Official Transcript of Proceedings

NUCLEAR REGULATORY COMMISSION

Title: Public Workshop to Discuss Instrumentation and Controls

Docket Number: (N/A)

Location: Rockville, Maryland

Date: August 18, 2015

Work Order No.: NRC-1813 Pages 1-79

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 INSTRUMENTATION

AND CONTROLS

CYBER SECURITY-BY-DESIGN AND

ASSOCIATED POTENTIAL REGULATORY IMPACTS

+ + + + +

TUESDAY

AUGUST 18, 2015

+ + + + +

The Public Workshop met in the Commission Hearing Room, Rooms 1F16 and 1G16, NRC Headquarters, One White Flint North, 11555 Rockville Pike, Rockville, Maryland, at 1:01 p.m.

NRC STAFF PRESENT

CATHERINE ALLEN, NSIR/CSD

STEVEN ARNDT, NRR/DE

SUSHIL BIRLA, RES/DE

BERNARD DITTMAN, RES/DE/ICEEB

TERRY JACKSON, NRO/DE/ICE

KIM LAWSON-JENKINS, NSIR/CSD

ERICK MARTINEZ, RES/DE/ICEEB

JAN MAZZA, NRO/DARR/ARPB

DAVID McINTYRE, PA

JONAH PEZESHKI, NSIR/CSD *

DAVID RAHN, NRR/DE/EICB

LANCE RAKOVAN, EDO/AO/CPM

PAUL REBSTOCK, RES/DE/ICEEB

JOHN RYCYNA, NSIR/CSD

RICHARD STATTEL, NRR/DE/EICB

RUSSELL SYDNOR, RES/DE/ICEEB

TUNG TRUONG, NRO/DE/ICE

BARRY WESTREICH, NSIR/CSD

DEANNA ZHANG, NRO/DE/ICE

* Present via telephone

CONTENTS

	Page
Welcome and Meeting Logistics	4
Introduction of Participants	6
NRC Staff Topical Presentation	8
Facilitated Open Discussion	23
Opportunity for Public Comment	43
Closing Remarks/Adjourn	78

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

1:01 p.m.

MR. RAKOVAN: Thank you, Emily. Again, my name is Lance Rakovan. I'm a Communications Specialist here at the Agency. I'm going to try to help keep things on track, facilitate a little bit, and basically just help out with this meeting today. The purpose of today's workshop is to discuss current NRC thinking on incorporating cyber security design reviews into the NRC's licensing reviews, including scenarios of these reviews and obtain industry stakeholder feedback for staff consideration. This is a Category 2 public meeting by NRC's definition, which means that the primary discussions are expected to occur between NRC and industry representatives.

There is a time scheduled towards the end of the meeting, I believe around 4:00 or a little after 4:00 by the Agenda for public questioning of NRC staff at that time, but until then, we look for the discussions to, again, primarily be between NRC staff and industry. The Agenda is pretty simple today. We have a presentation by NRC staff and nuclear industry representatives, some open discussion between the two, and then, again, we'll have a short time for public questions. If you're participating by phone today, we do have Emily who's going to be assisting us. She'll let you know how to weigh in once we do open the floor to questions and comments.

We are taking a transcription of today's meeting, so if anything's happening in the room where it's disruptive, side noise, et cetera, I'll probably take some steps to remedy that situation. If you can, please use a microphone when you speak. Again, that'll help, not only those on the phone hear us, but also make sure that we get a clear transcript. The other thing that I will ask, especially of those in the room, please identify yourself when you speak. That not only will help the transcriptionist follow who is talking, but, again, will also help those on the phone follow as well.

For those of you here in the room, emergency exits can be found pretty much at the four corners of the room. Restrooms are out the door here to my right and then to the left. We do have public meeting feedback forms, copies of the NRC presentation, and, I believe, the Agenda as well at the door, again, to my right. I believe that the presentation was shared and posted on ADAMS and can be linked to on the public meeting schedule as well, so those of you following on the phone lines, you should be able to find the NRC presentation there if you go to our public meeting schedule page on our public website.

Before I go ahead and turn things over to our first speaker, I'd like at least those folks around the room to introduce themselves. If we could go ahead and start here to my right.

MR. STATTEL: Hello, I'm Richard Stattel. I'm

representing the INC Branch and NRR.

MR. JACKSON: Terry Jackson, Chief of INC Branch in Office of New Reactors.

MS. ZHANG: Deanna Zhang, INC Technical Reviewer, Office of New Reactors.

MS. LAWSON-JENKINS: Kim Lawson-Jenkins, I work in the Cyber Security Directorate at the NRC.

MR. GEIER: I'm Steve Geier. I'm with the Nuclear Energy Institute and I'm a Senior Project Manager with NEI.

MR. CLIFTON: Gordon Clifton with NEI.

MR. RAKOVAN: Okay. That's those of us at the table. I'll ask folks that when we get to the open question and answer part that folks identify themselves as they go ahead and make a comment, including those on the phone, so we can make sure that we have an understanding. There's also a sign-in sheet for those of you who are here in the room. If you wouldn't mind signing in there to give us a good indication as to who attended in person today and for those of you on the phone, you were asked to provide your name and any organization you are with, so that will give us a good indication as to who called in one way or another. With that, I believe I'm going to turn things over to Terry, correct? Excellent.

MR. JACKSON: Okay. Terry Jackson with Office of New Reactors. And I just wanted to make a few opening remarks. One

is I want to thank everyone for joining in on this public workshop today addressing cyber security and design. And as Deanna will later go on and she will talk about the purpose for why we were developing a SECY paper to address this particular topic, but this is actually the second public workshop that we've had and as a result of the first one, one of the requests from the industry was to provide some examples of how the NRC would see the different options that would be going into the SECY paper work out. So that's our intent today is to provide some examples. And also to entertain any questions or comments that you may have with regards to this effort.

Then we also realize that there are several other efforts within the Agency and the industry with regards to both instrumentation and controls and with cyber security. We're not prepared to address those topics today in this meeting. There are some other meetings in the future that will address those topics as well. But today we just wanted to focus on this topic of cyber security and design.

MS. ZHANG: Thank you, Terry. So my name is Deanna Zhang. And today I want to present to you some of the scenarios that we came up with as requested based on the feedback we received at the last public meeting. Before I go into these scenarios, I just want to recap a little bit on our last meeting. So during our last meeting, we presented on our proposed SECY paper that we

plan on sending up to the Commission, where we want to seek the Commission's direction in allowing the staff to proceed with reviewing cyber security design information as part of licensing. This would be to complement what's currently in -- what's required by 10 CFR 73.54.

And as we said last time, we're not seeking to extend any cyber security technical requirements. This is more of a change in the licensing process. So we will be doing licensing reviews of design information submitted by the applicants and licensees and then we will be writing a safety evaluation report based on our review. And some of that information will then be able to be referenced as part of the cyber security inspections. And, therefore, reduce the level of information that will need to be provided during inspections and that will be inspected.

So let me proceed with the slides. So next slide. So this is just the list of acronyms that I'll be using. Next slide. So, again, the NRC's in the process of developing a draft SECY paper seeking the Commission's direction on evaluating cyber security related design features as part of licensing. And the scope is only for safety and important-to-safety digital assets. So this does not include the entire scope of 10 CFR 73.54. In addition, again, we do not seek to expand any of the cyber security technical controls and requirements specified in 10 CFR 73.54 and the accompanying Reg Guide 5.71.

So in the SECY paper, two of the options will modify the licensing process to enable the review of cyber security design features. One is very tailored to the boundary controls between the cyber security defensive levels. The other one is broader, which includes more cyber security controls specified in Reg Guide 5.71. So, again, during the last meeting, we got the feedback that industry would like to see us go over a few scenarios as far as what kind of information do we expect to see from a licensing submittal and how will we conduct our reviews and then how would that information be credited or referenced during the cyber security inspection. Next slide.

So we came up with three scenarios. For Scenario 1, this one is described in Reg Guide 5.71, Section B.1.4. And this is on the one-way boundary device between Level 4 and Level 3 and between Level 3 and lower Levels. And the specific item we'd be reviewing within this Section is the implementation of a one-way data flow using hardware mechanisms. So, next slide. So we've kind of broken this up into what we expect from a Design Certification applicant under the Part 52 process and then what we would expect to see from a licensee submitting a License Amendment Request pertaining to a digital upgrade of a safety system or some important-to-safety system through the 10 CFR 50.59 review.

