Official Transcript of Proceedings

NUCLEAR REGULATORY COMMISSION

Title: Public Workshop to Discuss I&C Cyber Security-by-design and Associated Potential Regulatory Impacts

Docket Number: (n/a)

Location: Rockville, Maryland

Date: Thursday, April 9, 2015

Work Order No.: NRC-1501 Pages 1-97

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

U.S. NUCLEAR REGULATORY COMMISSION

+ + + + +

OFFICE OF NEW REACTORS

+ + + + +

PUBLIC WORKSHOP TO DISCUSS I&C

CYBER SECURITY-BY-DESIGN AND

ASSOCIATED POTENTIAL REGULATORY IMPACTS

+ + + + +

THURSDAY

APRIL 9, 2015

+ + + + +

The Public Workshop met in Rooms 01C03 and 01C05, NRC Headquarters, Three White Flint North, 11601 Landsdown Street, Rockville, Maryland, at 8:30 a.m.

NRC STAFF PRESENT

CATHERINE ALLEN, NSIR/CSD

SUSHIL BIRLA, RES/DE

BERNARD DITTMAN, RES/DE/ICEEB

RUSS FELTS, NSIR/CSD

TERRY JACKSON, NRO/DE/ICE1

MICHAEL JONES, NRO/DARR/ARPB

IAN JUNG, NRO/DE/ICE2

RUI LI, NSIR/CSD

ERICK MARTINEZ, RES/DE/ICEEB

JONAH PEZESHKI, NSIR/CSD

PAUL REBSTOCK, RES/DE/ICEEB

DAVID RAHN, NRR/DE/EICB

JOHN RYCYNA, NSIR/CSD

RICHARD STATTEL, NRR/DE/EICB

JOHN TAPPERT, NRO/DE

BARRY WESTREICH, NSIR/CSD

DEANNA ZHANG, NRO/DE/ICE1

TABLE OF CONTENTS

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

(8:31 a.m.)

MR. JONES: Good morning, everyone, and thanks for coming to the meeting on I&C Cyber Security-By-Design Discussion.

This is a Category 2 Public Meeting. That means that there will be an opportunity for the public to make comments and to ask questions of the NRC Staff at specific times on the agenda.

Let's see. We've got some logistics. In case there's a fire or an emergency, we're going to exit this room. We're going to go out through the guard station. We'll muster outside. We'll make sure that everybody on the sign-up list is with us.

And there are bathrooms around the corner. Over by the cafeteria on this floor. No escorts required on this floor.

The meeting is going to be transcribed. So, we're going to ask that everyone that speaks please use the microphone. I'll be happy to bring one to you at any time. Let's talk one at a time and please put your phone on vibrate or turn them off.

For folks on the line, please make sure

that your phones are muted. You can do that by hitting star-6 and I'll cue you in when there's times for the public and for industry on the phone to jump into the discussion.

Our agenda is a bit flexible today. It depends on the amount of discussion. We didn't have any industry submittals or presentations. So, after our presentation, we'll go right into NRC and industry discussion Q&A.

We've got a couple of speakers to lead. First, I'd like to introduce Russ Felts and he's the Deputy Director of the Cyber Security Directorate from the Nuclear Security and Incident Response Office at the NRC.

Russ.

MR. FELTS: Yes, I really just wanted to offer a few comments to sort of frame the discussion.

I suspect that a lot of folks who are participating in this meeting might be concerned that what we're contemplating here is to require design cert applicants to demonstrate how they will meet requirements of 73.54 and I wanted to clarify for anybody that has that misconception that what we're talking about here is not broad consideration

of how cyber security is met at the design stage.

But more properly a very narrow look at certain aspects of cyber security during the design stage and really looking at finding ways to enable a designer to show that the design that they have proposed is not going to be so challenging to actually implement the cyber security program that the COL applicant would have some outrageously difficult program to have to implement in order to meet requirements of 73.54.

So, we're going to get into a lot more discussion of that. But I just wanted to lead off the discussion so folks aren't percolating over that, you know, misconception throughout the meeting.

MR. JONES: Next, we have Deanna Zhang who's going to give some introductions and she'll be leading us through the staff presentation and I guess ordinarily we just go around the room and get everybody's name, but why don't we wait and as speakers come, you give your name and your affiliation. We'll get it that way.

Okay. We'll go around. So, just pass a mic down and --

MR. LI: Rui Li with NSIR/CSD.

MR. MARTINEZ: Erick Martinez, NRC Research.

MR. JACKSON: Terry Jackson, Office of New Reactors.

MR. JARRETT: Ron Jarrett, TVA, Digital Program Manager.

MR. HERB: Ray Herb, Southern Nuclear, I&C Design.

MR. BAILEY: Mike Bailey, Duke Energy, Engineering Director for Digital Engineering Support.

MR. WESTREICH: Barry Westreich, Director, Cyber Security Directorate, NRC.

MR. FELTS: Russ Felts, Deputy Director, Cyber Security Directorate.

MR. YEATES: Brad Yeates, Southern Company, Cyber Security Program.

MR. CONNELLY: John Connelly, Exelon, Cyber Security Program Manager.

MR. GROSS: Bill Gross, NEI.

MR. BIRLA: Sushil Birla, NRC Research.

MR. RYCYNA: John Rycyna, NSIR/CSD.

MS. ALLEN: Cathy Allen, NSIR/CSD.

MR. DITTMAN: Bernie Dittman, NRC

Research.

MR. CLARKSON: Greg Clarkson, NuScale Power, Reactor Protection System Design.

MR. GIBSON: Matt Gibson, Electric Power Research Institute.

MS. BERGMAN: Jana Bergman, Scientech.

MR. JUNG: Ian Jung, NRC, Office of New Reactors.

MR. TAPPERT: John Tappert, NRC, Office of New Reactors.

MR. REBSTOCK: Paul Rebstock, office of Research.

MR. RAHN: David Rahn, Office of NRR.

MR. PEZESHKI: Jonah Pezeshki, NSIR/CSD. Also, the leader of the Cyber Assessment Team.

MS. ZHANG: Deanna Zhang, Office of New Reactors.

MR. STATTEL: Rich Stattel, NRR.

MS. ZHANG: Let me move this a little closer than that. Can you guys hear me? Good. Okay.

So, good morning. I would like to welcome everyone here to our Cyber Security Design Requirements Workshop and I would like to thank you

guys for traveling here. I know some of you guys had to travel pretty far and also look forward to discussing some the potential options we're thinking about for incorporating cyber security design requirements into the NRC's regulations.

Next slide. So, I know that Russ kind of laid out the scope a little bit, but I wanted to go into it a little bit further.

We're planning on discussing options for including cyber security design requirements into power reactors into the NRC regulations and we just want to emphasize we're not planning to discuss any other cyber security initiatives such as the NEI petition for cyber security rulemaking. We understand that there are other venues to address those activities.

Next slide. So, during today's presentation, we'll be providing an overview of potential options. We're including cyber security design requirements into the NRC's regulations. These options will only apply to power reactors including both new and operating reactors.

And keep in mind, these are only, you know, our own initial thoughts. So, we would like

to solicit your feedback regarding these potential options and maybe, you know, if there are new options that we have not considered yet, we would like to listen to them.

And also, we're not looking to add new technical requirements, but maybe changing some of our licensing process to see if we can perform some of the reviews of cyber security technical controls during licensing. But, in order to do so, it might entail some rulemaking. So, this is much more of a process change than, you know, any new technical requirements.

Next slide. So, before we present the different options we're considering, let me just go off some of the background with respect to, you know, our current regulatory frameworks and the guidance that's available to kind of set the stage.

So, the following the events of September 11th, the NRC underwent a comprehensive review of the security requirements and potential vulnerabilities at our regulated nuclear facilities. The NRC issued security orders more to impose requirements to enhance security and this included consideration of cyber security. This is a bubble was already required. What was required

in the regulation at that time.

Subsequently, the NRC published NUREG 68.47 which provided guidance in methodology for conducting cyber security self-assessment.

And following in 2005, the NRC endorsed NEI 04-04 which also provided guidance for developing and maintaining a cyber security program at licensed nuclear facilities and at that time, the licensees had committed to implement voluntarily NEI 04-04.

In 2009, the NRC issued 10 CFR 73.54. This is the regulation which required licensees to provide high assurance that digital computers and communicate systems and networks are adequately protected against a cyber attack.

And following in 2010, the NRC published Reg Guide 5.71 which provided an acceptable method for complying with the requirements of 10 CFR 73.54.

Next slide. In 2010, the NRC endorsed NEI 08-09 which was developed by NEI to assist licensees in complying with the requirements of 10 CFR 73.54. So, licensees could either use 10 CFR -- oh, could use NEI 08-09 or 10 CFR or Reg Guide 5.71.

In 2011, the NRC issued Revision 3 to Reg Guide 1.152 and just to remind everyone, in Revision 2 of this Reg Guard, the NRC did include guidance to address cyber security because we didn't have any other means to address cyber security at that time.

However, since 10 CFR 73.54 was issued along with its complementing reg guide, we removed that, the cyber security portion, guidance within that regulatory guide.

We still kept apportioned direct access controls which is to establish a secure development operational environment for digital safety systems where measures should be included to direct any non-malicious vulnerabilities that's in the design. More to insure integrity, reliability and functionality of the digital safety system while it's in operation.

