Official Transcript of Proceedings

NUCLEAR REGULATORY COMMISSION

Title: Advisory Committee on Reactor Safeguards
Digital Instrumentation and Control Systems
Subcommittee Meeting: Open Session

Docket Number: (n/a)

Location: Rockville, Maryland

Date: Thursday, February 23, 2017

Work Order No.: NRC-2906 Pages 1-173

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

DISCLAIMER

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

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

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

UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

+ + + + +

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

(ACRS)

+ + + + +

DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS

SUBCOMMITTEE

+ + + + +

OPEN SESSION

+ + + + +

THURSDAY

FEBRUARY 23, 2017

+ + + + +

ROCKVILLE, MARYLAND

+ + + + +

The Subcommittee met at the Nuclear Regulatory Commission, Two White Flint North, Room T2B1, 11545 Rockville Pike, at 1:04 p.m., Charles H. Brown, Jr., Chairman, presiding.

COMMITTEE MEMBERS:

CHARLES H. BROWN, JR., Chairman

DENNIS C. BLEY, Member

MARGARET CHU, Member

WALTER L. KIRCHNER, Member

JOSE A. MARCH-LEUBA, Member

JOY REMPE, Member

JOHN W. STETKAR, Member

MATTHEW W. SUNSERI, Member

DESIGNATED FEDERAL OFFICIAL:

CHRISTINA ANTONESCU

ACRS CONSULTANT:

MYRON HECHT*

ALSO PRESENT:

MATTHEW BARTLETT, NMSS

JOSEPH DEUCHER, NMSS

JAMES DOWNS, NMSS

CRAIG ERLANGER, NMSS

JAMES MALTESE, NMSS

CARDELIA MAUPIN, NMSS

MICHAEL SHINN, NRC Contractor

ANDREA D. VEIL, Executive Director, ACRS

*Present via telephone

C O N T E N T S

Opening Remarks, Introduction of Members, and Comments on Procedures 4

Overview of the Schedule for the Rulemaking on Cyber Security at Fuel Cycle Facility Licensees 8

Overview of Changes to the Draft Regulatory Guide (DG-5062) since November 2, 2016 11

Overview of the Draft Proposed Rule and Associated Documents (non-public) 105

Public Comments/Questions 146

Adjournment 147

P R O C E E D I N G S

1:04 p.m.

CHAIRMAN BROWN: The meeting will now come to order. This is a meeting of the Digital I&C Subcommittee. I'm Charles Brown, Chairman of this Subcommittee meeting.

ACRS members in attendance are Matthew Sunseri. Did I pronounce that right this time? Got it. Margaret Chu, Charlie Brown, Dennis Bley, John Stetkar, Jose March-Leuba, Walt Kirchner, and Joy Rempe.

And some others may join us. But they're not here right now. So, I won't announce them. Christina Antonescu of the ACRS staff is the Designated Federal Official for this meeting.

The purpose of this Subcommittee meeting is to review the technical basis supporting the fuel cycle cyber security rulemaking, the draft proposed rule language, the draft guidance, SECY paper, and other related fuel cycle cyber security rulemaking documents as required.

Today's briefing will also include discussion on the comments that the I&C Subcommittee made on these same topics in an earlier Subcommittee meeting on November 2, 2016.

At that meeting we also considered or determined that there was going to be another need -- a need for another meeting based on the lack of completion of a couple of the documents that we were looking at at the time.

And then we are presently scheduled for, or potentially scheduled correctly, for a full Committee meeting in May.

The Advisory Committee was established by Statute and is governed by the Federal Advisory Committee Act, FACA. That means that the Committee can only speak through its published letter reports.

We hold meetings to gather information to support our deliberations. Interested parties who wish to provide comments can contact our offices requesting time after the meeting Federal Register Notice is published.

That said, we also set aside ten minutes for spur of the moment comments from members of the public attending or listening into our meetings via a phone line. Which we do have open today.

Written comments are also welcome. The ACRS section of the US NRC public website provides our charter, bylaws, letter reports, and full

transcripts of all full and subcommittee meetings. Including all slides presented at those meetings.

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

The rules for participation in today's meeting have been announced as part of the Notice for this meeting previously published in the Federal Register.

As shown in the Agenda, some presentations will be closed in order to protect information that is proprietary, pursuant to 5 USC 552(b)(c)(4). Attendance at this portion of the meeting dealing with such information will be limited to the NRC staff and its consultants, and those individuals and organizations who have entered into an appropriate confidentiality agreement with them.

Consequently, we need to confirm at that time that we have only eligible observers and participants in the room for the closed portion.

We have received no written comments or requests for time to make oral statements from members of the public regarding today's meeting.

As always, we have one open bridge line established for interested members of the public to listen in. Also, the bridge line will be open at the end of the open portion of the meeting to see if anyone listening in would like to make any comments.

In addition, a second line is open for Myron Hecht, our consultant to participate in both the open and closed meetings.

A transcript of the meeting is being kept. And will be made available as stated in the Federal Register Notice. Therefore, we request that participants in this meeting use the microphones located throughout the meeting room when addressing the Subcommittee.

The participants should first identify themselves and speak with sufficient clarity and volume so that they maybe readily heard. And then, also please silence all cell phones, pages, iphones, ipads, and all other appropriate digital appliances.

We will now -- and communication appliances. We will now proceed with the meeting. And I will call on Mr. Craig Erlanger, Director of the Division of Fuel Cycle Safety, Safeguards and

Environmental Review of the Office Nuclear Material and Safety and Safeguards, NMSS, to start the presentation.

Craig, it's all yours.

MR. ERLANGER: Thank you. Good afternoon everyone. We appreciate the opportunity to brief you this afternoon on the topic of fuel cycle cyber security and our proposed rulemaking and regulatory guide.

We have a full agenda as was just mentioned. The first topic we are going to cover is the overview of the schedule for the rulemaking on cyber security.

I'm going to turn it over to Cardelia Maupin who is going to lead us in that discussion. And thanks again for the opportunity to present this afternoon.

MS. MAUPIN: Okay. Thank you, Craig. One -- the very first slide, --

CHAIRMAN BROWN: Microphone, please.

MS. MAUPIN: Thank you. Thank you so much. This is Cardelia Maupin again with NMSS, Master Rulemaking and Project Management Branch.

And we are leading this aspect of the rulemaking. As you know, once the -- we accept the

regulatory basis, then it comes over to the rulemaking portion of NMSS. And that's where we are now.

As Craig mentioned, we have a number of, I would say, exciting topics for you. The very first of which we're going to talk about our schedule, as Craig mentioned.

My colleague, which is going to be exciting. And also, we're going to talk about the preliminary draft of the reg guide. All of these are listed on slide two. And along with, we have the ADAMS accession number there for you.

We will also talk a little bit about the proposed rule package and the associated. All of these are drafts at this time. The drafted -- associated draft regulatory basis.

And the next slide, although you probably know all of these acronyms, but because this is a public meeting, we have to have -- we put in all the acronyms for those members of the public who might not be as familiar with these acronyms.

And I will not go through these acronyms. Because I know you all know what 10 CFR stands for. And NRC and all those kind of things. So, but for members of the public, we did include

a list of acronyms for this presentation. That's on page number three.

The next slide is dealing with an overview of our rulemaking schedule. As you can see, we've provided for you a little table here with the objectives, the target date, and the dates for our SECY paper.

As you can see, the regulatory basis has been completed and was completed back in March 22, 2016. And thankfully, we did that a little bit ahead of schedule.

However, right now we are in the proposed rulemaking package of, as I said, the proposed rule aspect of the rulemaking process. And the target date for that, as you can see there, it was March 15 were to -- are to get it to the Commission.

March 17 of this year it is to go to the -- I mean, to the EDO. That first target date there is to the EDO, March 15, 2017. That's to the EDO.

The March 17, 2017 is when it's due to the Commission. In terms of the final rule package, the due dates are as you see there, February 1, 2018 to the EDO. And June 11, 2018 to

the Commission.

So those are our target dates at present. The package is still undergoing office concurrence. So, I just want to say there might be some challenges in terms of meeting those dates. I want to say that up front.

The next slide, as I said, the proposed rule is currently in concurrence process. And we're resolving some of the comments that are coming out of that process in terms of the overall requirements, trying to get everyone on the same page.

It's so important for us to get on the same page in terms of the staff before we give it to the Commission. So that's where we are now.

We also have the draft regulatory guide in the concurrence process. And these other things, the interim staff guide and inspection procedures, those would be developed after we've come to, you know, agreement on the proposed rule package and a draft guidance document.

Now I'm going to turn it over to James Downs who would do the next portion of the presentation.

MR. DOWNS: Okay. Thank you, Cardelia.

As Cardelia mentioned, my name is James Downs. I'm the Technical Program Manager for Fuel Cycle Cyber Security. I work in Craig's Division.

Before we move one, were there any questions on the overall process or time line? Or anything like that? I didn't want to just flip through those slides and not provide an opportunity for questions.

(No response)

MR. DOWNS: Okay. Hearing none, --

CHAIRMAN BROWN: I will ask one question.

MR. DOWNS: Sure.

CHAIRMAN BROWN: She mentioned that you thought your dates were in jeopardy potentially. And they're out for concurrence.

So, I mean, that meant to me you don't think you're going to meet the March 15 date?

MR. DOWNS: Yes. As Cardelia mentioned, it will definitely be a challenge to meet those dates.

CHAIRMAN BROWN: Yes, okay. I just wanted to make sure that was not just a toss out. That literally you're struggling through the concurrence process so you can get it to the EDO,

right?

MR. DOWNS: That's correct.

CHAIRMAN BROWN: Okay. That was all.

MR. DOWNS: Okay. Slide number six. What we've got here is just an overview of the various facility types that we've got on the fuel cycle side of the house.

We've covered each of these different facility types in significant detail during the November briefing. This is something here that we just wanted to kind of jog everybody's memory.

You know, we're talking about conversion, enrichment, fuel fabrication, and that depleted uranium deconversion facilities. On the next couple of slides we've actually got a list of the various licensees that fall under these different facility types.

Again, so we've got the uranium conversion, uranium enrichment, which is -- includes both gas centrifuge as well as laser separation facilities.

Slide eight, we've got fuel fabrication facilities for commercial use, fuel fabrication facilities for nuclear navy and research test reactors, fuel fabrication for mixed -- performing

the mixed oxide process. And then we have one depleted uranium deconversion facility.

We should note at this point that five of the facilities that have shown on slide seven and eight, are currently not in possession of licensed material.

So, what we have in the proposed rule is a provision -- I should say what we have in the draft proposed rule, is a provision that provides an exception such that those licensees would not be required to submit a cyber security plan until six months prior to possession of the licensed material. So, it doesn't put an undue burden on those facilities.

Okay. With slide nine, just going to get into an overview of the draft reg guide, the content. And specifically the next several slides. We've got about 20 slides or so on the draft reg guide.

The key of my presentation was to kind of focus on the changes that have occurred since the November briefing. The slide nine here, we've got an overview of the content.

The key thing here is the structure of the draft reg guide hasn't changed at all since

November. We're still following the same standard structure for reg guides.

Slide ten. So each section of the reg guide, we've got a brief description of what was included in that section. So, the Section A, which is the introduction section, you've got proposed -- what the purpose and the applicability of the reg guide is, as far as the actual regulations, associated guidance, and just a general purpose of NRC reg guides.

The key here again is there were no significant changes to this section. There were some editorial changes made to follow the format that was provided by the Office of Nuclear Regulatory Research.

CHAIRMAN BROWN: So you'll be talking about the rule in the closed session?

MR. DOWNS: That's correct.

CHAIRMAN BROWN: Okay. Thank you.

MR. DOWNS: And obviously, I learned in November, this is definitely not a shy group. So, stop me as I go if you have questions, please.

Section B, which is the discussion portion of the draft regulatory guide. This includes the reason for the issuance. Basically,

what the lay of the land is -- the regulatory landscape is right now.

Some of the background and harmonization with international standards. There were two significant changes in the discussion. Previously we have a summary of each of the sections. Which seemed a little redundant.

So, we have removed that summary. I think it saved like three or four pages in the reg guide. So, that was a significant change.

Also, we previously had a phased implementation time line that was present in the draft reg guide. We no longer have that. The reason for that is really the purpose of a draft reg guide is to describe the methods and procedures that the staff considers acceptable for establishing, implementing and maintaining a cyber security program.

With that in mind, the time line just didn't seem to fit that purpose. So what we did was, we took that time line out. We moved it into the Federal Register Notice for the proposed rule.

It's one of the questions in the discussion section there. So, we haven't lost track of it.

But it's still the same general time frame that we were talking about before. Which was after NRC approval of a cyber security plan, the licensee would have six months to identify and document vital digital assets.

And then 18 months to fully implement the rule. And that 18-month time frame was given to us back when the Commission provided their SRM on SECY-14-0147. And that just corresponds to that 18-month time line.

Any questions on the discussion section here at all?

(No response)

MR. DOWNS: Slide 12, which is the staff regulatory guidance. This is where we really get into the meat of the reg guide. So, this is broken down into 12 different sections.

Each section corresponds to a specific provision in the proposed rule. Again, the structure of Section C is unchanged. So there were no changes from the November publication.

CHAIRMAN BROWN: One question. Is the order -- cyber security program perform its objectives. And then you go to the team as opposed to the plan.

Is there something -- some reason for this subordination? Or is -- I would have thought you had a program then a plan. Then you -- the team is not -- that's a subset of the plan.

I just wanted to make sure I understood that -- I missed -- I didn't miss something in the reg guide.

MR. DOWNS: So the intent there was to kind of lay these out in the order that a licensee would consider them.

CHAIRMAN BROWN: So the team comes before the plan?

MR. DOWNS: Yes. Because in order to draft the plan, you're probably going to have to assemble something like a team.

CHAIRMAN BROWN: Oh, okay. All right.

MR. DOWNS: So that's -- yes.

CHAIRMAN BROWN: Thank you.

MR. DOWNS: Obviously the actual compliant cyber security team, you know, you've got nothing to -- NRC would have nothing at that point to say -- per se inspect that team too at that point in time.

CHAIRMAN BROWN: That's fine. You can go on.

MR. DOWNS: Okay. So, slide 13. Again here in Section C.1 we've got a quick overview of the various general requirements. Including the team, the plan, identification of assets, addressing performance specifications, implementing procedures, and managing the cyber security program.

One of the changes here that we made is a change in terminology. And that we actually made it in the rule, of the proposed rule as well, that our -- we previously discussed interim compensatory measures.

We've changed that terminology now to temporary compensatory measures. It just may seem -- it's more or less a technicality. But the ICM terminology is traditionally associated with orders at the NRC.

So, we felt the change to TCM would eliminate that confusion. So, it's just a semantics thing more then anything else.

So the only thing we have to worry about being in conflict now is with Turner Classic Movie Station. But, we don't need to worry about that too much.

So, slide 14. The cyber security

program performance objectives. Again, we've got three performance objectives to detect, protect against, and respond to a cyber attack capable of causing a consequence of concern.

One of the points of confusion that was raised during the --

CHAIRMAN BROWN: Can I --

MR. DOWNS: Go ahead.

CHAIRMAN BROWN: Excuse me, can we go back a slide to 13?

MR. DOWNS: Sure.

CHAIRMAN BROWN: Somewhere within the draft guide it states, or I think it states that you were informed for these attri -- or these concepts for this approach based on the Reg Guide 5.71. Which was implemented for power reactors and sites.

And if you read 5.71, there -- the primary organization or path was focused on identifying a defensive architecture. And then within that defensive architecture, you would evaluate digital assets and how they fit within each of that concept of defensive architecture.

Defensive architecture is only mentioned three times in the draft guide. And it's not until

you get to the audit or review section of what they do periodically every year or three years, or something like that.

And so, it appears to me that you've started this process by saying hey, we're going to just identify all the digital assets in the plant. Start at the bottom, and we'll go and evaluate each rock, each grain of sand, each chair, each table, to find out whether it is digitally enabled or not.

And then we will develop a methodology for assessing and what do we do with them. And that seems to me to be a little bit lopsided, you know, the wrong direction.

So, I would just like for my own edification to have an idea of why you think you want to start down at the grass, the bottom line of these things without considering laying out how is the facility structured from a defensive basis?

And then what particular parts fall that need their digital assets even addressed? I mean office spaces would necessarily have to be addressed, I guess, in some circumstances to the same degree. But yet they're -- now they're all treated with the same -- the same broad brush.

MR. DOWNS: Okay. So Charlie, what you've hit on there is a key difference between the reactor side of the house, --

CHAIRMAN BROWN: Yes.

MR. DOWNS: And the fuel cycle side of the house. And when I say the key difference, I'm actually talking about the way that the safety regulations are laid out for reactors and the way that they're laid out for fuel cycle facilities.

Fuel cycle facilities are required to have an integrated safety analysis. In that safety analysis you actually identify accident scenarios that produce specific consequences of concern.

So they've done that leg work at the grassroots level. Our intent with this rule was to piggyback on that work that has already been done, and say okay, well, you've identified accident sequences that potentially have these consequences of concern.

And that's why the focus of our proposed rule is all on those consequences of concern. So, we're not concerned about the laptop that's sitting in somebody's office necessarily. Or as you put it, the tables and chairs.

What we're really focused on is the

digital assets that are associated with those consequences of concern. And we feel that our licensees, given the basis of -- the safety basis that they've established in the ISA, it's actually a better starting point for them rather then talking about some nebulous defense of architecture that could be very difficult to define.