So for Design Certification applicants, we would expect to see some design descriptions of this device on how it

physically enforces one-way communication between Level 4 and Level 3 and between Level 3 and lower Levels. So some example would be that an applicant would state that the device uses optical isolation, that only has a fiber optical transmitter on the higher security level and a fiber optical receiver on the lower security level. And there would be no fiber optic receiver on the higher security level. Therefore, information could only be transmitted one way physically from the higher security level to the lower security level. Next slide.

So for a licensee who's submitting a LAR, if -- as part of this LAR, the design changes the existing communications between Level 4 and Level 3 and between Level 3 and lower Levels. The licensee would be submitting design descriptions of the device, again, showing how it physically enforces one-way communication. And similarly with the information provided for the Design Certification applicant, descriptions of how that one-way communication would be enforced. Next slide.

So for NRC review, we would look at the boundary device as well as review the diagram schematics to verify that the design incorporates the use of the fiber optic receiver and fiber optic transmitter, that they're in the appropriate locations based on the schematics. For Design Certification applications, we do expect to see an ITAAC provided that will be used to verify that the as-built system employs this design and that the as-built

boundary device meets the design commitments provided in the Design Certification application. For LAR submittals, the staff will audit the development process for the device and may witness the after-acceptance testing on this device as well as review the FAT results during the audit. And, Rich, feel free to chime in for some of the --

MR. STATTEL: No, you're doing fine.

MS. ZHANG: Okay. Don't want to speak for you guys. So in this scenario, for the inspection of the one-way boundary device between Level 4 and Level 3 and the other Levels, so we expect to conduct the inspection to verify that the device is installed and documentation exists that identifies the boundary device as a Critical Digital Asset. The CDA will be controlled under the plant cyber security program. And, oh, next slide, sorry. And we do not see a need to reconfirm that the device performs its intended function during the inspection. So that part will be what's going to be credited from the licensing review. Next slide.

So for Scenario 2, we will -- this one reviews the means used to protect the time-stamps utilized in Layer 4 of the cyber security defensive architecture. So Reg Guide 5.71, Section B.2.8 discusses the technical controls regarding the time-stamp source utilized for Critical Digital Assets. In this Section, it states that Critical Digital Assets should use a time source

protected at an equal or greater Level than the CDAs. This time-stamp synchronizes the time of all CDAs from a dedicated source protected at an equal or greater Level than the CDAs existing on the security network. Next slide.

So in this case, the Design Certification applicant provides design information on how time-stamps are generated for important data from both safety systems and important-to-safety systems that are likely to be in Level 4. They will provide information on how the time-stamp is acquired from a protected source. So, for example, we've seen applicants provide a -- propose to use GPS as a time-stamp source. And as we all know, GPS can be easily spoofed in that case.

So for this particular design, if a COL applicant inherits that particular design, they would either have to make design changes or come up with some other means to protect -- to time-stamp their Critical Digital Asset data. So, they would also need to discuss some security features that could be used to protect the source of the time-stamp signal. For licensees, similarly as discussed, they would provide information on how the time-stamping source is protected if that time-stamping is on a system that's included as part of the -- that's modified and included as part of the LAR. Next slide.

So for the NRC review, we would look at the design descriptions to determine whether the security features that

protect the time-stamp is acceptable and that the time-stamp source is securable. For Design Certification applicants, we would expect to see an ITAAC that will verify the time-stamp source for the as-built system and that security features for the time-stamp source meets the design commitments. For the LAR submittals, the staff may perform an audit regarding how the time-stamp source is generated and review the security features for the time-stamp sources, probably as part of the audit during the FAT and the FAT results summary. Next slide.

So as far as the inspection, we will be conducting the cyber security programming inspection to ensure that security features were protecting the time-stamp source, that it is implemented as described, installed as described in the Design Certification, and that documentation exists that identify these features. And they will verify that the time-stamp source is protecting the same cyber security defensive Level as the system that will be receiving the time-stamp. So they will have to make sure that the time-stamp source is part of the overall cyber security program and that it is protected at the same Level as the Critical Digital Assets that it is responsible for generating the time-stamp for. Next slide.

So, this next scenario, it's actually from Section C.12.5 of Reg Guide 5.71. This is actually one of the management controls, it's not actually a technical control specified in Reg

Guide 5.71. In this one, this Section specifies that the licensee or applicant needs to ensure that the acquired products meet specified security requirements and, specifically, that the products are free from known, testable vulnerabilities and malicious code by identifying and eliminating these following vulnerabilities. And they go through a list of known vulnerabilities, such as overflow code or other types of code vulnerabilities. Next slide.

So, for the Design Certification applicants, we expect that the Design Certification applicant will submit a test plan that documents how known testable vulnerabilities and malicious code will be identified. So, again, because the system hasn't been implemented, we don't expect to see that the code has been identified, the malicious code has been identified, that would be a future activity that will be done. But this plan should document what are some of the methods that the applicant plans to employ to identify these vulnerabilities and malicious code. And, of course, provide an ITAAC that would implement this test plan.

And we do recognize that vulnerabilities may change over time, so some of the information that's captured in the test plan may not be applicable, but we don't -- so this will have to be a much more higher level plan that we would have to verify as part of the ITAAC closure. The inspection activities would verify that this plan has been up-to-date with new vulnerabilities that

may have developed. Next slide.

So, similarly for the licensee, they'll probably similarly submit a test plan. But because of the fact that there's not so much a time difference between when the test plan is generated and when the activity performed for the test plan will be implemented, we do expect to see more details here as far as how testable vulnerabilities and malicious code would be identified. And then there will be plans for documenting how any of the identified testable vulnerabilities can be controlled.

For some of these items, we don't expect that they can be eliminated, particularly if it's embedded in a safety system software and the code can't be removed, so then we'll talk about some of the other means that could be used to control such vulnerabilities and malicious code. And because this is a LAR, we would expect that the summary of the test results be provided. So, next slide.

MR. STATTEL: So, this is Rich Stattel. Just a couple words. If Deanna's given you the impression that we have this all figured out, that really wasn't our intent here. Really the development of these scenarios was really an exercise to try to provoke some thoughts on how we could coordinate our efforts in the licensing review area with what NSIR would performing in the inspection area and the programmatic aspects of cyber security. So, we're really trying to solicit some feedback from the industry

and get some ideas.

One of the areas I will mention in the operating reactors area is the scoping of this and whether these reviews would become mandatory in the future. It's very uncertain in my mind how this would play out because the scopes of our reviews are generally determined by the scopes of the modifications being done at those plants. And a lot of times or very often, they would not include things such as the one-way devices that Deanna had mentioned in the first scenario.

So the question comes, do we still rely on the programmatic aspects or is there some additional activity that we would have to implement during our license review and basically extend the scope of our review to include those aspects of the design. But at the same time, we do recognize that as our technical reviewers are performing these evaluations, we become familiar with the designs of the system, it's really an opportune time to evaluate the cyber security system attributes.

So, it's really -- I feel that there's some benefit to doing these activities during the licensing reviews as opposed to deferring them to the inspection activities where we may not necessarily have the experts there that are capable of performing those evaluations effectively. And it becomes less, everything becomes a lot less efficient when we defer that to the inspection space. So really we'd just like to hear back from the public and

from the industry on these ideas and see if we can kind of expand on these concepts.

MR. CLIFTON: This is Gordon Clifton from NEI. We appreciate your looking for subject matter expert input on it because the industry's got some passionate people on this and I'm sure we won't have any trouble bringing forth some of their good ideas. Before we get into the details, I agree with what you're saying completely there, Rich, that the scoping and whether this is mandatory all will affect the resource consumption in putting designs in and there's an appropriate time. As we found in pilot projects for other industry items is that there's an appropriate time for each document to come forth in a final format and what you could end up doing with these audits and early visits is be seeing something in a very preliminary standpoint.

But on the other hand, if you look at it, the time we become liable for it is when core is loaded, or as the regulations call for now, is late in the game to get started on a cyber security. So we appreciate the interest in the NRC and the industry and the vendors to start this process of being aware of cyber security considerations very early. And they aren't necessarily, as you identified, part of a design. Because it's more in the interface of the digital widget than it is of the actual component itself. Although you can have with code, you can have your problems in the code, so we need to keep quality control.

What comes to mind in a big picture is these scenarios are great and I appreciate you bringing them forth on that, the question I was going to ask is, do we have a driver that caused these type of responses or, let's say, do we have demonstrated problems and examples where we have shortcomings in the existing Part 50 process, Part 52 process or in the QA programs or on the SER process now? Because from my standpoint, I don't think we have shortcomings on it. That I'm thinking what we can bring forth is perhaps an enhancement of what we have. And I'm not sure we need regulatory assistance for that enhancement if we can put into guidance or something that's not hard driven as rule as you put in your comments.