And lastly, in 2013, the NRC endorsed NEI 13-10 which was developed to provide guidance for implementing a consequence based approach to implementation of the cyber security controls for the length of these critical digital assets.

So, let's go a little bit more into the 10 CFR 73.54. I just want to make sure we're on

the right slide.

So, 10 CFR 73.54, it provides a programmatic regulatory framework for the licensees and COLs to protect digital computer and communication systems and networks against cyber attacks. So, I want to emphasize it's programmatic based.

It requires licensees and COL applicants to submit a cyber security plan that is reviewed by the NRC. However, this regulation does not require licensees and COL applicants to submit any cyber security design information for NRC licensing review. It also does not require design certification applicants to submit design information or provide a cyber security plan.

So, really for new reactors, the first opportunity for the NRC to verify compliance of the cyber security programs is after the combined license is issued. Which may be long after the referenced design certification was complete and for operating reactors, the design information becomes available for inspection when the system is entered into the licensee's cyber security program.

So, this timing difference increases

the risk the COL holders or licensees who are ultimately responsible for complying with the NRC's cyber security regulations will have to address any vulnerabilities in this design after the design has been completed.

Next please. So, the ACRS has raised concerns regarding control of access to plant equipment and networks in which they emphasize that control of access to critical plan systems should be reviewed as part of design certification and COL application reviews. They have also raised a similar concern regarding the licensing reviews on operating plant digital I&C upgrades.

Next slide. So, the ACRS has recommended uni-directional communication from Level 4 to Level 3 and from Level 3 to Level 2 of the cyber security defensive architecture. That is enforced via a communication flow enforcement device and the design of this device would be reviewed during licensing.

So, that slide is a picture of a recommended approach that is described in Reg Guide 5.71 and previously the ACRS has also raised similar concerns when Reg Guide 1.152 Revision 3 was updated to remove the cyber security guidance.

In that case, ACRS believed that cyber security controls should be reviewed during the licensing to demonstrate compliance to 10 CFR 73.54 and they did not find that was -- that we should remove the guidance for cyber security from Reg Guide 1.152.

In addition, the NRC has received feedback from design certification applicants that the staff should review cyber security design features as part of the design certification application review.

For example, GE Hitachi submitted the ESBWR Cyber Security Program Plan as part of the ESBWR design certification application.

Similarly, Westinghouse submitted the AP1000 PMS Computer Security Plan.

But, since demonstrating compliance to 10 CFR 73.54 is the responsibility of the COL applicant, staff was not able to review aspects of the plan addressed in 10 CFR 73.54.

And recently, NuScale requested the NRC review cyber security features as part of their design certification application that they're planning on submitting. However, as you can see, we still run into the same challenges that we would

not be able to perform those reviews during licensing or design certification.

So, there are international standards that recommend that cyber security requirements be defined as early as possible in a system's lifecycle. For example, IEC 62859.

And we do see that consideration of cyber security early in the system development lifecycle can improve both a system's ability to resist a cyber attack and limit the adverse consequences of a successful cyber attack.

We do want to recognize that some licensees have worked with vendors to incorporate cyber security controls as part of the development of digital I&C systems. However, this is a voluntary measure.

And because design certification applicants are not required to address cyber security, we feel all applicants must address the requirements of 10 CFR 73.54 later during licensing process and as a result, cyber security controls are often not considered during the early stages of system development lifecycles and if a vulnerability exists within the installed system, the licensee would have to either modify the system

or implement a compensatory measure to mitigate that vulnerability.

And this approach may not be as effective as developing a more secure and robust system that's provides inherent protection against cyber attacks.

So, another benefit that we see is that incorporation of cyber security design requirements into the NRC's regulation would enable the NRC to review the applicant's or licensee's proposed cyber security measures earlier in the licensing process.

So, we see that incorporation of cyber security design requirements into the NRC's regulation would enable the NRC to perform licensing reviews of applicant's and licensee's proposed cyber security measures earlier in the process and that cyber security design requirements will provide an added level of regulatory assurance for new reactor designs and for new safety I&C systems to be installed in operating reactors. In this case, the COL holder or licensee would be able to reference the staff's safety evaluation on the cyber security design controls in their cyber security program.

For example, if the staff review the design of an information flow enforcement device like a data diode during licensing and confirms that this device provides the unit direction of communication flow enforcement via hardware means, then the COL holder and licensee would be able to reference the staff's safety evaluations to support subsequent cyber security inspections.

We're currently looking at three potential options to incorporate cyber security design requirements.

The first one is to develop cyber security design requirements to complement the current programmatic cyber security regulations in a more holistic manner. This would be applicable to both design certification and COL application as well as licensees seeking approval of digital upgrades for safety and important to safety systems and we want to state that although we recognize that tends to be a part of 73.54 covered systems that are associated with safety and important to safety as well as EP and security functions, the design requirements would only be applicable to systems that perform safety and important-to-safety functions. So, we're not looking at all SSEP

functions. Only safety and important-to-safety functions.

And also, licensees and applicants could provide -- we see, you know, that one thing that's to be provided would be information that demonstrates that cyber security controls were considered during the design of systems that perform safety and important-to-safety functions. This could be the result of cyber security vulnerability assessments conducted for systems and information on how any vulnerabilities identified are mitigated.

Next slide. So, it would be kind of similar to how SDOE reviews are done, but to address cyber security to address malicious acts, too.

So, the second option is to develop regulations to require that technical controls for information flow enforcement be submitted to the NRC. So, this is a much more limited review. So, specific to the controls specified in Section B.1.4 of Reg Guide 5.71 which is the one-way, hardware-based data communication path between the Levels 4 and 3 and Levels 3 and 2. The cyber security defensive architecture.

So, we're limiting the scope to a much

smaller review. It only would be targeted at the battery devices between the different levels of the cyber security defensive architecture.

Next slide. And, of course, the last remaining option is just to do what we are doing right now which is to continue to verify compliance to the licensees' operational cyber security program via inspection without first conducting a cyber security design review of any system.

Next slide. So, just to summarize, we are considering options for incorporating cyber security design requirements for power reactors. This effort is continuing to address concerns raised by the ACRS as well as Design Certification Applicants.

We want to emphasize that the NRC is not looking to add new cyber security requirements, but potentially changing the licensing process to enable us to perform cyber security reviews as a part of licensing. This is meant to complement the existing cyber security programmatic requirements and not change that programmatic requirement.

We are currently considering these three options and we would like to hear back from industry stakeholders and also, if you have any

recommended options that we have not considered.

So, can open it up to discussion right now.

(Whereupon, the above-entitled matter went off the record at 8:54 a.m. and resumed at 9:10 a.m.)

MR. JONES: Okay. Welcome back. Sorry for the technology fiasco here. We're going to shift over to all handheld mics. So, folk on the speaker's table here, may sure you use a handheld mic and in the audience, I'll just bring you a mic whenever or we'll pass it. One or the other.

Also, please make sure that when you speak that you give your name and your affiliation please. Thank you.

We're going to start off now with a few words from Richard Stattel from staff.

MR. STATTEL: Thank you. I just wanted to add a little bit of perspective to Deanna's presentation.

There's really two different dynamics that are going on with cyber security. One has to do with the operating plants and that's where I'm being -- I'm representing that side and the other

is the new plants and they're very different dynamics because the operating plants what we're finding is they're doing very few modifications. So, we have very little opportunity to review cyber security features in the systems or those programs.

So, for the operating plants, the programmatic requirements from 73.54 are really -- we're getting a lot more bang for our buck than we would get if we were relying on licensing review activities and on the new plant side, it's kind of the opposite. Because on the new plants, we're reviewing designs right now and we're not reviewing the programs because the programs don't go into effect until we get the COL applicants involved.

So, all those inspections and the cyber security plan implementations are kind of future activities. So, what we're trying to do is we're trying to be consistent between the operating and new plants and try to cover the gaps because I think there are gaps or at least perceived gaps. We're receiving that kind of feedback from ACRS and from industry and we're trying to fill those gaps and that's really what this workshop is all about as far as identifying what the gaps are.

I think, you know, the staff has had a

lot of internal discussions. So, we think we have an understanding of it, but we'd also like to get both operating and new reactor perspectives on that as we go forward today.

So, I just want to add that perspective and background. Thank you.

MS. ZHANG: So, did you --

MR. BAILEY: All right. My name's Mike Bailey. I'm with Duke Energy.

First off, I want to thank the NRC for the opportunity to participate in these discussions about the design for digital I&C as well as cyber security requirements and processes.

We have looked at the information that was provided as part of this meeting. We had some discussions within the industry ourselves trying to better understand and one of the things we wanted to come out of this with is a better understanding of the effort that is under way and what we're trying to address through this effort.

We do have several questions to try to address. Trying to clarify some of our understanding of what has been proposed or what is being looked at at this point in time.

In the initial discussion and kickoff,

we talked about the fact, I guess, there's no plan for cyber security requirement changes as part of this particular effort. Also, some of the discussions up here talked about the fact that we're looking more at process changed.

Some of the information in the slides tended to point towards the fact that we're actually looking at design requirements or regulations. So, we're trying to understand what was actually being proposed in regards to are we actually looking at design regulations or requirements or additional digital requirements that are not currently out there as part of this effort.