And in essence, after you would implement a cyber security program, you redefine your defense of architecture then at that point. So, it's, you know, I don't want to speak to what's in Reg Guide 5.71.

But there is no question that it is a different approach. And the reason that we have a different approach is because we feel that it better fits the group of licensees that we're talking about.

CHAIRMAN BROWN: Do the consequences of concern also include -- the way I read -- now, I don't want to -- I'm trying to be careful here and not mat myself into the rule.

MR. DOWNS: You don't have to be too careful. Because there was a public version of the proposed rule.

CHAIRMAN BROWN: Yes. It's --

MR. DOWNS: So, we can kind of speak to that.

CHAIRMAN BROWN: Relative to the discussion we had the last time.

MR. DOWNS: Right. That's right. That's right.

CHAIRMAN BROWN: The fundamental focus it seemed to me, and this is my memory working now, because I didn't go back and look at everything in the last meeting, was that it was focused on accountability of special nuclear material. Not necessarily processes of manufacturing fuel.

Now, obviously you can lose material in the process of manufacturing. But not the compromise of the proper manufacturing relative to concentrations or percentages of this or that or whatever.

But it was fundamentally an -- trying to account for and not lose special nuclear material. Regardless of whether it was high enrichment, medium, low, or just chemical and other products.

Is -- and that's what I got out of reading the draft guide again after the, you know, this version that we looked at for this.

MR. DOWNS: So, there are four different

types of consequences of concern that we've got spelled out in the proposed rule.

CHAIRMAN BROWN: Are you going to talk about those relative to the draft reg guide?

MR. DOWNS: We can, yes. The -- I don't know --

CHAIRMAN BROWN: I took a quick though your later slides.

MR. DOWNS: Yes. No, I mean, it's -- so it's -- okay, it looks like we get to it a little bit on slide 17.

CHAIRMAN BROWN: Well, your example, Appendix G, --

MR. DOWNS: Right.

CHAIRMAN BROWN: Dealt with a process issue.

MR. DOWNS: That's correct.

CHAIRMAN BROWN: And not an accountability issue but a process issue of, you know, alarms and pressure and temperature sensors and things like that.

MR. DOWNS: That's correct. That will be a safety consequence concern in that situation.

CHAIRMAN BROWN: That's a safety consequence. Well, --

MR. DOWNS: Right. Right.

CHAIRMAN BROWN: That's a consequence of concern. I guess that is a conse -- but it's still not a -- it's not an accountability of special nuclear material concern. So, the example is a little bit different then how you would deal with an accountability issue.

I couldn't really see as we went through here, really grabbing onto the accountability part where I could focus, I mean, my own, you know, poor old mind was thinking about processes as much as accountability of materials, so.

MR. DOWNS: So, and we'll get to Appendix G. But, in a nutshell, Appendix G uses -- it lays out two different consequences of concern there as it speaks to different areas of that factitious facility that's described in Appendix G.

What you've got is a consequence of concern that deals with, as you alluded to, a process line that could potentially rupture and cause an exposure to either an individual onsite or a member of the public offsite. And that would -- that exposure fits into the -- as the proposed rule has it laid out that before the consequence of concern, which is a latent safety consequence of

concern.

That radiological exposure of 25 rem or greater, an intake of 30 milligrams or greater of solvent uranium.

CHAIRMAN BROWN: Right.

MR. DOWNS: And right down the line. The other part of that example on Appendix G of the draft reg guide lays out a physical protection of classified matter. And that the physical protection that's in place to protect that classified matter, it had digital aspects to it.

So therefore to prevent those -- that -- so to adequately protect that classified matter that's where the -- another consequence of concern comes into play. And that's the latent security consequence of concern.

MS. MAUPIN: If I can jump in. I think what I'm hearing Charles ask about, and you can correct me, Charles, if I'm wrong.

Is the materials accounting, the MCA materials accounting issue.

CHAIRMAN BROWN: Yes.

MS. MAUPIN: Is that what you're --

CHAIRMAN BROWN: Yes. That's kind of what I was.

MS. MAUPIN: And it's my understanding that they've been involved in this much longer then I have. But it was my understanding that after going and doing the onsite reviews at the various fuel cycle facilities, and also after the numerous public meetings and exchanges that we had with the licensees and stakeholders, initially when the reg basis was done that was going to be a part of this.

But after we got involved into the actual requirement and rulemaking process, it was my understanding we thought that that was an issue that was already adequately addressed. And that that was why it was not included as a part -- continued on as a part of this rulemaking.

I think that was his -- to that.

MR. DOWNS: Let me add just a little bit to that. So it was adequately addressed in the Category 3 facilities. Because material controlled accounting isn't a tremendous concern at Category 3 facilities for as far as the cyber security aspects of it though.

However, the proposed rule does include the first two consequences of concern, which the first one is design basis threat. Right? And that would be your Category 1 facilities.

That you do have an element of material and accounting there. Radiological sabotage, theft and diversion, that sort of thing at Cat 1.

The second consequence of concern is the safeguards, the latent safeguards consequence of concern.

CHAIRMAN BROWN: That's the Category 2.

MR. DOWNS: Category 2, correct. Correct. And that you deal with similar unauthorized removal of special nuclear material, loss of nuclear material control and accounting.

And that's dealing with the specific quantities of special nuclear material of moderate strategic significance. And then the third just for sake of inclusiveness, we've got the active safety consequence of concern.

So, those are the -- I've kind of loosely covered the three various consequences of concern. The draft reg guide tries to speak in general to them. Because you actually consider -- the process would consider those consequences of concern, the digital assets associated with them, kind of generically.

It doesn't matter whether you have a digital asset that falls into one or the other.

The only difference is is the controls that you would apply at the very end of the process.

So, when you have a digital asset that's identified for a design basis threat, you would still perform the same analysis and look to identify alternate means to perform that function that could potentially be compromised.

As you would if it was a consequence of concern that dealt with an act of safety. You would still look for that -- perform that same alternate means analysis so to speak.

CHAIRMAN BROWN: So you consider the lack of specificity relative to materials, special nuclear material accountability in the Category 1 or 2 range is, I mean, it's just not talked about. Other then that's one of the latent consequences of concern.

But it's not -- the way you're doing your assessments, it doesn't cover them explicitly. The only place it shows up is like in your example, to try to see how you would make judgments on the alternate means.

MR. DOWNS: That's correct.

CHAIRMAN BROWN: Is that what you're -- did I say that right?

MR. DOWNS: Pretty close. Yes. There's really no difference in the process that we've kind of laid out there. And acceptable approach between the various consequences of concern.

Again, the only difference comes at the tail end when you go to apply the controls. We do have separate groups of controls that are tailored in robustness so to speak, to address the -- each of the consequences of concern.

MR. DEUCHER: And this is Joe Deucher. Just to add onto what James is saying. The other thing that it does is it ties directly back to the design basis threat for say your Category 1 facility.

So they already have the existing requirements that they have to work through regarding their material control and accounting, regarding theft and diversion. And all we're doing is, we're just tying back into this to say, you have to look at this from a cyber perspective.

If you have any systems, or as we call them, digital assets that are associated with this consequence of concern that are in use that don't have any existing protections, or if they were compromised, would cause, you know, the potential

for there to be a loss of material control and accounting or the potential of sabotage that you have to go ahead and engage in measure.

You have to take the cyber security controls that are there. You have to look at the digital asset and apply them. Because now you consider it a vital digital asset. Meaning that, you know, it's important. It needs to be protected.

No different then from the physical side of the house with regard to the physical protection of your Category 1 facility under the design basis threat. So, really it's just kind of dovetailing into what's already there.

And that's why to a certain extent you're not seeing a lot of discussion of it in the reg guide. Because it's really just this add on of, okay, you're already looking at it for design basis threat, we need you to look at design basis threat in the sense of cyber security.

CHAIRMAN BROWN: Okay. I'm only going to now smoke this one more time. I guess I would have expected something in a purpose or an early discussion that states -- that would have made a statement that the purpose of these cyber controls

is to ensure that we have adequate protection guarding against the loss of special nuclear material as well as the production of, you know, special controls for -- or controls for the production of fuel or in the source material in whatever form it's supposed to be.

I didn't see that either place. It's just more talking about evaluating vital digital assets. And a little bit -- the reason for it, you wouldn't do it if you didn't care about the other stuff.

MR. DEUCHER: And again, this is Jim Deucher. Part of that probably maybe the fact that the reg guide as it's designed, is dealing with both Category 1, Category 2 that's nonexistent, and Category 3 facilities, and also Part 40.

So really, we're trying to catch a wide brush. And it may very well be that, you know, we can take another look at it again to see if we need to hone in on this.

But at the same time, we're also trying to be, to recognize the fact that it's going to be looked at by the Category 3 facilities. And we don't want them to get the impression that they have to do more given the fact that, say for

example, they don't have an insider threat requirement, which the design basis Category 1's do.

So, it's a balancing act. And we are through the guidance trying to ensure that we're making that balance so that every facility type can look at the guidance and get a clear understanding of what's an acceptable approach for them to meet the regulation.

So it maybe just some more editorial work on our part.

CHAIRMAN BROWN: Okay. Go on. Sorry to delay you.

MR. DOWNS: Slide 14. Thanks. So again, just cyber security performance -- cyber security program performance objectives, excuse me. The objectives haven't changed.

The significant change in Section C.2 is that there was some confusion that the detection elements that are discussed in this section were separate and unique and different from those that are actually included in the cyber security controls.

We want too just -- we added some clarifying language there that we're not looking

for anything additional beyond the controls. And again, the controls are only applicable to vital digital assets.

So that's what we're, you know, we're not looking for a global detection program at these facilities that would have a significant impact where -- again, we're just keying in on those vital digital assets.

The guidance here in this Section 2, it summarizes principals of detection, like understanding your daily traffic. Knowing how your system should operate, proactive administrative control, providing response, and, you know, again it talks about how all those principals can be automated and have defense in-depth through the actual controls themselves.

MEMBER MARCH-LEUBA: Yes. So I'm glad you're giving it some thought on how they can do this things. We talked in November that that can be really, really, really expensive.

MR. DOWNS: Right.

MEMBER MARCH-LEUBA: With emphasis on the really. So, unless you give some guidance about exactly what level of protection you require, it can be very expensive.

MR. DOWNS: Right. And that's -- in the -- we think that in the controls it gets to that level of protection. But again, you know, it is a draft document. And we're looking to have that feedback, you know, from industry or from any stakeholder on the acceptability of those controls.

MEMBER MARCH-LEUBA: And that's where the challenge is coming from. You just put an air gap and you don't have to do that.

MR. DOWNS: Yes, it's -- yes, yes, we heard this. You know, and again, back in November we had that same conversation with the air gaps.

And you know, we tried, as you'll see in the presentation here, we've added some information on the air gaps. But, at the same time the staff struggled with, you know, that an air gap doesn't address all of the attack vectors where a cyber attack can come from.

MEMBER MARCH-LEUBA: I understand how you have seen these, just have an insider threat.

MR. DOWNS: That's right. That's right.

MEMBER MARCH-LEUBA: But I guess we got a bigger one.

MR. DOWNS: That's true. Absolutely. And we tried to demonstrate in Appendix G in our

example, how if you had an air gap or a data diode, or you know, some sort of separation there that you can take credit for that as you go through and address the controls.

MEMBER BLEY: But if you don't have one, if you didn't have one, there's still other things to worry about. If you don't have one, ensuring that you're okay is, as far as I can tell, darn near impossible.

MR. DOWNS: It's more difficult. No question about that. Yes. And then now --

MEMBER BLEY: I think it's impossible but that's just me.

MR. DOWNS: So, what we did do, we can't require that a system be air gapped. Because there maybe a good reason, a good business reason that that system needs to be -- have some level of connectivity.

And during our site visits, we saw a number of these systems that needed to have connectivity from a business standpoint.

MEMBER BLEY: Two directional connectivity?

MR. DOWNS: Well, that's the question. Is it really -- and that's something that our

licensees are going to have to evaluate. Because there are -- one of the reasons, and we've heard from this group as well as the stakeholders during our public meetings is, oh my gosh, those controls that you've got are just extensive. It's crazy the number of controls that you've got.

Well, the controls that we've got in there are designed for this situation where you can't put it in there yet.

MEMBER BLEY: What do you think the first thing that's going to happen the first time we don't have gap in one direction and something gets attacked?

MR. DOWNS: Well, that's --

MEMBER BLEY: I'll tell you, it won't take long to decide we've got to have more indication.

MR. DOWNS: But I don't -- I don't bel -- one way -- that level of separation on the reactor side of the house, I mean, there are ways you don't necessarily have to do certain things over there. Is that correct, Mike? Or what's the --

MR. SHINN: In general. Mike Shinn, NRC Contractor. In general on the reactor side, if

it's related to safety or security, we expect it to either be completely isolated, that is to say there's no external connectivity at all.

Or that it's unidirectional in that those devices can send information out, but nothing can come back in. And that's the case at our --

CHAIRMAN BROWN: And it's a hardware based, not a software-based one they got.

MR. SHINN: Correct.

MEMBER BLEY: And that wasn't always true. That it was hardware based. It wasn't always true. But I'm glad it is now.

MR. SHINN: Perhaps it wasn't. But it is now. We do use the diodes.

CHAIRMAN BROWN: If you go back nine years ago, it was not one way. It was not hardware based. The fact is, everybody thought their software was so outstanding that they just -- flat walls were out. They were great. Nobody could ever beat them.

MR. SHINN: We did not feel that way though. We agreed that they needed to be -- physics is hard to argue with.

CHAIRMAN BROWN: Exactly.

MR. SHINN: That's why we like the

diodes.

CHAIRMAN BROWN: I would echo Dennis' comment. That you're going to hear this over and over again from us. We might as well beat the death out of this point.

You did cover in Section 6 a new -- a new thing you added, 6.2. I think it was 6.2. Maybe -- along with alternate means. But the example you used in Appendix G gave a little bit of flavor to the nonconnectivity. I'll call it air gap.

It didn't talk about really one way hardware-based communication. Because it was a local station that was doing something.

But that was a -- it segues back a little bit to the idea of the defensive architecture of some kind. I mean, you don't have to have what I call a global defensive architecture.

You can have a conceptual defensive architecture which says hey, there's critical information that we don't want to be accessible anywhere. That doesn't mean you have to spend lots of money, you know, laying out this, that, or the other thing.

But there are areas where you don't want -- you don't want data to go anywhere. And it doesn't have to. I mean I've forgotten where I read it, whether it was in one of the other pieces of paper about the comment that somebody from his home could change the setting on a process control.

And I don't know if that was something you all give us as an example of something. I'm trying to remember if -- because I wouldn't have read it anywhere else.

Okay, I think it was in one of you all's responses to something that was -- which seems to be anybody in their right mind, they did it wirelessly. Which is even more insane.

I mean, you talk about not being able to prohibit stuff, but wireless communications within a fuel cycle facility would seem to me to be a no -- just -- I can't find the right -- the word I would like to use I don't want to say over the air, so.

But you're going to hear this over and over again. And that -- because I think that both of us agree that an air gap is a great start. It doesn't protect you against an insider guy. Somebody can always do something funny.

But, somewhere you got to draw -- you've got to -- where do you put your confidence? In the guy that's calibrating the milliamp simulator in your example in Appendix G, which it stops there.

You have no protection. If that guy decides he's going to screw it up and, you know, miscalibrate it, what if it's a software-based milliamp simulator? Wireless connected.

MR. DEUCHER: Right. But again, this is Joe Deucher with NMSS. We would argue that that's where the detection piece and the response piece come into play.

Because just like any other IT system, it's great to have the protections in place. But we know that that's one third of the story. You've got to keep an eye on the network traffic.

Because, I mean, on any given day some new technology could come out and render it --

CHAIRMAN BROWN: Well, if you don't network it -- no. You don't network it. You don't have to network stuff. I mean, everybody likes to network it because it's cool.

We'll have a network. We'll put all our stuff there. We can download it. We can shift it around. Just really marvelous.

But a network is the death nail of a defensive architecture.

MR. SHINN: Mike Shinn, NRC Contractor. If I may, in the guidance we did try to strike a balance. I'm sure as you know, Charlie, I'm a big fan of diodes too.

So, for the Category 1 sites, we did provide guidance around an acceptable architecture that would require no remote connectivity for the facility.

CHAIRMAN BROWN: This is not a -- not in this reg guide.

MR. DOWNS: It's in Appendix C.

CHAIRMAN BROWN: Is that in Appendix C?

MR. SHINN: Yes. It's -- correct. Yes.

CHAIRMAN BROWN: It's hidden. I Just found it. It's there.

MR. SHINN: And one of the challenges we have, which Joe brought up earlier is, combined with the fact that we have a range of different types of facilities, Cat 1, Cat 2s, Cat 3s, Part 40s, they're all effectively unique.

So, when we went out and looked at the facilities, we realized that we couldn't provide even for the Cat 1s generic guidance to say this is

an appropriate architecture. Because they all use different technologies. They all shared information differently. They do different things.

So, you were correct that it ends up effectively being buried because we have to tie that guidance to a specific consequence of concern. So, if you happen to have a DVT, then that asset can't have remote access.

If you don't have a DVT and it's a latent safety on a Cat 3, okay. It might be acceptable to have remote connectivity provided that these other safeguards are in place.

