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.

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

ACRS CONSULTANT:

STEPHEN SCHULTZ

DESIGNATED FEDERAL OFFICIAL:

WEIDONG WANG

CHRISTOPHER BROWN

*Present via teleconference

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

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

MR. BEARDSLEY: Twenty-eight.

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

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

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

MEMBER BROWN: 5061, Rev. 1.

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

In July 2021, the staff provided the

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

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

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

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

MEMBER HALNON: One quick question.

MR. BEARDSLEY: Oh, yes.

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

MR. BEARDSLEY: Yes.

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

MR. BEARDSLEY: So the cyber security plan

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

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

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

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

MEMBER HALNON: No greater than --

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

MEMBER HALNON: I just want to distinguish

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

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

MEMBER HALNON: Okay. Thanks.

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

MR. BEARDSLEY: Critical digital assets.

MEMBER BLEY: Critical digital assets.

MR. BEARDSLEY: Yes.

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

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

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

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

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

MEMBER BLEY: Next year? Okay. Thank you.

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

MR. BEARDSLEY: It's more than that.

MEMBER BALLINGER: Okay. More than that. A lot?

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

(Simultaneous speaking.)

MEMBER BALLINGER: No higher than green?

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

MEMBER BALLINGER: But how many greens?

MR. BEARDSLEY: There were a number of greens.

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

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

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

performance over the course of the inspection program.

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

(Simultaneous speaking.)

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

(Simultaneous speaking.)

MEMBER BALLINGER: Multiple inspections at multiple plants?

MR. BEARDSLEY: Correct, yes.

(Simultaneous speaking.)

MR. BEARDSLEY: Multiple inspections at multiple plants.

MR. BEARDSLEY: Correct, yes.

(Simultaneous speaking.)

MR. BEARDSLEY: Multiple inspections at multiple plants.

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

MR. BEARDSLEY: Right.

MEMBER HALNON: -- that issue got resolved.

MR. BEARDSLEY: Yeah.

MEMBER HALNON: And a couple of other issues --

MR. BEARDSLEY: Correct.

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

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

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

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

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

MS. JOHNSTON: Okay. Thanks, Jim.

(Simultaneous speaking.)

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

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

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

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

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

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

(Simultaneous speaking.)

MEMBER BROWN: Could you back and repeat

that again?

MS. JOHNSTON: Sure. So -- okay.

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

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

MEMBER BROWN: That's it.

MS. JOHNSTON: Okay.

MEMBER BROWN: Thank you.

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

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

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

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

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

MS. JOHNSTON: Sure.

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

MS. JOHNSTON: Yes. Okay, that --

MEMBER BLEY: -- knowledge about that?

MS. JOHNSTON: That is correct. So the

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

(Simultaneous speaking.)

MEMBER BLEY: I am.

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

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

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

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

MS. JOHNSTON: Okay.

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

MS. JOHNSTON: Sure.

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

(Simultaneous speaking.)

MEMBER BROWN: The issue is coming down to

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

MS. JOHNSTON: Sure.

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

MS. JOHNSTON: Right.

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

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

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

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

MS. JOHNSTON: Sure.

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

MS. JOHNSTON: Right.

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

And then it's got a bunch of other stuff

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

MS. JOHNSTON: That's right.

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

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

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

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

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

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

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

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

And fundamentally, that's all the changes

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

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

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

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

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

So that's a separation of how do you get

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

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

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

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

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

satisfied with rev 1.

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

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

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

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

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

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

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

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

MS. JOHNSTON: Right. So --

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

MS. JOHNSTON: Understood.

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

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

MS. JOHNSTON: Okay.

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

MEMBER BROWN: Oh, no.

(Simultaneous speaking.)

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

MS. JOHNSTON: No, no, no.

CHAIRMAN SUNSERI: -- do you have a --

MEMBER BROWN: Start shooting those arrows.

CHAIRMAN SUNSERI: -- do you have a presentation?

MR. BEARDSLEY: We do.

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

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

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

MEMBER BROWN: Well, let me interrupt you then.

MS. JOHNSTON: Okay.

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

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

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

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

(Simultaneous speaking.)

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

MS. JOHNSTON: Okay. So --

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

MS. JOHNSTON: Right. So --

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

MS. JOHNSTON: Right.

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

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

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

And that process, as I understand it,

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

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

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

(Simultaneous speaking.)

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

MS. JOHNSTON: Understood. Feedback received. Understood.

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

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

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

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

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

(Simultaneous speaking.)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(Simultaneous speaking.)

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

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

(Simultaneous speaking.)

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

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

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

MS. JOHNSTON: Understood.

(Simultaneous speaking.)

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

is protected by the data diode.

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

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

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

MR. BEARDSLEY: Without a doubt.

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

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

MS. JOHNSTON: Okay.

MEMBER BLEY: Everybody does it.

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

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

MS. JOHNSTON: One other --

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

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

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

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

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

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

(Simultaneous speaking.)

MR. BEARDSLEY: One other question.

MEMBER BROWN: -- do her thing.

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

MEMBER BROWN: I'm sorry, Vicky.