MR. RAKOVAN: Well, hold on. Let me step in a second. I thought the intent was for the NRC to get through their presentation --

MR. CLIFTON: Okay.

MR. RAKOVAN: -- before we started discussion. If that -- if we want to go off-script, that's fine. But I just -- I want to step in to see what the intent here is, if I may?

MR. CLIFTON: Thanks for keeping us on track.

MS. ZHANG: Thank you. So let me go through -- I'm almost done with these slides. So --

MR. RAKOVAN: Okay.

MS. ZHANG: -- we can --

MR. RAKOVAN: Okay. Thank you.

MS. ZHANG: -- move then into answering Gordon's question. So let me just finish these last few slides. For this slide, the -- which discusses what the NRC license review would look like for Scenario 3. So the staff will review the test plan to determine whether the test activities are sufficient to identify testable vulnerabilities and malicious code. And for Design Certifications, we will look at the ITAAC to make sure that's it's sufficient to capture what would be verified as part of the ITAAC closure process. And for LARs, the staff will review the summary of the test results and may conduct audit during the development process.

So for the NRC inspection, next slide. For Design Certification applicants, during ITAAC closure, we will be conducting an inspection to ensure that the test plan was accurately implemented and any identified vulnerabilities and malicious code will be adequately controlled. We'll be looking at the documentation as part of this verification, as part of the inspection. And for the cyber security program inspection, the NRC will inspect the documentation provided as supplemented by the staff's previous review. We would also look at that this Critical Digital Asset has been incorporated into the overall planned cyber security program to ensure that as vulnerabilities change that the effectiveness of the controls are still adequate. Next slide.

So, again, for this proposed SECY paper, we are seeking the Commission's direction on evaluating cyber security related design features as part of licensing. We do not intend to expand the scope of what's currently stated in 10 CFR 73.54, just what will be reviewed as part of licensing. And for Design Certification applicants, we feel that this proposal will provide added assurance that certified designs can be secured upon implementation.

And for NRC licensing review of cyber security design controls, we hope it could support subsequent cyber security program inspections and thereby reducing the information that needs to be reviewed as part of cyber security inspections. So this concludes my presentation and we'll move into the question and discussion portion. So with that, let me go ahead and turn back to Gordon, I think, with his question. If --

MR. RAKOVAN: Please. If you would, could you just give a -- rephrase if you could, briefly?

MR. CLIFTON: Sure. I guess what I was bringing to the table is these are great scenarios of what's out there. But I was wondering if we have examples that you've seen that perhaps we're not aware of where we've had a shortcoming in cyber security that -- where something was broken and we're trying to fix? Or are we just looking to enhance the process so we all have a greater comfort zone that when we implement the systems as you pointed out

here, that upon implementation that's when we're most liable with it?

MS. ZHANG: Okay. So I do have a couple examples. But I don't want to call it shortcomings. Because we don't want to say that our current cyber security regulatory framework is broken or anything like that. Just as we said before, this is to facilitate implementation of the cyber security program. And this is to compliment it, not that there needs to be anything -- but this is to help support it. So, for Design Certification, and you can probably see, there's a little bit of a difference between new reactor applicants and a current licensee seeking a License Amendment Request.

And what we've seen in the two examples I'm going to talk about, they're Design Certification applicants. So in one case, an applicant picked a time-stamp, a GPS as their time-stamp for both their safety and important-to-safety, all their Level 4 systems. And when we looked at this, obviously that source is not securable. However, because there wasn't an active COL that maybe would drive that design at the -- feature at the time, that part was specified in the certified design. So if an applicant were to come back and say, well, that can't be secure, well, we can't use that source. They would need to make certain design changes and probably much later in the development process, maybe much later in the development process.

So that's one thing we would like to help prevent is that when we have Design Certifications proposing designs that are not securable, that we can get it ahead of time and help drive it to something that is securable. Something similar was another applicant proposed a firewall between Level 4 and Level 3 systems. And, again, this is something similar. We noticed that, that it was a firewall. And although there was a COL applicant, we informed of this, there wasn't a proposed design change.

They said they would have to do something after the fact, after Design Certification, after it gets into the plant, they may have to add another device on top of the firewall. So, as you can see, these two examples shows how the securable aspects of the designs were not really thought out during the Design Certification.

MR. CLIFTON: Early on?

MR. JACKSON: I think one of the other things we saw too was that, especially on the new plants, when they're developing a new INC system, that they're not really separating out cyber security and the INC safety aspects either. They're developing them simultaneously. So they're part of the requirements if they need be. So, therefore, when they come in to the NRC for license approval and so forth, they're separating out cyber security from the safety aspect because, at this time, we're not reviewing the cyber security aspects in the INC safety review. So it takes a

little bit of work and a little bit of coordination on their end to separate back out, even though it really is done concurrently.

MR. STATTEL: I'd like to point out, clearly the scenarios weren't developed in a vacuum and clearly our experiences kind of factored into the development of these. But they are hypothetical. So don't read too much into these scenarios. Really the idea was just to get the thought process going. We also have experience in the operating realm in our applications and in our safety evaluations. We've evaluated one-way devices that are credited in cyber security programs and we've done, to a certain degree in the early applications for Oconee for example, we did some cyber security evaluation portion of that application.

So -- but please don't read too much into these. We're really not pointing at any shortcomings of past projects or current, ongoing projects. Really what we tried to do is we developed the scenarios based on our experience and we tried to jot down some notes here on how -- what would be the best way that we could approach these things in the future. And really, that's kind of the direction we're kind of seeking from the Commission as far as policy and how we address these cyber security issues going forward and doing it as efficiently as we can. And it is a challenge, I will say that.

MR. CLIFTON: The challenge for you is drafting the SECY with the words that you prefer, a direction to take in the

future and then looking for approval of that. And we appreciate it on the industry side for you opening up the dialogue, if you will, so that we can discuss it in public formats and come back to optimize it as what we have. Have you got an implementation schedule for your SECY? Are you looking in 2015, early 2016 or anything like that?

MS. ZHANG: Yes. So currently, we're scheduled to provide the SECY paper to the Commission at the -- sometime this calendar year. So, it is an aggressive schedule.

MR. STATTEL: Yes, it is. But --

MR. RAKOVAN: I'm going to step in real quick and just remind folks if you could introduce yourselves when you speak so those on the phone can follow. Thank you.

MR. STATTEL: Sorry.

MR. JACKSON: This is Terry Jackson. And so I think our next step is after incorporating feedback from this public meeting, we would try to finalize the SECY and get it to the Commission. Gordon, I think you asked another question earlier as well. You were asking if we needed really like a rule making to do this or could it be done in guidance. And I think where we're at right now is we're kind of leaving that up to the Commission. And that's part of what we're seeking direction on, all the way up to rule making.

We kind of see right now the point where we would need

at least some kind of policy decision with regards to that because the policy was basically set to implement 73.54 as a programmatic rule. So that wouldn't necessarily force anyone to bring any kind of design information in. So it really is up to the Commission to decide if they want to go all the way to rule making or if they want to stay with guidance. Or there's also the third option we have in SECY, which is basically stay with what we have right now.

MR. CLIFTON: And so, do nothing and use -- this is Gordon Clifton with NEI. Doing nothing and using existing processes, as Deanna pointed out, is we're pretty pleased that it's working and we have confidence that when you're looking at enhancement here, a step forward. I'd be concerned if we put rule making in that got into too much details of how to do something. We want to keep rule making up at level where it tells what's required, what criteria are expected to be met. And then we'll use Reg Guides and lower level guidance material to say how to do things or provide an approved path to do something. Reg Guides are best purposed for that.

But we don't want to get into an order or rule, something that is trying to design components and enforce inspection intervals that are perhaps unnecessary. And if we get into, like you and I have talked and projects have graded approaches, some of these things would be foolish use of resources to go with a full auditor inspection if you have a very small

modification.

MR. STATTEL: Right. This is Rich Stattel. One of the things that occurred to me when we were developing these scenarios and writing down what our proposed actions would be, is that a lot of these actions, I would say the majority of actions that you see listed in these slides here are things that we already do. So, for example, if a cyber security requirement was going to be implemented within the design of a system, that would become part of the design requirements. And we already review those and we already review how they're implemented and how traceability is established.

So, you really can't separate the cyber security aspects from the design elements of a system or the design processes because they are part and parcel. So, currently -- in our recent experience, we don't see a lot of 73.54 criteria being implemented within the design of safety systems, for example. A lot of it falls outside of that into the important-to-safety classifications or they're being foregone for other reasons. So their programmatic approach is more on the lines of protecting the crown jewels, rather than imposing the protections within them.