But I don't think we would disagree that reducing the attack surface is a bad thing. That's a good thing. That substantially reduces the likelihood that the asset will be compromised. And it can reduce the amount of controls that you need to apply the asset.

I hope that answers the question that we certainly do in some cases, state that we would expect there not to be remote connectivity where there is an appropriate consequence concern. As well as other considerations that we learned when we went out and looked at these facilities that James talked about earlier.

For some of our licensees, the concern they communicated to us was that they needed bi-directional communication for the facility to function. That was not the Cat 1s though. I will say that.

MEMBER BLEY: So, might I -- if you've got a monitor at home, then.

CHAIRMAN BROWN: Yes. I guess if you're going to run it from home you can do that. Yes, Walt?

MEMBER KIRCHNER: May I interrupt? A few things come to mind. I was looking at your table of facilities.

And just the other day you -- the agency published a report that I think was prepared by Sandia. Which goes on to include DOE facilities that do recycling of different kinds, right? Or treatment of spent waste and so on.

So, I guess what I'm -- where I'm going with this is, it would seem to me that the consequence of concern that involved safety, that's the actual processes that are being done in the facility.

And by the way, that report has a rather comprehensive description of all of the different

technologies and vulnerabilities, et cetera, et cetera, that in one form or other probably involve process instrumentation and control.

Why wouldn't you treat that Category like you would treat a reactor facility? Because it seems to me that the information control part, we already have systems to deal with that.

You deal with classified information. It's suitably protected whether it's air gapped or tempest or whatever. That's a different category.

But it would seem to me, and there are systems in place that deal with that in both -- certainly in the NRC, over in the DOE and the DoD.

But, when we get to the actual processes on the floor in the facility where you have safety consequences of concern that involve either radiological exposure, explosions, criticality and so on, why would you not treat these like you treat the reactor facilities?

MR. DOWNS: So, to just kind of respond to that. This is James Downs with Fuel Cycle. The magnitude of those consequences are considered different then most within the agency.

It's, you know, when you're looking at with the reactor, I mean, you're looking at core

damage. When you look at a fuel cycle facility, you're looking potentially at an exposure of 25 rems.

That they -- the threshold --

MEMBER KIRCHNER: Certainly on the DOE side, the exposure could be a lot more then 25 rem.

MR. DOWNS: Absolutely.

MEMBER KIRCHNER: I'm not sure how you came to that answer of 25 rem. But --

MR. DOWNS: Again, it's the regulations that --

MEMBER KIRCHNER: Well, I know what the regulation is. But that's not necessarily the bounding estimate on the exposure that might --

MR. DOWNS: No. That's correct. You would have a potential criticality. Obviously it would expose you to a lot more then 25 rem, so.

But, the population would be exposed to that 25 rem would be different, you know, compared to the population potentially affected by core damage of a reactor. The population affected by a criticality of a fuel cycle facility, you know, it's different orders of magnitude when we're looking at the affected population.

So, that's the -- the --

MEMBER KIRCHNER: Well, that gets into a debate between workers and the general populous.

MR. DOWNS: Right.

MEMBER KIRCHNER: And risk frequency and so on. Are there any things in the DOE system that are vulnerable to this that -- do you share with them in terms of what they've done in these areas?

Certainly when you're dealing with, you know, spent nuclear fuel and waste, that's significant danger and hazard, right? To begin with. You know, they have to deal with the same set of problems.

So, are there things that they have done that are applicable here? And how the measures that they've implemented for this purpose, is there any value there that you can extract and apply here?

And is it reflected in your draft guide?

MR. DOWNS: Yes. So, one of the things that we've drawn on, as you pointed out, the protection of classified information, DOE has a very robust set of requirements for protection of classified information.

Some of which -- some of our licensees that possess classified information on networks,

they actually have to follow the DOE or NSA requirements for that classified information.

Some of our facilities also have unclassified networks that are accredited by the Department of Energy or NSA as the case maybe. And we were evaluating the appropriateness of that level of protection as compared to our regulatory -- the proposed requirements that we're looking at to see if there is any potential to avoid duel regulation in those instances.

The thing that -- that's what DOE does as far as classified information goes. As far as protection of safety systems in comparable facilities at DOE, we actually got a call within the past month from a DOE Project Manager who is looking to improve upon the requirements that DOE currently has for those facilities.

And was looking to us and our proposed regulations as potentially using them as a model. And kind of bouncing some ideas off of us.

So we -- and in honesty, I believe we're ahead of DOE when it comes to safety systems.

MR. SHINN: And Mike Shinn, NRC Contractor again. Just to add to what James said. I think maybe to get to the essence perhaps of the

question that you were asking.

The set of controls that we put together at the -- at one end of the spectrum is that we would apply at a power reactor because of what James said. There are facilities that have significantly lower consequences of concern to a power reactor.

At the other end of the spectrum, there are elements in that program that we would not apply at a power reactor. Because the power reactor's consequences of concern are actually lower then what we would see at those types of fuel cycle facilities.

So there are elements of this program that are more rugged maybe is a good way to put it. Or more robust then what we would have at a power reactor.

And in those cases, if you had a safety system associated with that type of consequence, then it would have those enhanced measures applied to it. And as I mentioned earlier, one of those is no remote access.

So, I think we've got a balance here. You know, with the power reactors we have a homogenous set. You know, it's guidance for

essentially, you know, a tea pot, you know, to boil water.

For the fuel cycle facilities, we have to cover everything from conversion to, you know, naval reactor production facilities and enrichment and everything in between. So, that's why we have those four levels.

And in some cases for some safety systems, they are protected at least as adequately as a power reactor. But more then likely better protected then a power reactor safety system would be.

MR. DEUCHER: And this is Joe Deucher. One thing to add, essentially NRC, DOE and NMSA, we're all playing from the same sheet of music. And that would be the NIST, National Institute of Standards and Technology guidelines.

Your classified systems, the requirements for that are all based on what's called the 853. Which is this set of controls that we're talking about specifically for our rule and our guidance.

We've taken those controls as a model. And effectively modified them, enhanced them to suit what we see as the needs of these various

consequences of concern for the fuel cycle facilities.

DOE just like NRC itself is required to apply the NIST guidelines to its systems and to its facilities including the various labs and its other sites. And how it's working through that, I mean, we've had some glimpses.

Obviously James spoke to this latest conversation. It's an evolving issue in terms of this, what we'll call cyber physical space that didn't exist prior to 2010. It wasn't an issue.

It was really about breaking into computer systems, breaking into information systems, that sort of thing. But again, since 2010, and most recently in 2015 with the attacks in the Ukraine to the power companies, I mean, there's much more emphasis on being able to take cyber technology and be able to jump over the physical systems to damage switches and other devices to stop a production facility.

And again, being that NIST is our, you know, authoritative source for lack of a better term for what to work from, they've jumped ahead. They've got guidance out now for industrial control systems. They're developing guidance for cyber

physical systems.

So again, there's a wealth of information there that we're taking and looking to digest and build into a rule and into the guidance for us that we think is most pertinent for our -- for the fuel cycle facility licensees.

But then on top of it we're saying, by the way, these are also our authoritative sources. Go ahead, take a look, and see if there's anything else that you want above and beyond what we're already offering you.

You can go out there and you can take a look at this. And see if it helps you in other areas of your facility.

But again, just to point out that we're all really working from the same documents. It's the NIST documents. And that goes to like again, just to reiterate, for classified systems as well as unclassified systems. Their controls are based on the same information.

CHAIRMAN BROWN: I found what you were talking about. And I see where I missed that. The enhancement for digital assets or something like that. Thank you.

MR. DEUCHER: You're welcome.

MR. DOWNS: Okay. So slide 14. Here again, we've laid out the performance objectives. Obviously the discussion that we've had, had legs.

And part of that was because these performance objectives are, you know, fairly general. They cover, you know, a large portion of the program.

So, moving on from that, slide 15. Which is Section C.3 of the draft reg guide. Here we talk about the cyber security team. The responsibility of the team. The makeup of the team. The training and qualifications. The various man -- the management structure and the relationship to operations.

Some of the significant changes here, we've -- I fell like we've reduced some of the prescriptiveness that was in there as far as it came to the team.

Especially the qualification. We had some very specific qualifications we felt -- we provided as examples. We've removed those.

We've clarified the intent and roles of -- of roles and responsibilities for the program sponsor or the program manager, a cyber security specialist and the technical staff.

Given some of our discussion back in the November time frame, we've added some information on there as far as software goes. For example, you know, custom software is only considered if it can cause a consequence of concern. Therefore, it would be a vital digital asset potentially.

So that's how we talked about software. And then again, we're also reiterated --

CHAIRMAN BROWN: Custom software, I remember reading a little bit about that. But most of these people, most of these facilities use what I would call commercially available software as opposed to -- I would think if you developed your own software as custom software, that it would be less susceptible to having outside influences with updates and patches and all that other kind of stuff.

I mean, once you buy commercial stuff, you just hook it online. And there's all this stuff that's constantly being downloaded to take care of "security concerns" and their own self prescribed goodness that they can prescribe that will protect your software when it's installed on your computer which is.

MEMBER MARCH-LEUBA: Yes. What Charlie

says. You're putting that on the record. There is also millions of high school students trying to break into that commercial software.

So, your private software, there's nobody.

CHAIRMAN BROWN: The custom software, as far as -- I would think would be far more -- I don't know if that's what you said or not.

But the custom software that you develop yourself for your processes it seems to me would be far less susceptible.

MEMBER MARCH-LEUBA: Unless -- yes.

MR. DOWNS: It depends. Yes. It depends. It depends on the robustness of that software. What the considerations were in its development.

As I recall during our site visits, you know, again some of these facilities are, you know, 60 years old. So, you know, they've got what at the time, it was, you know, they have a custom program to do a certain thing, it may or may not have taken, you know, the attack vectors that are present today into consideration.

So, it's present again. And we saw some, you know, I remember on some of our site

visits we saw very, very, you know, recent modifications that have been made that have very, very up to date, you know, software.

MR. DEUCHER: And again, this is Joe Deucher. Just to add. What we're looking for out of this program is the licensees to then employ the ideas of secure coding, the proper level of testing and development, vulnerability assessment. You know, your configuration management, your updating of the software.

But ensuring that, you know, the product that they're working with, assuming it's a vital digital asset that it's going to be as secure as possible. And a lot of that's in how it's developed and how it's maintained. And that's also included.

And the details of that are included in the individual cyber security controls that are in the appendices of the document. And again, the level of robustness as James has said, depends upon the consequences of concern.

I mean, we're going to be looking for more robustness at a Cat 1 dealing with formula quantities of material of we've got a software program that's being run for that. Potentially

versus say a latent safety system at a Category 3. Just as an example.

MS. MAUPIN: This is Cardelia Maupin. I would just like to mention as well that some of the facilities are voluntarily updating some of their systems. And have, you know, during some of our public meetings, and have mentioned this.

And also, NEI has assisted us in our -- of working with us and what they've done with their, you know, stakeholders. And so there have been some voluntary measures to update cyber programs. Even though our, you know, rule was not in place.

So, I just wanted to put that on the record.

CHAIRMAN BROWN: Okay. Addressing Joe's comments. He's gone though all the great -- the entire umbrella of fantastic teams and updating and everything else. And you'll have a greater staff doing the IT work then you will even running the plant.

And by the time you finish -- that's what it looks like when you look at this.

MR. DOWNS: Well, to be --

CHAIRMAN BROWN: Even your example in

Appendix G, which was pretty simplistic. You know, just two little things and assessing what they were.

And then you start looking at your, you know, how you've got to control all that from the documentation all the way from the -- your cyber security team all the way down through the various response teams and all the other type stuff.

It just seems stack all that stuff together and you've got a huge -- you're starting to impose a huge cost on the fuel cycle facilities.

And I -- where is the balance? This stuff is out -- everybody agrees we need some type of regulatory, you know, rulemaking, I think. Besides, the Commissioners have already said they want one.

So, it's a matter of making it the rule and a reg guide that provides some flexibility and balance. But yet if you allow the -- any part of the world to be expanded into, it can get pretty complex. Pretty intensive and pretty cumbersome and burdensome.

I'll let you go on with your stuff. It's just that it's very comprehensive throughout this entire guide.

MR. DOWNS: I think the very last bullet on this slide speaks directly to what you're talking about. And that's that in our discussions with the various stakeholders, it's been very, very clearly stated to us that some of our facilities may not have a single vital digital asset.

CHAIRMAN BROWN: Nobody has a smart phone?

MR. DOWNS: Not that -- well, remember what a vital digital asset is. Right? A vital digital asset is something that its compromise would cause a consequence of concern.

CHAIRMAN BROWN: No. I understand that. But I mean --

MR. DOWNS: Right. So, -- and if it's a vital digital asset, there is no alternate means to maintain that function that's needed to prevent the consequence of concern.

So therefore to us it's risk significant and has to be protected. What we're saying here is, some of these facilities, they may not have a vital digital asset. So be it.

What we're looking at there is, is that -- and we specifically said it numerous times now in this addition of the draft reg guide, that the

size of the team and the scope of the program is actually scalable to what you've got.

In other words, you may only have one person on a team if you've got no vital digital assets. The scope of that person's duties maybe to, you know, maintain the configuration management aspects of it.

And just because you've got no vital digital assets doesn't mean that you've got no digital assets that are associated with a consequence of concern. Remember that's the next step up, digital assets associated with consequence of concern.

So, the configuration management aspects, you may have credited some alternate means in that situation. So you want to make sure that your configuration management you don't eliminate those alternate means.

You don't add new digital assets that could potentially be vital. You know, it's a matter of the maintenance of the program there.

So we still feel that even if you have no vital digital assets at a facility, a team would still be needed. But it may be a much smaller team then somebody at another facility that, you know,

we've heard could potentially have thousands of vital digital assets.

We would anticipate that that program, yes, it maybe much larger. But again, the cyber security risk associated with a facility that has thousands of vital digital assets, we feel that could potentially be a -- it's more risk significant.

So yes, they may need to spend a little bit more money on that to solve that problem.

MS. MAUPIN: And this is Cardelia Maupin. If I could jump in here.

I think that what I'm hearing from Charles is, are resources being diverted from something that's a matter of safety? And to do the things that we're asking.

We're going to be asking those type of questions under our cumulative effects regulation and questions that we have in the, you know, in our proposed rule package. Is that, as you are well aware, the Commission has taken on this initiative to make sure that we don't have the licensees doing so many things that they neglect issues that are vital to safety.

And I think that I was hearing that as -

-

CHAIRMAN BROWN: That's one aspect of it.

MS. MAUPIN: One aspect of your question.

CHAIRMAN BROWN: And that's a big aspect in many circumstances. You rob Peter to pay Paul. And all of a sudden Peter's not doing very good work anymore.

MR. DEUCHER: And again, this is Joe Deucher. One thing to mention is, in the closed session I think we can address some of these other issues in more detail.

CHAIRMAN BROWN: Okay. All right. Just to put some thoughts out on the table. That's all.

MEMBER KIRCHNER: So, along those lines, I was struck by your last bullet too. The size of team is scalable with the number of vital digital assets.

Let me hypothetically throw out that I've got literally hundreds or more of digital devices controlling a process. How does that scale?

It would seem to me in stepping back it would -- I mean, I know of examples of where we've

imposed over our normal I&C CIO like functions. And it hasn't improved the security.

Don't quote me on that. But, what I'm saying is, you're layering on lots of things. Why is this not integrated into the responsibilities of the I&C team that is already at that particular plant?

And why isn't it an inherent function to define functional requirements for the system?

CHAIRMAN BROWN: Myron?

MEMBER BLEY: Whoever's on the phone, please mute your phone.

CHAIRMAN BROWN: Yes. Please mute your phone. Thank you, Dennis.

MEMBER KIRCHNER: Wouldn't the -- I'm trying to come to this in a different way. Wouldn't the requirements that you want for the purpose of the reg guide, become part of the design criteria for such a system to operate such a facility? And therefore be an integral part of the architecture, et cetera, et cetera?

I'm just struck by this statement here. The size of the team is scalable based on the number of digital assets.

I think somewhere in there I read that

you can aggregate digital assets so that you don't multiply your problems?

MR. DOWNS: That's correct. So, just to kind of speak to what you're talking about. The -- nowhere in the guidance or in the rule does it say that the team had to be dedicated. That's their only job duty.

We've tried to leave the flexibility for the licensee such that they could determine the roles and responsibilities could be taken by, as you pointed out, a current group of IT individuals potentially. But, we just didn't want those responsibilities to blindly be given to those individuals.

Because they may not have cyber security background. They may be great with IT. They may be even great with hardware, but not really understand the concepts of cyber security.

So again, we tried to maintain the flexibility such that, you know, not being dedicated as to maybe a licensee would prefer to have a dedicated team. It's kind of that -- left that up to that discretion.

MR. DEUCHER: Right. And just to add on. This is Joe Deucher. We've modeled this

process similar to what happens with a NIST accreditation. That a federal agency or an IT system historically would go through.

Where you've got your IT system built. And that design criteria certainly, as much as possible, security gets included into the design criteria.

But then coming forward after that system is built, you would look at its risk profile. In this case, it would be associated with a consequence of concern.

So if, you know, taking an example, let's say it's associated, we're at a Category 1 facility. You know, it's a process line that's processing formula quantities of material. So, we know that it's associated with a DVT consequence of concern.

