# Official Transcript of Proceedings

# NUCLEAR REGULATORY COMMISSION

Title: Advisory Committee on Reactor Safeguards
Digital Instrumentation and Control

Docket Number: (n/a)

Location: teleconference

Date: Friday, October 22, 2021

Work Order No.: NRC-1727 Pages 1-204

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

# DISCLAIMER

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

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

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

UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

+ + + + +

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

(ACRS)

+ + + + +

DIGITAL I&C SUBCOMMITTEE

+ + + + +

FRIDAY

OCTOBER 22, 2021

+ + + + +

The Subcommittee met via Videoconference, at 9:30 a.m. EDT, Charles Brown, Chairman, presiding.

COMMITTEE MEMBERS:

CHARLES H. BROWN, JR., Chairman

RONALD G. BALLINGER, Member

VICKI BIER, Member

VESNA B. DIMITRIJEVIC, Member

GREG HALNON, Member

WALTER L. KIRCHNER, Member

JOSE MARCH-LEUBA, Member

DAVID A. PETTI, Member

MATTHEW W. SUNSERI, Member

ACRS CONSULTANT:

MYRON HECHT

DESIGNATED FEDERAL OFFICIAL:

CHRISTINA ANTONESCU

ALSO PRESENT:

SCOTT MOORE, ACRS Executive Director

SABRINA ATACK, NSIR

MEKONEN BAYSSIE, RES

JIM BEARDSLEY, NSIR

ERIC BENNER, NRR

SUSHIL BIRLA, RES

CHRISTOPHER BROWN, ACRS

LARRY BURKHART, ACRS

TOM DASHIELL, ACRS

RONALDO JENKINS, RES

JEANNE JOHNSTON, NRR

ANYA KIM, RES

KIM LAWSON-JENKINS, NSIR

ERIC LEE, NSIR

HOSSEIN NOURBAKHSH, ACRS

MERAJ RAHIMI, RES

DAVID RAHN, NRR

ERICK RODRIGUEZ MARTINEZ

MICHELE SAMPSON, NSIR

TAMMY SKOV, ACRS

DINESH TANEJA, NRR

WEIDONG WANG, ACRS

DEREK WIDMAYER, ACRS

BRIAN YIP, NSIR

CONTENTS

P R O C E E D I N G S

9:34 a.m.

CHAIR BROWN: All right, I'm going to call the meeting to order. This is a meeting of the digital instrumentation and control Subcommittee. I'm Charles Brown, Chairman of the Subcommittee Meeting.

ACRS Members in attendance are Matt Sunseri, Vesna Dmitrijevic, Ron Ballinger, Dave Petty, Walt Kirchner, Vicki Bier, Gregory Hallman, and is our consultant, Myron, on right now, Christina?

MS. ANTONESCU: Yes, Myron is on the phone, yes.

CHAIR BROWN: Okay, I didn't see the other thing. Thanks, Myron.

MR. HECHT: Good morning, Charlie.

CHAIR BROWN: Jose March-Leuba will be late, he has something to take care of. Christina Atonescu of the ACRS Staff is the designated federal official for this meeting.

I presume, Christina, the court reporter is on.

MS. ANTONESCU: Yes, Member Brown.

CHAIR BROWN: The purpose of this meeting is for the Staff to brief the Subcommittee on proposed Revision 1 to Regulatory Guide 5.71, Cybersecurity

Programs for Nuclear Facilities, Draft Guide 5061, Revision 1.

The ACRS was established by statute and it was governed by the Federal Advisory Committee Act, FACA. That means 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 office requesting time. That said, we set aside 10 minutes for comments from members of the public attending or listening to our meetings.

Written comments are also welcome. The meeting agenda for today was published on the NRC public meeting website as well as the ACRS meeting website. On the agenda for this meeting and on the ACRS meeting website are instructions as to how the public may participate.

No request for making a statement to the Subcommittee has been received from the public. Due to COVID-19, we are conducting today's meeting virtually. A transcript of the meeting is being kept and will be made available on our website.

Therefore, we request that participants in this meeting first identify themselves and speak with

sufficient clarity and volume so that they can be readily heard. All presenters, please pause from time to time to allow members to ask questions.

Please also indicate the slide number you are on when moving to the next slide. We have the MS Team phone line, audio only, established for the public to listen to the meeting.

Based on our experience from previous virtual meetings, I would like to remind the speakers and presenters to speak slowly. We will take a short break after each presentation to allow time for screen-sharing as well as the Chairman's discretion during longer presentations.

Lastly, please do not use any virtual meeting feature to conduct sidebar technical discussions. Rather, contact the DFO if you have any technical questions so that we can bring those to the fore.

Before I proceed onto Ms. Lawson-Jenkins to share her screen and Michelle to provide comments, I'd like to remind everybody this is a Subcommittee meeting and comments or suggestions or recommendations which appear to be recommendations made by Committee Members as well as myself are our opinions and are not the Committee opinion.

They will not be Committee opinions until we formally complete this process with a full Committee meeting and we prepare a letter report, where we will end up with a consensus set of comments, observations, or recommendations.

We will now proceed with the meeting and I will ask Ms. Lawson-Jenkins of the cybersecurity Branch and the Office of Nuclear Security and Incident Response to share her screen with us, which she has done, while Michele Sampson, the Deputy Director of the Division of Cybersecurity Policy in the Office of Nuclear Security and Incident Response for any introductory remarks you care to make before we begin today's presentations.

So, Michele, it's your floor.

MS. SAMPSON: Thank you, good morning. We appreciate this opportunity to brief the digital INC Subcommittee on our revision to Regulatory Guide 5.71, cybersecurity programs for nuclear power reactors.

We will share with you how the regulatory guide update was informed by lessons learned from our oversight inspections at the operating fleet, and changes in standards and technology.

The Staff have inspected each operating station at least twice over the past nine years,

evaluating both their interim implementation and subsequently the full implementation of each cybersecurity program.

Additionally, during the 11 years since Reg Guide 571 was published, the national institute of standards and the International Atomic Energy Agency, IAEA, have developed standards for nuclear applications and industrial control systems that provide additional guidance that we have incorporated into this revision.

Our NSIR Staff are working closely with the regional cybersecurity inspection branches and NRR's Division of Engineering to prepare for inspection of future digital INC upgrades.

We do not anticipate that licensees will need to submit amendments to the licensee cybersecurity plans as a result of the digital INC upgrades. However, we expect that inspection will be a key tool that we use to verify the continued effectiveness of cybersecurity protections.

The Staff have supported Region 4 and the NRR vendor inspection team during inspection of the Waterford digital INC upgrade factory acceptance testing. We have also supported the pre-licensing activity for the future Turkey Point digital INC

upgrade.

NSIR is actively evaluating cybersecurity threat through our Intelligence and Threat Assessment Branch and interagency liaison.

Our Staff are working with the Office of Research to evaluate future innovation activities and to understand the potential impacts on the current cybersecurity infrastructure with safety and security as our primary focus.

The cybersecurity program as it's defined in Reg Guide 571, is a holistic program that addresses the protection for safety, security, and emergency preparedness digital assets through defense in-depth across their lifecycle.

The regulatory guide describes the steps to conduct a detailed analysis of critical systems and the associated digital assets to understand the whole of what's being protected and ensure a comprehensive cybersecurity program.