So, we don't have a lot of experience with reviewing the implementation of those aspects. And our current SDOE approach to performing our licensing reviews really concentrates on protecting the safety functions and not really looking at the

malicious aspects of that. So that's one of the things that could potentially change as a result of the direction we receive from the Commission.

MR. CLIFTON: All right.

MR. STATTEL: So you need to be aware of that as well.

MR. CLIFTON: I think that's what --

MS. ZHANG: Yes.

MR. CLIFTON: This is Gordon Clifton from NEI. That's what you addressed earlier, right?

MS. ZHANG: Yes.

MR. CLIFTON: It's a separation between physical security versus electronic security --

MS. ZHANG: So --

MR. CLIFTON: -- devices.

MS. ZHANG: Yes. So as Terry had mentioned, if we want to -- this isn't just requiring an applicant to submit some design information. But even if we want to review voluntarily submitted cyber security design information, there needs to be probably a policy decision there as currently we do not do that per policy. So that's why we are seeking the Commissioners' direction. Because we have had Design Certification applicants come in and say, here's our proposal, can you review it? And we did not have the ability to do that under our current policy.

MR. CLIFTON: This is Gordon Clifton. I'm not sure

ability is the right word there, but you didn't have, let's say, a regulatory driven --

MS. ZHANG: Yes.

MR. CLIFTON: -- requirement to do that. But we had an example at Diablo Canyon, where NSIR came and audited but as the project manager of NRC made it clear is that there was no regulatory need for inspection, inspection findings, and enforcement because that was outside their purview, their scope at the moment. So that's where we appreciated that it was brought up, it was an issue. But it was a volunteer basis from the industry, utility to encourage the audit, let them come on site, show them what was going on, develop the confidence that it was being done, even though it wasn't regulatory driven. And so, I think that's supporting what all of us are saying is, what's working now is working. We only need to polish the apple or enhance what's already working right now.

MR. STATTEL: Right. And that -- this is Rich Stattel. That was a pilot project, so we were kind of just --

MR. CLIFTON: Seeing if it would work?

MR. STATTEL: -- kind of breaking the ice on this. At the time that those audits were performed, the design really had not been complete or implemented in the Diablo Canyon project. I will say -- now you can read the reports, right? And there's really no safety conclusions resulting from that. There's some

observations. But now that some time has passed, we're nearing completion of our safety evaluation, but, again, we're not really addressing the malicious code aspects of that at all. And that's still really deferred to the programmatic aspect.

So how the licensee implements that system within their cyber security program is really going to be the subject of future inspections. So there wasn't any concerted cyber security review effort as part of this application. So, we really haven't figured it out. Even though we've learned a lot from the pilot, I will say, but we really haven't figured out exactly how to tackle this.

MR. CLIFTON: This is Gordon Clifton again. Go look for it at the installations? Or installation testing or something like that? But then it's so late, if there's a problem that we --

MR. STATTEL: And that's --

MR. CLIFTON: -- didn't catch earlier --

MR. STATTEL: And that's the risk that --

MR. CLIFTON: -- it stops the calendar and --

MR. STATTEL: Yes.

MR. CLIFTON: -- hurts us.

MR. STATTEL: Yes. We recognize that there's some risk there. Particularly with the -- in the operating plants as a new system is being implemented, if no cyber security review or

evaluation was done during the licensing review, then the danger is they get down to the installation and either through the inspections or through just the process of implementing that system or putting into their cyber security program, they identify shortcomings and now they're in a place where they have to make design changes, create new requirements for that system that had not been evaluated by the NRC. So they may be handled under a 50.59 process or maybe not. I'm not exactly sure how that would go. I guess it would depend on the significance of the findings at that time.

MR. CLIFTON: Yes. You'd hope -- this is Gordon Clifton again. You'd hope it would be in the modification process. Because the 50.59 is just going to be whether we bring the process to you for LAR-type processing or we take care of it ourselves. But the process that would find and incorporate necessary enhancements to the cyber security plan would be in the modification process. And we would expect that starting 13 to 15 months beforehand.

MR. STATTEL: So --

MR. CLIFTON: But that -- there's nothing that you see as the --

MR. STATTEL: Yes.

MR. CLIFTON: -- SER author that would identify that, that had been accomplished.

MR. STATTEL: Yes. So, Rich Stattel again. So there's kind of a dual purpose to the SECY paper that we're writing. One is to help us as far as defining what is our review process going to look like and how does this coordinate with the NSIR activities when the inspections are performed. The second is, it's a little bit more subtle, but it's really -- under the current process where we're really only looking at the malicious aspects of cyber security at the very end or at the implementation stage of design, we may be inadvertently discouraging addressing them early on in the design.

Which is clearly -- I think the industry knows, that's the better place to do it. So it's kind of a matter of perception. I think most people understand that it's better to do the vulnerability assessments and to address them early in the design phases. But we're not looking at them then. We're not looking at them until they're implemented under our current processes. So there's kind of a gap there, it's kind of a timing gap.

MR. CLIFTON: Right. This is Gordon Clifton. When we look at a milestone for installation, we could identify a milestone in there to commence involvement with cyber security concerns. But that's still just a bullet on the milestone calendar. That's -- where to set it is a choice we all have to discuss.

MS. ZHANG: And -- this is Deanna Zhang. And for new reactors with Design Certification applicants, sometimes there is

no COL applicant to work with the Design Certification applicant at their time of Design Certification --

MR. CLIFTON: Right.

MS. ZHANG: -- to get the design such that it is securable once implemented.

MR. CLIFTON: So what we need to work together with is come up with some optimum positioning, if you will, of the start date for involvement with cyber security. And then looking at the boots and gun as well as the small wires aspects of it. Okay.

MS. LAWSON-JENKINS: Hi, this is Kim Lawson-Jenkins. I just wanted to add one comment about the example we have about finding the vulnerabilities early. I appreciate the example for using test plans. But there's another scenario that could have been said for doing those kind of vulnerability -- to find those in, I think you said, in the coding phase. Because now you have compilers that will eliminate vulnerabilities.

They'll say, if they find it, while you generate and compile the software and pull it into a build. And to find that there, you're really reducing the attack space that -- much earlier in the cycle so then you only have to worry about the newer vulnerabilities. So there's a lot of scenarios here where it's really advantageous to get things out earlier. And to reduce the attack space and worry about the newer threats that are coming along, rather than the same things we've been seeing year after

year.

MR. CLIFTON: Right. This is Gordon Clifton. Rich, you could probably bring the example of Oconee, where you had to go back and look at code and the security that went with the code development while it was early on stages.

MR. STATTEL: And we do. We do that frequently during our application reviews. What is new here though is the NSIR involvement. Because even during the inspection activities or the audit activities that we did with Diablo Canyon, I don't think the inspectors had a lot of previous experience or opportunities to get involved in that design implementation or the design development, the design processes.

So it's a little awkward because they're not used to doing that. They're used to reviewing or doing inspections on a completed design implementation operating in the plant and we're on the other end of it, where we're looking at the design processes and the development of the design. So where do we meet in the middle? I think that's the crux of the matter here.

MR. CLIFTON: This is Gordon Clifton again. We're counting a lot on the quality control of the vendors who are creating the code. Because we're getting into a situation where we're going to have topical reports and packages. And digital packages are going to come to us pretty much black box. And they may have 1,200 installations around the world elsewhere working

just fine and our opportunity, NRC or current reviewers, would have a great deal of difficulty getting into the code that's been in place for years and years and practiced and sealed.

MR. STATTEL: Right. Now, I will mention -- this is Rich Stattel again. I will mention that we do recognize that. And we recognize that the licensees, the ultimate licensees aren't always involved in those development processes, particularly in the platforms. So for that reason, we do perform a, not a cyber security review, but we perform a secure development and operating environment review of the platforms themselves. And that does -- that review does involve assessment of how the vendor is identifying vulnerabilities and hazards that may be present in that system and how they're addressing them.

So that's kind of our effort, that's what we've done so far in trying to address those early on. But, again, it can be years, it can be five, ten, 15 years between the time that those platforms are developed and the time they end up actually going into a plant and performing safety functions. So there's a long span of time and a lot of development activities that occur during that period of time.

And it's a little daunting, but that's really what we're trying to address here to try to, A, encourage early identification of vulnerabilities and means of addressing them and also provide basically a two-stage, as part of the licensing

process, we would evaluate how those are being assessed, how the regulations are being met, and then once they're installed, the inspection would basically be the final coverage of the regulatory requirements.