So we know already the controls or the performance specifications for whatever we do to protect it, we've got that. And we've got that to work from.

So essentially what would happen is, this digital asset's been identified. We've identified that there is no way other to protect it. Or that it is important enough that if it's

compromised, something bad would happen.

So we're now to the point where we've got this list of controls. We've got this system that we're trying to protect. We look down the list of controls and we come up with various things to protect it.

And again, a lot of this is going to be built into the system. Whether it's a log in. It could be audit controls that are already there. By audit controls, meaning that any time somebody turns it on or touches it or makes a change, it's recorded.

So again, when you look at the controls, they're very -- they are detailed. But really what they're talking about is a lot of existing features and capabilities that are out there in a digital device.

And all that the team would do is just basically go down the list and identify what is going to meet this requirement. What is going to meet this specification.

And then they go back and they confirm it. And then once it's confirmed, you're basically good to go. You come up with a list of, if there's anything new that I need to do with it, any what

we'd call in the reg guide, measures.

Maybe I need to add a firewall. Maybe I need to add a data diode. Maybe there's a particular device that needs to be included. All that gets recorded.

And now I'm using the system. As far as I am concerned, I have protected it to the level that I can. And then going forward, I keep an eye on it.

I'm going the updates that I need to do. If any changes with that system are associated, I would do that. So again, I'm maintaining the protection of that vital digital asset.

So, it's modeled on again, similar to how things are done in the federal IT space with accreditation. That it's an ongoing life cycle process.

MEMBER KIRCHNER: Thank you.

MR. DEUCHER: Sure.

CHAIRMAN BROWN: You talked about the computer security team, or cyber security team can have other functions. However, you state in here that whatever other functions they have can't interfere with their cyber security duties.

In other words, those are primary.

Which means, you know, I guess what type of responsibilities do we have in any, I'll call them profit-making, manufacturing facility where you maybe doing something else.

And that's one other thing they all say you can stop it and something else loses control while you're off dealing with it, you know, for three or four days tracking down a cyber attack of some kind. And finding all the individuals that anybody had talked to. And writing reports. And stuff like that.

I mean, that seems to be kind of not very easily accomplished within the confines of an organization that's trying to run a plant or what have you. Just say, hey yes, fine. Drop whatever you're doing. You have to go do this.

And whatever you're doing just falls by the wayside for the next week and a half or week, or days, or whatever it happens to be. That's a little bit inconsis -- I'm just saying, there's a little inconsistency in your comment about they can have other duties.

Because as soon as you -- they get ancillary duties to what their previous primary duties was, but this is going to take precedence,

that would seem to be a problem.

But you've almost said you've got to -- to me, the way I read this, you almost have to have people dedicated to a cyber security team.

MR. DOWNS: The other way of looking at this too, is that some of our facilities have cyber security expertise at the corporate level that they feel that they can credit for the -- as actually being onsite.

And obviously it depends on the actual make up of the facility, the infrastructure, the networks, right on down the line. The different -- the different vital digital assets that this role would get to as to whether or not that would be feasible or not.

But, you know, if you had a corporate support position that only visited the site once a year, that may not be exactly who you want on your, you know, fulfilling some of these roles on your cyber security team. They may not -- in that one time a year visit, they may not be able to fulfill those roles.

So, it's like I said, we were trying to, when you write the guidance document, we're trying to incorporate both sides of the spectrum there.

It would be very unusual for a facility operator, a line operator, to have that cyber security expertise that, you know, you kind of want them to have.

So, we're trying to -- again, it's possible. But, we are trying to say that as far as the cyber security team requirement that is clearly specified in the regulations, in the proposed regulations, we're not saying that it has to be dedicated.

But we're also trying to put a level of importance to it such that it's not overlooked.

MEMBER KIRCHNER: Well, philosophically would -- I guess what I'm trying to get to, I know recognizing where we are, you have preexisting facilities. And you have newly identified threats.

So in a sense not to use this word incorrectly, but it's like a back fit. We have to address in these facilities --

MR. DOWNS: That's correct. Yes. A back fit is actually a good word. They are new regulations.

MEMBER KIRCHNER: New regulations and existing facilities. So you have to kind of ensure that these facilities can be operated safely. And

not compromise classified information and such.

But what I'm struggling with is in rulemaking space, the idea of defining basic functional requirements or expectations for these facilities. And then allowing the actual operator, owner, licensee to adapt the plant accordingly.

And superimposing cyber security teams on top of them, that's like trying to put quality on after the fact. And somehow in this day and age, it seems to me if, and I'm not a digital I&C engineer, but that would be an inherent responsibility for that staff at such a plant.

To know that threat and to be, you know, up to date. And it's just part -- you know, times change. And your job responsibilities grow accordingly.

So, what I'm getting at is does this reg guide and rulemaking get to the principals that you're trying to achieve? Or is it just going to put an administration -- administrative overlay to back fit the existing plant?

Say I was going to build a new facility from scratch. Wouldn't you want this level of protection built in? Knowing that it continues to evolve.

But that's, you know, there's probably no field that evolves quicker then I&C these days. So, you see what I'm trying to get at?

You know, what are the basic principals that you want to achieve or requirements and criteria? Rather then kind of an administrative overlay and putting it, you know, putting it -- overlaying it on the existing facilities.

And maybe that's too philosophical at this point.

MEMBER CHU: Can I add some ans -- actually it's related to Walt's. You know, this whole area, I worry the technology's advancing so fast. Okay?

And anybody with a malicious intent, okay, they really want to do what they can, come with the highest technology and so on and so forth. So, I'm fearful like how do you prevent cyber security?

This is kind of related to Walt's thing. You need people who really progressing with the technology. And then this proactive way of thinking, it's not just complying with certain, you know, rules, administrative rules.

And then how do these site people, or

even corporate people, get trained and keep up? You know, because if you don't know what's possible, you don't know how to prevent something from happening.

And so that's one of my worries. How do you as a regulator, encourage that advancement of knowledge at those critical sites? Because I don't know what the answer is.

But there maybe some creative way, you know, to put it into the regulations. Because that's a key part I think for this to be successful.

MR. DOWNS: As you both kind of pointed out, there is -- there's an existing fleet of fuel cycle facilities today. And we're well aware, we saw the slides, you know, the numbers that we're looking at.

It's not a huge number of facilities. Those facilities have been in existence for quite some time. So, the approach that the -- of this rulemaking is to provide basically a bunker, a cyber security bunker of the existing configurations that are present at each of these facilities today.

And the staff, we feel that that

approach is -- would be the least amount of burden on our facilities. To come out and say hey, you really need to -- you need to redesign your systems and back this in, would be extremely costly and overly burdensome is the way that we've approached this.

We also -- getting to Margaret's point about the progression of the threat. The way that we've written this proposed regulation, it is truly a performance-based regulation.

There are life cycle considerations that are baked into this rule when you get down into the review of the cyber security program. And there is no real stagnant part of this rule.

It's not -- we're not putting out a specific list of controls that if you do A, B and C, you'll be okay. We haven't said that.

What we've said, we've established cyber security program performance objectives. And those objectives are, they were considered such that in the evolution of the cyber security threat, the basic principals of addressing that threat would remain the same within those performance objectives that are specified.

So, -- and again, in the review of the

cyber security program, towards the end of the proposed rule, we've got a, you know, that the review includes an audit of the effectiveness and adequacy of the cyber security program. And that's at a specified interval.

It will be yearly for, you know, the Category 1 facilities. And tri-annually for the other facilities. And we feel like that if it's a tri-annual review, that there -- changes in the threat could be captured at that point. And we maintain that level of safety that was intended by the rule.

It no doubt is a challenge though. It is something that it is a, you know, cyber is a constantly moving target. It's constantly -- the threats are evolving, I guess is the right word to say.

MR. DEUCHER: And to add onto what James said. This is Joe Deucher with NMSS. And to Margaret's point specifically about training.

We've got essentially you would argue three levels of training requirements baked into the rule -- into the overall rule and into their overall program.

In the rule itself, we're asking for

their teams to be equipped and trained. And that would be an ongoing -- again, that's tied directly to the program objectives for them to be able to effectively protect -- protect and respond to cyber attacks associated with the consequence of concern.

In more detail, there would be additional training requirements for the actual vital digital assets that they find. So if there are vital digital assets that they have associated with one or more of these consequences of concern, whether it's a DVT or a safety, there are levels of training that would be required for, based upon the controls, again in the detail of the controls, for the operators of those systems, for the administrators of those systems, the maintenance personnel, as well as the cyber security people.

So, we're talking about subject matter training that would go along with it. And that would exist for the life of the vital digital asset. No different then any federal IT system that exists.

Within the NRC you've got subject matter training, you know, for your security people as well as the general operators and administrators of those systems. It follows the same logic.

And again, it doesn't really matter what the threat is. It's the fact that they have to do this on an ongoing basis.

And we tried to capture it so that at a bare minimum, even if it's one team member that they have, that team member is staying on top of this.

And through the program review, through ultimately the inspection protocol, the interim staff guidance, and these other activities that will follow on, assuming that the rule, you know, goes all the way through to final, there would be this process in place to evaluate, you know, the training level for this individual, or these individuals.

To ensure that they're doing what they need to do to keep themselves abreast of what's going on in the threat environment to be able to respond accordingly. And also to know their systems, their vital digital assets and their components, so.

MR. DOWNS: Yes. Similar to what Joe was talking on. Here is actually a capture on our next slide, slide 16.

CHAIRMAN BROWN: Yes. Let's go ahead

and -- we're going to have to move along. Because it's about a half an hour to go. We can move on.

MR. DOWNS: Yes.

CHAIRMAN BROWN: We took 30 minutes for 15 slides.

MR. DOWNS: Slide 16 -- no, some of these chapters there were no changes to. So, they'll kind of go through pretty quickly here.

So, cyber security plan. Some of the things we're talking about here that the -- the fourth bullet point down describes the measures for the management and performance of the program.

That's a life cycle type concept there. So, this is, you know, it is in the plan. Significant changes to this section since November, shifted some stuff around and pertaining to the discussion of the cyber security plan.

And we also clarified the guidance on cyber security incident response. There was some confusion here as to, is cyber security incident response part of emergency planning? Is it -- how does it all factor in?

Basically what we've -- we've kind of drawn the line, if it's prior to a consequence of concern occurring, you've got -- it's considered

cyber security incident response.

Afterwards, the emergency plan for that facility after a consequence of concern, that's covered in the emergency plan. So, there's a relationship between the two. And the guidance gets into that section a little bit.

Moving onto slide 17. Here in Section C.5 of the guidance document, we discuss the consequences of concern in greater detail. We provide the -- where each of the consequences was informed from given the current regulations for fuel cycle facilities.

The significant change here is, we added some additional discussion on what's considered an active consequence of concern and what's considered a latent consequence of concern.

Again, active is a direct result for the cyber attack. A latent is something that requires a secondary event after a compromise of the function by a cyber attack.

Slide 18. This is Section C.6 of the guidance document. In this section we go through the methodology for identifying digital assets and determining vital digital assets.

Again, we've talked about some of the

significant changes here. We tried to elaborate on software a little bit more.

One of the take aways from the November briefing was a discussion of the feasibility and reliability of credible alternate means. And so we took some of that from -- there's a reactor NUREG on -- for fire protection that actually deals with feasibility and reliability of manual actions.

So, we took some of the features, enhancements from that.

MEMBER STETKAR: You took some of them. But you still don't even refer to those NUREGS to give a licensee a pointer. I checked.

MR. DOWNS: It seemed -- you're absolutely right. It would be difficult for a licensee that's focused on cyber security to think about in relations -- we tried to translate it the best we could.

That was our goal there. You know, we talked about environmental factors, notification equipment, indication confirmation procedures, adequate staffing, demonstration of the action.

What we did there was, we really took the -- what we thought were the germane equivalent concepts and translated them over. But if it

missed the point or missed the target, let us know.

One other thing of significant change, we also clarified some of the consideration of support systems. Again with a support system, you're really focusing on resources that are necessary for the VDA to function properly.

A licensee would consider the level of dependence between a VDA and support system to determine if a compromise of the support system could provide an input to a vital digital asset that would cause a consequence of concern, directly cause a consequence of concern, or preclude the VDA from performing the function needed to prevent the consequence of concern.

And again, everything ties back to the consequences of concern. And then again, as we previously discussed, we provided some additional guidance here on firewalls, air gaps and data diodes and their considerations.

Any questions on -- comments on identification of assets? It's a fairly long section. And I just thought that.

CHAIRMAN BROWN: The only suggestion I guess I would have made, you made the comment in

the Section 6 in terms of identifying on air gaps and data diodes, et cetera. That their use did not address all threats.

It was kind of a negative connotation. Yes, you can use them. But they do not address all threat vectors.

And I don't think in any of our previous deliberations or our comments in the previous meeting even, would have commented or thought that yes, you can walk away with a data diode or an air gap. There's obviously insider threats.

But instead of -- to me, I would have written that paragraph as a positive that utilization of air gaps or one way data diodes for those areas where external access or control of access from an external means is critical. That it provides a vital reduction in, you know, a focus of what threats you have to address.

And so you're fundamentally limited now down to the stuff that occurs in an insider threat or inside the plant. Or a communication from one system to another. Or somebody in there with a cell phone that can communicate, you know, that can change a setting or something like that.

It's an insider circuit. And so it's a,

I think, a positive, I don't want to call it spin, because it's not spin. But a positive statement relative to the utilization of air gaps.

That wasn't even in there when we were talking back in November. You all added that. Which I thought was a very good addition.

But the only thing I was concerned about was the lack of identifying how it really did reduce in many ways the efforts that would be taken and needed by the facility or the operation in order to protect themselves. Not everything, but it is a step in the right direction.

So, while you can't mandate it, I -- well, of course if it were me, I would -- it would be in the rule. And I would mandate it for wireless.

And the same thing for wireless. To say look, utilization of wireless increases, you know, your vulnerabilities and the difficulty of protection.

You hear it all the time right now with people with their wireless thing running around. I know -- people I've known have been sitting in at one of these little internet cafes and all of a sudden, they're hacked.

So, or somebody's gotten their information. But I mean, it's that type of the way to address those aspects that say yes, we can't -- you don't have to say we can't prohibit it.

But you say hey, not using them certainly reduces the effort and the cumbersomeness of what you have to do within the facility.

MR. DOWNS: Yes. I appreciate that comment. The staff will take it back and basically what I'm hearing is that we want to tell what good they do.

CHAIRMAN BROWN: Yes.

MR. DOWNS: Rather then focusing on what they don't do.

CHAIRMAN BROWN: That's right. And that the only thing you --

MEMBER BLEY: Or the positives to make. Positives.

CHAIRMAN BROWN: Yes. And you're only left with now focusing on. Insider threats are in many circumstances a lot easier to deal with then external stuff when you don't know the characteristic of what's going to be coming in from an external source.

MR. DOWNS: Right.

CHAIRMAN BROWN: You don't know either on the insider, but it's a lot more constrained in terms of the people, how you can monitor it, how you can control it, what they can bring into the plant. Access to certain facilities or certain types of equipment can be controlled much more easily.

MR. DOWNS: Yes. And the staff will definitely take that back. And as a comment, we appreciate that feedback.

CHAIRMAN BROWN: Okay.

MR. DOWNS: Yes, this -- we're just a little bit of a mind set where the staff was coming from with that. With discussion with some of the stakeholders, we've heard numerous times that I've got a firewall. I don't need to worry about your controls.

And that's -- so that's where the staff is coming from.

CHAIRMAN BROWN: And a data diode is not a firewall.

MR. DOWNS: It's very different. That's right. And I just want to, you know, -- so that's where were constantly coming from that position.

And so I appreciate what you're saying

though.

CHAIRMAN BROWN: But if you put the other side -- I'm just saying, once you put the other approach to saying it, the positive aspect to it, --

MR. DOWNS: Right.

CHAIRMAN BROWN: They can argue firewalls all they want. You can't stop it.

MR. DOWNS: That's right.

CHAIRMAN BROWN: But, you can certainly send a message that we're going to make it -- it's going to be a lot easier on you.

MR. DOWNS: Yes. Again, I appreciate the comment and we'll definitely take that back.

MEMBER BLEY: James, I've got something. I haven't known where to ask this. So, I'm going to do it now.

MR. DOWNS: Now's a good time.

MEMBER BLEY: I'm going to do it now. I missed the November meeting. I'm sorry for that. It would have been nicer to have brought it up then.

What I'm going to ask is kind of tied to something Dana brought up a long time ago in another context. Was, across the NRC, we deal with

nuclear reactors, we deal with fuel cycle facilities, we deal with all kind of facilities.

And shouldn't the requirements we put on licensees be proportional in some way to the potential consequences, the likelihood and potential consequences that come from such facilities?

NEI had talked at least in the documents they sent around the last time about some kind of risk informed graded approach. And I -- this is a question.

It seems to me that I can imagine a very large burden for screening digital assets at a facility. Starting at kind of the bottom up.

What are all of these assets? And the approach that starts there, if we have a facility with fairly hazard, given something happens, we're not going to hurt very many people.

Would it make sense, and Category 2 or Category 3 facilities maybe fit that. I know you don't have any Category 2s now. But you might one day.

Wouldn't it make sense to work backwards? You know, start with the materials that are there. Lay out scenarios of release. And see

what the likelihood -- well, you don't know the likelihood yet, but see what the consequences could be.