MS. ZHANG: We are not planning on adding any additional technical requirements, but from a process perspective, we do need new regulations in order for the NRC to perform the design review.

So, currently, it's programmatic requirements and as such -- and it doesn't design certification applicants. As such, any information that's -- even if it's submitted voluntarily, we have no means of performing a licensing review for that.

MR. BAILEY: And Rich touched on, and Deanna, you touched you it as well, some of the I guess areas that you sort of see this gap that we need to try to cover with these programmatic changes.

One of the things as an industry we had talked through is between Part 50 and Part 73. There seems to be a pretty good dovetailing between what is actually covered in the design certification piece as well as the programmatic cyber security area and as a result of that, I mean, there was even some presentations that had been done with ACRS back in 2011 on February 23rd with Jay Amin and Matt Gibson at that time. Covered how those various requirements and regulations that currently exist work to insure safety and security of the existing systems that are being installed.

What gaps do we see? And I understand the process gaps. But do we see any gaps in regards to regulations that would not insure security or safety at this point in time with what's currently being done in the design certification or the cyber security review process?

MS. ZHANG: I think, you know, NSIR can chime in if what I'm saying is not correct.

Just to give an example, I guess, we've seen where design certification applications where there's a lot of interconnectivity between different systems, safety, critical -- basically critical systems and systems that, you know, are less critical from a cyber security perspective, but because everything's interconnected in accordance with Reg Guide 5.71, they would all need to be protected at the same level and thus from, you know, when the design certification applicant made that design, you know, it added -- it basically required more systems to be protected from a COL applicant who's going to inherit that design and as such, you know, there would be more risk involved or they wouldn't have to modify the design or make, you know, or protect more systems.

MR. STATTEL: I'll add to that. I can speak from the operating plant side again. The perceived gap really has to do with the amount of attention that we give to cyber security during the design review.

So, as you know for the Oconee Reactor Protection System design, we actually did perform a cyber security review because it predated the current policies and the rule. So, there wasn't

really any transfer to the program that occurred during that review.

When we presented to ACRS the Diablo Canyon application, they asked a lot of questions about the design review and what we were considering from the cyber perspective and basically, no, we're not considering that during our review now, but that will be covered later on at the time when these systems get implemented into their cyber security program.

So, the way we anticipate that going forward is the plant or the licensee would identify the new system as being a critical digital asset. They would do the assets. They would identify the security impacts of that and then they would take those measures. All future tense. Right? So, the perceived gap is that time frame between when we do our license amendment review and when the system actually gets incorporated into the cyber security program.

So, it's a time difference and there's not a direct turnover from what the staff reviews as part of the design and what NSIR would be performing their inspection items for. Okay.

So, and I think it's similar, but a

little different for the new plants and, you know, I haven't been receiving the same feedback from the new plants. So, for the new plants, it's different in that they have really no opportunity because they're not seeing the detailed designs. Because a lot of that's deferred to the closure of the ITAACs and the DACs. So, there's currently no emphasis on the cyber security aspects.

So, the fear is that they do not get addressed as the design goes forward and then when the COL picks up that design and takes over and initiates their cyber security plan, you know, it'll require new design changes and other like backward type reviews. Backward looking reviews.

So, I think that's more of a risk factor with the new plants.

MS. ZHANG: And from a new plant perspective, you know, as we had mentioned before, 73.54 does not apply to design certification applicants.

So, there is a much greater timing difference potentially. So, a design certification might come in with no COL applications to come with it. So, they may not be well informed of the cyber security needs of future

COL applicants.

MR. HERB: This is Ray Herb, Southern Nuclear.

I'd like to ask a question to clarify the scope of this proposed new regulation.

Currently, Part 50 is very clear on safety components. It becomes less clear in the non-safety arena.

How is this potentially going to cloud that issue even further?

MS. ZHANG: So, for new reactors, it's any systems that we would review normally under a design certification for Part 50.52.

We would review those systems if there are any cyber security controls implemented for those systems. So, if it's not a system we would normally review as part of design certification or COL application review, then we would not do a review of that particular system.

MR. HERB: Okay.

MS. ZHANG: And it's something similar if there's --

MR. STATTEL: Yes, let me say a couple of words on that. That's a very good question and it's something we've been kind of struggling with.

Because if I hear you currently, your concerned that the -- we're expanding the scope of cyber security review into the non-safety and important-to-safety regimes. Right? Is that correct?

MR. HERB: Correct.

MR. STATTEL: Okay. And there is some truth to that. So, for example, during the Oconee review, we did do a design review of the device that is basically enforcing the one-way communications from the safety system and that was a non-safety component of that system.

So, I think it's true, you know, that cyber security really goes beyond just the safety system. You can't just draw a box around the safety system and say because -- you know, because I did this design review or because it's designed correctly, then it's secure from a cyber perspective.

So, you really have to -- you do have to expand the scope beyond that and where you draw the lines, I think that's something that's kind of up in the air. That's something we really need to discuss.

MR. BAILEY: Staying on the scope

topic, just a follow along question with it.

We talked about the interconnectivity, a lot of interconnectivity of digital components or systems at the plant.

Now, the scope part sort of pointed to new reactors. Things that would be on the NRO scope. Basically, instrumentation controls that would be looked at.

The examples that Rich provided for Oconee and Diablo Canyon were safety specific. Safety system specific.

Granted we did go out with a non-safety device to address one-way communication, but most of the interconnectivity that you get into is on the non-safety side where you start getting into control systems that actually control the plant and need to share information as well as your plant computer and plant information systems that interface information out to operators or to maintenance and plant engineering personnel.

So, from a scope standpoint, most of your connectivity really happens when it's on non-safety and I would think things that typically aren't reviewed for NRO or NRR from a design certification standpoint.

MS. ZHANG: And, you know, I think we need to look into how much would extend into non-safety systems. Typically, for new reactors right now, we do look at the control systems. Particularly when it impacts safety. That would be our focus, too. But with cyber security as 10 CFR 73.54 defines important-to-safety functions, there might be a little bit of a difference.

So, we will need to reconcile that and that's something that we would have to look into.

MR. STATTEL: Yes, I would just add. So, for the operating plants, typically, if we're looking at a license amendment, we really get all that's in our purview is that safety system.

So, it's really impossible to address all of the cyber security aspects outside of the context of the installation and all the interfaces to the non-safety systems. So, I don't think it's a complete answer.

I don't think -- you know, we could expand the scope of our -- of what we do during the design evaluations, but that's not going to get us to where we need to be as far as having assurance of cyber security. So, it really still has to have some programmatic aspect.

So, NSIR still needs to be involved. They still need to perform the inspections. We're really relying on the cyber security plans and the implementation of those plans to provide the assurance for security.

But, at the same time, I think the technical staff is kind of in agreement. You know, we believe that we're capable of performing additional scope of review during our safety evaluations to kind of help that process along and give some added assurance.

So, I don't think there's any one answer to that.

Particularly in operating plants, I think that our purview is really limited to the safety system. So, we really can't go outside of that. We're not looking at the system in the context of the installation and all the interfaces.

I don't think that's true necessarily for the new plants. I think they do have the whole system in front of them. So, they actually do have a broader perspective on that.

MR. BAILEY: And, Rich, on the Oconee example, I know whenever you all -- we went through the efforts on the port tap aggregator to do the

isolation. I didn't necessarily consider that branching outside the system myself because it was more or less a -- all the issues we've been talking about with the safety-related software and how it dealt with the isolation capacity. That was just another means to address isolation and so it to me was actually -- even though it was a non-safety element, it is still part of the actual system and requirements for the system. So, I didn't see that necessarily as a branching out into non-safety myself too much.

MR. HERB: I have an additional question related to scope.

The design requirements for a protection system are to protect the health and safety of the public through protection of the barriers to release of radioactivity.

In some cases, some of the cyber security design requirements make conflict with that original design purpose of our protection system.

How are you going to handle that if you incorporate that into Part 50? Those design requirements and wouldn't it be better to leave those requirements in 73.54 when the cyber security

threat picture often changes as time goes on? Where the function of the protection system is static and often remains the same forever and so, I think you see where I'm coming from. Changes to the threat vector could impact your design of your safety system over time if you've incorporated some of these design factors into the design of your safety system.

MR. PEZESHKI: Okay. The reason why I wanted to speak first is you had mentioned a transition from 73 space to 50 space and I don't believe that is the goal here.

The intent is not to generate design level cyber security requirements to replace the programmatic requirements. The idea is more or less to create cyber security design requirements that will dovetail with the programmatic level. The idea being that industry can tackle cyber security concerns earlier in the process to better meet the programmatic level cyber security requirements.

MS. ZHANG: And even in the current guidance in Reg Guide 5.71 as well as Reg Guide 1.152, we emphasize that we don't want cyber security features to adversely impact safety. So,

performing the safety function has to always come first.

If there are cyber security controls, not necessarily features, that could be adopted when you're designing the system to make it such that it's, you know, less likely that a cyber attack will be successful or reduces the attack vectors, then I think that is what we're looking at. You know, reviewing. Not necessarily that a particular, you know, like something like an IDS, intrusion detection system, is implementing a safety system.

So, we definitely want safety -- the safety function to be the priority.