Kim will walk through these critical requirements for developing an effective cybersecurity program today.

As part of our review of updated standards and other guidance, the Staff have reviewed Reg Guide 1.152, Revision 3, criteria for use of computers and

safety systems of nuclear power-plants and identified appropriate reference points in the draft of Reg Guide 571 to reference to Reg Guide 1.152 prior to EDO direction earlier this year.

Following receipt of that direction, the Staff reviewed the draft and continue to feel that it has clear guidance to encourage the consideration of cybersecurity during design as well as a clear description of the cybersecurity requirements that must be met before an operating license can be issued for a new reactor.

In addition to considering new technologies as they pertain to the operating fleet, we are also preparing for a new advanced reactor design.

As you heard at the July 22and meeting with this Subcommittee, the cybersecurity staff are actively developing a consequence-based framework for advanced reactors with the goal of ensuring an equivalent level of protection in a technology-neutral framework.

We have and will continue to engage with a broad range of stakeholders to gather insights as we move forward rules, techs, and guidance.

We believe that a consequence and

performance-based approach will provide the most effective framework to ensure safety and security given the potential breadth of reactor technologies and the ever-changing cyberthreat landscape.

Issuing the revised Reg Guide 571 is one of our first steps moving in that direction.

The concludes my remarks and I will now turn to Kim Lawson-Jenkins. Thank you.

MS. LAWSON-JENKINS: Thank you, Michele, for the introductory remarks. As was said, my name is Kim Lawson-Jenkins, I'm a Staff Member of the Cybersecurity Branch in the Office of Nuclear Security and Incident Response.

My colleague, Brian Yip, is advancing the slide for me so Brian, let's advance to Slide 2. I'm going to start with an overview of the presentation where I first talk about the key messages of it, the background of Reg Guide 571, and then the inspection program that we've had here at the NRC.

We're specifically getting to the major updates that we had to the reg guide and discuss the conclusion and questions and answers. That will be a final question and answer.

I'm really looking forward to questions and answers throughout the presentation on different

slides to find any clarification as needed. Slide 3?

Since 2012, operating nuclear power-plant licensees have implemented cybersecurity programs and the NRC has implemented effectiveness oversight of the ECSPs. This was mentioned by Michele in her introductory remarks.

I want to emphasize there has been no changes in the Staff's position since the introduction of Reg Guide 571. Only clarifications that we found were needed throughout the implementation of the different programs.

And one new NRC regulation, Title 10 CFR Part 73-77, which was the new rule for cybersecurity event notifications. The draft guidance 5061 reflects the lessons learned that we've had since the issuance of Reg Guide 571 in 2010.

And it's going to form the basis of how we go forward in the future with the program. Next slide, please, Brian.

As Michele also mentioned, there was a presentation to this very same Committee in July and I'm going to just briefly cover some of the same ground because it is really critical to understand the work that we've actually done within the Cybersecurity Branch that's going to be reflected in this new

update.

In 2009, the cybersecurity rule was made effective, that's 10 CFR 7354. And the following year in 2010, the NRC and NEI established regulatory guides guidance for implementing a cybersecurity program.

And both of those documents were deemed acceptable for use by licensees. In 2011, the industry and NRC agreed on interim milestones, Milestones 1 through 7, to implement a cybersecurity program.

And those interim guidelines were implemented in 2012. From 2013 to 2015, the NRC conducted inspections of the milestone implementations. The new cybersecurity notification rule became effective after the interim plans were effective.

And starting in 2107, we began inspections of the full implementation of the cybersecurity programs. During all this time there was a lot of work that was done.

We've worked with industry, generated security frequently asked questions and guidance for the licensees when there was some questions about how to really implement the program.

NEI 1310 Assessment of Cybersecurity

Controls was generated by the industry, which is by a document that says based on the consequence of the devices being protected by the system that's being protected, a set of security controls will be applied.

We participated in several workshops and table-top exercises with the industry to clarify what we saw as appropriate implementation of programs.

So, there was a lot of work going on, not just the inspections but a lot of the discussions back and forth with industry so that we had a common view of what adequate implementation of the program would be.

Next slide, Brian, Slide 5?

CHAIR BROWN: Can you stick with that slide for a minute?

MS. LAWSON-JENKINS: Yes, Slide 4.

CHAIR BROWN: I want to provide just an observation on a perspective.

This is not bad, good, or anything else, it's just an observation based on how back in the 2009 timeframe when we started down this path of trying to deal with the cyber issues, I came on the Committee in 2008, May.

And I actually wrote the letter on Rev 0 for Reg Guide 5.71 for the Committee, along with

George Apostolakis, who was on the Committee at that time as well.

And thinking on the big-picture aspect, we did really focus or understand one of the key points of the introduction part of Rev 0, where you talk about this reg guide -- I might as well, instead of paraphrasing, since I have it open, it said this regulatory guide applies to operating reactors licensed in accordance with 10 CFR 50 and all that kind of stuff.

It very clearly states that. We were just starting into the ESVWR AP1000, the new design Applicants that were on board.

We never connected the dots on the fact that this said only operating reactors was going to prevent the use of these concepts during our review of the new Applicants.

I'm not criticizing anything, that's just a fact. We didn't think about it at that time from that standpoint.

As you're well aware of, we've made that comment several times over the last few years as well as in one of our more recent letters on the ability to use the methods in this document during the certification process for new license applications.

So, I will have some observations along those lines, I'm just giving you a hint as we go through this. You've probably heard me say this 400 million times now over the last periods of time.

And if I look at the new Reg Guide as you all have proposed it, and I happen to have that open also, the applicability paragraph says the same thing only in much shorter words.

It deletes a bunch of other type stuff and I will be making the observation or the suggestion I hope when we finally finish this all up that we need to, and as a result of our letter to Chairman as well in terms of trying to get agreements from everybody.

And EDO's response where it was mentioned that we would be receiving 5.71 and 1.152 and 7-19 to make it more easily utilized under those circumstances.

And so I will probably be proposing something along the line that the methods used described in this reg guide may be used during design certification phase for new applications to ensure control of access, which is what it is for safety systems.

Because they don't have any cyber software in them. They cannot have virus protection software,

it would compromise their normal operations. So, it's really control of access, not a cyber issue.

And that means we really need to pay attention to the communications methods.

So, I'm just giving you a heads-up, I think this was based on the letters and the responses and the EDO's memo to the Commission that this is an ideal place to make some observations in the applicability that the methods used in here can be used for other purposes.

So, I'm just giving you a head-up and a little bit of focus on how we started this 10 years ago, 11 years ago, and how that knowledge of how it needs to be applied needs to be more broadly thought about.

So, that's an opening thought process to keep in mind as we go through here, okay?

MS. LAWSON-JENKINS: Okay, we will discuss this I'm pretty sure, like you said, multiple times through the document.

CHAIR BROWN: There's other items sort of related to that, some are a little more specific, some are a little bit more broad.

One of the things I will bring up, and it's important to note this in the beginning so I'll

bring this up as well is prior to computer-based systems, it was all analog, there was no concern about what I call electronic access to systems.

It was all physical administrative control of people getting down into the plant, opening up drawers, making set-point changes, fixing stuff, adding new circuits, whatever.