MR. CLIFTON: Going back to what Kim's saying, the challenge that we'd have in setting this milestone for starting the review is the challenge in ownership too. Because at the early stages when the code is written, especially in a platform basis, the ownership is with the vendor, which NRC doesn't have direct hooks on. And the licensee can request and ensure that in their specification development that they put these type of requirements in, but when we go back for platforms that were written, like you said, five, ten, or 15 years earlier, to go back to assess whether there was a code anomaly in there is a real challenge if it belongs to somebody else, it isn't to the vendor's control yet, their ownership, or anything like that. So not an easy task, no question.

MS. LAWSON-JENKINS: No. I've worked in software development. I agree it's not an easy task. But to, at least, to start to look at where the flaws are, where the vulnerabilities are, and to do ongoing updates to keep moving forward. Because, as you say, these things have been in the field for years, but new vulnerabilities come every day and they have to be addressed and there's a process for addressing that, so that whenever you do

bring it into a new device, you know you've gotten the latest best software at that date.

MR. STATTEL: Right.

MS. ZHANG: Yes. So I think what we're trying to say is that we're trying to set up -- have the licensees set up a baseline when they take in that platform. So they will evaluate and test for known vulnerabilities and malicious code. And, as you have brought up, there probably was some quality assurance process used. We saw that for the TELEPERM XS for the Oconee review, back when they were developing the system. They did have some measures that they did to prevent malicious code from being injected into the system.

But on top of that, you have vulnerable code. That is something that a quality assurance project would not be able to capture. And that's why you need to test for known vulnerabilities at the time that you are adopting this platform for this particular application.

MR. CLIFTON: And that's -- this is Gordon Clifton again. That's using third party software typically, right?

MS. ZHANG: Yes.

MR. CLIFTON: Which then we have to validate that as an appropriate means as well. So it's a cascading sense of responsibilities that it will be a challenge to direct or to put it in writing.

MS. LAWSON-JENKINS: And the last thing I want to say, at least on this topic, is that it really forces everyone to understand what the product does, what's in the product. And a lot of times, we buy things where the seller is making the assurance, this product does this function, it does this type of security feature. And then at the end of the day, how do you know what software's in there, what software's performing that function?

There have been vulnerabilities, like for example, with OpenSSL. New vulnerabilities have come up and people don't know what software's in their product. So you don't even know the vulnerability's there. So when you start this process of engaging with the suppliers, understanding really how are they providing these services, what software it's built on, then you can go forward and say, okay, we'll have to watch for these advisories on this type of software, you understand that. And it is a long process and it's involved, but then you have better assurance that you are protected and then meeting the rule.

MR. STATTEL: Absolutely. Did we want to open to the floor to -- I guess it would be a good time, I think, to basically get some feedback on the individual scenarios, if anyone has questions about what we've written in the slides here?

MS. ZHANG: Lance?

MR. RAKOVAN: Okay. Sounds good. Emily, if you would,

could you go ahead and start taking some questions or comments from the phone lines and start a queue?

OPERATOR: Thank you, sir. At this time, anyone wishing to ask a question or make a comment, please press Star 1 on your touchtone phone. Please be sure that your telephone is unmuted and clearly records your name when prompted so that your question may be introduced. Once again, if you're wishing to ask a question or make a comment, please press Star 1 at this time. And it does take just a few moments for the questions to come up.

MR. RAKOVAN: Thank you. And for those of you in the room, obviously you don't have to hit Star 1, you can come over to the podium that we have here. And if you could just, again, introduce yourself and any organization that you're with, we'd appreciate that.

OPERATOR: And, sir, we do have a question from the telephone lines.

MR. RAKOVAN: Okay. Please go ahead.

OPERATOR: And that question comes from Jay Amin. Sir, your line is open.

MR. AMIN: Okay, hi. Okay, I have a couple of comments. On the examples, if an LAR is submitted, say for an operating plant, the key thing to look at is the architecture for the change and the connectivities and how cyber is addressed. This is what I would want to see as an NRC. Because if you kind of leave it

vague, then it is very difficult to ascertain how the connectivities are impacting or how cyber security comes into play. So the connectivity part and the architecture are key elements that you want to look at up front.

And then, also, if one does -- if the architecture shows and the connectivity shows that everything is behind the existing diode, then I don't believe there is a reason to even look at the diode that has already been implemented and bought off previously. Unless there is a reason to look at it. For example, if I'm installing a massive platform and I already have a diode and then I'm sending data outside that diode, that could interest you because I'm sending data that is going to be quite a bit of data going through a diode that was installed for, who knows, maybe a small bandwidth versus a larger bandwidth. But that's one example.

Another comment that I had is, I'd like to have everything move towards a standard. And that's something trying to work in the backgrounds to see who IEEE sees this. But when you look at cyber, it is no more than one element of many digital design attributes. For example, seismic environment, EMI, RFI. And I don't think so that every time we address digital, we need to be too prescriptive.

And I believe that the code reviews for malware and anything else, and I'm talking application codes, unless there is

an operating system from Microsoft that was modified by an integrator, you want the V&V process to address cyber security as one of the elements. Because that's where you want to do that, because V&V tests code, they review codes and scripts. So that's where you want to integrate it. So I think the focus should be to integrate some of these elements of cyber that touch base with software and all of that into the V&V process going forward.

MR. STATTEL: This is Rich Stattel. Thanks for your input, Jay. I kind of want to respond to your first question with a question back to you. Why -- I do agree with you that the architecture and the interfaces are basically key features of a system that I always want to review on a system. Why would you think that would be more or particularly applicable to a license amendment as opposed to a new reactor design?

MR. AMIN: Well, it could -- I don't know. It depends upon what the application is on an operating plant coming on an LAR and for a new plant. And the reason why I say that is my simple mind says that if you want to -- if I'm bringing in a new application today for Comanche Peak or, say, for example, anything new, then I got to be smarter based on all the experience levels.

So, in other words, you want the architecture because if you do not address things in either a holistic manner, where everything inhabits, like somebody used the diamond example, then that is fine if it's acceptable, but if not, then if you're going

to go implement security controls within the platform, then you have to have an architecture that determines how the connectivities, how the flows will occur, so that you can then assure yourself that you can carry that design through the implementation.

Because, remember, there is functional design that comes into play where a software person may say, hey, functionally I should allow this widget to talk to this particular non-safety-related item. And so you want some rules in place up front. You cannot do that unless you establish some of those up-front architecture rules. Because I think software, malware, and all that, I believe IEEE 10-12 should address that for consistency and standardization.

The only thing that will not work is on the operating system, like I said. Because I'm not sure that Microsoft is going to provide code to everybody to review. They will provide you out of the box trusted software and a version number and a certification that it's free from malware and a list of vulnerabilities that still may be open, known vulnerabilities. So that becomes your starting point.

And then at the integrator's facility, like you said before and, I guess, Gordon Clifton had been talked about it, which is that you have a secure development environment that would then ensure that any changes made to operating systems were done under

a process in a secure environment. Because I think you'd have a false sense of security if we believe that we are going to go do a code-by-code review on a Windows operating system. I'm not sure that's going to happen or it's -- because the vendors would cut us off.

MR. STATTEL: Okay. This is Rich Stattel. Thank you for that input. I'd like -- there's a couple aspects of this I would like to speak to. One is the V&V activities. And I agree with the idea that the V&V activities could be a useful means of addressing cyber security vulnerabilities. However, it would require kind of a paradigm shift because 10-12, IEEE 10-12, as many of you know, is really a serial or sequential process for developing a system and with an end goal of installing it into the plant.

And the challenge here, when it comes to cyber security, is that a lot of the vulnerabilities and the vectors can happen after the fact. So after the system is running, it's operating the plant, performing safety functions, these vulnerabilities become apparent or they get developed after the fact. And the 10-12 processes, the V&V has been completed prior to installation in the plant. So it's really not set up to directly address those. Although I think the activities are wholly appropriate, but you can't -- it's hard to envision a V&V process that would be ongoing that you're constantly re-performing

the V&V activities.

So I think that's a challenge. I'm not on the 10-12 Committee, so I don't know exactly where -- how IEEE 10-12, the membership is trying to address these aspects. But they do include activities to address the architecture of the system. So you had mentioned that in your first question. I believe the architecture is very important and it's something that we do concentrate on in both the new reactor reviews, design reviews, and the operating reviews. It's a little -- I kind of feel that it's a little bit easier to do in the new reactor designs because you have the whole system, safety, non-safety, out in front of you when you're doing the Design Certification reviews.

Whereas, in the operating plants, we're kind of having to shift our MO here because we're typically only looking at a little piece of the system that's being upgraded. And it's -- to get an idea of what the architecture of that is and what the overall perspective of that system is, you really have to go beyond the scope of the license amendment itself. So that's been challenging for us, but we do that on a regular basis.