MR. STATTEL: Yes, I sure -- I think what you said, Ray, is kind of supporting the idea that we really do need to maintain the programmatic requirements.

I always say that, you know, the safety systems, these are the crown jewels that we want to protect. We don't really want to complicate them and add these measures into them and we've been working with international agencies. IAEA has a new safety guide that's out that has guidance to that effect.

So, if you're choosing whether or not to implement a cyber security measure, if you're choosing whether to implement that on a -- within a safety system or within a non-safety system, there is guidance out there and we're also working with the IEEE 74.32 group to add to -- include that guidance for the U.S. plants.

So, however, the option is still there. So, if there are measures, if there are Reg Guide 5.71 measures that you choose to implement within the safety system, I'll use the intrusion detection not that I would ever expect anyone to put those kind of features into a safety system, but if you choose to do that or any of the other measures from the Reg Guide, the idea that we turn a blind eye to that, you know, as part of our safety evaluation review and we rely on the program by itself to evaluate the impacts of that or the effectiveness of that, that's kind of what this -- what we're talking about here. That's what we're trying to cover.

I think it's beneficial to have the technical staff review those features if the applicant chooses to implement them in the safety system at the time of the safety evaluation. I

think that's beneficial because, you know, we're the ones that would, you know, have the expertise in that area.

MR. GIBSON: I don't think I believe the --

MR. JONES: Again, for all the speakers, please give your name before you speak. Thanks.

MR. GIBSON: Matt Gibson with EPRI. Just want a -- a process observation. You look at this thing technically. Something you should consider is that a design process involves tradeoffs. Right? I mean, so you take all the competing system requirements and you figure out, you know, how I should do this. Well, one of the things you want to keep in mind is that from a cyber security point of view, the designer has a lot of options to address the cyber security requirements of 73.54 that are outside the actual design of the system.

So, I think when you think about this problem think about the sequential timing of when the design decisions are made. It's true that a COL applicant or a DCD or vendor has to come up with at least some level of design to get certified.

At some point though, those design decisions are at a certain point in time in the design certification. Later on when a COL applicant adopts that, one of the things they have to do is continue that process by evaluating that design against their chosen cyber security programmatic implementation requirements.

The point I was going to get is let's keep in mind that some of this has a timing -- from a technical process point of view, there's a timing concept and design process that you could disrupt if you go too far with trying to move some of these topics at different places in the design sequence. It can have an unintended consequence and that's just a comment I want to bring to the table.

MR. JONES: Other comments?

MR. STATTEL: Yes. I do agree with you and, you know, I think a lot of this falls back to engineering judgment, but the fear that we have and when the decision was made to basically shift reliance onto the programs, I had a concern that even back then, you know, six/seven years ago, that the inspection teams that were looking at these cyber programs wouldn't necessarily have the technical background to be able to review the

impact on the designs and that's where the concept of the SDOE came from.

So, when we do our technical reviews, you know, we're looking for if you've implemented any of these cyber measures, we want to have some assurance that it doesn't have any adverse impact on the safety function.

So, we have some competing objectives here. So, one of the things is we want your safety systems to be a simple as possible. We only want them to do functions that are safety functions and on the other side, we have these cyber security requirements that are saying make the system more complicated by added cyber security functions. Right?

So, you know, the decisions get made at various points during the design process. We just want to make sure if the decisions are made early enough and we have that opportunity during the design reviews to evaluate those designs, that we don't miss that opportunity. Because if we simply defer everything to the inspection teams, I think there's a risk or there's a danger of things falling through the cracks.

So, people will implement cyber

security measures that don't get evaluated. They don't get properly assessed for impact on the safety functions and, you know, we could have problems down the line without having had those design reviews done up front.

Now, SDOE was intended to address that. How well it does that, you know, I guess that's, you know, a matter of, you know -- there are different cases that you could study.

MS. ZHANG: Just very quickly. We're not looking at implementing everything within Reg Guide 5.71 or NEI 08-09. This will be selective maybe controls that could be considered earlier and this is more about a consideration of them. Not necessarily implementing those controls and definitely, you know, if you had to implement it within the safety system, I think that a lot more attention needs to be paid for that.

We do see a hand off between the design certification applicant and the COL applicant.

Now, you know, we -- it's not like everything can be done by the design certification applicant, but if there's something they can do to kind of -- it's a look ahead to enhance the security of their design, I think that could be done earlier

and I think that would make it a little bit better for the COL applicant.

MR. STATTEL: One other point. As Deanna mentioned, we've had several design certification applicants submit cyber security plans or documents, licensing documents and the fact that they are able to create those documents, you know, clearly it's kind of a -- kind of testifies that there are certain cyber security measures that they're incorporating into their designs at the early stages. Which is a good thing.

And the fact that our process doesn't really allow us to review that and credit that in those advance stages, kind of points to a problem and I think that's where the ACRS' concerns are really coming forward.

MR. GROSS: I have a process question. Is there sort of a time horizon you're working to for the SECY paper? Do you have a, you know, commitment to the Commission to get something to them by a certain date?

MS. ZHANG: We don't have a formal commitment to the Commission, but we are looking at completing it by the end of September.

MR. GROSS: Do you expect that there would be additional public workshops to discuss the progress and the development of the SECY paper before September?

MS. ZHANG: Well, you know, if that's something that the industry would like, we could definitely set that up.

MR. JARRETT: I guess I'd like to -- Ron Jarrett, TBA.

Rich, you mentioned Diablo Canyon review. We've discussed 74.32, NUREG 1.152. In those documents, there is cyber-related or security-related requirements.

So, I assume when you did Diablo review, you looked at those areas.

MR. STATTEL: Not really cyber security. So, our review is really limited to the secure acknowledgement and operating environment.

MR. JARRETT: Secure. Yes.

MR. STATTEL: So, I guess -- you know, our review guidance doesn't have the word cyber in it.

MR. JARRETT: I understand, but there's a lot of aspects in that. There's some aspects in 74.32 that do touch on it and I guess

I'm trying to get a feeling of what additional things -- you know, there's -- we've improved 74.32, 2010 added more requirements that were in the original Reg Guide Rev 2 and now, we're out to -- with a new version of 74.32 that even expands that area. So, I'm trying to see -- get a feeling of what additional things would be reviewed in addition to what's in that document.

MR. STATTEL: Okay. There's two different scopes at hand here. One is the scope of IEEE 74.32 which goes beyond what our review scope for our safety evaluations is. Our intent, because right now kind of the guidance is kind of duplicated in the Reg Guide and in the IEEE standard, these changes we're currently making to the IEEE standard make it consistent, and Deanna can speak to this, too, make it consistent with our current Reg Guide review criteria.

Our plan is the next revision of Reg Guide 1.152 would basically delete that section and we would simply endorse the IEEE standard for the SDOE aspects.

We do -- right now, until we get some direction from the Commission and that's kind of the purpose of this paper here, our policy is really

to limit the scope of our review to SDOE.

So, in other words, we're not ignoring the cyber security requirements. But, again, the SDOE perspective is if cyber security measures are being put into the design, we are evaluating whether those features have any impact on the safety functionality of the system. So, our safety evaluation is still focused on safety. Okay.

So, it's a little different perspective.

MS. ZHANG: So, for the SDOE review, I just want to remind everyone that it's focused on addressing non-malicious acts.

So, if there is anything that, you know, was there to address malicious aspects, too, we cannot make a judgment as far as the -- you know, whether it could be used to address malicious acts. Our safety evaluation would only consider to address non-malicious acts.

MR. JARRETT: Just a follow-on question. When we worked on ISG4, it was to allow two-way communication safely. In essence, it was kind of like a data diode, but with two-way communications. You weren't -- if you implement

that, you should not be able to affect the safety system. You know, that's been relevant to the 74.32 and so, where is that headed in this area?

MS. ZHANG: Well, what we want to -- you know, so, we do recognize that a lot of things that we do for safety could also be used to address security, but it's not necessarily a complete overlap.

So, you know, although some things can be used to credit -- you know, to address cyber attacks, too, but doesn't necessarily mean that that's the only thing that would be effective at addressing all cyber threats.

So, that's why you do need the programmatic aspects, a cyber security program in addition to whatever we do for our safety review.

MR. PEZESHKI: And also since during the SDOE review malicious acts are not considered, none of that can be referenced or credited for the eventual programmatic 5.71 or 73.54 review. So, as I said, one of the hopes here is that this will give the industry an earlier bite of the apple for ultimately meeting their 73.54 requirements.

MR. REBSTOCK: I'm Paul Rebstock from the Office of Research. I was involved in the

development of ISG4.

And the bidirectional communication that that allows is extremely limited and I am not sure that it's fully appreciated just how limited that is.

That process allows for the non-safety system to send some data to the safety system which the safety system can then read and figure out what to do. It explicitly does not allow the non-safety system to send any commands to the data -- to the safety system. It can send a number and the safety system can be programmed that if that particular number has a certain value, then it can go do something that's already been programmed. But there is no way to send a message into the safety system that would cause the safety system to do something unexpected.

So, some of the systems that I've seen under development don't do that. They seem to think that they're following ISG4, but they allow commands to be submitted into the safety system and I think there's some confusion there.

MR. GROSS: Hi. This is Bill Gross from Nuclear Energy Institute.