When we started using the computer-based systems, those physical security systems don't work. There's no way they will protect you from electronic access.

And therefore, the communications from what I call the safety-related stuff like reactor-trip safeguards, control systems for the reactor monitoring.

And as the Commission noted in a later SRM, there's a number of the balance of plant systems that are also you call them critical or related to safety-type operations, where they can't have their control functions contaminated by cybersecurity software.

So, those become a control of access issue and how you protect those from electronic access, which means you really don't want anybody outside the plan communicating with them.

So, that's the focus we've been focusing on. They key is control of access has changed. It used to be physical, now it's electronic and physical.

And the electronic needs to be more carefully considered during the design phase and that's what we've been talking about over this period of time.

I just wanted to make that differentiation because there's a paragraph in here where I will be flipping the way that paragraph was written to provide some context to it.

But I'm not saying anything is right or wrong, I'm just saying that's the real world and trying to make sure the whole program, that's the NRC, the Committee, and anybody else thinks about it in a manner that's consistent with where we were, where we are now, and what means can you use?

Because literally safety systems, you cannot put virus software in their operating system. You cannot constantly update it, you will just contaminate it, and you will really set yourself up for vulnerabilities with external access downloading new upgrades.

Even if you do it internal to the plant and bring them in, you have to be careful how you do

that, whatever CDs or thumb drives, or however you update the software, you have to be careful you don't introduce problems.

So, anyway, that's just a little bit of history and background also in terms of the way I look at it. I did deal with this in my old program in the naval nuclear program for 22 years as we introduce this stuff from 1977 to the year 2000.

So, if I sound like I'm hard over, I'm very passionate about that if nobody's figured that out by now.

MS. LAWSON-JENKINS: We have a passionate group of people also in the Cybersecurity Branch.

CHAIR BROWN: Thank you very much, Kim, for letting me yodle on here.

MS. LAWSON-JENKINS: No problem. Let's go to the next slide, Slide 5.

I specifically put this picture in the background because whenever I was giving presentations on the cybersecurity program or explaining it, I felt people were focusing very much so on the controls, security controls.

If we apply enough security controls we won't get a violation, not really understanding, or at least not clarifying to us as the inspectors, why the

controls were applied.

And as a computer scientist looking at this and looking at the systems, if you look at the rule, the rule talks about protecting SSEP functions. It does admit critical digital assets, it really doesn't even mention cybersecurity controls.

What it says is there must be a plan in the program to protect computer systems and communication systems that perform SSEP functions. That's what the rule says.

CHAIR BROWN: Can you clarify? SSEP is safety --

MS. LAWSON-JENKINS: Safety important to safety, security and EP.

CHAIR BROWN: Emergency planning?

MS. LAWSON-JENKINS: Emergency preparedness, sorry.

CHAIR BROWN: Thank you.

MS. LAWSON-JENKINS: So, it is safety but also important to safety and we're going to see that a little bit later on in one of the slides. Both the NEI document but definitely Reg Guide 571, which we generated, mentions critical digital assets.

So, these are the assets in there systems that affect SSEP functions. The licensees can

implement their plans apply security controls to the critical digital assets, I'm going to call them CDAs now so I won't repeat the name.

The apply the controls to the CDAs but to do that effectively, it was clear that they needed to acknowledge the attack surfaces and attack pathways. And you've alluded to this, you alluded to this in your discussion on the last slide.

You must understand access control, you must understand how an attacker might try to get into your system and try to gain access to some of these devices. So, this revision of the guidance discusses attack surfaces, attack pathways more.

I think we had the term pathway in there but not really the term attack pathways. We never talked about attack surfaces, which you have to understand when you're look at vulnerability updates and things like that.

So, this yellow circle where it says acknowledge of attack surface and pathways, that's a clarification we added to be able to apply security controls effectively you must have this information or must understand this information.

And we also emphasize continuous monitoring of your plan to make sure that the security

controls were implemented effectively and that they stay effective throughout the lifecycle of the plant.

You don't just apply them at the beginning and not look at them again. They have to stay intact and that is also mentioned in the rule. So, this is the big picture.

It's just not applying cybersecurity controls and saying we've done it, we have a plan.

We have to continually monitor it and look at the effectiveness of those things. Is there any question about this? Member Brown, you said we were going to keep talking about certain things with access control.

We're going to keep drilling back to this knowledge of the attack surface and pathways that we're continuously monitoring to make sure we see the controls that we did apply are effective in the plant.

Next slide, Brian. I'm going to speak briefly about the Milestone 1 through 7 inspections because they are really critical.

They were a great foundation on how to implement a cybersecurity plan in the cybersecurity program, which is pretty complicated.

There's a lot of information and a lot of data that has to be gathered and controls that have to

be implemented to implement a plan.

So, the milestone inspections and the implementation of the milestones was a wonderful first step because they focused on the most critical things.

Number one, there was the establishment of a cybersecurity assessment team, which is a cross-functional across the main team that will be responsible for establishing the program, implementing the program, and making sure the program remains effective.

Milestone 2 was to identify all critical digital assets in the plant in the facility.

Milestone 3 was to implement a one-way deterministic device that would protect the safety, important to safety and security CDAs from plant equipment that was not in the program or that was in a lower security level than the security safety and important to safety equipment.

That one-way deterministic device protects the equipment against unauthorized access from wired communication. You can only send the information in one direction from behind the data diode to a lower security level.

You cannot use wired communication to send information to the devices that protect behind the

data diode. That is the point of that control, that milestone, and it's very important for protection to prevent cybersecurity attack using wired communication.

And I'm stressing that wired communication part.

CHAIR BROWN: I agree with you, actually, and there's and interesting change you all made to the bullets underneath the defensive architecture figure. I think it's now Figure 5 or 6, I don't remember which, where I will bring your point that you just said.

I will kind of emphasize that and how that seems to be being compromised. We're going to have a little discussion on that at some appropriate point here, I'm not exactly sure where it is yet.

MS. LAWSON-JENKINS: We'll be coming to it because we talk about the defensive architecture a few slides ahead.

CHAIR BROWN: I think I remember seeing that when I reviewed the slides. One other comment on the one-way deterministic, there's always an argument about what that means.

In the world I came from before, that meant literally a one-way hardware-based optical

coupler-type transmission device from a safety system to some other system and couldn't be reconfigured by software.

You really literally had to go into the equipment and take it out. Obviously, the data that's just going through the device has all the software because you've got to send fields through it, data streams.

But the device itself only went one way, could not be reversed by somebody tweaking some software command, kind of like your laptops and everything else.

The reason you have bi-directional communication in our laptops, personal computers, and you have what they call deny but accept with exceptions.

In other words, you generally deny bad stuff but you allow good stuff to come in. And there's a software feature that allows that good stuff to come in while it's trying to prevent the bad stuff from getting in.

That's your virus protection on your laptop. So, it's bi-directional is what I'm saying and we see that every day. I don't look as a one way, those are literally one way and cannot be reversed

except by taking out the component and putting in a bi-directional component.

And if you have bi-directional, which is software-controlled, that means there are some type of command structures if you use that bi-directional to make it one way. There's a command structure that says it's only going to function with one of the functions.

So, we've got to be very careful how we talk about it. Deterministic to me is very deterministic, is my only point. It's a hardware base in only one direction, not configured by software.