So, for example, the Diablo Canyon project that's currently under review, it's really just a PPS. It's a very limited scope upgrade of the reactor protection system and the ESFAS system. But we required the applicant to describe all the interfaces to all other systems and we -- in their application,

they did include a very detailed description of what those interfaces are. So we have a pretty good understanding of that architecture. And I think we would carry that forward into any future reviews. But it is a little bit more challenging in the operating realm because typically we're seeing piecemeal upgrades when these license amendments come through.

Now, as far as the standards development, it was your second question, I can speak a little bit for the IEEE standards. They -- it has been debated at the impact level and we've had a lot of discussions in IEEE 7432, of which Deanna and I are members of that working group, there's a lot of people who think that the IEEE should pursue developing a separate standard just to deal with the cyber security aspects of digital systems.

And that's -- it sounds like a good concept and a good path to go down, but it's very challenging because a lot of those same people who you would need to develop that type of standard are also on these other committees and developing the standards for 7432, which deal with all the multitude of other aspects of digital systems that have to be addressed. So I will admit, we haven't really addressed it very thoroughly within IEEE 7432.

MS. ZHANG: Well, we actually took an effort to remove it because we felt that it's a broader subject that's beyond the scope of IEEE 7432. And, in addition, one of the things that we have to recognize is that anything that would be related to cyber

security that would be developed would -- it's going to be a long development process. So we're not going to get a standard that's going to come out any time soon from the IEEE group regarding cyber security.

MR. STATTEL: No. The other thing I'm very adverse to is the development of duplicative standards. And since we have guidance on cyber security implementation in Reg Guide 5.71, I believe it might not be too beneficial to try to duplicate those type or modify that set of guidance --

MS. ZHANG: Unless it's --

MR. STATTEL: -- inside of IEEE space.

MS. ZHANG: -- at implementation. Yes. More of an implementation type of guidance of Reg Guide 5.71.

MR. CLIFTON: This is Gordon Clifton. That's what I was just leading to is implementation. Because Kim's talking about code writing, you're talking about involvement in the development of the process and approach. You're looking at implementation in the site. We're looking at in an inspection process, audit process, a review from milestone, from soup to nuts. We're looking at when it gets started to actually when it's in plant and you have a very, let's say, code fault and you get a trigger long after installation, that's the way we get a fault in digital. It's a two step process, you have the error in the code and then you get a trigger later on.

But we're looking at something that goes from soup to nuts. We're not in a single point that's going to work acceptably. And we saw that when we were at the audit that occurred at Diablo Canyon. They came out and they looked at it and stuff wasn't ready for their perusal at the moment. But it was way past the code writing. So multiple stages in here and, like you said, that's going to be a challenge of implementation of how to look for cyber from start to finish without slowing down the process unnecessarily or duplicating other process that's already in place. And we've got 5.71 and 1.152 are both in place that are working pretty well right now for their own respective parts.

MR. STATTEL: I do agree and I believe they have been effective. And we have been using them for a number of years now. Now, it hasn't been that many years so --

MR. CLIFTON: Or that many examples.

MR. STATTEL: -- and it only takes one incident to prove me wrong, right?

MR. CLIFTON: Right.

MR. STATTEL: But I do believe a lot of the measures that have been implemented will be effective in maintaining the security of these systems. Now, we have learned a lot and the industry has matured and over the last ten years, I got to say, the discussions even five years ago were much different. Because what we were really discussing then is, do we do these reviews as

part of the licensing application or do we do them just simply by programmatic and inspection activities? And it was just an either/or type discussion.

And it may seem to you that we're having the same discussion today, but in truth, I think we've all learned that neither approach really covers the whole range of cyber security issues. So it's a complicated matter and I think it does deserve a multi-prong approach. So I think approaching it basically from the top down, from the inspection perspective, as well as from the bottom up, where we do some review of cyber security at the license review stage, I think that's appropriate. And that's really what we're suggesting in the SECY paper. And that's what we will be recommending to the Commission as a policy going forward. So I think there's benefits to both sides.

MR. CLIFTON: We cover everything Jay brought forth?

MR. STATTEL: Probably not. But I'm sure Jay will point out the aspects --

MR. CLIFTON: Omissions.

MR. STATTEL: -- we missed of his questions there.

MR. AMIN: No, you haven't. I mean, that's good. But I'd just like to point only one thing on the V&V. The V&V is for a large-scale system, whether it's in an operating unit or whether it's a new build application. But the baseline V&V software doesn't change. If you put it under configuration management and

all the tight controls, then it's not going to change. The key thing is the -- after installation, during the operations and maintenance phase, how are those systems managed, maintained, and reviewed and evaluated for cyber security? And that is where we as licensees, when you look at Reg Guide 5.71 controls, are implementing some of those elements into our processes.

Because that's what's going to drive change, right? If I'm going to make a change to an operating system, I'm going to change a safety alert screen with another screen that has an updated software or identical software, the process because of cyber security as we march towards Milestone 8 will be address all those elements.

MR. STATTEL: Okay. So there was two things I heard in that discussion. One was the graded approach aspect. And that's something we're trying to address in the ISG6 process. So we do have some ideas for how to scale based on a full reactor protection system versus single components. And I think there's some progress to be made there. And the second part of that --

MR. CLIFTON: Configuration management and then maintaining it once it's going.

MR. STATTEL: Yes, right. Basically it refers back to the process or the cyber security plan, implementation of the plan or the --

MR. AMIN: Correct.

MR. STATTEL: -- the programmatic aspects of that. And I think that's just as important. The plants need to be diligent. They need to be constantly looking out for new threats and identifying different vectors. And that's where your programs come into play. Our inspections kind of go out and make sure that you're meeting the regulations, but the real defense we have against cyber security attack is really going to come down to how well those programs are implemented on an ongoing basis at the plants.

MS. ZHANG: This is Deanna. And as we said before, we're just trying to set a baseline so that when you install the system into the plant, we know at that point that there was a good look to make sure that it is a secure design such that when you do put it into the plant, you can let the cyber security program then take over. So it would be additional on top of what was done as the baseline, not -- you wouldn't have to look at all vulnerabilities that weren't identified prior to that.

MR. AMIN: And, no, I agree. You have to understand, up until now configuration management was for digital attributes. Now, with cyber security nuances, there is also configuration management that pertains to cyber security. We never went into vertical depth of version numbers for like equipment and software and all that. Now, every change coming in is challenged to make sure it's identical, if so, how is it proven it's identical?

Because a vendor may call everything, oh, it's identical. When you look at it, it's not. So licensees are getting a lot smarter in that area and that will significantly help cyber security.

And then the -- several initiatives in the industry is looking at to address the threat and vulnerability, how do we become smart in addressing vulnerabilities? Because you can't just go poll the internet every day looking for vulnerabilities. So we have to be smart about what we have and what are the vulnerabilities associated with it. And many times many vulnerabilities do not apply because most of the vulnerabilities I see many times are network related. If your systems are not even network connected behind diodes, you still have to assess that, but there is no threat vector that makes it in. And, of course, I worry more about the portable media.

MR. STATTEL: There was -- I just remembered. There was one other question you had asked about is the review of the data diode and the repeat reviews on subsequent applications. We have, like for instance, the Oconee -- the data diode that was used for the Oconee, that device was evaluated by the NRC and it was a fairly extensive evaluation. That same device is being used at Diablo Canyon and we did not repeat that evaluation. So we do credit the precedent that we set and we try to be efficient and not repeat our evaluations when we get those results.

MR. AMIN: Well, that's good.

MR. STATTEL: So, I'll just mention that.

MR. AMIN: Okay.

MR. RAKOVAN: Just a quick question before we continue on. We were scheduled to take a break around 2:10. Do we want to go ahead and keep going at this point or do we want to take a break? Just looking at the table to get a general thought. Keep going? Keep going? Okay. We do have a comment or question from the room. If we could go ahead and -- that was my understanding. Go ahead and then we'll go back to the phones, please.

MR. NEFF: Hello. Dave Neff, Exelon Nuclear. My perspective is licensing, so it's not so much implementation and INC kind of work, but from a process standpoint. So back on Slide 15, you talked about revising safety or important-to-safety systems and equipment. And the cyber security rule applies to security, safety-related NEP functions. And it also brings in the important-to-safety equipment as well. But your scenarios would include security, doesn't -- you're intending to exclude security, is that correct?

MS. ZHANG: No. We actually -- we are only -- for this SECY paper, the scope is only safety related and important-to-safety systems. So, for licensing, that's what we'll only focus on now. For the cyber security program, we do recognize that the scope is broader than that.