And for the cases with lower consequence, at least maybe an approach that way is easier. And that you find what could happen that could be bad. And then look for the digital assets that could enable such scenarios.

We might spend a tremendous amount of effort identifying all sorts of digital assets in a facility for which there's almost no scenario that no matter how you enable that scenario that it leads to substantial consequences.

And it just seems we might be burdening people in such facilities a lot for no potential gain.

MR. DOWNS: So, when you speak to those -- the consequences, our licensees have already done that work. They've already done that safe -- as part of their integrated safety analysis or process hazard analysis.

MEMBER BLEY: Yes. So they know what those are.

MR. DOWNS: They already know what they are.

MEMBER BLEY: So --

MR. DOWNS: So, it's a matter of building upon that. We're not asking them to go back and redo that.

MEMBER BLEY: But if you're saying now, go out and find all the digital assets. And now look and see what could happen with those, it means they've got to do an awful lot of work on these digital assets.

If none of those things they already found lead to substantial consequences, maybe it's not --

MR. DOWN: But why would you not reference that safety analysis and say that we've already done this. And we've got --

MEMBER BLEY: And that's satisfied then?

MR. DOWNS: Yes. Absolutely.

MEMBER BLEY: Okay. So they don't need to go look for digital assets if they don't need --

MEMBER STETKAR: Just to be clear.

MEMBER BLEY: Nothing's going to get enabled by those digital assets that appeared on that.

MEMBER STETKAR: Your claim is that the ISA is already -- if the ISAs have identified in

IROF, Item Relied on for Safety, IROFS, they will have a digital star if you will, by the IROFS that are digital. Is that correct?

MEMBER BLEY: No.

MEMBER STETKAR: They don't --

MEMBER BLEY: I'm sorry. That wasn't for me to answer.

MR. DOWNS: So that's part of some of our facilities do. Some of our facilities don't. And that's where we need to, if you've already done that, if you know that a specific process line can cause a certain consequence of concern, you would have to look at that process line and the associated accident sequences -- access sequences thereof to determine, do I have digital assets on that process line that could cause a consequence of concern.

MEMBER BLEY: If they haven't done that last part yet. But if there's only that one -- let's for simplicity, there's only one scenario associated with one line that they found could lead to substantial consequences, then the only digital assets they have to look for are ones that could affect that line.

MR. DOWNS: Exactly right.

MEMBER BLEY: Okay. When I read it, I didn't get it that way. I got they had to go find them all and then figure out what to do about them.

MR. DOWNS: And that's why we tried to associate it with a digital asset. What your starting point is a digital asset that's associated with a consequence of concern. That's the starting point.

And then from there you look and determine if, okay, do I have an alternate means that would prevent --

MEMBER BLEY: I'm sorry. Yes, that's what I understood. Now, a consequence of concern is just defined by the facility?

MR. DOWNS: No. The consequences of concern are very specific in the regulations. And they align with the safety regulations and the security regulations that are already in existence.

So that's where in Section --

MEMBER BLEY: When I read the words that define consequences of concern, it's if I have a class one -- a facility with Category 1 materials, then I'm in the --

MEMBER STETKAR: It's design basis threat materials.

MR. DOWNS: Well, okay. So at a Cat 1 facility, a good place to look here would be page 25 of the draft reg guide.

What you would be looking at here is that -- so each of our facility types, we've got the consequences of concern there that would be considered by that facility type.

So, you're speaking specifically to Category 1 fuel cycle facilities that's in your letter D there on page 25.

MEMBER BLEY: Uh-huh. I'm not there yet. But go ahead.

MR. DOWNS: So, a Category 1 facility would be considering the latent design basis threat. It would also consider the active safety and the active safety and security consequences of concern. There would be three of them.

MEMBER BLEY: But safety -- those things aren't associated -- depending on how much of what kind of material, where the processes lie inside the plant, that stuff might not be able to get out and hurt anybody.

Those are the -- they're more like potential consequences then actual consequences of scenarios.

MR. DEUCHER: Except for the fact that -- again, this is Joe Deucher. And, correct me if I'm wrong. With regard to the -- with regard to the fuel cycle regulations, worker exposure is a part of this as well.

So, that has been taken into account in terms of the consequences.

MEMBER BLEY: That's okay, too. But, that definition you just read doesn't -- isn't tied to what's in the ISA. It's tied to just the stuff inside this facility.

MR. DEUCHER: Okay. So, --

MEMBER BLEY: And not how much of it. Well, Category 1, 2 and 3 have to do with how much. You could use your Appendix G as an example.

CHAIRMAN BROWN: That was a process example. Process one and process two. He's talking about the processes.

If you look at the ISA, there's a process for making stuff. One, two, three, number of stages that they can --- okay, four stages.

Stage three now involves processes where if it goes out of wack, you get disruption, corruption, spread of contamination, whatever it is, consequence of concern. And it's got a digital

asset.

Stage one, two and four and five don't have that. In other words, the ISA -- I don't have a failure more that can result in any problems.

So you only have to look at stage three. And that's where I've got a digital asset. That's the one I have to focus on. Is it vital or not? Do I have an alternate means or not? Whereas one and two don't.

He's -- I think he's looking at more of I'm making stuff. The ISA is identified in accident sequence with my process. Where in that sequence can that accident occur? And what equipment or non-equipment, or manual operations, are associated with that?

MEMBER BLEY: Can enable that scenario.

CHAIRMAN BROWN: Can enable that consequence. Okay. Now, it maybe a safety. It maybe a safety and security. It maybe a design basis threat. It can be any one of those.

But it's associated with the ISA. And you talked about the ISAs that they would be -- I think it's in this thing somewhere.

But yet you don't put any emphasis on -- in his example, of trying to focus or narrow the

line of stuff that has to be dealt with.

MR. DEUCHER: Well, and again, to answer this as best I can. This is Joe Deucher with NMSS. We feel that we've narrowed it with regard to the consequences of concern that we've specifically listed.

And the ISA would just be one source of information to go to. It would also be the security plan if you're --

MEMBER BLEY: But -- okay. Just let me try something.

CHAIRMAN BROWN: Go ahead, Dennis. Here.

MEMBER BLEY: If I look at just what I think are the definitions. Where you have latent, you have four consequences of concern.

You have a latent consequence of concern design basis threat. And --

MR. DOWNS: All that information would be -- for latent design basis threat, --

MEMBER BLEY: Yes.

MR. DOWNS: It would be taken out of the security plan or the material control accounting log.

MEMBER BLEY: But that just essentially

means there's enough stuff there if I stole it and took it out of the plant I could make a bomb out of it.

MR. DOWNS: That's right. That's the intent. Is to protect the functions that safeguard that sort of material.

MEMBER BLEY: And therefore, if there's a scenario by which I could have a theft and move this stuff out, that's a scenario I want to know about. But that's a very high consequence event if it plays all the way through.

But when we get down to the lower ones, latent consequence could -- it concerns safeguards that's again, primarily a threat for theft to get it out and --

MR. DOWNS: Specifically, that would be a -- it's physically at a Category 2 facility.

MEMBER BLEY: Yes. Yes.

MR. DOWNS: If it were that. That would -- is applicable.

MR. BLEY: That's right. In Category 1 you've got more stuff then that. So you could take more.

MR. DOWNS: At Category 1 you're only dealing with the design basis there. Right.

MR. BLEY: Yes. But you could do -- I guess you could do a dirty bomb or something or some disbursal device if you stole that.

Now we get down to safety. Now we're down at the point, you know, those first two, the consequence of concern is it's really a big issue. It's a bomb of some sort or some harmful device that they could build if they stole the stuff.

When we get down to the category of concern three on safety, there it seems to me we have to go to the ISA and say, what are the scenarios that could lead to a problem with this material? Could it be released somehow? Could it do harm to people? Could it do harm to workers?

And that's the place I'm saying there if we look at the individual scenarios that could lead to trouble, then we need to look at if it leads to enough trouble to be worth it, then we look at the digital assets.

If it leads to a release that's pretty small, we probably shouldn't spend a lot of money seeing what the digital assets are. Because if this thing actually happens, it's not a big deal.

MR. SHINN: So, Mike Shinn here, if I -- I hear what you're saying. And I'm pretty sure --

well, it was our intent that the guidance said what you just said.

MEMBER BLEY: Okay. That's great.

MR. SHINN: Yes.

MEMBER BLEY: I didn't get it.

MR. SHINN: So, I think the take away is to make that clear. Because --

MEMBER BLEY: And the same thing applies to latent consequence category four. When it's a consequence of category four for latent --

MR. SHINN: Oh, type four. Right.

MEMBER BLEY: Yes, type four.

MR. SHINN: Right.

MEMBER BLEY: Type three and four is where I -- they're tied to the ISA and limit the number of places you have to look.

If that's the intent, I think it's great. And I just didn't -- it just didn't come across to me.

MR. SHINN: That is the intent.

MEMBER BLEY: I don't know if it came across to you.

MEMBER STETKAR: No. My problem is, I read the guidance with a mind set that I had an ISA and I was going to use those, for lack of a better

term, sequences.

MEMBER BLEY: Okay. Groups of stuff.

MEMBER STETKAR: Yes. To guide where I look for digital assets. In other words, can a digital asset affect -- directly cause one of those? Or can a latent effect a digital asset compromise?

MEMBER BLEY: If I had that mind set I might be happier.

MEMBER STETKAR: If I had that in mind. But I viewed it with that mind set. And I thought the guidance was okay.

MEMBER BLEY: Okay.

MEMBER STETKAR: I just read it --

MEMBER BLEY: But I read it and what I got was you got to go find them all. And then see if they're important.

MEMBER STETKAR: Yes. See, I didn't read it that way is the problem. I didn't either. But I don't know how anybody else out there has been reading it.

MEMBER BLEY: Yes. So did Charlie. In any case, that's what many of us thought we saw.

MR. SHINN: I heard that loud and clear. And it's a good comment that that should be a

little clearer. But that is precisely the methodology.

Is you start with the sequences. You look at some alternative needs.

CHAIRMAN BROWN: Okay. Look at the ISA sequences?

MR. SHINN: Well, when I say sequences, I'm sort of painting with a broader brush.

CHAIRMAN BROWN: Yes.

MR. SHINN: Because it could be a security plan.

CHAIRMAN BROWN: Wherever you get it.

MR. SHINN: Wherever you get it from. And you look at your --

CHAIRMAN BROWN: And theft isn't going to be in the ISA. That's coming from somewhere at least --

MR. DOWNS: On page 26 of the guidance is exactly -- is where we laid out what informs the identification process.

MEMBER STETKAR: Yes. But it depends on how you read it. If you read it from my perspective, the first thing says, integrated safety analysis or process hazard analysis, or both.

So I read it as primary. And I go back to Appendix G and the first step is, go look at your ISA and IROFS and all that kind of stuff.

But, -- I could see how you could read it differently.

MEMBER BLEY: But, I got the impression folks the NEI folks read it the way I've read it.

MEMBER STETKAR: That could be. That could be.

CHAIRMAN BROWN: I read step one where it said, digital assets associated with the consequence of a concern. And my first thought was, okay. I've got a process.

Start with material and there was something else. That entire process could result in a consequence of concern. Therefore, everything associated with that it could be 30 or 40 items along in the process chain.

And -- but, you know, and I didn't even start thinking that --

MEMBER STETKAR: But the equivalent in a nuclear power plant is a consequence of concern is core damage. Now, you say well, I don't want to have core damage.

CHAIRMAN BROWN: Well but John, let me

finish here. You know, the possibility of core damage.

MEMBER STETKAR: It's a possibility.

CHAIRMAN BROWN: I got enough stuff that can't --

MEMBER STETKAR: But you go out and you look at every single valve in the plant. And then say, but can it cause core damage?

So first you have to do that whole inventory. That's the way you read it.

MEMBER BLEY: Yes.

CHAIRMAN BROWN: That's the way I read this thing.

MR. DOWNS: I'm sorry.

CHAIRMAN BROWN: No. I read it the same way he did.

MEMBER STETKAR: I'm sorry, you said you read it the way I did.

CHAIRMAN BROWN: I read it as if you had to go look at every phone.

MEMBER STETKAR: Oh, okay.

MEMBER BLEY: Me and Charlie.

CHAIRMAN BROWN: And -- but yet -- and that's why -- that's why I started picking on the Section 6, the data diode and the other stuff.

Because that was a way to reduce the vulnerability of external access into a plant that could cause some consequence.

MEMBER STETKAR: But that's a generic sort of thing.

CHAIRMAN BROWN: That's a generic overview. But then when I said the -- I didn't glom onto the ISA as a way to reduce -- make a further cut into a process.

And you can have a process lined where five of the six or seven steps, they can go wrong, but nothing happens. Perhaps steps five and six out of seven could cause a severe problem. That's where you focus.

You don't want to say wow, the whole process. And I've got 27. But now I can focus it down to four. That's all I'm trying to get to out of Dennis' comment.

That there's another vehicle for reducing the scope of what people have to look at. And it's a positive way of looking at it relative to the integrated safety analysis that they already have to do when they identify items required, you know, for safety. Okay?

MEMBER BLEY: I'm really glad to hear

your intent. So, I'll leave it at that.

CHAIRMAN BROWN: Well, the intent is there. But if it doesn't come across that way to people.

That's why if you write it in a different manner where you explain that there are various means to approach this, you know to reduce the category or the number of things you have to look at, that just makes it easier for the industry to deal with. That's all.

MR. DOWNS: So, I think just to point out here, you've got four consequences of concern. Three of them are latent.

Meaning that you've got your cyber attack that compromises something. Then you need a secondary event to come and actually cause the consequence of concern.

CHAIRMAN BROWN: Yes. Right.

MR. DOWNS: That secondary event, that's where that's going to -- it should already be looked at if it's a safety event, if it's a security event.

CHAIRMAN BROWN: Should be.

MR. DOWNS: And that's -- so where is that information going to be? That's where it's

going to be.

The only one that's a little different is that active safety piece.

CHAIRMAN BROWN: Well, I would disagree with you. Because I think you can look for parts of a line where something could get buried and then it pops out later.

You can do it the same way if you don't have as part of an overall process. So whether it's active or latent, you keep focusing back on this giant bubble of consequences of concern.

Which sets the spectrum over which you have to evaluate your processes with that question. But yet pieces of the processes underneath those consequences of concern don't have to be covered blanket-wise if you look at them relative to your analysis in terms of addressing how you protect that overall process line.

MR. DOWNS: Yes. I'm hearing what you're saying. I appreciate the comment. And we'll definitely take it back and try to rework it so that we are focused on, you know, where are those potential secondary events are already captured in existing information.

Again, just to finish what I was saying

with --

CHAIRMAN BROWN: Do you want me to write it for you? I'm just teasing.

MR. DOWNS: Just to finish what I was saying with the active safety, it should -- it must be noted that the current integrated safety analysis present at our facilities do not consider a malicious actor.

So, the reason that matters --

CHAIRMAN BROWN: Who -- that doesn't matter.

MR. DOWNS: It does matter. Because you can have a situation where you've got say a crane. And a crane is lifting, you know, something. What's the failure mechanisms in that crane?

The failure mechanisms in that crane could potentially be structural. It could be mechanical. It may not -- those ISAs didn't consider a malicious digital actor.

CHAIRMAN BROWN: But the failure itself is a source of a potential thing where it smashes down and blows stuff, you know, it smears it all over the place. I don't have to worry about whether it's malicious or not.

Whether it breaks because it wants to

break, or it breaks because some guy falls asleep at the switch, or he decides to do something and flip it just so he can take a vacation next week.

MR. BARTLETT: So, this is Matt Bartlett, NMSS. So, the malicious piece matters because in your example you said, there's one through three and five and six that don't have any identified consequence in the ISA. That's true.

And so, you would tend to rule them out. What we're saying is, there maybe a malicious accident or a malicious attack that's not identified in the ISA that may impact one or two. And therefore it needs to be considered.

And there's a specific regulation --

CHAIRMAN BROWN: When you look at that process, you look at some place where somebody could surreptitiously compromise the process. That's different then a remote access.

It's different then even a failure of the process. You know, it depends on -- I mean, how do you look at it all the way along the line?

MR. BARTLETT: I guess what we're saying is, it's broader then the things identified in the ISA. There maybe other things there that you need to consider.

MEMBER BLEY: And James talked about some of those earlier.

MR. DOWNS: I don't think that changes our take away from what you're saying. Right.

CHAIRMAN BROWN: Well, I'm looking to see. We're only about a while behind. So, it's 3:00 -- I think we're -- where's my schedule?

Well, we've got to finish. We'll go ahead and take a break now at 3:00. And we'll come back in 10 minutes, not 15 by that clock. I'll use Dick Skillman's approach to doing business.

And we'll finish up the open session. Okay? How much -- we've got 12 slides left. So, we'll go maybe an hour.

No. We'll take a break right now.

MR. DOWNS: It's whatever you all want it to be.

(Laughter)

CHAIRMAN BROWN: That's it. Then we're -- I mean, we're -- I mean, we've hit a lot of the stuff that we wanted to talk about anyway.

So, I'm going to recess now. And we'll be back at ten after 3:00.

(Whereupon, the above-entitled matter went off the record at 2:59 p.m. and

resumed at 3:13 p.m.)

CHAIRMAN BROWN: Okay. The meeting is back in order. You can start again.

James, have at it.