And I feel compelled to tell a story

about cyber security in the early days and I got involved in IT in about 1995 and at that time, it was -- cyber security in IT was a bit -- it was the wild, wild west. It kind of still is, but it was really bad then.

And I would imagine for those of you that had been at that game at that time, you remember Windows 2000. The most secure operating system every built. That was the vendor claim.

So, let's assume at that time two things happen. First, Microsoft paid an awful lot of developers an awful lot of money to be able to make that claim and those costs were passed on to the purchaser of the product.

Second, suppose that NRC had endorsed the safety and security features of that at that time. Right.

Now, roll the camera forward 20 years and you take a Windows 2000 box out of the -- you know, out of the box it comes in. It's no longer the most secure operating system ever built. Right.

The licensee who's now purchased this thing has to install it and build an operational program to secure it. So, now not only are they

paying for the vendor to have built a product that's not secure because time has gone by, but now they have to build the operational program that we're currently required to build to protect it. All right. So, the costs are being incurred twice for the same level of cyber security. All right.

So, there is a gap as Rich pointed out between when the NRC approves the design of a system and when it's built into an operational program.

But I would claim that even if that device was secure at the time that it was certified because of the emergence of and the changing nature of the cyber threat and our understanding of the ability to exploit systems, it's not secure by the time you install it and you still need the operational program to do it.

I think, you know, another point is if you claim that if we can't review cyber security features at the time that it's designed or we don't have the capability to do that and that limits our ability to understand how we can secure it when we're -- you know, when we're going to put it into operations, really calls into question whether or not we have the capability to implement 73.54 to protect the plants that we have today that are

replete with digital systems both non-safety and in the balance of the plant that were never designed with cyber security features integrated into them. All right.

So, while I appreciate as having, you know, two degrees in computer science the deep desire to integrate cyber security features into the design of systems, it's a temporary -- it's a temporary fix to a problem that gets bigger and harder over time and, you know, as was pointed out, if simplicity is an attribute of safety, simplicity is also an attribute of security.

I've never seen a complex system adequately protected against cyber attack.

So, if you want to protect something against cyber attack, whatever it is you're trying to protect should be as simple as possible. Makes it much easier to do.

MS. ZHANG: We appreciate that remark there.

We don't see this as -- that any review we do for safety or important-to-safety system as the end all. That this is going to be a completely secure system.

There are going to be additional

measures that's going to have to be implemented on a programmatic level because of evolving threats and so, what we want -- what we hope to accomplish is that if they do choose, if a design certification applicant or a vendor does choose to kind of consider cyber security earlier in the progress and they want to have the NRC review those particular measures that there is a means for them to do that.

But, of course, you know, that doesn't remove the fact that we still need a cyber security program to address evolving threats.

MR. STATTEL: I mean, I guess part of the workshop here, one of the main objectives is to kind of solicit feedback.

Is there -- I'm not hearing a lot of resistance or push back on the idea of us performing these types of reviews during the design certification process or during the license amendment review process. I mean, am I incorrect in that assessment?

MR. GROSS: Yes.

MR. STATTEL: Okay. That's what I want to hear. I want to hear, you know, the push back. I'm really -- you know, the discussion's kind of gone around in circles here and we're talked

about two-way communications and we've given a lot of good examples.

So, I think a lot of us understand, you know, what the problems are, but we really need to decide on a path forward for our regulations. How we go forward and regulate and insure security of these systems. So, I guess I want to get us back on track as far as getting that feedback from the industry.

MR. BAILEY: I think Brad wants to say something and then we'll actually address directly your question or comment.

MR. YEATES: Yes. My name is Brad Yeates with Southern Company.

So, I'm not going to give you that push back just yet. I'll let somebody else do that, but I did -- I think you're not hearing it yet because we're still trying to understand and really, really seeking to understand. So, my question is still along those lines.

So, what I have heard is kind of two different perspectives or there's two objectives you're trying to accomplish.

The first one I think is very consistent with the safety evaluation and that is if an

applicant -- a design certification applicant or a COL applicant chooses to implement cyber security controls into the design of a system, you want the ability to review those controls to insure that they do not have an adverse impact on the safety function and that makes perfect sense.

And I would submit that you have that authority today. That is part of the safety evaluation.

So that you would not need additional rulemaking to assert that, you know, jurisdiction.

MR. STATTEL: And I agree with that.

MR. YEATES: Yes. Now, the other aspect that I'm hearing, I'm hearing mostly from Deanna, is that you're seeking the opportunity earlier in the design process, in the time frame, to require the implementation of cyber security controls in the design.

And I think that's the area where, you know, we need more understanding of really what does that look like. You know, where is that? What we've seen in the presentation is focused mostly on the isolation aspect. But there's, you know, in the Reg Guide 148 -- or yes, 148 or 146 controls --

MR. STATTEL: I think an example would serve us well at this point. So, let's pick a really simple example that a system developer wants to have a password protection feature in their system. Right? So, and we've seen these systems.

So, we could review that during the design evaluation and we could say okay, we can enter different passwords, enter incorrect passwords, make sure they don't work, but that doesn't really give us any real assurance that the system is secure because how they control that password, how they share it, you know, with their staff members when the licensee gets the system is really -- that's -- you know, if they just put it on their public website and give everybody access to it or they make the password a non-strong password, it's just 1, 2, 3, 4, then they're really not accomplishing that security objective.

But what I can do during the safety evaluation is I can look at the lines of code or I can look at that actual design features and I can look at the testing that was done on that and I can get that assurance like you say that nothing -- entering the incorrect password isn't going to prevent the safety system from tripping the

reactor. Okay.

And that's that assessment we currently do. So, we're already doing that. That's correct.

Now, I don't -- I think requirement is not really what we're after here. We're not -- to ask me, the technical evaluator, to make an assessment of whether that password protection is going to maintain the security of that system without knowing what the licensee's going to do or how they're going to control passwords, that's asking too much of me.

But you have the option, I think. I think if the applicant is willing to put those measures in place, I guess there's some degree of assurance that can be achieved as long as you put the right condition. So, you can establish the rules for setting that password. You can establish limits on what the password can be or how it can be disseminated.

So, I think what we're trying to do is give you the option. Right. So, like we said before, you know, we already have applicants, design certification applicants, that want to put those types of measures forward, but we're really

not set up. Our processes aren't really set up to do the cyber evaluation part of that. We're only set up to do the SDOE evaluation.

MR. YEATES: So, if I were to restate that, repeating back what I'm hearing, you're seeking the authority then during the design review to certify compliance with 73.54 or at least aspects of it.

MR. STATTEL: I guess I'm going to let the -- see we -- right now, we don't have the authority to do that in the safety evaluation processes. So, I guess I'm going to defer to NSIR to answer that question.

MR. FELTS: Yes, I tried to -- Russ Felts, Deputy Director, Cyber Security Directorate.

As we started off the meeting, I tried to have the early stage dispel the potential for that interpretation. That what we're looking to do is a review that would establish compliance with 73.54 at the design cert stage because 73.54 requires an operational program and so, there's so much more that needs to be done that would be impossible to accomplish at the design cert stage in order to meet 73.54.

We are --

MR. STATTEL: I think it's more intended to set you up so that it would be easier for you to complete that certification.

MR. FELTS: Easier to complete and more importantly not impossible to complete. Right. We don't want a design sitting on the shelf that is so potentially interconnected or has features that make it virtually impossible to meet the programmatic and performance requirements in 73.54.

MR. STATTEL: Right. So, reverting back to our example, if I have done an evaluation and I have reviewed the password protection feature not only from a safety perspective, but from a cyber perspective in terms of how those are controlled, what measures are put in place to control that, we can document that and that becomes information that the inspector that's inspecting your cyber security program can use to verify that those measures are being appropriately implemented and it would -- you know, I think the idea is that would go a long way towards achieving the certification that you need to get.

MR. FELTS: Yes, and again, I think

it's important for us to have this conversation we're having right now keeping in mind the options that -- potential options that we laid out. Right.

Option 1 would be to review at the design cert stage the application to verify that the licensee or the applicant has considered cyber security. It's very high level. Essentially to verify that they haven't designed a system that can't be secured. I mean, that's really ultimately what we're talking about.

Option 2 is verifying that the design incorporates an architecture that limits communication at certain levels to enable that defense in depth requirement in 73.54 to be met.

And then Option 3 is the no action option.

And as we said at the beginning of the meeting, we are seeking input here. If the industry or others, other stakeholders, have ideas on other options we should consider, we're interested in your input.

MS. ZHANG: Yes, and also, you know, for the -- just the password example, we could look at the design of that feature and say, you know, if you claim it's, you know, a ten-letter password,

we can verify it's a ten-letter password, you know, and that it would only accept a ten-letter password.

Stuff that's really on the design side. Not how effective it is at protecting a cyber threat.

MR. STATTEL: This also goes back to a lesson we learned with the Oconee review. So, as I mentioned before, when we did the Oconee review, our intention was to perform a cyber security cyber-based review as a part of the design evaluation.

And what we found was we really weren't able to get any kind of high assurance that the system would be secure once it went into operation because there was too much that had to happen during the installation and there was too many things that the licensee -- we were relying on the licensing to do in order to establish the security of that system.

