isotopes are combined into RN group for each barrier.
 - Release fractions of each RN group associated with that medium is calculated given driving forces (e.g., temperature, pressure).
 - Release fractions are combined with the relevant inventories to determine the quantity of material that is mobilized. That incoming material is then:
 - Combined with the radionuclides already present in the next barrier and then
 - Regrouped for subsequent mobilization
 - The dose consequences for radionuclides that are transferred into the gas space are evaluated with RADTRAD and ARCON.

LWR Example

MELCOR

Ag	Ba	Ce	I and CsI	Mo and CsM	Te	U	Xe and H2O
B	Cd	Cs, CsI, and CsM	La	Ru	Te and H2O	Xe	NA

Limitations

1. Approval of KP-Bison for use in fuel performance analysis as captured in KP-TR-010-P (KP-FHR Fuel Performance Methodology).
2. Justification of thermodynamic data and associated vapor pressure correlations of representative species.
3. Validation of tritium transport modeling methodology.
4. Confirmation of minimal ingress of Flibe into pebble matrix carbon under normal and accident conditions, such that incremental damage to TRISO particles due to chemical interaction does not occur as captured in KP-TR-010-P (Fuel Qualification Methodology for the KP-FHR).
5. Establishment of operating limitations on maximum circulating activity and concentrations relative to solubility limits in the reactor coolant, intermediate coolant, cover gas, and radwaste systems that are consistent with the initial condition assumptions in the safety analysis report.
6. Quantification of the transport of tritium in nitrate salt and between nitrate salt and the cover gas
7. The phenomena associated with radionuclide retention discussed in this report is restricted to molten Flibe. The retention of radionuclides in solid Flibe is beyond the scope of the current analysis.
8. The methodology presented in this report is based on design features of a KP-FHR (details provided in report). Deviations from these design features will be justified by an applicant in safety analysis reports associated with license application submittals.

NRC Staff Evaluation of the KP-FHR Mechanistic Source Term Methodology, Revision 1

Michelle Hart
Senior Reactor Engineer
Office of Nuclear Reactor Regulation

Presentation to the ACRS
November 30, 2021

Introduction

- KP-FHR Mechanistic Source Term Methodology topical report, KP-TR-012, Revision 1 (August 2021)
- Applicable to Kairos Power fluoride salt cooled, high temperature reactor (KP-FHR) designs
 - Including a nuclear test reactor and commercial power reactors
- Methodology to develop event-specific radiological source terms and short-term atmospheric dispersion values for EAB and LPZ at distances less than 1,200 meters
 - DBAs for siting and safety analysis
 - AOOs and DBEs for use in NEI 18-04 methodology to categorize events, classify SSCs, and evaluate defense-in-depth
 - Does **not** address source terms and atmospheric dispersion for normal operation and effluents, BDBEs, or control room habitability

Staff Review Focus

- Staff review focused on the bases for models in the methodology
 - Radionuclide transport and retention in the fuel, Flibe, gas space and buildings
 - Tritium production, transport and retention
 - Aerosol formation and deposition
 - Near-field atmospheric dispersion and use of ARCON96

Mechanistic Source Term Approach

- Methodology develops MSTs by evaluating sources of radioactive materials at risk of release (MAR) and release fractions for each barrier that contains the MAR
- DBA MSTs are developed crediting only the TRISO particle and Flibe coolant radionuclide retention as the KP-FHR functional containment
- MSTs for AOOs and DBEs are developed using a more realistic accounting of radionuclide barriers
- Staff finds the MST approach acceptable because it is consistent with
 - Safety analysis regulatory requirements
 - Discussion of MSTs in SECY-93-092 and RG 1.233
 - Description of functional containment in SECY-18-0096

Vaporization of Radionuclide from Flibe

- The NRC staff finds the methodology acceptable because of conservative assumptions and KP-FHR design features

Conditions and Limitations

- Kairos Power proposed 8 limitations on use of the TR, which were acceptable to the Staff
- Includes relationships to other Kairos Power TRs under review
 - KP-FHR fuel performance methodology TR and use of KP-Bison computer code
 - KP-FHR fuel qualification methodology

Conditions and Limitations

- The Staff imposed two additional conditions and limitations
 - #9: Use of the methodology is limited to the KP-FHR design. The combination of TRISO and Flibe allows for assumptions that may not be valid for liquid-fueled MSR.
 - #10: Applicant to provide information to justify that the calculation of tritium absorption onto graphite is not sensitive to the assumptions on tritium diffusivity and solubility in Flibe.

Changes to SE

- Changes made to the SE since issuance of Draft SE do not impact the NRC staff conclusions

Staff Conclusions

- KP-TR-012, “KP-FHR Mechanistic Source Term Methodology,” Revision 1, provides an acceptable methodology for development of event-specific mechanistic source terms for use by KP-FHR designs in offsite radiological consequence analyses for AOOs, DBEs, and DBAs
- Staff approvals are subject to the Limitations and Conditions of the SE

Acronyms and Definitions

AOO	anticipated operational occurrence
ARCON96	Atmospheric Relative Concentrations in Building Wakes computer code
BDBE	beyond design basis event
DBA	design basis accident
DBE	design basis event
EAB	Exclusion Area Boundary
Flibe	salt mixture of lithium fluoride (LiF) and beryllium fluoride (BeF ₂)
KP-FHR	Kairos Power Fluoride-Salt Cooled High Temperature Reactor
LPZ	Low Population Zone
MAR	materials at risk for release
MSR	molten salt reactor
MST	mechanistic source term
NEI	Nuclear Energy Institute
RG	regulatory guide
SE	safety evaluation
SECY	Commission paper
SRM	staff requirements memorandum
SSCs	structures, systems, and components
TR	topical report
TRISO	Tristructural isotopic