MS. LAWSON-JENKINS: For a security control in the reg guide that's a security control B.1.4, which is information flow control. And in that one, it says that to implement true one way communication, that you have to have a hardware base.

It cannot be software.

CHAIR BROWN: It's buried in an Appendix.

MS. LAWSON-JENKINS: No, that's the security control. When we write violations, it's usually because --

CHAIR BROWN: I'm sorry, I'm interrupting only because it's in the appendix but it's not adequately reflected up in the rest of text, up in the

beginning parts where all the positions are or the guidance is located.

It's not emphasized as much, it is after the architecture but then there's some other exceptions written. deterministic is deterministic is all I'm trying to say.

Safety systems, when we send data out, it should be one-way, hardware-based, not configured by software and that's a design issue because there's no cybersecurity in those systems, there's no virus software.

It's under the contacts and that's why we've been talking about using these methods for allowing these methods to be discussed during the design certification for new applications.

(Simultaneous speaking.)

MS. LAWSON-JENKINS: This is really important for me to clarify. The Staff position in the regulatory guide is very important because it explains why the plan does certain things, why the program should do certain things.

It's very important. But what the licensees actually implement is Appendix A, B, and C, that is what they implement.

So, while the guidance up front is very

important for clarity and to understand why things should be done, what they are actually implementing is the template that's in Appendix A and the security controls that are in Appendix B and C.

So, that's really important. I'm not dismissing any of the front matter because we want it to be right, we want it to be correct, and be accurate, but what the licensing actually implements is what they have in Appendix A, B, and C.

CHAIR BROWN: I'm familiar with B.1.4. That's the only really --

(Simultaneous speaking.)

MS. LAWSON-JENKINS: -- one of the best.

CHAIR BROWN: It's the only one that's worthwhile. I'm trying to not be negative.

MS. LAWSON-JENKINS: I understand, I do.

CHAIR BROWN: It's very, very clear. I'll let you go on now. Some of this is not only for you all but it's also for me to express it and also for our members to hear it.

MS. LAWSON-JENKINS: I appreciate the dialog, I'm not being facetious, I really do because every time we discuss and explain this, we make the process better.

We try to clear up any misconceptions.

Now we're getting ready for Milestone 4. Because Milestone 3 addressed hopefully why this couldn't be the case but at least is for us preventing a cyber attack, Milestone 4 is going to do hopefully the same thing for portable media and mobile devices.

They have to have some access control for those devices so those SSEP functions are protected

MEMBER HALNON: Kim, this is Greg Halnon, quick question on that. Back in about spring or so of 2018 there was a big industry issue with the monitoring of the kiosks.

Could you explain what the problem or issue was and how it was resolved?

MS. LAWSON-JENKINS: That was actually an issue I had so that's why I can appreciate Member Brown because everyone has some things they think are really important and I thought the kiosk was really important.

If you look at the reg guide, it doesn't say how the licensee should do this, it just says what they should do.

Industry decided on the solution that they would have a kiosk that would be used to scan the portable media and that would verify no virus issue would be introducing any kind of new attack pathway.

You make sure that whatever you're uploading is free of known malware and that's fine, and that's what we wanted to do, that's what it should do. The issue was the industry didn't want to label that diversity as stated compensatory damages, a critical digital asset.

MEMBER HALNON: The kiosk itself?

MS. LAWSON-JENKINS: The kiosk itself. At the end of the day, as an attacker, an attacker really doesn't care what a device is labeled as.

For safety procedures and working at nuclear power-plant procedures are very important because you want things to be done consistently and correctly all the time.

And the same for the humans, we have labels so we can do things consistently well all the time. But the attacker doesn't care, they only care what the function that's being performed on that device and how they can take advantage of the weaknesses.

So, that was one issue I had, whether you call it CDA or not. It doesn't matter, it's what it is, what it does that matters.

The other issue is they implemented a defensive architecture which we'll go into a bit

later, where you have the different security levels.

We implemented the one-way deterministic device to protect Level 3 and 4 from the rest of the network and other security levels.

If you have one device where you're putting portable media into it and it touches all the security levels, you have basically negated the protection that you did for Milestone 3.

So, you have to have a way of -- and the other thing is that there are two ways you can put a security control on a CDA or you can apply a security control to a CDA.

Even the device itself, you can put the control on it, you have to log in to access the CDA and it will track whatever you do on the CDA. The protection is actually on the CDA.

Are you going to apply this protection to something in the environment where the CDA operates? In this case it was the kiosk and the CDA is going to inherit the protection from the kiosk.

So, that can secure the control for portable media access that would apply to the CDA, you're going to say, okay, it doesn't have it really on that device but it's inherent from the kiosk that's operating in the environment.

And the point that eventually the NRC made clear to industry and we agree on in the public meeting is that a CDA cannot inherit protection from a device that's protected to a lesser extent than the CDA itself.

That doesn't make sense. So, they agreed that if you're going to inherit protection from a device, that device has to be protected at the same or greater level.

MEMBER HALNON: Is that concept now in the NEI documents that govern what the industry is doing?

MS. LAWSON-JENKINS: There hasn't been a formal update to NEI 8 or 9. I know in some of the addendums there are some word to that effect, especially when it comes to the portable media.

MEMBER HALNON: Its seems like it's a pretty important point, that you just said very eloquently and clear should probably be in the same way very eloquent and clear in the documents so we don't have to have another public meeting to explain that to the next generation of cyber folks.

MS. LAWSON-JENKINS: You can inherit the protection. In fact, a lot of the examples where we would explain things, actually, the kiosks in the way they got better as we were expecting them.

Because like I said, they were providing protection for the CDAs and we said, okay, if you don't put these protections on the CDA, you must have it on that device, where you get the protections from.

MEMBER HALNON: I get it, I appreciate that, thank you so much.

MS. LAWSON-JENKINS: Okay.

MEMBER KIRCHNER: Kim, this is Walt Kirchner, can I just follow on to Greg?

So, does that mean the portable test devices or something that's brought in to update a critical digital asset actually has to be handled in cybersecurity space at the same level or above the piece of equipment that's being updated?

MS. LAWSON-JENKINS: Yes, that's with anything that touches that CDA.

CHAIR BROWN: Can I amplify Kim a little bit? I totally agree with her.

In this world, Walt, do you remember back in the analog world when you went to realign a set of equipment you had specific test equipment that was calibrated and check and tested before you brought it in to do it.

These days, if you're going to bring in a laptop or some other device to update your system,

download new software or a change to the software in the operating system or change set-points if that was necessary, that laptop now becomes, quote, a piece of very special test equipment.

And it has to be protected and not, in my opinion, when we use those laptops when we started downloading, initially we used to take out the programmable read-only memories, put a whole new one in.

We didn't have to worry about downloading anything. We did it at the factory, we could observe everything, very close controls on every bit of the software so we just replaced the PROM.

But later, we now had e-squared PROMs and we could now not have to go through the manufacturing process. And we found that if we were going to download new stuff using a laptop if we were going to do that, we had to consider that a prime piece of equipment.

And it had no other applications on it. There was nothing fuzzy in it, it could do nothing except transfer data for the specific stuff we put into it. It had no other functions allowed to be part of it.