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

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

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

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

MS. LAWSON-JENKINS: Yes, thank you.

MEMBER BROWN: Thank you.

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

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

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

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

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

There was an -- the draft guidance was

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

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

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

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

were going to implement.

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

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

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

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

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

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

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

And the licensees and the applicants are

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

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

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

MS. LAWSON-JENKINS: Absolutely.

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

MS. LAWSON-JENKINS: That is true.

MEMBER HALNON: -- to understand it, need

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

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

MEMBER HALNON: -- in the right way.

(Simultaneous speaking.)

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

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

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

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

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

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

MEMBER BROWN: Without -- you don't have

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

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

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

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

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

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

(Simultaneous speaking.)

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

(Laughter.)

MEMBER BROWN: That's all right.

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

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

MEMBER BLEY: That's what it sounded like.

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

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

(Simultaneous speaking.)

MEMBER BROWN: Okay. All right. That's

good. Go ahead, Kim. Thank you.

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

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

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

MEMBER BLEY: Okay. But you don't call

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

(Simultaneous speaking.)

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

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

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

MEMBER BROWN: This is the same as --

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

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

(Simultaneous speaking.)

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

MEMBER BROWN: -- which was a good idea.

MS. LAWSON-JENKINS: So it made clear what

we --

MEMBER BROWN: I understand that.

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

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

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

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

And I think this is tied to that first

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

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

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

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

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

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

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

As I said, we added a lot of text

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

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

MEMBER BLEY: Kim?

MS. LAWSON-JENKINS: Yes.

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

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

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

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

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

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

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

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

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

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

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

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

(Simultaneous speaking.)

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

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

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

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

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

(Simultaneous speaking.)

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

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

to respond adequately to any kind of problems.

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

(Simultaneous speaking.)

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

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

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

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

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

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

(Simultaneous speaking.)

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

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

MS. LAWSON-JENKINS: I know.

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

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

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

(Simultaneous speaking.)

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

MS. LAWSON-JENKINS: Next slide, please.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

MS. LAWSON-JENKINS: Okay, okay.

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

MS. LAWSON-JENKINS: Okay. Well, for --

(Simultaneous speaking.)

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

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

the same software everywhere. Okay.

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

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

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

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

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

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

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

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

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

Next slide, please.

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

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

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

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

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

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

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

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

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

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

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

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

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

(Simultaneous speaking.)

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

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

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

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

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

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

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

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

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

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

MS. LAWSON-JENKINS: No.

MEMBER BROWN: I just saw it, so --

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

(Simultaneous speaking.)

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

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

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

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

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

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

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

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

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

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

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

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

(Simultaneous speaking.)

MS. LAWSON-JENKINS: Physical --

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

(Simultaneous speaking.)

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

MS. LAWSON-JENKINS: Yes.

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

MR. BEARDSLEY: That is correct.

MEMBER BROWN: Am I reading that correctly?

MR. BEARDSLEY: That is correct.

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

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

MS. LAWSON-JENKINS: Okay, okay.

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

MS. LAWSON-JENKINS: Okay.

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

(Simultaneous speaking.)

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

it's implemented using hardware mechanisms.

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

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

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

MEMBER BROWN: Okay.

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

MEMBER BROWN: No.

MEMBER BLEY: -- object to that.

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

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

MEMBER HALNON: Okay. So this is --

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

MEMBER HALNON: -- what's physically tossed.

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

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

MEMBER BROWN: But fundamentally, it comes

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

MS. LAWSON-JENKINS: It is reactive.

(Simultaneous speaking.)

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

MS. LAWSON-JENKINS: Yes.

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

MS. LAWSON-JENKINS: Exactly.

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

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

(Simultaneous speaking.)

MEMBER BROWN: Oh, no. Absolutely.

(Simultaneous speaking.)

MS. LAWSON-JENKINS: Okay, okay.

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

MS. LAWSON-JENKINS: So using --

MEMBER BROWN: It's very hard.

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

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

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

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

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

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

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

MEMBER BROWN: Can I hold --

MS. LAWSON-JENKINS: We were talking about --

MEMBER BROWN: Can I hold you up for a

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

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

MEMBER BROWN: -- our 3:00 o'clock time. And it's our fault. It's not your fault. It's not your fault. Do we have a little extra time coming up after this?

(Simultaneous speaking.)

CHAIRMAN SUNSERI: How much time do you need?

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

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

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

MS. LAWSON-JENKINS: I think we --

MEMBER BROWN: -- go ahead and --

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

MEMBER BROWN: Okay.

MS. LAWSON-JENKINS: -- explain them. I'll ask for each one, any questions. And I'll keep

going.

MEMBER BROWN: I'll try to restrain myself.

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

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

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

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

acceptable way of doing this. Next slide, Mike.

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

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

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

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

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

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

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

Some stuff like safety systems can't have

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

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

MEMBER BROWN: -- in our report.

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

(Simultaneous speaking.)

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

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

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

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

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

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

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

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

MS. LAWSON-JENKINS: Okay.

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

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

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

MEMBER BROWN: We can handle that one.