MR. DOWNS: Thank you, sir. So we're going to start off on slide 19. Slide 19 is Section C.7 of the Draft Regulatory Guide. This section discusses the -- at a high level the cyber security controls, kind of what a control is, how you address it, and how to consider the various measures. There was no significant changes to this section. The concepts all were the same as presented back in November. So if there are any questions on controls from a general standpoint, we can talk about those now.

CHAIRMAN BROWN: I'm -- did you have a comment? Oh, I had just -- I might have had a -- this is not a technical comment, I don't think. In 7.1 -- where is this? Oh, the first paragraph, second sentence says, "The controls are subject to NRC review for acceptance in accordance with 10 CFR 73.53(d)(2). And I think it should be (e)(2). Just don't ask me how I found that. I was looking for something and it just popped out. It's the rule. Did you see it?

MR. DOWNS: I see what you're saying, yes. Yes.

CHAIRMAN BROWN: You agree or disagree?

MR. DOWNS: It's actually both, but, yes, I think --

CHAIRMAN BROWN: I don't agree. I read (d)(2) and it's so vague that you can't tell what's going on.

MR. DOWNS: So (d)(2), "Establish and maintain cyber security controls that provide performance specifications to detect" --

(Simultaneous speaking.)

CHAIRMAN BROWN: No, 75.53(d)(2) -- did I lose a (d) here? (a), (b), (c), Consequences of Concern. (d), Latent -- where's (d)? (a), (b), (c). This thing is so complicated. (b), (c).

MR. DOWNS: So paragraph --

CHAIRMAN BROWN: (b), (c).

MR. DOWNS: -- (d) of the proposed rule is the Cyber Security Program. And (d)(2) is specific --

CHAIRMAN BROWN: Is the Cyber Security Program, right?

MR. DOWNS: (d) -- correct, (d) is --

CHAIRMAN BROWN: And it says establish

and maintain. And this says are subject to NRC review. Doesn't say anything about review in accordance with

-- (d)(2) doesn't say anything about review, but (e)(2) does. (e)(2) says, "Policies implementing need not be submitted for Commission review and approval, but must be documented and available for inspection by the staff."

MR. DOWNS: I appreciate what you're saying. We'll take it back and look at it. Again, the review here is for acceptance in accordance with

-- is what the -- part of the Draft Reg Guide says, so --

CHAIRMAN BROWN: Says, "Are subject to review for acceptance."

MR. DOWNS: Right, so the --

CHAIRMAN BROWN: But then, and it's also inconsistent.

MR. DOWNS: We'll have to -- yes, we'll have to --

CHAIRMAN BROWN: One says you don't need to do it and the other says you do. The Cyber Security Plan was the only thing I saw in the rule that required NRC approval. Everything else was

nobody has to look at it until we -- unless we want to audit it.

MR. DEUCHER: Right. Again, this is Joe Deucher. Just one clarifying comment. The controls are part of the plan. So there are sets of

controls --

CHAIRMAN BROWN: Well, everything's part of the plan. Everything under the plan is part of the plan.

MR. DEUCHER: But the part that actually is submitted to the NRC would just be their plan of action, their intentions plus their sets of controls. With everything else that they do remaining on site and available for inspection or onsite review.

CHAIRMAN BROWN: Anyway, let's go on.

MR. DOWNS: Yes, we got it. Thank you.

Okay. Slide 20.

CHAIRMAN BROWN: And I'm just going to make one comment first. The plan says you got to have controls. The other thing says we don't have to look at the details unless we want to. That's the way I viewed the plan. The plan says you have to have controls, but the other things says we

don't have to look at all the details unless we have to.

Anyway, go on. I don't want to -- it's too trivial to argue about right now. We'll nail you at the Full Committee meeting.

MR. SHINN: Well, in that case, just so you know, the intent was for this to be just like it was for the reactors. So we've got the same level of detail to the license --

(Simultaneous speaking.)

CHAIRMAN BROWN: Yes, I didn't go back that far into 5.71 to see that.

MR. SHINN: Yes, our intent was to have the same degree of information we had to do the LARs for the --

CHAIRMAN BROWN: Okay.

MR. SHINN: -- power reactors.

CHAIRMAN BROWN: That's fine.

MR. SHINN: So if we didn't ask for the same level, we'll certainly go back and change that.

CHAIRMAN BROWN: That's -- that was -- I was just trying -- looking for consistency.

MR. SHINN: Okay.

CHAIRMAN BROWN: That's all I was

looking for. Whichever way you want to do it is fine with me. It's just a matter of consistency. And you call them vital digital assets here, not critical digital assets in 5.71. I didn't -- I was going to ask you why the difference, but I decided we didn't need to waste any time with that.

Now we're on slide 20?

MR. DOWNS: Yes, sir. So Section C.8 describes the implementing procedures and the temporary compensatory measures. Again, there were no changes here other than the previously mentioned change from ICMs to TCMs, because we love our acronyms.

Slide 21. Section C.9 of the Draft Regulatory Guide. We're talking about the configuration management aspects of the program in this section. One of our takeaways from the November meeting was to clarify the guidance on the -- how modifications need to be considered. Basically we clarify that any change that could adversely impact the licensee's ability to meet the Cyber Security Program performance objectives: again, detect, protect against and respond to an attack capable of causing consequences of concern -- those changes would be considered through this

configuration management process.

The concept of having this configuration management system is taken from the existing requirements that most fuel cycle facilities have to comply with in 10 CFR 70.72. So this isn't a new concept for them. It's just kind of saying include cyber within this existing framework.

Moving onto slide 22, this is Section C.10 of the Draft Reg Guide. We discussed the review of the Cyber Security Program. Again, we've got two different frequencies of review. You've got manual for the Category 1 facilities, or triennial for all others. There were no significant changes to this section of the guidance document.

Slide 23, event report and tracking. So the actual requirements haven't changed. The guidance has changed a little bit. The -- we've added some additional guidance in here as to what should be considered for event tracking and information for notifications to the NRC. The reason we did this is because in Reg Guide 5.83 -- that's the Regulatory Guide on cyber security event notifications for power reactors. It's the similar type of information that would have to be

transmitted to the NRC or tracked as it would pertain to events that don't meet their notification threshold to the NRC, just tracking internally.

CHAIRMAN BROWN: Under event reporting what categorizes item (c), emergency classification? it's on page 41.

MR. DOWNS: Yes. So those would -- that would be derived from the Emergency Plan from our facilities. They have -- if a specific event --

CHAIRMAN BROWN: Well, if you had to have an evacuation or if you had to do this or --

MR. DOWNS: Right, you've got a site area emergency, you've got a -- right on down the line, whatever it may be. That's where that comes from.

CHAIRMAN BROWN: Does that -- are there internal plant parts that fall into the emergency -- I've seen the evacuation plans or what we -- emergency planning that you have to go through, but does that include internal plant stuff as opposed to just outside the plant out to the exclusionary boundary or possible other population?

MR. DOWNS: Yes, so our --

CHAIRMAN BROWN: I was trying to figure

out where -- it just -- I didn't know what an emergency classification was. Run like hell? It's okay to stay in place? Hide in a bathroom?

MR. DOWNS: So we can add a little bit extra language in there that has derived from the site's --

CHAIRMAN BROWN: Do the vendors know what that means?

MR. DOWNS: It says derived from their emergency plan, correct. That -- and that -- we can add that extra piece in there.

CHAIRMAN BROWN: That's -- that was a little bit of confusion to me. The -- there was another one in here. At the time they report -- this is all under the auspices of one hour after the discovery that you've identified it as a cyber event, and yet that item (f), the event description has a lot of stuff: audit, failed equipment, what occurred during the event, why the event occurred, how the event occurred. It seems if you want to get a notification out, that seems -- that particular item, item (f) seems to be a little bit over -- it doesn't mean you don't get some of that.

It's just if you got to have a one-hour

notification after you figure out, you'll want to get the thing out. You don't want to sit around for two days trying to figure out how many of these I've got and have it right. That's all. Just trying to reduce the -- reporting can be a considerable burden if you ask for information that is not going to be used other than be put in a file cabinet somewhere. I'm not saying that negatively, but I -- but the purpose is to have it on record.

MR. DOWNS: Well, and it's -- yes, so than the other purpose is is that as it's reported to the NRC Headquarters operations officer they would be able to assess whether or not there is the potential for this attack vector to be applicable to other facilities and --

CHAIRMAN BROWN: Yes, but you -- that doesn't have to be done -- that's -- the point being is you want to get the information out. And then you -- if you have to, you can follow up and provide more detail at some point. It just seems trying to cram everything into that hour when, oh, my God, this was a cyber hack, you want to let people know, you want to know where it is, whether you had an emergency. There's some things you'd like to know. But trying to give a -- that event

description seemed to have other than a summary description that you say, hey, look, it compromised this piece. We've taken care of it and we're cleaning up the mess, whatever that means.

I just -- I'm just trying to put a little bit of sanity or suggest that you evaluate the detail of that -- needed in that one-hour report, because there's later reports that you all ask for, if I recall properly --

MR. DOWNS: There's no other reporting requirements --

CHAIRMAN BROWN: No, I'm -- no, you're right. I missed that.

MR. DOWNS: -- having that loggable-type situation.

CHAIRMAN BROWN: Event tracking, a record of the following events within 24 hours of their discovery and tracks them to resolution. That's in the next paragraph.

MR. DOWNS: Right. Again, it's a loggable onsite that's inspected at a triennial frequency --

(Simultaneous speaking.)

CHAIRMAN BROWN: The sentence that's still garbled, "a records the following events" --

MEMBER REMPE: Doesn't that follow up with --

(Simultaneous speaking.)

CHAIRMAN BROWN: Yes, I -- it -- I don't know what's the -- a record of the following events?

MEMBER REMPE: Yes, but again, in addition to the poor grammar that is not the initial one-hour report.

CHAIRMAN BROWN: No, this was a -- this is 20, but it's 24 hours of their discovery and tracks them to resolution. So I mean, there is another report to be done.

MR. DOWNS: So the way that that should be is if a licensee records the following events within 24 hours of their discovery, because again this -- the Reg Guide provides an acceptable approach. That's why you want to say "a licensee." So the licensee was taken out of there, apparently omitted.

CHAIRMAN BROWN: What if they can't get it done in 24 hours because they're still trying to fight the event? You're going to stop working on the event?

MR. SHINN: This is Mike Shinn again.

James, I think we may have addressed this in 5.83. We could go look at that Reg Guide, but I know this -- we had some fairly involved discussions about precisely what you're talking about here.

CHAIRMAN BROWN: What's 5.83?

MR. SHINN: That's the Regulatory Guide for --

CHAIRMAN BROWN: Oh, okay.

MR. SHINN: -- the reporting rule for --

CHAIRMAN BROWN: Oh, okay.

MR. SHINN: -- the reactors. And we took the same language model and time periods from that. And I think this concept is addressed in that Reg Guide. it's a rather long Reg Guide, so I don't remember every word in it, but I do know that we discussed this when we --

(Simultaneous speaking.)

CHAIRMAN BROWN: I don't think we looked at that. I don't remember looking Reg Guide, so that's -- I'm not saying -- I'm not complaining. It was long. Anyway, I'm just bringing up that 24 hours seems to be you're not going to stop everything, that you're going to have people that know what's going on to do it and you don't want to take them out of coordinating the event recovery if

they have to. So I would just suggest you evaluate that. A timely manner once the event is stabilized or something like that. I don't know.

MR. MALTESE: This is Jim Maltese from the Office of General Counsel. I would note that we do have 24-hour event reporting requirements in other parts of our regulations. In the event that there was a mitigating circumstance that a licensee couldn't give us notification in that time frame, I think that might be something we would consider in terms of enforcement discretion. But the 24-hour windows are

-- wouldn't be unique to this rule in terms of what's in your regulations.

CHAIRMAN BROWN: I would -- okay, I understand that, but I would still suggest letting them know that. That's all.

MR. DOWNS: Yes, so like Mike Shinn said, we'll take a look at the language in Reg Guide 5.83 and see what other supporting statements need to be added in there to clarify.

CHAIRMAN BROWN: Well, you don't have to be a lemming and continue running off the cliff just because 5.83 does it that way.

MR. DOWNS: Apparently there was a

significant amount of discussion though on exactly what you're saying, which is --

CHAIRMAN BROWN: I gave you a suggestion.

MR. DOWNS: Yes.

MR. SHINN: Many, many years --

CHAIRMAN BROWN: If you give people an allowance --

MR. SHINN: -- about just this.

CHAIRMAN BROWN: -- okay? That's all. Just let them know they have an allowance and they're going to have a stake driven through their heart. Just let you know that we can't finish it now. That's all. And get them the information you can. That was the only suggestion on that.

And then under documentation, the recorded event should contain at a minimum: personnel involved -- item (g), personnel involved or contacted; e.g., contractors, security personnel, visitors, plant staff, perpetrators or attackers, NRC personnel, responders and other personnel.

I hope somebody's keeping a list as you go around trying to take care of the event to make sure every word is recorded and you have somebody's

name given every time they provide a conversation of three sentences to you. Just the wording of that is very, very burdensome. Key personnel involved certainly limits -- and without listing anybody -- certainly provides some -- or supervisory personnel involved. That's probably even more important to know that there's some bosses that has -- that can take responsibility involved.

MR. DOWNS: Yes, I'll be 100 percent honest with you, we thought that you guys already reviewed that Reg Guide and were happy with these words, so --

CHAIRMAN BROWN: No --

MR. DOWNS: -- apparently --

CHAIRMAN BROWN: -- just some of them.

MR. DOWNS: -- that was a miss on our part. So we will definitely take these comments back.

CHAIRMAN BROWN: There's 108 pages worth of words.

(Laughter.)

CHAIRMAN BROWN: I'm 75. I have a hard time reading five pages a day without falling asleep.

MR. DOWNS: (Off microphone.)

CHAIRMAN BROWN: Oh, you mean from the November Subcommittee meeting?

MR. DOWNS: No, I was talking about from the issued Reg Guide 5.83 on the reactor side of the house of --

CHAIRMAN BROWN: We didn't see that, so --

MR. DOWNS: Apparently not, so we have to track back to that and --

(Simultaneous speaking.)

MR. SHINN: The good news is it's a pretty short Reg Guide. It's about 16 pages.

MR. DOWNS: Yes, so one of our --

MEMBER STETKAR: That's okay. Trust me, if we had looked at it in a Subcommittee meeting or a Full Committee, I would have had a copy of it here. And I don't have a copy of it, which --

MR. SHINN: I believe you're right. I don't recall.

MEMBER STETKAR: -- is a good --

(Simultaneous speaking.)

CHAIRMAN BROWN: I know we didn't look at it because I probably would have been involved also.

MR. DOWNS: So obviously one of the

concerns is is you've got this Reg Guide that's inconsistent with the reactor Reg Guide and then why is that the case? So we've got -- I appreciate what you're saying. And then words like "key personnel" definitely provide some latitude that could be afforded to our facilities without losing the intent of the statements. So we'll definitely -- again, we appreciate the comments and we'll take them back with us.

CHAIRMAN BROWN: Okay. That's enough on that one. You can go on.

MR. DOWNS: Slide 24, record keeping. Yes, we have record keeping. It is what it is. No significant changes.

Slide 25, glossary and references. Yes, we have glossary and references. There were several new terms identified in -- since the November briefing. I don't think there are any tremendous surprises in here. We tried to stay consistent with what was provided in the NIST Special Publication 800-53, as well as existing NRC guidance.

Several references were added for previously un-referenced documents and basically -- previously we would just say Title 10 of the Code

of Federal Regulations, and we thought that included all of the sections. It's just common draft -- in Reg Guides to be more specific than that, so that's why the list of references has dramatically increased. The first page there is just specific sections and parts of 10 CFR.

CHAIRMAN BROWN: If I'm not mistaken, just to make this a -- just a understanding, Appendix A fundamentally takes the text, takes the headlines and some of the specific items and puts them into the form of the template that you're talking about in terms of -- is that correct?

MR. DOWNS: Slide 26. Yes.

CHAIRMAN BROWN: Okay.

MR. DOWNS: Appendix A. That's exactly what Appendix A does.

CHAIRMAN BROWN: Oh, I -- yes, I was a slide ahead, wasn't i?

MR. DOWNS: Yes, you just --

(Simultaneous speaking.)

CHAIRMAN BROWN: Sorry about that.

MR. DOWNS: -- skipped right through glossary and references.

(Simultaneous speaking.)

CHAIRMAN BROWN: -- good idea. We

didn't need to work on that one.

(Laughter.)

MR. DOWNS: So, yes, sir, the Appendix A takes the overall Reg Guide and provides it in a template and is -- would be -- it would facilitate the licensee to produce a Cyber Security Plan.

CHAIRMAN BROWN: Okay.

MR. DOWNS: Okay?

CHAIRMAN BROWN: I will note that that's one of the few sections where defensive architecture missed back in the review of the Cyber Security Program. That's one of the three places. You're supposed to audit for the defensive architecture, however, you never talk about ever developing a defensive architecture anywhere in the text. That's kind of an inconsistency in those -- in the three places it's mentioned.

And based on our earlier conversation, this -- again this is a suggestion, that since you do talk about defensive architecture in these areas for their plan, etcetera, okay, that it might be useful to at least identify that one method that can be used by a fuel cycle facility vendor would be to develop a defensive architecture and assess vital -- or assess digital assets within that as

well. I mean, that's one of the alternatives they can use. That way it makes some sense when you get in to assessing and using that to audit for -- I mean, if you're going to audit for it, that means -- sounds like they have to do it, or they -- excuse me, they should do it since this is a Reg Guide.