It did nothing else, it was totally

protected, just as Kim commented on. You've got to put it in a cocoon and protect it to make sure it has no connection to the outside world ever.

MEMBER KIRCHNER: That's where I was going, Charlie, but is that actually what is the practice in the field? Because the temptation --

(Simultaneous speaking.)

CHAIR BROWN: I don't know for industry.

MEMBER KIRCHNER: The temptation to take a multi application piece of equipment in that could do multiple functions or upgrades of safety equipment is tempting, right?

So, how do you make sure that piece of portable or test device is clean absolutely, like you described it, Charlie, where you had a piece of equipment that had only one function.

It's different with an actual laptop. You can bring a lot of stuff with you. And so, Kim, is it required through your reg guide that such a laptop or other device is thoroughly scanned before it goes through access control?

You are ensuring that piece of test equipment or laptop or whatever device it is is thoroughly scanned for malware and any other problem?

MS. LAWSON-JENKINS: During inspections we

look at things that have to do with the portable media and mobile device program. So, we've inspected the procedures being used.

For instance, we look at how the equipment is labeled and whether the equipment is used on a certain security level and how they keep track of those things.

And the procedures when they check out equipment and when they put it back in and any kind of sanitizing.

They have processes for this, they know we are looking at this all the time. And in the end, if they have a defensive architecture, they have to have processes and procedures and technology that will support that architecture.

So, we have seen this on inspections and we've seen effective implementations and sometimes we've seen violations. Every year we look at all the different violations that we've seen, we bend them together, see if there's been progress over the years.

I can definitely say in the portable media and mobile devices, it has come a long way since 2013. There are not nearly as many, if any, violations in that area because we have gotten much better at it.

So, we don't basically say how to do this

but we do look at the procedures to make sure however they are using and implementing their programs, it does not violate the security architecture they put in place and validate the protections they did for the higher security levels.

MEMBER KIRCHNER: I guess my big concern here, my history is dated, I'm from the analog world. But when I look at the potential to bring in equipment that could contain malware, would all these devices be scanned first at access control?

And then what's the standard you scan to? This is an evolving threat and there are a lot of malware programs out there. Is there any standard that you apply?

It's one thing to have procedures, I agree wholeheartedly with what you're saying, how do you keep the malware protection up to date?

MS. LAWSON-JENKINS: Usually, there are different scanning engine that are used for the virus, when you're looking for the viruses. We're talking only about known viruses now.

MEMBER KIRCHNER: Of course.

MS. LAWSON-JENKINS: So, there are different scanning engines to use so usually, at least the kiosk that we've inspected used multiple scanning

engines because then you could get different types of malware, one that may be better as certain types of malware than others.

So, there are usually multiple scanning engines. Just keep in mind, they have a maintenance rule.

There's programs they have from some of their other portable media and they take credit for a lot of that but they still have to comply with what we've implemented for cybersecurity.

Because there was a maintenance rule and a maintenance program in effect, like you said, for safety. So, there is some credit taken for that but as far as scanning and things like that, like I said, we look at their procedures.

When we've seen that the scanning we think might be insufficient there will be observations, warning, whatever, about that. And like I say, right now their programs are effective.

I think that is really I would say one of the positive things that have come out of the program. Because like I said, we didn't tell them how to do this, we didn't tell them how to do Milestone 4 and there was a lot of discussion and back and forth.

Now we're starting to move to different

areas as we get to Milestone 7 of how you keep a program going and make sure the controls were effective. That's where we get more into the vulnerability updates.

So, in a way, I won't say it's a moving target but the focus changes at certain points and it's going to do that for any program over the lifetime of it, especially when you get new threats, new attack pathways, new things like that.

So, it's a moving target, we're always trying to stay ahead. And the things that were implemented in Milestone 1 through 7 really did a lot to make the programs effective.

There was work to get them to where they are today but this was a great foundation and I can't say that enough, as someone who came in after this was all decided.

MEMBER KIRCHNER: You can't see me on video. I'm shaking my head saying yes so thank you for your response.

MS. LAWSON-JENKINS: Obvious signs of tampering, that's Milestone 5. That's for the physical attack pathways, there are five attack pathways and we are going to discuss three of them here.

It's the wired pathway, the portable media and mobile devices, and physical access. Milestone 5 helps with physical access a little bit, seeing what's being done with the equipment to see whether or not you have unauthorized equipment attached to a CDA.

Someone shouldn't be powering up their mobile phone using a computer. I admit it hasn't happened but that's my point.

When the guards were doing walk-arounds looking at things, or even employees, they would see and make sure that nothing other than work equipment should be attached to CDAs.

Milestone 6 was getting a subset of CDAs identified in Milestone 2, and applying security controls. So, this was to start looking at the methodology that was being used to apply security controls to CDAs.

And in Milestone 7, once those controls were applied, then you just don't apply them and forget about them. You have to monitor and make sure they're still effective and are operating correctly and doing what you expect them to do.

So, this was the foundation that we built on it and like I said, I think the industry and the NRC has really done well in this.

MEMBER KIRCHNER: Kim, this is Walt Kirchner again, I don't have up to date experience in the plant like Greg does. In practice, is there a more restricted access?

Does this imply more restricted physical access to things like reactor protection system and such? Is that what you mean by physical security controls or a higher level of digital --

MS. LAWSON-JENKINS: It depends but unfortunately, with security it depends. The licensees have leveraged very much two things in their program, the physical security if they're being used.

So, a lot of the physical and digital assets are located in protected and vital areas so they're going to leverage that. And obviously, the wired communication that this equipment is protected by a data diode.

So, I think what you're getting into then is more of a safety security interface question. How many technical controls are you really going to apply on the devices located in the most protected area? And that will vary.

MEMBER HALNON: Walt, I think the answer to your question is yes and the physical controls.

Since this was...I hesitate to use the

word backfit but a lot of things were looked at that were outside protected areas and the items that were in the past able to be accessed or physically in the general vicinity of people.

It's much like the FERP controls where you have separation of duties and you have separation of now physical access to certain rooms and other things like that. So, there are some of both put in place.

MS. LAWSON-JENKINS: A lot of the equipment we're talking about when we see the protected area, they are on Level 3 and 4 behind the data diode and those are dedicated computers.

Obviously, they're not talking to anything on lower levels and we'll be coming up to some more information but a lot of CDAs, including BOP are protected on Level 3 and 4 also.

MEMBER KIRCHNER: This has implications for -- your colleagues are working on 10 CFR 53 rulemaking and to do what Milestone 6 is implying as well as Number 3 in particular, it seems to me if you can do a lot of that by design upfront, like Greg said, with the existing plants, you're in a situation where, I'll use it, quote, unquote, a backfit kind of might be necessary to restrict physical access, et cetera, et cetera to those the most important critical

digital assets.

But going forward, it would seem to me that when one starts laying out the architecture for the INC and the plant, both in terms of electronics if that's the right word and physical space locations, then one can be I think much more effective in marrying the digital cybersecurity to the physical cybersecurity to implement this much more efficiently and effectively.

Do you see where I'm going? Just by a layout of plant, the back cabinets so to speak, where they are, who has access, how you do that, how you design the system it would seem.

CHAIR BROWN: Walt, let me provide an example of what we're talking about. Kim, one of the recent things we've looked at, reviews we did, that had the reactor protection, the safeguards, and that data was sent out.