So, if you look -- if you read the Oconee safety evaluation, there's a section in there called -- I believe it's recommended inspection items. So, we realized that we were not going to be able to complete our cyber security evaluation

during the design evaluation. So, we kind of kicked that over to the inspectors and they followed up during the installation and during the start-up testing and they were looking at what the licensee -- what measures the licensee was taking. Locking keys, password protection, controlling USB ports, things like that.

And so, I mean, that was our really only recourse there. So, we kind of pushed that out to the inspection space anyway.

So, I think we're really talking about a similar type of turnover and feed forward program between the safety evaluation -- we want to communicate with NSIR. We want to communicate with the future inspectors who are going to be evaluating the cyber security programs. So, you know, we want to have that early on understanding of the design.

MR. YEATES: Yes, and this is Brad Yeates.

So, just a matter of making sure that it's on the record here, too, the process that we went through for the COL application for the AP1000 at Vogtle 3 and 4, we were required to submit our cyber security plan along with that COL application

so that that plan was -- received a safety evaluation.

Now, the vast majority of plan is programmatic in nature, but there is one aspect that is technical design in nature and that was the defensive architecture. So, within that plan, we laid out a relatively detailed architecture that described the communication of functions within the plant and that was reviewed and approved early, very early in the design process.

So, I would just submit that there currently is an early design review of that technical aspect of the cyber security design that is part of the Part 52 licensing process.

MR. JACKSON: This is Terry Jackson with NRC.

So, just to go along with some of our experience with AP1000, I remember they did submit to us sort of the cyber security plan and so forth. I remember the discussions we had with them as it was in -- it was mixed in with the I&C design information as well.

We ended up requesting that Westinghouse take that -- the cyber security information out. The reason was because the

staff, the I&C staff, couldn't make a call whether it met 73.54 or not and we couldn't leave it in there either because we didn't want someone to think it was some sort of tacit approval if it was left in there and nothing was said about it. So, they ended up having to remove that information.

Now, in the cyber security plan review, they may have reviewed some design aspects to a certain degree, but it's probably at a higher level.

I think overall when the staff was working on, you know, this SECY paper -- and I think one thing to understand is that, you know, we're talking about different kinds of design controls and stuff. We haven't really sat down and identified which ones may be in the scope and which ones may not be in the scope at this time.

We felt it was fairly premature because we wanted to go to the Commission and see do they even want us to go here before we expend a lot of resources on it.

Now, in the back of our heads, I think there were some things that we thought would be beneficial and we thought well, maybe the industry may think that this will add to efficiency. So,

for example, we talked about the secured development and operational environment reviews that we do in the safety review and we go through and look at that process.

Now, it's very similar to probably like the vulnerability assessments and stuff that are done on the cyber security end. So, they look similar and we -- you know, we were thinking well, if we're doing this and then later on, someone else is going to go out and inspect the same thing, but look at it from a malicious standpoint, is there a possibility for efficiency in combining the two and do that up front?

So, I think that's kind of the thoughts we had. We didn't necessary have a concrete idea as to what kinds of design controls may go in here. If the Commission gives us direction later on and say you got to do this, that's kind of like a phase two afterwards.

MR. STATTEL: I'm hearing a little mixed message here though because I've heard from industry. So, for example, ESBWR submitted a cyber security plan. My understanding is that they did not -- the NRO did not perform a safety evaluation of that plan or issue a safety

evaluation of that plan. Now, AP1000 preceded that. So, they might have -- that might have been done prior to the current policies becoming -- going into play.

So, you know, because the feedback that Deanna pointed out is that the design certification applicants want to submit plans and want to get safety evaluations performed by the staff and the staff's unable to do that, but then you're telling me the AP1000, that's exactly what had happened. So.

MR. JACKSON: I think that was under the COL applicant versus the design certification.

MR. STATTEL: Okay. Okay. Understood. Okay.

MR. BAILEY: I guess we've had a lot of discussion here and it's been very beneficial and fruitful to what we were looking at from our industry discussions that we had prior to the meeting.

Sort of summarizing all the pieces that you heard and Rich, this goes back to sort of, I guess, your request for some feedback in regards to the various options and we felt as an industry.

As I noted earlier, definitely

appreciate the opportunity to be involved and have these discussions now with the NRC.

One of the things, like I mentioned earlier, we did have some questions. We had an initial opinion based on what we saw in the presentation and so, we had some questions to try to understand and clarify that and really appreciate the information that you all provided.

As a result of our initial review and the feedback through these questions and answers at this point in time and it sort of is a summary of what all's been presented between the efforts that currently exist with Part 50 and the efforts that exist in Part 73, as an industry, we prefer at this point in time Option 3 that currently has the fact that there's no additional actions needed because the current regulations cover what is needed to insure a secure and safe operating plant in regards to digital and cyber security.

That being said, we definitely still would be interested in further discussions or additional opportunities as Bill noted to be involved in further dialogue to try to see are there other options out there. We were basically just looking at Option 1, 2 and 3 and didn't have a lot

of time to really factor in what are all the other options. What are some, you know, scope and boundary type aspects that could be tied to this?

Some of the other -- just to reemphasize the points that have been made, the items to support Option 3 and why we feel as an industry we are providing a safe and secure method by going with Option 3 is that Options 1 and 2 at this point in time don't substantially provide anything additional that's outside of Part 50 or Part 73 design and cyber security program aspects that would increase or enhance safety and security beyond what's already being done at the facilities themselves.

Part 50 covers the safety design review. There's a lot of industry guidance out there and standards that actually insure that things are safe and the right equipment is installed with the right controls and then Part 73 insures that we've got a secure platform and secure program at the operating units.

Also, the licensees themselves, one option in here is to do one-way transmissions as part of the cyber security program activities as well as the new operating reactors cyber security

programs. Data diodes or isolation devices are already factored into the designs. So, from that standpoint just having additional requirements or policies in place wouldn't change anything that's currently already in the system or in the programs that we have at this time.

As far as the burden, this sort of alludes to some of the things that Bill touched on. The aspect of including it, paying for it as part of the design and then paying for it again as part of the efforts of 73.54 programmatically. We're not really seeing a potential to reduce the burden, but we're actually seeing the potential to increase having to deal with it twice as we go through the reviews and the program implementation aspects.

And then the last point from a summary standpoint is that at this point in time and the framework that we have both for new reactors as well as current operating reactors, we're not seeing a major gap where we're actually having designs that are insecure, designs that do not factor in safety as well as through the design reviews that had been done and also through the inspections that are being addressed at this point.

So, in summary, that would be the -- I

guess, the feedback overall from the industry and that is based on the initial review and just the questions that we had, but we are open to additional discussions.

MR. HERB: Again, I'd like to reiterate. This is Ray Herb, Southern Nuclear.

When we say industry, we are talking operating fleet and not the vendors and the -- I mean, the design review applicants potentially.

MR. BAILEY: Thank you.

MR. JUNG: Ian Jung with the New Reactors.

Thanks for the feedback. That's exactly the purpose of this workshop. Is to get the industry feedback.

Terry Jackson and I are in New Reactors.

I just want to share a couple of points for more targeting new reactors and defense reactors. Okay.

For Option 1, it's three/four years, I mean, that we have gone through internally as well as externally with the ACRS and some of the applicants.

There are multiple letters written on kind of broad ACRS concern regarding the two

aspects of this whole licensing versus inspection framework of the cyber security. ACRS has specifically wrote letters regarding their desire and recommendation that cyber design element should be reviewed in licensing -- at the licensing stage with the right expertise. That was one concern.

So, I think the staff has taken at the office level -- through office level discussions that there were multiple options and one of them was a rule about any terms of inspection element that that has implemented in a joint expertise -- inspector -- inspection staff jointly is, you know, participating in inspection activity, That's ongoing.

There was a sort of a background that led into this potential option. When the ACRS spoke to the Commission about their concern on this broad brush of licensing versus inspection, the Commission was silent on it. So, I think ACRS eventually kind of gave up on raising additional concerns on that.

Option 2 became more of a bigger issue for ACRS last two or three years. Wrote actually multiple letters. Okay. One for mPower DSRS.

Difficulties on this standard. IEEE -- I think IEEE Standard 603 briefing to the ACRS as well as Office of Research plan. I think there was another letter.

And for Option 2 to consider at least for practicality perspective is -- is for South Texas and other applicants and US-APWR as well, they ended up voluntarily addressing it to address ACRS concerns to get their license -- licensing application approved.

So, in reality, South Texas operating records already have those diode air gap measures in place for those boundary devices. So, practicality-wise, I see either -- the reason we couldn't go back to ACRS, don't worry about it. It'll get done under programmatic element down the road. They simply didn't like that answer.

They started -- ACRS, I think, provided that recommendation that we could within current framework interpret the certain regulation in such a way this element can be part of the staff guidance that we can modify and review under IEEE 603 and other elements.

So, I think -- so, right now, we are in a stalemate with ACRS on that. So, we'd like to

hear potentially or consider for the industry for new reactors and defense reactors to have that very narrow element to be something that we can put it in the books so that we don't have that stalemate. Because technical solution not only cannot do it and then actually empower NuScale and South Texas MHI. They all have no problem doing -- specifying that element as a part of the licensing now. Right.

So, Option 2, I want the industry to consider that element. Otherwise staff and applicant as well as ACRS will I expect to continue to have this unnecessary significant burden on -- going back and forth on that. I think it's going to still continue to come to the Commission level on this issue for a while. So, I'm just suggesting that to consider.