MR. DOWNS: Well, beyond that the actual -- there's a rule requirement that the review includes an audit of the effectiveness and adequacy of the Cyber Security Program including but not limited to applicable cyber security controls, alternate means of protections and defensive architecture of the digital assets identified.

CHAIRMAN BROWN: Yes, but there's again in the --

MR. DOWNS: So what you're saying is in the body of the Reg Guide we don't talk about defensive architecture at all. So we need to --

CHAIRMAN BROWN: They've got three places. I can tell you where they are. Section 4.1(h), 9.2(e) and there's one other place. Did I do good?

PARTICIPANT: You did good.

CHAIRMAN BROWN: Thank you. 4.1(h), 4.

-- 9.2(e) and I've got another one.

PARTICIPANT: You can do a word search and find it very easily.

CHAIRMAN BROWN: I've got it. I've got a little star in here somewhere. I can't remember where it was. It's in here somewhere. I've got one of my little sticky notes.

MR. DOWNS: So again, we appreciate the comment. We'll take it back to --

CHAIRMAN BROWN: It's just a -- again, it's just a suggestion to try to provide -- if you're going to audit something, you certainly should tell the guy that he ought to provide at least some guidance on developing one of some sort of generalized words.

Okay. Where are you now, 27?

MR. DOWNS: Going to move to 27, yes. Appendix B. So these would be the controls for all vital digital assets for all consequences of concern, basically anything that's cross-cutting across everything. It's -- if you've got a VDA, this is the minimum that you have to do. This is -- it's a core set that's common to all VDAs.

CHAIRMAN BROWN: It's all -- it applies to all consequences of concern?

MR. DOWNS: Correct, and what you'll see in here, a lot of this is programmatic-type -- or not requirements. These are programmatic controls that -- for instance, it talks about that the architecture --

CHAIRMAN BROWN: I didn't have any problem with this one. Did anyone else have any questions on this slide?

(No audible response.)

CHAIRMAN BROWN: Going to 28?

MR. DOWNS: Okay. So slide 28, Appendices A through F. Basically each one of these appendices is unique to the specific consequence of -- type of consequence of concern that the vital digital asset is associated with. And there were no significant changes in any of these appendices.

CHAIRMAN BROWN: The appendices were useful, I thought. That's personal opinion, not a Subcommittee or Committee opinion.

MR. DOWNS: Good, because we took a whole heck of a lot of time making them up, let me tell you. (Laughter.)

CHAIRMAN BROWN: Out of thin air, right?

MR. DOWNS: Yes, right. Okay. So

that's -- slide 29. This is the example. The feedback that we received in November was that our example was significantly lacking. You all may have used some stronger language than that, but that's our takeaway. So Appendix G was -- we had a complete rewrite to try to show the implementation of the entire process from identification through configuration. That was our effort there.

CHAIRMAN BROWN: Okay. Hold on. Don't leave this one yet.

(Pause.)

CHAIRMAN BROWN: I guess I didn't have any real problems with this one. It was a simple example trying to illustrate alternate means and air gap and the concepts you put in there. Very easy to deal with because it was not complex. So that is an improvement. I guess the only statement I had that a laptop is traditionally not considered an air gap digital asset. But if it's just sitting there as a laptop and it doesn't have wireless capability and it's not connected to anything --

MR. DOWNS: You've added a lot of "ifs."

CHAIRMAN BROWN: Well, most laptops are not connected to anything and may or may not --

MEMBER BLEY: I think that's at your

house, Charlie.

(Laughter.)

CHAIRMAN BROWN: Just because I don't us DVRs and don't have a smartphone?

MEMBER BLEY: You have a laptop that's not connected.

CHAIRMAN BROWN: And don't text?

MR. DOWNS: Well, I think just to kind of summarize, the intent of Appendix G was to demonstrate a certain level of acceptable documentation, a certain level of detail. Again, as you alluded to, some of the benefits that air gaps would have when addressing the controls. And the last thing was provide an example of how grouping and inheritance for controls is beneficial and could reduce burden.

CHAIRMAN BROWN: The only statement I think you made that was an assumption was on page 7 where you talked about tools for the VDA. The milliamp simulator calibration uses no special software, but yet there's -- the only thing you say in the text is that it has no external connection capabilities. You never talk about it not being software-based. I presume you're assuming it's an analog-style milliamp simulator similar to the one

I have in my workshop.

MR. DOWNS: That was the intent, yes.

CHAIRMAN BROWN: Although a milliamp simulator these days, a test instrument has probably got a microprocessor in it somewhere --

MR. DOWNS: Right.

CHAIRMAN BROWN: -- and everything. So my point being it's an end, that if it's software-based, which you don't allude to in the example, then it needs its own whatever assessment of its digital asset capability and its reliability in terms of being able to be used to provide that last stop of being it's okay going forward. That's all.

MR. DEUCHER: Right, in this instance; again, Joe Deucher with NSS, it could be considered a support system and --

CHAIRMAN BROWN: Yes, I mean, I just --

(Simultaneous speaking.)

MR. DEUCHER: -- make the decision, right.

CHAIRMAN BROWN: It just wasn't clear from reading that part of the example. It wasn't a logical end stop based on your earlier -- it was an assumption. And it's not a big problem, it's just

an assumption that's not clear.

MR. DEUCHER: That's correct. It --

(Simultaneous speaking.)

CHAIRMAN BROWN: So it really should be a non-software control or non-micro -- non-computer-based simulator is what you really need to say instead of just it's a milliamp simulator. That's all.

MR. DOWNS: Duly noted.

CHAIRMAN BROWN: Okay?

MR. DOWNS: Yes.

CHAIRMAN BROWN: That's the end of that.

MEMBER REMPE: So I wasn't at the November meeting and I'm just trying to process a lot of this, but is your vision that the Cyber Security Plan is submitted back here to headquarters and you review it, or is it something that a regional office would review? Are audits done by headquarters personnel or regional personnel? How would this be implemented?

MR. DOWNS: So it would be submitted to the headquarters staff as part of a license amendment request.

MEMBER REMPE: Okay.

MR. DOWNS: And the staff would review

it and provide the approval of the plan. At that point then implementation of the plan would be inspected through the regional inspection office. So that was kind of what we were -- a lot yet to be determined with the actual inspection process and the staff involved and that sort of thing, but traditionally the inspections are done out of the regional office. So that was kind of --

MEMBER REMPE: And extra training would be required or provided to the regional office?

MR. DOWNS: Regardless.

MEMBER REMPE: Okay.

MR. DOWNS: Yes, absolutely as to whoever -- and one of the things that we covered there in the beginning was the -- on slide 5 we talked about the associated program development. We would have a Standard Review Plan associated with the review. Standard Review Plan provided the staff for reviewing Cyber Security Plans. And then an inspection procedure to guide the NRC inspector's evaluation of implementation of the plan. Both of those elements of the program have not been developed yet to date.

MEMBER REMPE: Thank you.

MEMBER STETKAR: James, one of the

things -- I asked this back in November and I just want to make sure I understand it. In Appendix G -- and I have -- you've revised the appendix. If I read Appendices B through F, I come up with I think 153 distinct controls that I'm supposed to evaluate for each of my vital digital assets, right? You don't have to do the body count. I did. The point is there's a bunch of them.

In your example in Table G.4 in the appendix you list -- as an example, one, two, three, four, five six, eight. You don't list the other 145 where -- do I -- as the licensee do I have to explicitly address each of the other 145 and say this one doesn't apply for the following reasons? You've addressed the eight that apply and describe how you've addressed those, but I as a licensee have to address the other 145 and say why they don't apply?

MR. DOWNS: That's correct, you would have to address --

MEMBER STETKAR: Okay.

MR. DOWNS: -- the other -- that's right. And it may be done through -- you may have a --

MEMBER STETKAR: That's what I -- that's

fine. I just wanted to make sure that --

MR. DOWNS: Yes. Yes, you're on it. Yes.

MEMBER STETKAR: Those are my notes from back in --

(Simultaneous speaking.)

MR. DOWNS: There are multiple ways to do that effectively and efficiently, but, yes, they're -- right.

MEMBER STETKAR: Well, the key is efficiently --

MR. DOWNS: Right.

MEMBER STETKAR: -- because for each vital digital asset checking off boxes, 153 boxes saying no, no, no, no, no, no, no, yes is prone to not thinking. Okay.

CHAIRMAN BROWN: Before we go on, Myron, are you there?

MR. HECHT: Can you hear me?

CHAIRMAN BROWN: I can now.

MR. HECHT: Really?

CHAIRMAN BROWN: Yes.

MR. HECHT: Okay. Before I was mute.

CHAIRMAN BROWN: Okay. Well, we un-muted you. Theron just told me. I wasn't aware

that you were muted. Sorry about that.

MR. HECHT: I wasn't before through the noise earlier.

CHAIRMAN BROWN: You were not, were you?

MR. HECHT: No.

CHAIRMAN BROWN: Okay. Well, they left also, so we're good now. I apologize for you being muted.

MR. HECHT: That's fine. Could I ask some questions or do you want to just move on?

CHAIRMAN BROWN: Depends on -- go ahead. We'll see if we want to answer them or not. Okay?

MR. HECHT: Okay. Okay. On definitions; this is the most important question, the version that I have was of definitions for vital digital assets still says "devices" in the glossary. It doesn't really speak about software. So even though you made references earlier to various controls that you stated for software, at least the version that I have, which apparently was produced on January 24th, still has devices -- still has digital assets I should say, not vital, but digital assets defined in terms of devices.

CHAIRMAN BROWN: Not software-based devices?

MR. HECHT: Right, just devices.

MR. DOWNS: Well, yes, so this is James Downs with NMSS. We're assuming that the software would reside on the device, so therefore --

MR. HECHT: You talk about software as being a digital asset and if it's not a device, that means it's not digital asset.

MR. DEUCHER: Myron, this is Joe Deucher, NMSS. Again, the way we would expect the licensees to look at it would be in line with looking at the NIST family of controls where the application itself would just be one part of it. It would be the platform it's residing on, it would be its physical protections, it would be just basically every way in and out of that particular application.

So we would want them to look at it holistically so they could develop the protections, if you will, around that asset holistically. Because there will be some interaction between the hardware level, the software, the operating system, kind of all of it.

And also the benefit for them would be they could take credit for some of the capabilities. Rather than having to bake certain

security capabilities into the software itself, they could say, well, there's audit capabilities in the operating system, log-in capabilities there. So there are certain things that I could take advantage of that exist in either the hardware or the operating system rather than just the straight software.

MR. HECHT: Well, the operating system is software, isn't it, just to get to that example? And I was just thinking how much does it take to broaden that definition, because otherwise it can lead to a lot of -- I wasn't thinking about it in terms of --

CHAIRMAN BROWN: Are you there?

(No audible response.)

CHAIRMAN BROWN: Myron?

(No audible response.)

MEMBER BLEY: We don't hear you anymore.

MR. HECHT: Oh, really?

CHAIRMAN BROWN: We hear you now.

MR. HECHT: Oh, okay. I wasn't thinking about this in terms of how it's addressed in the controls. I was thinking about it as whether it needs to be protected or not.

And then you get to the subject of if I

have virtual machines and I have all my virtual machines on one physical processor, does that mean I only have one VDA?

MR. DOWNS: Yes, that's exactly what it means.

MR. HECHT: Well, I might question that, but I guess I would point that out as a problem.

Second question is with respect to talking about custom software. You said that custom --

(Simultaneous speaking.)

CHAIRMAN BROWN: Myron, hold on a minute before you go to that. On the digital asset thing, I guess I hadn't thought about it when I was scanned through there. It's just an electronic device or an organized collection of devices, etcetera, that processes information, communicates data or is programmed. You don't have to have a microprocessor or a computer to do that. It can be a fuel programmable gateway which has a fixed system of processing. I've got a frequency counter at home that's as digital as you can get and it doesn't have a single piece of software in it. It's all logic gates and everything else in order to do it.

I would suggest that he's got a point relative to if it's not a software controlled type digital asset, then -- that can be changed in its little stage of sitting there without ripping the whole thing out piece by piece, that you want -- there's a lot of controls that you buy that are FPGA or they're already -- they're -- they can't be changed unless you take the chips out and put a new chip in.

MR. SHINN: This is Mike Shinn. I think we would agree with you. And the process that we would expect the licensees to do is when they're looking at whether or not there's a consequence would be to say is there something that an adversary can do to this to cause that action. And a reasonable response could be, no, there's -- you can't change this thing.

Okay. Then you've demonstrated that there is no consequence through a cyber attack. It screens out.

MEMBER STETKAR: Unless you can modify a look-up table --

(Simultaneous speaking.)

MR. SHINN: Absolutely. I mean, just because it's hardware --

MEMBER STETKAR: Yes.

MR. SHINN: -- we can't just say, well, it's hardware. It always screens out. Because that's a fairly vague and nebulous word that could imply some aspect of it, it can be changed. Or maybe it's just a very naïve device. It gets a signal, it does something. It gets a signal, it does something. And it has no way to differentiate whether or not it's a malicious or non-malicious signal.

But the -- I want to say that I heard what you said and the whole intent is in that case that you described, that hypothetical, that asset would screen out.

CHAIRMAN BROWN: The point is to try to not make it -- make -- you're so encompassing that you require more assets than necessary to be thrown under the umbrella for assessment. And I agree if you've got a -- if you can manually change from a keyboard on the front of it the settings, that would be one thing. Few of those are in that mode, at least most calibration-type and other type of equipment comes that way. Okay. Well, anyway.

All right. Go on with the next one, Myron.

MR. HECHT: Okay. With respect to

custom software, I think the way you addressed it was to say that custom software is only considered if it is associated with consequence of concern. That's fine, but then the question is how is it considered? And I was looking at the controls you mentioned: B.14, C.25, C.29, etcetera, and I did not see in those controls anything that was unique to custom developed software. And what we're concerned about in the reactor side are what's in our secure development and operation environment.

In other words, there should be some kind of standards applied to the development of custom software so that it's basically robust to cyber security attacks. Things like coding guidelines to prevent stack overflow attacks and input validation and things you do to databases to prevent people from adding queries when they enter data into a field. And I don't see that here.

CHAIRMAN BROWN: Did you get that?

MR. DOWNS: I got it, yes. So this is James with NMSS. The controls that we've got listed here, Myron, are -- they're -- basically they assume that the software doesn't have any of the things that you're talking about. And we're not saying that the software that you developed has

to have any of those things. What we're saying is that if -- assuming that they don't have any of that, this is how you would protect it.

If it had some of those considerations that you're talking about, you could reference that and take credit for that as part of addressing some of the controls that are referenced on software. So it's not like you've -- we're trying to provide an example -- example controls that are set to the lowest denominator, so to speak. We're not trying to provide controls that are -- that take into software features that could or could not be there.

MR. DEUCHER: And again, Myron, this is Joe Deucher with NMSS, just to add onto what James is saying, being that the controls are coming from NIST and the 800-53 Special Publication, what you're getting there -- again, it's a wide swath. It's designed to be able to look for features for customized off-the-shelf software as well as just straight purchased software, as well as specially developed software.

You're looking for performance characteristics and performance specifications similar to what you're mentioning there, so that if I went down the list of -- in order to protect this

particular digital asset that had software on it, that was customized, that maybe one of the controls deals

-- would deal with some level of secure development and ensuring that there is proper code development. You could answer that question that way, that -- say that I used this particular secure coding methodology, because there are several that are out there that exist.

We're not trying to be extremely prescriptive. We're trying to keep things performance-based and we're trying to use a generally accepted standard as our authoritative source in NIST in order to be able to address this to be able to kind of cover the wide swath that we see in and amongst our facilities.

MR. HECHT: Well, NIST 800-53 was written basically for IT-type systems. And what you have in an SCF by and large is a process control-type system. It's just -- I'm not sure that's totally -- your argument totally addresses the question.

MR. DOWNS: Well, what I would -- Myron, what I would throw out to you --

(Simultaneous speaking.)

MR. HECHT: I would just point out that there's a lot of -- or I would imagine that there's a lot of very customized software in a gas centrifuge plant or in a laser isotope separation facility.

MR. DOWNS: And I would -- what I would suggest to you -- just as an example in federally-accredited systems that I've worked on in the past that were essentially customized, specialized developed software using the NIST guidance for a particular application -- in my particular example it was both and audio-visual system, if you will, of analog, as well as digital components, in addition to data-driven devices, in addition to computers. And the NIST was a good source to be -- and was flexible enough to be able to deal with all those different systems, devices and components to be able to ask the question how do you protect this from a given threat?

And i would also say that again what we've tried to do with the guidance wherever possible is since NIST has gone forward and developed the 800-82, which is specific to industrial control systems, they've overlaid on top of the 800-53, just like they're looking to do the

same thing for cyber -- for your Internet of things devices. They're using that 800-53 as the foundation. Everything kind of goes on top of it so that you could still use those requirements, because they are just specifications.

And I would contend that they are generic enough in terms of what they're protected against to be effectively utilized, whether it's an amplifier as a part of an audio system, as well as your standard IT, as well as your ICS.