We forced a one-way deterministic device that took some time to get people to agree, and then it went to a network. That network was connected to the outside world.

We insisted that there was an in-plant network that then went to an out-of-plant network. We insisted that in-plant network that received the

reactor protection and safeguards data and other data from other safety systems, its output had to be one way only.

It was in plant so that you had two barriers to the outside world. The initial, the in-plant network had a bi-directional software-controlled-type data transmission device.

And the Applicant eventually agreed to make that unit directional from the in-plant to the out-of-plant.

That's what we're talking about, that's a design issue but there's no virus protection systems, there's no software that you put in the systems, it's just literally a hard no door is allowed.

You're not allowed anybody in. You still have the physical access, people want to make changes when they walk into the plant. That's a physical thing, back to where we were 20 years ago.

So, that's what we've been trying to focus on and concentrate on to simplify and ensure the software systems don't run the risk of being connected to something, either a lower safety system or something that goes out external to the plant that they can't be backfit, malware or other types of problems.

That's why we've been insisting on literally one-way hardware based non-software controlled deterministic, lots of words, I love those words, data transmission devices.

And you can't come back through it the reverse direction no matter what you do.

MS. LAWSON-JENKINS: And on the screen now, Brian, advance to Slide 7 and that's what you see right now between Level 2 and 3. All the CDAs that have to do with safety, important to safety, security, are located on Level 3 or 4.

So, they have protected behind the data diode for wire connections.

MEMBER KIRCHNER: I like that but then if you look over from Level 4 to Level 3, that network could have been a Level 3 and you show a firewall. And a firewall is a bi-directional software-controlled data transmission device.

MS. LAWSON-JENKINS: That is true.

MEMBER KIRCHNER: So, that little white arrow becomes meaningless if you've got a firewall that's your main protection for it.

MS. LAWSON-JENKINS: It is not as strong, I will absolutely agree, up to a point, because it is possible to have a data diode inside of that device.

MEMBER KIRCHNER: You can? You could have done that but --

(Simultaneous speaking.)

MS. LAWSON-JENKINS: -- solutions, we do that in DoD because I worked on those.

MEMBER KIRCHNER: But you don't want that data diode to be able to be cut out because somebody wants to come in and do something for their own convenience.

MS. LAWSON-JENKINS: I understand and I agree but you have to understand, this is why I want to make the point about the data diode. One reason why it's a great device is it's very simple.

It's very easy to see it's doing what it's supposed to do. It protects for wired connection. With defense in-depth we have to do more than just prevent. There's no detect for instance, no detection function with a data diode.

It won't tell us that someone was trying to attack the network. There's no recovery detection, it's just preventative.

What that firewall will be doing is also monitoring communications and it could be looking for things, it could be detecting things that shouldn't be happening.

So, not alone but the firewall with the data diode is used to provide the defense in-depth.

CHAIR BROWN: Let me ask on the firewall then. You're describing a firewall which is not a data transmission device but a monitoring device that's sitting there to tell the operators somebody is trying to get in somewhere?

(Simultaneous speaking.)

CHAIR BROWN: But the problem with that is can now somebody come in from the outside via that and contaminate that network which is literally sending its data through via one-way deterministic devices?

You now have a connection to the outside world, effectively, and that's one of my concerns. I understand your monitoring point but when you do that monitoring function, it should have no connection to the outside world.

It should be an inside the network monitoring function and not connect outside the plant. It should connect inside the plant what's going on, not outside the plant.

MS. LAWSON-JENKINS: What connection to the outside world are we referring to?

CHAIR BROWN: An Internet connection.

MS. LAWSON-JENKINS: There is no Internet

connection there to the outside world.

CHAIR BROWN: Theoretically, you talk about a firewall, that firewall is monitoring something.

MS. LAWSON-JENKINS: It's moderating the communication between Level 3 and 4.

CHAIR BROWN: Who is it talking to?

MS. LAWSON-JENKINS: It will be pushing whatever it sees down from Level 4 to Level 3, and then from Level 3 to Level 2.

CHAIR BROWN: Who's going to be receiving that information to know there's something going on?

MS. LAWSON-JENKINS: Probably someone outside on the lower side of the firewall. Information is pushed out from Level 4 to Level 3, from Level 3 to Level 2, and then it's sent out.

CHAIR BROWN: So, it can't get out at Level 3 is what you're saying based on those diodes and the arrows?

MS. LAWSON-JENKINS: It does get out. There's no communication --

CHAIR BROWN: I'm sorry, I meant one way. That's not a bidirectional signal from Level 3 to 2?

MS. LAWSON-JENKINS: No.

CHAIR BROWN: Let me ask, I see this nifty

little diagram with your firewalls and data. When I look in the Reg Guide, that picture is not in there, it's nothing but white arrows.

MS. LAWSON-JENKINS: -- in all these diagrams. Because I knew this discussion we're going to focus on information flow control and access, I put this diagram. Even the one in the reg guide is a notional diagram.

CHAIR BROWN: I understand that but it's not as definitive. If I look at the reg guide I don't see fire walls. The appendices talk about firewalls but they don't relate the firewalls to this architecture.

Do you understand what I'm saying?

MS. LAWSON-JENKINS: The appendices talk about the controls or things that we expect boundary devices to do and one of the things we expect boundary devices to do is to monitor communications and to possibly enforce the communication rules that we have within the levels and across the levels.

So, that's why I said a boundary device. So, as I said, the data diode does one function, it prevents communication going to a higher security level but that's all it does.

Boundary devices have to do more than just

that, which is why firewalls are also used, in conjunction with the correct placement of a data diode. It would not be an adequate implementation to have only firewalls.

CHAIR BROWN: I understand your point on that. My concern is the firewall is there and can it get into the input side of the data diode such as that it now has access to the reactor protection system?

MS. LAWSON-JENKINS: All it can do is push information down from Level 3 to Level 2 or Level 4 to Level 3. That's like saying the data diode is very simple.

CHAIR BROWN: I got that on the data diode but the firewall is monitoring and it's monitoring everything in there, including the input side of the data diode. Anything that comes in, if it's monitoring, that means it's got access.

Can I go backwards back to the reactor protection system?

MS. LAWSON-JENKINS: The firewall, whether it's implemented as the data diode or not, is going to have to be part of the defensive architecture. I always say the things that are Level 4 are inheriting the protection of the data diode that's sitting on Level 3 and 2.

CHAIR BROWN: I may not be making myself -- the reactor protection system, and I'm sorry to belabor this, I just need to understand what you're talking about. It's a good conversation, I appreciate it.

I'm just looking right now at one of our other plants. We were sending data out, the data diode was right out of the RPS, the next one had a data diode, sending it some place outside the plant.

And now we're talking about somewhere in there, I don't know which side in the reactor protection system, there will not be a firewall looking at the input side of that data diode, coming out of the RPS.

There was nothing in the design that said that. But when I get to the network, you've got a lot of stuff in the network.

And so I understand the notion from 4 to 3, going from you've got other stuff coming through and you've got something to monitor what's in that network.

Is somebody trying to get into it even though its only communication outwards is via a data diode to Level 2? So, that firewall has to be monitoring what's in all the memory, what's operating

and everything else, which is on the input side of data diodes.