So, one last item is on the defense reactor policy statement of the 2008. Yes, the Commission -- there's one element regarding cyber security element where it's a policy set up in such a way that these -- among all the other features simplicity and all the easy to analyze, easy to approve licensing predictability and stipulate and all that. There's one element also includes a

cyber security and overall plant system design that are developed from the get go so that it minimizes the implementation challenges. There's some language to that.

So, sooner or later, it seems like we need to reconcile that policy against the real practice that's happening. It seems like policies that you have to design it's sort of inherently safe and secure design in the policy. But the practice we are doing right now, it might be okay. That's what you're thinking, but maybe we can continue to have a dialogue on maybe longer term future. That is policy versus real practice and hopefully, it's more economic or more logical since we need to consider that all the way.

I just want to share those thoughts.

MR. CLARKSON: Greg Clarkson with NuScale Power.

I'd like to pause a moment and consider the scope of what we talked about today. We've got new plants, existing plants, protection systems, monitoring and indication systems, control systems, corporate networks, a secure development environment, how they're developed, how they're deployed into the plant, the programmatic aspects,

design attributes. This is a lot.

And I've heard a lot of examples and a lot of the examples are very specific to a situation. My concern is, and I think maybe this is the concern I'm hearing, there is no single answer to this whole scope of what we're discussing.

So, some of the examples that Rich brought up on specifics of safety system design, that's where I'm at with what I'm doing with NuScale Power. I'm designing a reactor protection system. That the priority is to design a protection system that is safe, protects the health and safety of the public period.

In the design of that protection system, we identify hazards and we design a system to mitigate those hazards. Part of that design evolution is to consider malicious and non-malicious hazards, cyber whatever you want to call them. The black box doesn't know any different. How can it be defeated? How can the safety function be defeated whether it be malicious or non-malicious? So, it's a hazard.

We design mitigation strategies. We change the design. We sometimes live with the

hazard because the effect of a hazard is tolerable. But, at any rate, it's a hazard.

As it stands now, my understanding, and when this took effect in 2009 time frame, put into regulation in 2011, the staff was asked not to look at, one, aspects of these hazards if they are malicious cyber hazards. That makes no sense to me.

Because as a designer, I'm considering it as a hazard. The staff is reviewing that at that level of detail while the design is being -- well, somewhat shortly after the design has been made.

The level of knowledge and the level of detail and the level of review effort to get down to that level is so -- is such a burden, why not do it at that time?

So, from that perspective, it makes a lot of sense to me for -- I don't know if it's Option 2. I've lost track of the options. But, Option 1. Okay.

So, in that example, it makes a lot of sense to me, but on the other hand, I've been a part of retrofit or existing plant upgrades for a protection system or an ESFAS system. I've done a turbine control system. I've been a part of a

process plant computer upgrade. That's a different situation and that doesn't apply the same as it does in doing a reactor protection system design.

So, I think that's -- I guess to boil this all down that's the challenge. Is -- we're talking about very specific scopes and how to understand how any changes would affect those scopes. I think specifically for the NuScale Power situation where we're designing attributes into the protection system to mitigate hazards, I think it makes a lot of sense for the staff to look at those as both malicious and non-malicious hazards and credit the designs that have been in place so that that can be carried forward throughout the full licensing process on into operating a plant and being programmatically implemented.

MR. PEZESHKI: First, I really wanted to thank you for your comments. You pretty much hit the nail on the head with what we were trying -- what we are trying to accomplish with Option 1 and you put it very succinctly and I really do appreciate that.

The main reason for the wider scope was

really to achieve regulatory consistency across newer reactors and existing reactors. When putting this together, we were fully cognizant that this was not really a giant leap forward for the existing fleets, but simply just the sense of achieving consistency. It was I'll say the reason why we're going for -- considered cyber security as oppose to these are controls you must implement which would be insane and I think you can agree with that. What if we started specifying like you must have password protection on all your systems? No, that's nuts.

But consideration of access control with us accepting the fact that your answer may simply be that's going to be programmatic. We're going to leave that for programmatic. We've got a lovely room with a lock on it. We're fine. That's fine as well. It was considered.

But, yes, it's absolutely not going to have a tremendous impact on operating reactors. It's really directed to the reactors, but we don't want 52 to be completely different than Part 50.

MR. STATTEL: The staff had discussed one possibility of basically bifurcating this and making different regulations for operating versus

new reactors, but I'm really opposed to this idea. I think we need to be consistent. I mean, the new reactors become operating reactors and to have to deal with different sets or different criteria for a reactor depending on when it was designed and built, I think that's a burden that we would be pushing to the future that we would always regret. Okay.

So, we're really trying to push for some commonality and consistency between the operating and new reactors even though we recognize that the problems are very different for them.

MS. ZHANG: But if you have any suggestions of, you know, maybe not total bifurcation, but if there is something different we do for design certification applicants and COL applicants versus a license amendment request, then definitely we would like to hear that.

MR. BAILEY: Mike Bailey again with Duke Energy.

I think just from an overall standpoint, I think the last two points from new reactors as well as from the vendors pointed to a couple of things.

As you look through the wording and

what's in Option 1 and two and three at this point in time and part of the reason, you know, because our industry discussions prior to the meeting involve utilities that had new reactors under development and also had existing plants as well. So, we looked at it from a consistency standpoint and the overall picture. The things that are stated right now are rather broad.

I think we've had some real good discussions about specific examples and I think we could probably get some alignment on specific examples and I think if as we have further discussions, if we can further define the scope, further define where these actual options are. The example on the new reactor side was very limited and very focused were the words used.

Whereas, the options currently presented are very broad and encompassing and so, from that standpoint, that was the one big concern we had from a new reactor as well as an operating reactor standpoint.

Where exactly do we land? If we say our feedback would be Option 1, then once we get into the details, we're really okay, well, okay, we really like Option 3 now. So, I think that's one

thing we probably need to have additional discussions on and get further details so we can actually get some of that alignment between both the NRC and the utility at that point.

MR. HERB: Again, one last thing, too, from the industry, from the existing industry, there's already a lot of uncertainty with digital systems and particularly digital in safety and I think that adding additional requirements inspections to consider malicious versus non-malicious when they really result in the same issues may just drive the industry to put in analog protection systems.

MR. GROSS: Which you can buy on eBay.

It sounds to me digital's not really, you know, nuclear digital I guess is really sort of a strange beast that I don't really have a good understanding of, but it sounds like the measures and the guidance and the requirements that are in place today regarding access control for these I&C systems appear to be more than adequate for non-malicious acts.

Is that a true statement?

And the concern that we're addressing here is whether or not we should be integrating a

treatment into the design to thwart or be able to defend against a malicious act against the I&C system for cyber security.

You know, the NRC's regulatory framework that incorporates cyber security is in its DBT requirements. Where a cyber attack is one attribute of the radiological sabotage design basis threat. So, it's one tool in the adversary's toolbox and I get a little concerned when we talk about now sort of having this standalone vision that cyber is somehow different and we need to treat it different.

My concern is if we start requiring licensees or providing clear expectations on how a licensee should incorporate or treat cyber security, i.e., how the safety system should defend itself against malicious acts just for cyber opens the door for us now to require the system to be designed to withstand a physical act within the DBT as well and I really do think that that is a -- that's a tremendous change in the way the Commission has treated safety or, you know, the design of these facilities and the implementation of the cyber security program and the physical protection program.

MR. STATTEL: I'm not sure I understand your point because I kind of disagree. I think our current policy is actually pretty consistent with the way we have treated, for instance, analog I&C systems in the past.

So, for example, we did not -- design engineers did not necessarily consider malicious acts or sabotage-type activities for designs of I&C systems back in the 1970s and the '80s.

However, the NRC did require security protection at the plant. So, the physical security was put into place and it was treated separately. It was treated as a separate entity.

So, the way I see it is the way we have separated this for cyber security for digital systems, it's actually pretty consistent with the way we treated these systems even before the digital systems were coming into play.

So, I'm not quite sure I understand your point.

MR. GROSS: I may have misstated. But you accurately characterized my concern. Which is there is and Reg Guide 1.152 Rev 3 makes a very clear demarcation between the safety system as designed, you know, up to this point to address non-malicious

acts and the Part 73 program as implemented to protect the system against malicious acts.

What I see in this paper is throwing all that out the window and saying design features should be incorporated into the I&C system so that it can withstand a malicious act just for cyber and that opens the door to do the same thing for physical and that's where I get concerned.

MS. ZHANG: We're not asking for that. It must be -- yes, it's not our intent to specify that cyber security features must be incorporated into the design, but if you were to consider cyber security earlier in the design process, you know, you can submit that information for NRC review.

I think it's similar for physical security, but I may be wrong. If they voluntarily submit physical security information, you know, we can review it.

MR. GROSS: Thank you.

MR. JONES: I think at this point why don't we take just ten minutes and what I'd like to do is come back and then get our industry participants on the bridge line who haven't yet had a chance to throw questions in here. Let's start to bring that in.

So, if we could come back at why don't we say 10:45. Thank you.

(Whereupon, the above-entitled matter went off the record at 10:34 a.m. and resumed at 10:46 a.m.)