MR. HECHT: So if I understand your answer, I can have a piece of software that I put onto my facility that has all kinds of back doors, all kinds of vulnerabilities and weaknesses, and if I just make an argument, a plausible argument that my controls can defend against it, then I'm compliant.

MR. DOWNS: That is correct, because some of the software that they're using -- it could be entirely possible that the software is 20 years old. They can't change it. They can't do anything to it to modify at the software level, so they have to put in additional protections.

I can think of one example right now where there's an industrial control device sitting

out there today that there's a known vulnerability for it that cannot be patched because its memory is not big enough to take the patch necessary to defend against the vulnerability.

So your choice is you either replace it or you develop defenses around it. And that's what folks are going to run into going forward as new threats are identified and these older pieces of equipment are continued to use into service. And that's why when you look at -- what we've done with our controls is -- again, it's arranged around these different threats to be able to be as flexible and holistic as possible to give you that layered defense, for lack of a better term, defense-in-depth. And then you add on top of that your detection where you're looking at what's the traffic with this or what's the activity with this? And then response, if indeed something looks abnormal.

MR. HECHT: Yes, so you don't even want to consider addressing newly developed software? You're just going to say that any custom software can -- we have no standards, we have no cyber security, no built-in security as the DHS uses? None of that applies to anything that would be

going into these facilities?

MR. DOWNS: Well, it certainly can apply. It's what you choose to take credit for. I mean, a licensee could easily decide, you know what, going forward we're going to do secure development. We're going to use this development model and we're going to bake it in at this level. And that's what they choose to do. Or a licensee --

CHAIRMAN BROWN: Okay. Hold it.

Myron, hold it. We're going to have to move on here.

MR. HECHT: Yes. Okay. Well, I'll make that observation. You can do what you want with it.

CHAIRMAN BROWN: Okay. Yes, thanks. Is that it?

MR. HECHT: That's it.

CHAIRMAN BROWN: Okay.

MR. HECHT: I think I've used up my time.

CHAIRMAN BROWN: No, no, no. No problem. We've got all day.

(Laughter.)

CHAIRMAN BROWN: We don't have to leave

here until 8:00, in the words of one of my esteemed colleagues when we're running up against the clock.

PARTICIPANT: That's his meeting.

CHAIRMAN BROWN: That's his meeting. I try to do better. I'm failing today.

All right. This is the end of the open session. So I will turn around and see if there's any -- well, we've got to open up the public phone. Oh, wait. Is the public phone automatically open? Oh, okay. It's open.

Okay. Is there anybody in the audience that wants to make any observations?

(No audible response.)

CHAIRMAN BROWN: Is there anybody in the audience that would like to make observations?

(No audible response.)

CHAIRMAN BROWN: Thank you. Obviously none.

Is there anybody on the phone line? You want to say something to make sure the phone line is open? Somebody --

PARTICIPANT: It's open.

CHAIRMAN BROWN: Thank you. Anybody have any comments on the open phone line?

(No audible response.)

CHAIRMAN BROWN: Going once, twice, three times?

(No audible response.)

CHAIRMAN BROWN: Okay. That will be it. We will now -- what do we do, recess while we do this. MEMBER BLEY: We can recess, but you got to close the phone line.

CHAIRMAN BROWN: Okay. Get the phone line closed, please, Christina. Thank you.

And now we will recess and reconvene in a closed session here.

(Whereupon, the above-entitled matter went off the record at 4:04 p.m.)

U.S.NRC

United States Nuclear Regulatory Commission

Protecting People and the Environment

Design of the Highly Integrated Protection System Platform

Presentation to the ACRS
Full Committee

April 6, 2017
(Open Session)

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Agenda

- Background
- High-Level Description of the HIPS Platform
- Safety Evaluation Scope
- Regulatory Conformance

Background - Timeline

Date	Activity
December 2015	Topical Report (TR) 1015-18653-P submitted for review
February 2016	NRC Accepted TR for Review
June 2016	NRC Sent RAIs
July 2016	First Audit at NuScale's Rockville Office
August 2016	NuScale Sent Response to RAIs
November 2016	Revision 1 of TR docketed
January 2017	Draft Safety Evaluation Issued
January 2017	Second Audit at Ultra Electronics (Wimborne, UK)
February 2017	ACRS Subcommittee Meeting
March 2017	Issuance of Final Safety Evaluation
April 2017	ACRS Full Committee Meeting

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

HIPS Platform

- The HIPS platform is composed of logic implemented using discrete logic and field programmable gate array (FPGA) technology
- The HIPS platform consists of the HIPS chassis and a system of modules
  - Safety Function Module (SFM)
  - Communications Module (CM)
  - Equipment Interface Module (EIM)
  - Hardwired Module (EIM)

SE Review Scope

- The scope of the review was focused on:
  - Fundamental I&C design principles
    - Independence
    - Redundancy
    - Predictability and Repeatability
    - Diversity and Defense in Depth
  - Calibration, testing, and diagnostics capabilities of the HIPS Platform

Regulatory Conformance

- The HIPS platform design supports meeting the applicable regulatory requirements associated with the fundamental I&C design principles.
- 65 ASAIs have been established to identify criteria that should be addressed by applicants or licensees referencing this SE.
  - Quality Assurance
  - Equipment Qualification
  - Secure Development Process
  - MWS and PS Gateway
  - Human-Machine Interface
  - Displays

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Questions

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Acronyms

- ACRS: Advisory Committee on Reactor Safeguards
- ASAI: application-specific action item
- CM: Communication Module
- EIM: equipment interface module
- ESFAS: engineering safety features actuation system
- FPGA: field programmable gate array
- HIPS: highly integrated protection system
- HWM: Hard-Wired Module
- I&C: instrumentation and control
- ISM: Input Sub-Module
- MIB: Monitoring and Indication Bus
- MWS: maintenance workstation
- NRC: U.S. Nuclear Regulatory Commission
- RAI: request for additional information
- RTS: reactor trip system
- SDB: Safety Data Bus
- SBM: scheduling and bypass module
- SFM: safety function module
- SE: safety evaluation
- SVM: scheduling and voting module
- TR: topical report

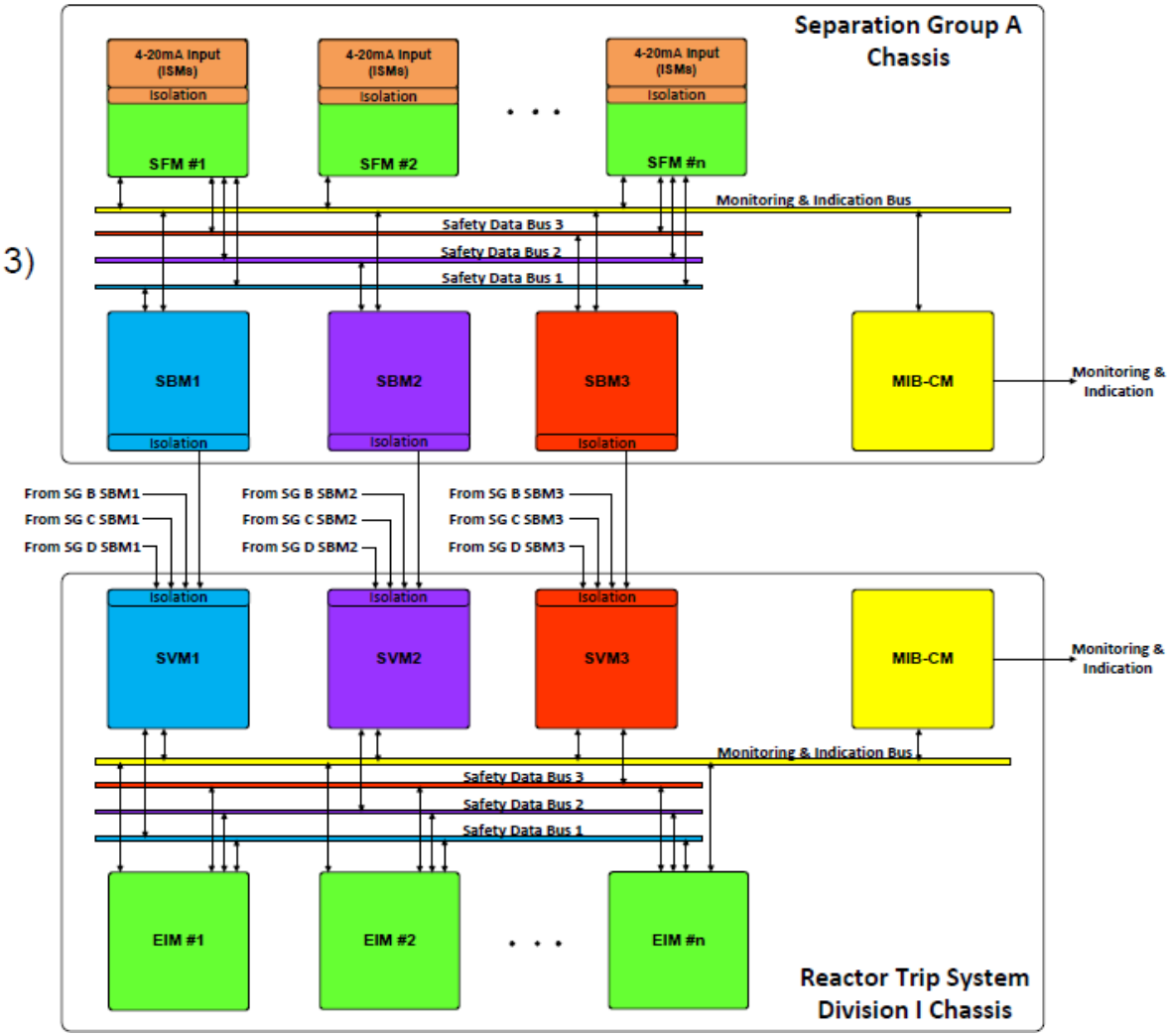
U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Backup Slides

Populated HIPS chassis with the trip/bypass plate

High Level Representative Architecture Safety Data Paths

- Safety Data Paths (1, 2, 3)
- Safety Data Path 1
- Safety Data Path 2
- Safety Data Path 3
- Monitoring and Indication Path



U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Independence

- Physical Independence
- Electrical Independence
- Communications Independence
- Functional Independence

The staff finds that the TR provides information sufficient to support conformance with the independence requirements in RG 1.75, RG 1.152, RG 1.53, and DI&C-ISG-04, or establishes ASAIs as necessary to fully comply with the regulatory requirements for an applicant or licensee referencing this SE.

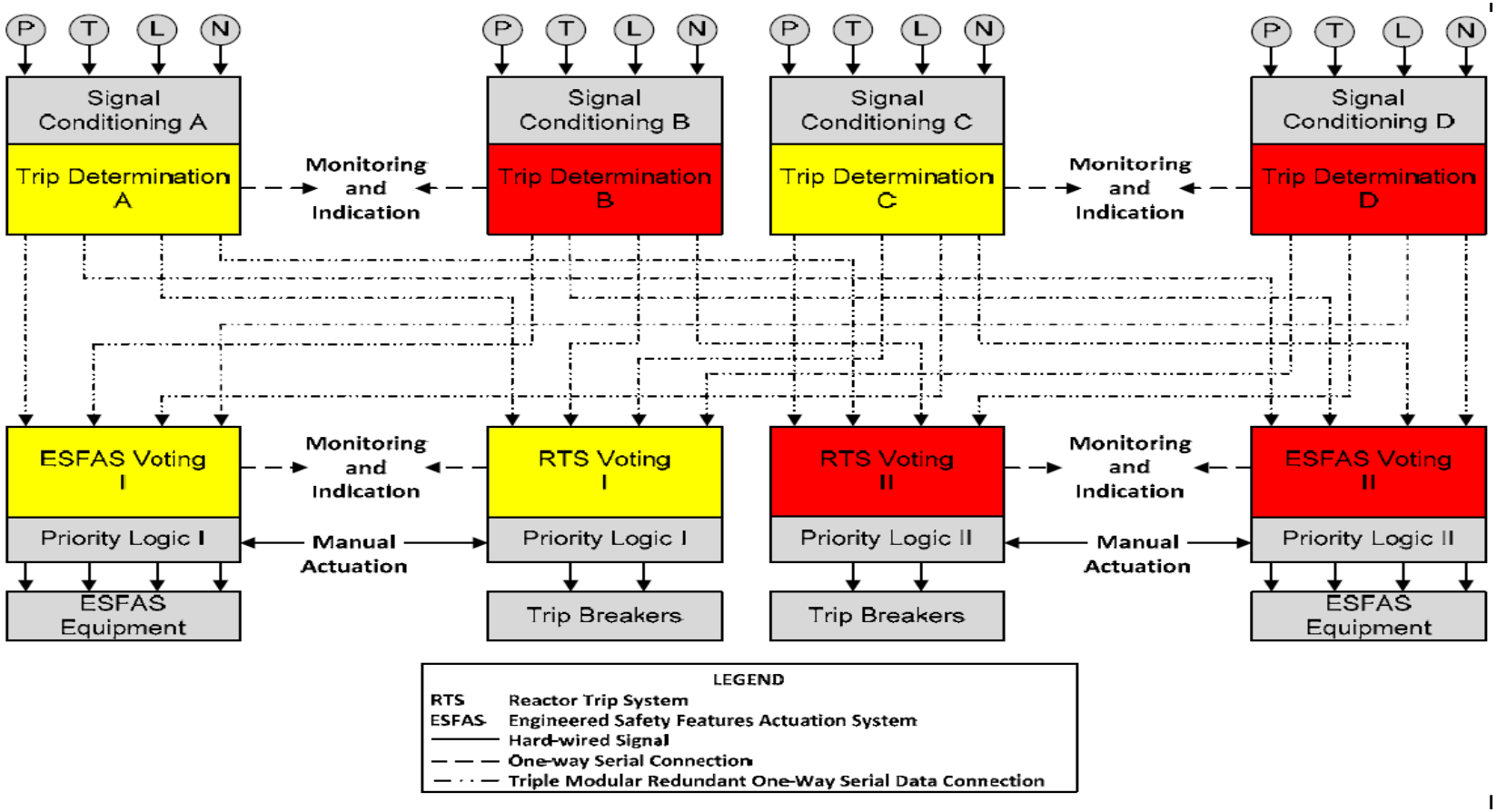
Redundancy

- Power Supply Redundancy
- Safety Module Redundancy
- Communication Redundancy
- Equipment Interface Redundancy
- Platform Redundancy

The staff finds that the TR provides information sufficient to support conformance with the regulatory requirements on the single failure criterion in RG 1.53, or establishes ASAIs as necessary to fully comply with the regulatory requirements for an applicant or licensee referencing this SE.

Diversity

FPGA Equipment Diversity Allocation in a Representative Architecture



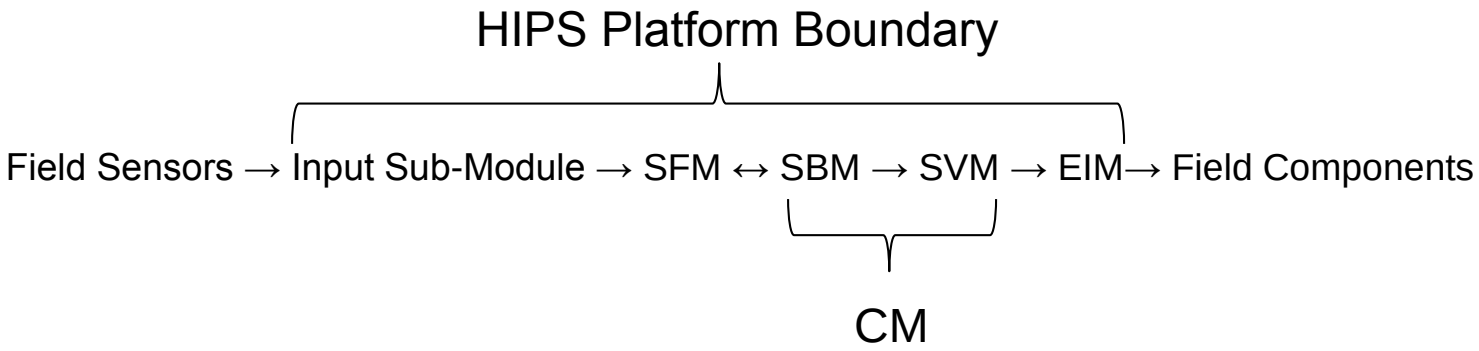
Diversity

Effects of Digital CCF for HIPS Diversity Strategy

Event	Module	A	C	B	D
Transient or accident (no CCF)	SFM	✓	✓	✓	✓
	CM	✓	✓	✓	✓
	EIM	✓	✓	✓	✓
Transient or accident with CCF (Case 1 – equipment (FPGA) and module functional diversity)	SFM	×	×	✓	✓
	CM	✓	✓	✓	✓
	EIM	✓	✓	✓	✓
Transient or accident with CCF (Case 2 - equipment (FPGA) diversity)	SFM	×	×	✓	✓
	CM	×	×	✓	✓
	EIM	×	×	✓	✓

Predictability and Repeatability

Typical plant signal data flow path in HIPS platform



Calibration, Testing, and Diagnostics Capabilities

- Section 8, “Calibration, Testing, and Diagnostics,” of the TR describes the diagnostics and maintenance features provided by HIPS platform and directly addresses IEEE Std 603-1991 Clause 5.7.
- These features include the use of BIST, CRC checks, periodic surveillance testing, and other tests in each type of module as appropriate to verify normal operation.