And if it's on the input side, it can go backwards into the rest of the systems that are feeding everything.

So, if the firewall had some contamination in it, corruption or malware, you then end up getting something transmitted back into the reactor protection system.

I'm all for monitoring but monitoring can be a double-edged sword.

MS. LAWSON-JENKINS: Anything you do, and I will agree with that, anytime you do anything, there's always a chance that someone can misuse it.

We see that in security all the time, when you put in the protective mechanism, whether it's downloading new software or whatever, and the attacker misuses that for their own purpose and will attack.

But that is why we've always been very stringent, as we said for the kiosk, for certain devices, this is an important point, where it's protecting multiple devices, you're going to have to protect that device at a high level.

So, that firewall has to have some self-protection mechanism to say something is going wrong,

I'm not working, something's not right. And then that's when some other mechanisms will kick in.

I absolutely agree with that anything we have a high-level 3 and 4, it in itself may be a problem but that's why those protective devices, those devices that are applying protections to the environment where the CDAs are operating, they themselves must be protected.

Like I said, this has been a mantra with us for quite a while.

CHAIR BROWN: I was interested in this because I was reading when I read Appendix B122, use of external systems, where you have one-way deterministic stuff specified, and the words are fairly clear.

I didn't have any problem with this so I'm not going to be giving you any suggestions. Because it says ensuring external systems cannot be accessed from CDAs located behind a one-way deterministic device.

MS. LAWSON-JENKINS: That's Level 3 and 4?

CHAIR BROWN: Yes, they're behind it.

MS. LAWSON-JENKINS: But it goes on to say, any manner that would result in a bypass that enables communications from lower to higher levels,

which is key. I'd love to be 122, I'd love to be 14, and C7 is also pretty clear.

Although a bunch of the appendices are littered with firewall determinations and where those get applied is interesting.

Because you don't see those during the design phase when you're just showing how the data get transmmitted from a reactor protection system to the outside world, through a network or not through a network.

It should be a one-way device and then you see the firewall thought process and say, hold it, is that going to impact? Can that now go backwards?

MS. LAWSON-JENKINS: For cybersecurity there is no way of getting around implementing defense in-depth. It is crucial that we can detect, respond to, and cover from cyber attacks.

And we cannot just rely on prevention because we have seen over the years in this last decade, and even further in cybersecurity, your protections can be circumvented.

I'm just making this general statement. You can have data diodes, you can place them in the architecture, and if you don't know all the communication pathways, that defense will be

circumvented.

CHAIR BROWN: I don't disagree with that. That's a terrible double negative, I'm sorry. I've got to reprogram my English courses from sophomore year in high school.

When we do a review on the design side for an Applicant, we get a very detailed one-line functional diagram showing all communication paths as well as showing that you maintain independence along with the redundancy.

Control of access is a major issue for us during our new application or new license application, new plant design application.

And if you look at the way it's shown, we have data leaving the reactor protection system via a couple of paths, both of them going through deterministic one-way hardware-based diodes.

We insisted on that and that goes out to the main control room and every place else, as well as they can go to your technical support center and can go to your emergency preparedness or emergency support center, whatever they're called, so people know what's going on data-wise.

That is a device, it's right in the bottom of the cabinet, if you want to call it that, or it's

on the circuit card with the computer operating system, the computer platform.

So, that is the pathway so I'm happy with that pathway but people keep telling us we can't talk about that in the design phase. That's just wrong and that's what we're trying to alleviate, is people telling us we can't ask that question.

And if we ask the question and they say something we're not going to make a regulatory determination on it.

And that's disturbing because you can't do anything else in the safety systems with any other type of virus protection the way you do in all the other systems, what I call normal use systems.

Administrative, business, recordkeeping, maintenance, training, et cetera. And the one-way device coming out of the RPS should not have a firewall sitting with it because it's only one wired connection going one way.

I understand the concern but the only way you're going to get bad stuff in is if you bring it in via somebody changing the software. And that's a case where you have to make sure you've got clean software that you plug in.

You can't vet anything in the system to

try to say it's not because you don't know.

MS. LAWSON-JENKINS: Right now, the way the systems are made, we have multiple CDAs on Level 3 and 4.

CHAIR BROWN: I'm just talking about 1.

MS. LAWSON-JENKINS: I understand that, I do.

CHAIR BROWN: -- control, there's all kinds of CDAs, if you want to call them that.

MS. LAWSON-JENKINS: Exactly, and they should be monitored and seen if appropriate information is going to cross there because there is as a computer scientist there is no perfect software.

There is no software that you install once and you don't ever have to touch it again.

CHAIR BROWN: We are in great mind meld relative to that.

(Simultaneous speaking.)

CHAIR BROWN: -- brains and we will be working just fine.

MS. LAWSON-JENKINS: So, obviously, we're doing risk-informed security so you want to minimize the risk on this. So, we have to have defense in-depth, like I keep saying, where we have to monitor --

I'd rather get to this later, I don't want to keep jump in around.

CHAIR BROWN: That's okay, we'll do that because I would ask you what does it mean risk-informed, we can have a little bit of hiking but not too much. I just filled that out and we'll talk about that later.

The point I'm trying to get across is we're trying to ensure the Committee and other folks that are doing the reviews, the NRR Staff, when they're reviewing a new design, can look at these systems.

And they can look at them in what's delivered by the vendor, not all of the ancillary stuff throughout the plant, not worthy interfaces, but the data they send out. The access they have in is blocked, prevented.

And we can argue about, well, we're still going to have monitor the system, you have to do that via other means.

But we still want to make sure there's a one-way deterministic device preventing other external to the plant stuff getting fed back in through networks or whatever because at some point, a couple of levels down, they're connected to the Internet,

like in Level 2 or 1.

MS. LAWSON-JENKINS: Really, the last point I want to make on this is that safety always trumps security.

We would not introduce something, the NRC cybersecurity inspection team, would not allow a safe security requirement to be introduced where we have to monitor that will negatively impact the safety.

CHAIR BROWN: I got that, I agree with that and I'm glad you said that, I like that statement.

That's not what we've been dealing with, we've been dealing with people saying you can't determine or make a determination that a one-way deterministic device is required for transmitting data.

We had a vendor that wanted to do it bidirectional so it could go both ways, right into the protection system. We said no and they eventually caved. But we're told by the Staff they can't make that guidance determination.

MS. LAWSON-JENKINS: I'm going to let NRR make that case.

CHAIR BROWN: But you're the king here. All I want to do is make sure that when we're

reviewing designs, and I made the comment in our letter, Reg Guide 5.71, we did this 11 years ago.

It had very strong protections that were put in there for these types of things but we were told we couldn't use it because it can't be done until the combined operating license standpoint or some time later once all the equipment is designed.

It said you've got to be kidding me.

MEMBER KIRCHNER: Charlie, this is Walt. May I interrupt a moment?

CHAIR BROWN: Absolutely.

MEMBER KIRCHNER: I wanted to ask, Kim, what is the set of systems that resides in Level 4 as a result of this reg guide? Is it beyond the reactor protection system to include security protection systems, et cetera?

Because I think what Charlie simply is saying is that visually, that one-way data diode between 3 and 2 needs to be switched with the firewall between 4 and 3.