MR. JONES: Okay. Folks, we're going to try and bring in some questions on the phone from industry. It's going to be really, really difficult to hear them based on how hard it's been to hear the operator so far. So, if we could, let's listen for the question coming in. It's going to come in through the overhead and then somebody gets it or if I get it, we'll repeat the question and then we'll take off from there.

OPERATOR: Thank you. We will now begin the question and answer session. If you would like to ask a question, please press star-1. You will be prompted on the earphone to record your name and again, that's star-1 to ask a question from the phone lines.

We do have a question in the queue.

MR. JONES: Go ahead.

OPERATOR: Our first question comes from Mike Berube. Your line is now open, Mr. Berube.

MR. JONES: Mr. Berube, please give your name and your affiliation.

MR. BERUBE: Yes, this is Mike Berube actually with GE Hitachi.

And a couple of things I wanted to mention. Earlier, you mentioned that for the ESPWR-certified design that our cyber program was not reviewed as part of the FSER and I'm looking at a section of that now, Chapter 7, that dealt specifically with the SDOE and our LPR for our cyber security program is mentioned in there many times and referenced several times in there as well as some additional LPRs that we have submitted and got NRC approval that relate to our software management plan and SQA plan.

So, the NRC is well aware of our efforts to integrate cyber security into the design of all the digital systems that make up ESPWR design.

MS. ZHANG: So, to answer that question --

MR. BERUBE: The other thing I wanted to point out was or ask a question was EPRI along with representatives from the industry has done a good job in putting together some cyber security procurement methodology and in there,

they even point out the relevant NEI 08-09 or Reg Guide 5.71 controls that would apply or could -- you know, a vendor could provide some added benefit to. Kind of a shared type of a responsibility and we are utilizing that guidance as we go forward.

So, I think some of what you're concerned about is kind of already being addressed in other areas and cyber definitely is being integrated into the design of the new plants going forward at least in our case.

MS. ZHANG: This Deanna Zhang. I'm going to respond to your questions.

For the first one, yes, we do recognize that the cyber security program plan that GEH submitted was reviewed, but it was only reviewed for the SDOE portion. There were clear statements that were written in the SER to state that it was not reviewed with respect to 10 CFR 73.54 for addressing malicious acts.

And for the --

MR. BERUBE: That's true. I agree with that. But I think that his statement earlier was that there was no cyber aspects at all in our review and that I just wanted to clarify.

MS. ZHANG: Yes, we just mean to

address malicious.

So, for the second point, we do recognized that industry vendors are taking measures to address cyber security early, but those measures would not be able to be reviewed by the NRC if that was desired by the design certification applicant or licensee.

So, we're just looking at means to perform that licensing review so that you can get a safety evaluation on those particular features with respect to malicious acts.

MR. JONES: Next question please.

OPERATOR: Our next question comes from Ken Scarola. Your line is now open.

MR. SCAROLA: Yes, thank you. My name is Ken Scarola from Nuclear Automation Engineering.

I just wanted to make a comment. I really don't have a question.

And I just wanted to say that many of you have probably seen my presentations or maybe -- or maybe you have heard my discussions about the obstacles to analog to digital migration.

And the most significant of those is the unpredictable costs of what digital systems really

take to install and I think everyone knows the changes that occur late in the design project for any reason and that would include a cyber security inspection at the plant can be detrimental to cost.

So, having an NRC review very early in the project is essential to achieve cost predictability and this is especially important when you have systems that include non-safety to safety by directional data communication.

So, I am fully supportive of what I've heard in this meeting today. I think the NRC or NRR and the NRO should be reviewing these safety systems designs for adequate cyber security measures.

That's my first comment. Just I'm very supportive of this.

Second, I wanted to emphasize the importance of what I heard from Rich Stattel about needing to have the same regulations and the same guidance for both new plants and operating plants. It can be really confusing downstream if we don't have the same guidance because as Rick said a new plant becomes an operating plant.

Therefore, it just makes no sense to me that we wouldn't even think about having different

regulations or different guidance.

That's all I have to say. Thank you.

MR. JONES: Thank you. Next question.

OPERATOR: And again, if you would like to ask a question, please press star-1. You will be prompted to leave your phone number, record your name and again, that's star-1 to ask a question.

And at this time, I'm showing no questions in queue.

MR. JONES: Okay. Would you put everyone back on listen only, please?

OPERATOR: Sure.

MR. JONES: Okay. Deanna, back to you.

MS. ZHANG: Again, I would like to thank you guys for coming here and for those who are participating on the phone. I think we've heard some pretty good feedback from everyone here and we would like to continue to engage industry in gaining more feedback from you as we progress in our -- in the development of our SECY paper.

MR. JONES: One last comment, if we're through with the industry NRC discussion, we need to offer the public a chance if there's anyone on the line. So, let me try that again.

Operator, are you still there?

OPERATOR: Yes, I'm here. We do have a couple of questions in queue and one moment please.

Our first question come from Kelly Deopani (phonetic).

MR. DEOPANI: Hello. This is Kelly Deopani from I&C Engineering, GE Hitachi.

The question I have is regarding performing static and dynamic analysis. My understanding is that performance of static and dynamic analysis is a security requirement. How the NRC will insure that this requirement is precisely implemented? So, this maybe goes under Option 1. After you identify the security requirements, you still need to perform some programmatic controls like performing static and dynamic analysis and the static and dynamic analysis are listed under 5.71, Reg Guide 5.71.

So, how does the NRC plan to enforce this requirement?

MR. PEZESHKI: Thank you. This is Jonah Pezeshki, NSIR.

So, first, I just want to state that the Option 1 that we've described that talks about

design level cyber security requirements is not intended to replace the current programmatic cyber security requirements nor the cyber security inspections that would occur after implementation.

So, to answer your question, those systems would still be subject to the cyber security programmatic level requirements and the corresponding inspections.

MR. DEOPANI: All right. Thank you.

MR. JONES: Next question please.

OPERATOR: Next question comes from Mark. Your line is now open.

MR. KING: Thank you. In the presentation materials --

MR. JONES: Mark, would you please give your name and your affiliation or general public?

MR. KING: Mark King, NuScale Power.

In the presentation, it indicates one section of Reg Guide 5.71, Section D.1.4 that would possibly be included during DCA.

Are there thoughts on entertaining or are you entertaining thoughts on any other sections being applicable? For instance, Appendix C, Section C.12.5 regarding some very specific things that the licensee would today be required to insure

of their contractors or vendors.

MS. ZHANG: That one was particularly called out because it addressed the defense architecture and the boundary device between the different security levels of the cyber security defense architecture. So, it was very specific to Option 2.

We have not looked at the wide range of security controls in Reg Guide 5.71 and done a 141 analysis of what we would look at. So, that's something we would consider in the -- as we were developing the SECY paper. More -- you know, and also as we -- if we were told that we can go proceed with rulemaking, then, you know, we would probably look at it in more detail, too.

MR. KING: Because some of those are specifically activities that would start during design time. So, it would seem appropriate.

MS. ZHANG: Yes, we understand. It's more specific to the procurement specifications addressing development. The development of systems.

MR. KING: Okay. Thank you.

MR. JONES: Next question please.

OPERATOR: Our next question comes

from Mike Berube. Your line is now open.

MR. BERUBE: Yes, this is Mike Berube from GE Hitachi again.

Just as a follow-up from earlier and I think it's been brought up a few times, this difference between non-malicious and malicious acts.

Does the NRC have a definition of their scope of what they are going to consider malicious acts that would need to be protected against and incorporate into the design?

MS. ZHANG: I think we just called the cyber threat as defined in 73.1. I believe it's the design basis threat.

So, I don't know if NSIR would like to add anything else. Okay. No.

MR. BERUBE: So, are there specific criteria in 73.1 that they are spelled out?

MS. ZHANG: I don't think so.

MR. BERUBE: So, that would need to be defined then as part of that SECY paper I assume?

MS. ZHANG: Maybe as part of the role. We have -- I don't know if we -- yes, I don't think we would probably be defining that as part of the SECY paper.

MR. BERUBE: Okay. Well, that is obviously important because if we don't know what is considered a malicious act, then we don't know what to protect against.

MR. PEZESHKI: Oh, I just wanted to clarify. In this case, the SECY paper would be a request from the Commission to proceed with rulemaking.

The specifics of what would be considered a malicious act and the specific controls would be considered once we get permission to proceed with rulemaking as a part of the rulemaking effort.

MS. ZHANG: But, currently, you know, to address the cyber threat, I think licensees understand what they need to protect against from a cyber attack. So, you know, I don't know what else we need to define in that case.

MR. BERUBE: So, you're saying to the licensees what characterizes a malicious act is already defined? So, can we just adopt that? Where would I look for that?

MS. ZHANG: Seventy-three point two.

MR. BERUBE: Okay.

MR. JONES: Thank you. Next question.

OPERATOR: Again, if you would like to ask a question, please press star-1.

MR. JONES: Okay. Hearing no other questions, I guess we'll conclude the meeting.

Thank you for coming and I want to point out that there are public meeting feedback forms here on the table or you can get them online underneath the public meeting notice and it's an attachment to the notice.

Any other final comments? Then we're done. Thank you.

MS. ZHANG: Thank you.

(Whereupon, the above-entitled matter was concluded at 11:02 a.m.)

1
2
3
4
5
6