(Laughter.)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

MEMBER HALNON: Right. I get that.

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

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

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

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

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

(Simultaneous speaking.)

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

(Simultaneous speaking.)

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

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

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

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

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

MEMBER BLEY: And I guess the key thing

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

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

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

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

MS. LAWSON-JENKINS: Yes.

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

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

MEMBER BLEY: So it's directly derivative

from it, yeah.

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

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

MS. LAWSON-JENKINS: For?

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

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

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

MR. BEARDSLEY: The changes they make to

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

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

MR. BEARDSLEY: Yes.

MEMBER BLEY: -- intentionally?

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

MEMBER BLEY: Okay.

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

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

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

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

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

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

document, we could defend everything in there.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(Simultaneous speaking.)

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

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

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

catch them.

MR. BEARDSLEY: That's a fair characterization.

MEMBER BLEY: Okay.

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

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

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

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

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

MEMBER BROWN: Exactly.

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

(Simultaneous speaking.)

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

MR. BEARDSLEY: Absolutely.

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

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

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

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

(Laughter.)

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

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

MS. LAWSON-JENKINS: Hopefully, no.

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

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

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

CHAIRMAN SUNSERI: Yes, we do.

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

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

MEMBER BROWN: Hearing none.

CHAIRMAN SUNSERI: Yeah, and then I guess

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

(No audible response.)

CHAIRMAN SUNSERI: Okay, nothing. All right.

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

CHAIRMAN SUNSERI: Go ahead.

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

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

MR. BEARDSLEY: Just thank you very much

for the opportunity.

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

CHAIRMAN SUNSERI: Yeah.

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

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

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

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

MEMBER BLEY: Is staff going to provide us

with hard copies or should I go print my own?

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

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

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

(Whereupon, the above-entitled matter went off the record at 3:09 p.m.)

Kairos Power

KP-NRC-2111-002

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 Methdology 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

KP-NRC-2111-002

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.

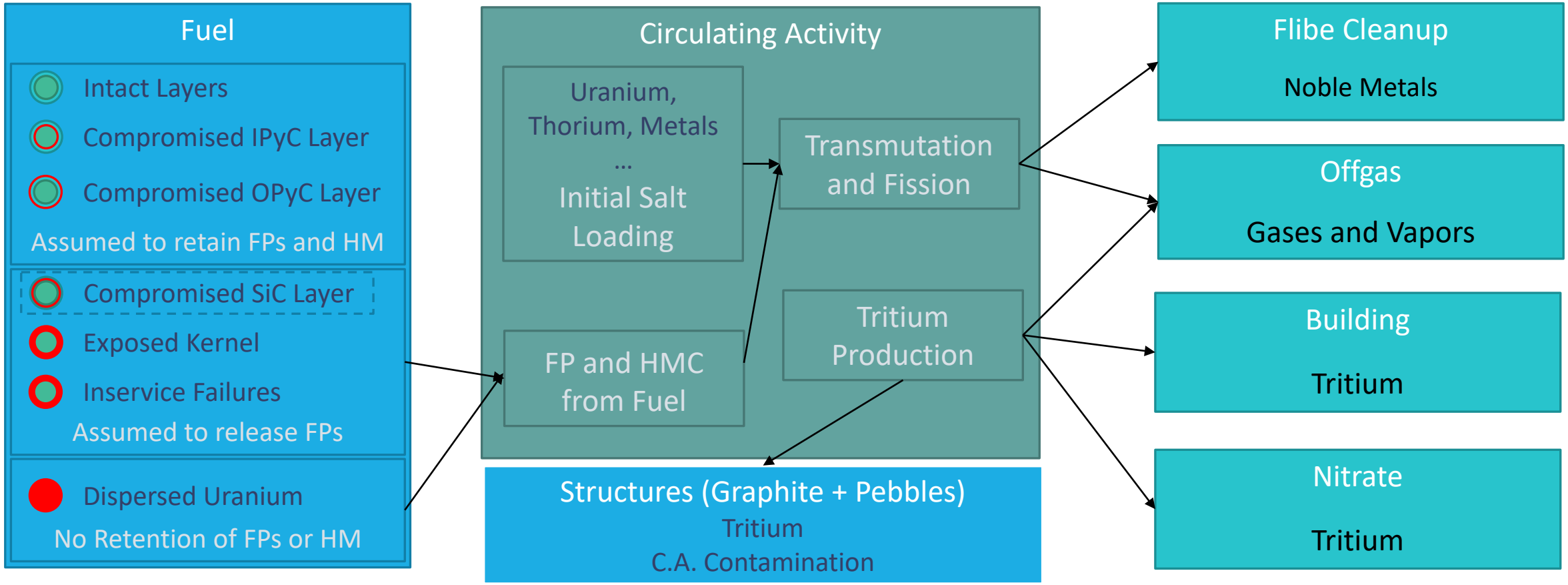
High Level Approach

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).

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

Sources of Steady State Material at Risk (MAR)



Kairos Power

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

LWR Example

Kairos Power

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.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

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 MSRs.
  - #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 (BeF2)
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