MR. NEFF: The elements of the cyber security plan

related to safety and safety-related or important-to-safety are covered under 50.54(p), because it's part of the cyber security plan. So you may get changes from 50.90 submittals for license amendments coming out of reduction and effectiveness of the security plan, not your 50.59 questions. Right? So from a licensing perspective, just remember that you might getting questions on effectiveness of the security plan, not effect on the core from a 50.59 perspective. Okay.

The other thing I want to bring -- a couple other points. NEI 13-10 initiative, are you familiar with the work that's going on with NEI and the NRC team? Probably not. You are? Okay. So a lot of the work right now on this revision is going after balance-of-plan equipment and trying to reduce the controls that are required for that equipment. So -- direct and indirect. So, when you're talking about important-to-safety equipment here in this scope, if we apply where we're headed with NEI 13-10, with balance-of-plan the amount of controls that would be necessary for BOP equipment is really reduced. So having a reduction in effectiveness of the security plan for BOP probably won't reach the level for a submittal.

So, let me encourage you to take a look at the NEI 13-10, the current revision, as we're looking to go into pilot phase next month with NRC concurrence, should be coming in here shortly for, not full endorsement, but at least our comments. So, that's

coming at us pretty quickly and we're looking pretty encouraging to implement that. So I think that will have some bearing on the scope of what you think might be applicable to this SECY, at least for operating power plants.

MR. STATTEL: This is Rich Stattel. Just for my benefit, because I'm not familiar with exactly where that initiative is going, is it intended to change the criteria for identification of Critical Digital Assets or changing the controls --

MR. NEFF: Controls.

MR. STATTEL: -- based on the safety significance of the --

MR. NEFF: The second part of it. We're not looking to revise what the definition of a CDA is, but rather what controls are appropriate for that based on its emergency preparedness function or its balance-of-plan function.

MR. STATTEL: I see.

MR. NEFF: And what the vulnerability is and how it could result in an attack. So Bill Gross and the NEI team can probably better feed you what exactly is going on with 13-10. I'm a little bit on the periphery. But I think that has a lot of value in reducing the scope of what you think this SECY might need to cover for an operating power plant.

MR. STATTEL: Thank you.

MR. NEFF: During the July Nuclear Information Technology Strategic Leadership, NITSL, conference in July, EPRI made a presentation around standards. So let me encourage you to go talk to your EPRI contacts. Because they're looking to really gear up and it sounded rather encouraging. It won't be this 2015 time period to get your answers, but I think there's -- and Bill Gross can get you that contact who made the presentation at the NITSL conference from EPRI. But I think there's some value coming to the industry and to the NRC as well from a standards perspective, even though, like you said Deanna, IEEE is going to take us a while. I think EPRI will as well, but there is work coming out that will be beneficial for future reactors and for design changes.

The last comment I had, suggestion, was have you looked at, and I don't know if it's applicable, but the standard review plan, NUREG-0800? So in my days of starting up from Limerick, we relied on the NUREG-0800 as to how you design a power plant. So I don't know if there's a modification to 0800 that would work here for you and maybe you need the Commission to tell you that's an okay way to go. But from my previous days, NUREG-0800 was like the bible to how to design a power plant. And if we met that design, then it went through the NRC review period process pretty easily at that point in time. So I don't know if you've already thought about that as an option, but if you're looking for an easy

standard, NUREG-0800 sounded like a good spot for me where I'd go to take a look at. That's all I had then.

MR. JACKSON: Terry Jackson. To address your last point there, I'm not quite sure we're at that point as to where we might modify aspects and so forth. We're mainly first looking for the Commission to determine, one, if they want us to make any change and then, two, if they do want us to make a change, what extent would that need to be done? Primarily looking for a policy direction, which would then either direct us towards rule making or something smaller scope, which may be like a regulatory guide or maybe standard review plan.

MR. NEFF: Okay, good. Thank you.

MS. ZHANG: And -- yes. And as far as with your other suggestions, again, right now, as Terry said, we're looking for the permission to do something from the -- their direction. So as far as the implementation later on, I think that's when we'll be engaging in the other groups more.

MR. NEFF: From an informed -- when you go to make, provide them an informed information, help them making an informed decision, I think some of these other inputs may help in your recommendation and some of the dialogue you might have with the Commission later on. Good, thanks.

MR. RAKOVAN: Okay. Emily, do we have any other speakers in the queue at this point?

OPERATOR: Yes, sir, we do. Our next question comes from --

MR. PEZESHKI: Jonah Pezeshki.

OPERATOR: Sir, your line is open.

MR. PEZESHKI: Hello. I don't necessarily have a question, I just have a few comments based on what I've heard. Oh, before I continue, this is Jonah Pezeshki, Nuclear Regulatory Commission, Cyber Security Directorate. So first, I just wanted to warn against getting too caught up in the prescriptive elements. I've heard a lot of comments about code review, whether or not that's possible based on the type of product that we're talking about, et cetera. I just want to remind that we're trying to maintain the same scoping that currently exists in both 73.54 as well as 5.71 and other applicable guidance. And so we need to avoid getting too deep in the weeds on this. I mean, right now we're talking about a very high level perspective.

At the same time, there were some comments about additional regulatory burden, additional audits, et cetera. I think it was mentioned earlier, but it's my understanding that our overall intent is to dovetail with current safety review processes in order to avoid any additional regulatory burden. I'm correct in saying this?

MR. STATTEL: That is our intent, Jonah.

MR. PEZESHKI: Okay. And I just want to make it

abundantly clear, because I know that there is definitely fear from the industry that there's going to be additional regulatory burden and additional processes that they have to adhere to and I don't believe that's our intent in the slightest. And so, really, this is just, as we said before, to give industry an earlier bite at the apple.

As many would tell you, cyber security is generally considered throughout the entire design, implementation, and eventual retirement of a system. We know that the licensees being, well, quite frankly, incredibly confident people, are already considering cyber security throughout the design process. This is really just to help ensure that there are no hiccups along the way that will eventually bite them during the implementation phase or post-implementation. Yes. If there's any questions or comments, but that's pretty much it.

MR. RAKOVAN: Okay. Thank you.

MR. PEZESHKI: Yes. Thank you.

MR. RAKOVAN: Emily, can we go to the next person, please?

OPERATOR: At this time, I'm showing no additional questions.

MR. RAKOVAN: Okay. I guess I'll go back to the table and see how you guys want to proceed.

MS. ZHANG: Gordon, did you have any of the questions

that Bill wanted to ask? Do you have that available?

MR. CLIFTON: This is Gordon Clifton. I think we've covered that ones that Bill had identified earlier. He was looking for confirmation that you didn't perceive we had problems out there we were trying to fix. We've clarified that, that's the situation, we're confident in what's out here. We're moving to allow or encourage or create an NRC involvement early enough in the stage that we don't have problems later on. And I think that's a common goal for both sides, for the industry and the NRC, is we don't want findings or failures or problems that stops production of power or safe operations.

And we can do that by being prepared earlier. And that's -- whether it's at code level or all the way at implementation, it's still a theme that's going through. One of the key aspects that we look at cyber security is it's sort of grout between the bricks. It's always out there, but it's not a stand alone item by itself. So it's difficult for us to write guidance on something that's addressing so many different aspects. For whether it's code writing or turning wrenches later on, boots and guns for the security people coming in, whether it's physical. I think we did a great job of separating those two a couple years ago. We were doing a good job of maintaining boots and guns from fine wire, electronic aspects. And now, as somebody mentioned, we've got portable aspects and wireless aspects as new challenges.

And we've identified in here we're going to be addressing vulnerabilities in the future. We don't know all of the ones that are coming out there, so we have to have some flexibility to change with what's going out. And Bill's concern was we don't want to try and fix something that's not broken, we don't want to make life -- consume resources that both sides, the industry and the vendors and the NRC, have unnecessarily. Because we can get good products now, we just want to make sure we maintain the quality that we have and then continue the same aspect.

And I think we're on the right path. It's a tough challenge. My guess is we'll come back with the Commissioners -- with direction to set a policy to be involved, but not to stop the process. But that's speculation in the future. And that's I think one that the whole industry can support. Terry's shaking his head, yes, here.

MR. JACKSON: Well, I was going to maybe -- because I think you started addressing the question I was going to ask. At the last public meeting, the industry more or less gave us their position on the SECY was basically take Option 3, which is not do anything. I think today what I hear is, is that there is caution about maybe making things too prescriptive or increasing regulatory burden where it may not necessarily be necessary because the current process works well

But if there is opportunity to enhance the process so

that there is some efficiencies gained, particularly one advantage I think I hear from you all is the ability to be able to start address cyber security earlier in the process versus later on. Then if we have those opportunities then that would be something I think the industry would want to support.

MR. STATTEL: This is Rich again. There were two messages that I got from the last meeting. And they were kind of conflicting. So, one of them was, there was a concern that any new guidance or regulation that comes out of this effort would basically do the double whammy on the applicant. So, in other words, we would have a shot at your systems during the license review and then the second shot when the inspectors get out to the plants and it would basically make things more difficult for them. That was the one aspect. Now, I think Deanna and I agree that, that's not our intent here, right? We're really just trying to do a more holistic approach to addressing cyber security with regard to regulations.

And then, on the other side, the other feedback we got was more from the new reactors vendors, where they really want us to do the reviews more during the Design Certification stage to eliminate the risk that would be posed later on during implementation. So, as we were developing these slides and as we were developing these scenarios and talking about this, I think we kind of were trying to keep both of those perspectives in mind.

And I don't know how successful we were. But our objective here is not really create any new requirements, is we just want to be more efficient at how we address cyber security throughout the process.

MR. CLIFTON: One of the things, lessons learned from the Diablo Canyon, was identifying what you're looking for and when you're looking for it. And if we can come up with a scenario where the NRC involvement isn't, as you called it, a double involvement, that while the book's open, somebody's looking over the shoulder to confirm, yes, that does cyber security as well as the interface with the plant that we expected or the performance we expected.

And part of that maybe is an inspection plan or guidance for your inspectors and/or auditors as the case may be, because we're looking at audits before implementation, that they have something specific that they're looking for. And if we have clarity of what you're coming in to validate or inspect or audit, and it's a short-term many times over, that's probably quite understandable and acceptable to put in to the modification plan. That you put a milestone that you're checking for code, you're looking for physical/digital characteristics, you're looking for implementation, you're looking for interface between the system and that digital widget.

Those are all -- could be ten years apart, but they

have to be an administrative check that we have all confidence that we've gotten involved early to make sure cyber security is progressing acceptably, that we're identifying hurdles that would be out there by the NRC inspector's experience or the site's development of answers to questions, and then we can get them resolved while they're small --

MR. STATTEL: Okay.

MR. CLIFTON: -- rather than while they're large.

MR. STATTEL: This is Rich again, Rich Stattel. With all that said, I do acknowledge, there's some danger there that --

MR. CLIFTON: Absolutely.

MR. STATTEL: -- there could be an increased burden. And it kind of all depends on how this plays out and how well we communicate with NSIR and the inspectors going forward. Now we have some experience with this, not only in the cyber security area, but in the licensing review area. So, in our past reviews at Oconee, for example, we did the license review of the license amendment and that was a pretty significant effort that went over the course of two years.

But it was also followed up by inspection activities that occurred on site when the site acceptance testing was performed and when the installation and during startup as well. And in those cases, there were several aspects of the design that

could not be reviewed at the time we were doing our safety evaluation. So we kind of had to defer those, right? And the way we did that is we made a list of recommended inspection items, that's part of the safety evaluation, and those were used to develop the inspection plans.

So we were communicating regularly with the inspectors and I actually -- several members of our group actually participated in those inspections. We went down to the plant and performed -- were part of the inspection team. So, I think that's key here too. If you don't have that communication, if you don't have some hand shaking going on with the inspectors, I think the danger becomes a lot greater that there's an increased burden and you have -- you're being attacked from two different sides here.

So, it's important and I'm not sure how to make sure that happens in the future. But I think that's an important aspect, maintaining the communications. In fact, we have an inspector from Region IV that's currently participating in our evaluation of the Diablo Canyon safety evaluation. So we do have overlap, we do have some experience with coordinating these efforts. And I would expect the same thing to occur for the cyber security.

MR. CLIFTON: This is Gordon Clifton again. One of the lessons learned we've had is in these processes we've done is Phase Zero Meetings, is what we're calling them. And these are before

the submittals, where we have open dialogue between the applicants and the NRC that identifies low hurdles, high hurdles, solid walls that we need to get around. And if you find yourself in a position that the policy is such that you don't have inspection and finding capabilities until implementation, as it is now, you could identify these earlier interfaces as Phase Zero Meetings with the applicant, the utility, whoever's building this modification.

And those Phase Zero Meetings we had at Diablo Canyon, what, four, six of them, something in that respect, over a series of months. And the communications affected the design significantly while it was on the paper and before it was being built. And it encouraged the flow of the modification very well.

With that success applied to cyber security, if you come in and have a Phase Zero Meeting to talk about, what did you do about code, what did you about malware, what did you do about what your plans here, without a penalty, then the communication aspect is the part that we're trying to encourage between the NRC and the utility rather than the enforcement of something that's wrong or violating a rule or something. And then it's really received as an assist, if you will, rather than a penalty or something to fear while you're in the early stages of planning.

MS. ZHANG: Yes. And we've been -- this is Deanna Zhang. And we've been doing this on the new reactor side for both Vogtle and Summer participating and supporting regional staff in

doing the different milestone implementations for the cyber security program as these systems are getting developed. But, again, I think what Rich said before was, there is a bit of a dichotomy here between new reactors, and I wouldn't say new reactors, I would say between Design Certification applicants and a licensee COL applicant.

And that's where we see there may be a potential gap is that Design Certification applicants, they don't -- 73.54 does not apply to them. And, therefore, some of these design controls that should be considered early on in the overall INC architecture and the system design, were not done as part of the Design Certification. And, therefore, a COL applicant may have to inherit a unsecurable design and then would need to do design modifications after the fact.

MR. CLIFTON: And that's pricey and neither one of us want to do that.

MS. ZHANG: No.

MR. CLIFTON: Have we developed any more questions on the phone?

MR. RAKOVAN: All right. Let's go ahead and check in one more time. Emily, by any chance do we have anyone who is wanting to make a question or comment at this time?

OPERATOR: I'm showing no questions at this time. However, as a reminder, it is Star 1 if you're wishing to ask a

question.

MR. STATTEL: I guess we can go on to discuss the next steps.

MR. RAKOVAN: Sure.

MR. STATTEL: I think we're at that point.

MS. ZHANG: So at this point, we're hoping to finalize this draft SECY paper and present it, send it up to our EDO's office for review prior to sending it up to the Commission. We do expect that we will be making a Commission or probably Commissioner TA briefing at some point. And that some of the things we discussed at these last couple public meetings would also be raised at that briefing too.

MR. CLIFTON: I guess I -- this is Gordon Clifton. I'd ask, do we get the public involved again in the --

MR. STATTEL: Well, you don't --

MR. CLIFTON: -- future that you see?

MR. STATTEL: You don't get to see the SECY paper until --

MS. ZHANG: It becomes public, I guess. Until --

MR. STATTEL: I guess it has to go through the EDO's office and then it would become public.

MR. CLIFTON: When it goes --

MR. STATTEL: Sometime after that.

MR. CLIFTON: -- to your TA -- the Commissioner --

MR. STATTEL: But I don't think --

MR. CLIFTON: -- TA reps?

MR. STATTEL: -- there would be any -- I don't think there's going to be any surprises. The subject matter is really what we're talking about here.

MR. CLIFTON: Good.

MR. STATTEL: So, I don't think you're going to see this as blindsiding you or anything like that. We're not proposing anything to the -- any concepts or ideas to the Commission that we haven't already discussed in these meetings.

MR. CLIFTON: That's good. And then following, the Commissioners will have a COMSECY, right?

MS. ZHANG: Yes. So we would expect to see an SRM that would reflect their decision.

MR. CLIFTON: And optimistically, we think Santa Claus is bringing that by the end of the year, right?

MR. STATTEL: Though I think the public would have an opportunity to chime in between the SECY paper and when the Commission makes its decision. Is that not correct? I'm not --

MR. CLIFTON: I don't think so.

MR. STATTEL: Okay.

MR. CLIFTON: I don't think I've seen it yet.

MR. STATTEL: Okay. So the first time the public would have access to this would be when the COMSECY paper goes out.

Okay.

MR. CLIFTON: Your work's cut out for you.

MR. JACKSON: But that's why we wanted to engage the industry in the past two public workshops is to get your feedback.

MR. CLIFTON: Yes.

MS. ZHANG: Okay. So with that, if we don't have any more questions, I would like to thank everyone for participating again. Taking this opportunity to get the feedback from industry and the public has been very important to us and we hope that it would better inform our SECY paper development. So, thank you. And hopefully you will see the SECY paper, the COMSECY paper at the end of this year.

(Applause.)

MR. RAKOVAN: All right. With that, we're closed.

(Whereupon, the above-entitled matter went off the record at 2:43 p.m.)

1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632