CHAIR BROWN: What else resides in Level 4? Are there systems beyond those? Because what you said is very important, safety is more important than security in the end. You have to look at that systematically too to see.

Security can always have a big impact on safety and consequences. But what systems would reside?

Is it not possible to construct an architecture not to make complexity but let me just rhetorically say Level 5 are the core reactor safety system functions that you need to protect, no matter what. And there's the data diode for those systems.

You can figure out ways to monitor whether such systems that have been tampered with and such by a physical inspection. And then at the next level, you may have lower important systems.

I'm not finding the right words, your security systems and so on, and actually, you would have a double data diode in my mind.

But I'm with Charlie that I just can't see how you can risk the reactor protection system, in particular, and all of its subsystems, just so you can monitor it.

That opens a door -- this is not my field but to me, in this world we're working in that opens the door to a potential -- it creates a vulnerability for the reactor protection system.

MS. LAWSON-JENKINS: Please keep in mind this is a notional diagram. I have seen system

architectures where you have multiple data diodes on Level 3 and 4, depending on how they architected the system, and that is information flow control.

So, they determine between whether it's a security system, BOP, important to safety, whatever, or safety system. They can have, and they do, I've seen implementations of multiple data diodes behind Level 3 and 4.

So, this is just an example of how to do this.

MEMBER KIRCHNER: I totally understand that.

MS. LAWSON-JENKINS: So, we look at it on an individual, plant-by-plant basis of how they did that.

MEMBER KIRCHNER: But you're thinking operating plants.

MS. LAWSON-JENKINS: Yes, I am.

MEMBER KIRCHNER: We're thinking new design plants where we have commented and asked to ensure there is a one-way data diode for data transmission out of a reactor protection system, safeguard system, those associated, if they feed the pumps and valves and controllers so that those systems, if they're computer-controlled, can't feed

back.

And the data that goes out to the other network and stuff has that one-way diode.

If you think about it in the old days in the analog systems, all your data, meter data, switch data, it came out through wires and terminal boards at the bottom of the cabinet, or on connectors.

That connector has now been replaced with a one-way data diode or should be, but that in the design phase when we're doing a new design. And right now the reg guide says this only applies for operating reactors.

MS. LAWSON-JENKINS: The rule, the cybersecurity rule, applies.

CHAIR BROWN: But they're saying, therefore, because the rule only applies to operating reactors, we can't say anything in the design stage.

MS. LAWSON-JENKINS: The rule says that you apply the plan and the program when the plant becomes operational.

CHAIR BROWN: Exactly.

MS. LAWSON-JENKINS: That's what we're following.

CHAIR BROWN: We can't backfit a data diode at that stage. You don't go back in and

redesign the equipment when you get five or six or seven years down the pike and you're now about to go operational.

MS. LAWSON-JENKINS: I'm not dismissing this because we are going to keep addressing this throughout the discussion by one of them to advance this a bit but to keep responding that the firewall isn't talking to a lower level or Internet past the data diode.

And also, for better or worse, this equipment that's located on Level 3 and 4, it probably will need to be updated, once in its lifetime at least. So, you will have to have some mechanism of performing updates.

I'm not even talking vulnerability updates. There may be maintenance that you have to do on that equipment and that's why we have to monitor and detect and respond to possible cyber attacks that have somehow bypassed that protection of the data diode.

So, that's all we're talking here. I understand the issue about design but I want to make it clear that nothing behind Level 3 and 4 is talking to the Internet.

MEMBER PETTI: Can I just ask a

clarification? This is Dave. The firewall shown between 3 and 4 notionally, you have it so that you can monitor. That's an intranet, not an internet?

MS. LAWSON-JENKINS: Intra.

MEMBER PETTI: I understand that, thank you.

CHAIR BROWN: You're correct. We'll quit discussing this, you're pointing out that the rules applies when the plant goes operational. We're working back at the license application with the design certification documents.

Let me finish real quick. We're being told you can't do anything of what we're talking about because it can't be addressed until seven or eight years later until the plant goes operational.

And therefore, the vendor can do whatever they want, we can't ensure there's one deterministic data flow out of the reactor protection safeguards, rod control, whatever systems you want to talk about if they've got communications or monitoring.

We can't address that in the design phase which, to me, that means I can't complete my design. And just because the rule, that's cybersecurity and I say there's no cyber in there, it's just control of access.

And yes, our design documents talk about control of access and the IEEE standards and everything else. That was fine back in the days when control of access meant you had to go pull a drawer open and go muck around with a potentiometer.

It's not like that anymore, control of access now is introduced, the electronic access, and we're just stuck with this log jam of trying to utilize the good stuff that's in this reg guide, because it's really quite excellent.

It's got really good information, it's well thought out, and it covers a lot of territory.

And we're told you can't even think about some of these concepts of data diodes and incorporating them at the design stage so that the equipment does have a door that you may want to do something else with later with other techniques.

But at least from that level of protection, it's already embedded in the design and we're told you can't deal with that. So, I have already mouse-milked this to the extent that I've destroyed your entire presentation.

And I apologize for that, Kim you've been very, very patient and you've done an excellent job. You've made it very clear where the rule applies.

It's a question of how in the world do we provide some clarification in this reg guide because it's one of the three to be looked at for providing guidance for design stuff, 719, the defense in depth and diversity stuff, and the 1.152, which largely deals with physical control in most of the cases.

That's where the hard spot is but you've made it I think more understandable to us to see how that's viewed.

And what I've been looking for is how can we provide some clarification under just the thought process, the big-picture applicability and a few other places that, hey, look, these methods are good and can be used in license applications for new plants.

And it's kind of interesting, in 5.71, it's on Page 6 I think, there are the words kind of. Everybody is shooting themselves in the foot is what I'm really saying.

There are words that say here's Page 6, the last part of the stuff where it's talking about Rev 3 of 1.152, this is under background.

It says if a licensee or Applicant chooses to address 73.54 through the use of design features, it then submits the details of those design features of the safety system intended to meet as part of the

license amendment request or design certification application for review and approval.

In such cases, the NRC will review these features in conjunction with the system's safety functions, only in conjunction with the safety functions, to ensure the reliability of the safety system is not adversely impacted by the inclusion of these security features.

In other words, right there it says we can do this because it will be reviewed only in terms of is the safety system reviewed? Not a cyber review. And I like those words, I would just like to have some additional stuff.

MS. LAWSON-JENKINS: I hope you can hear me.

CHAIR BROWN: Did you hear me? Are you there, Kim?

MS. LAWSON-JENKINS: Yes, unfortunately, I'm getting a bad network quality indicator here. So, I turned off my camera hoping that I don't --

CHAIR BROWN: I'm just saying your words under the background on Page 6 refer to this even though these were intended to meet cybersecurity stuff, really, they're for safety system applications, the way it said, to ensure reliability of the safety

system is not impacted, et cetera.

So, I just think those could be unfuzzied a little bit. I haven't quite figured out how to do that yet but that's what I've got in mind for amplifying this to make the example that, hey, you can't have virus protection.

But for safeguards, safety systems, control, as well as other critical balance of plant stuff, these can be used. So, it shouldn't impact that, it's just trying to get the thought process across it.

This reg guide has good stuff in it and it shouldn't be deferred for seven years after the DCD has been approved.

MS. LAWSON-JENKINS: I just want to suggest we keep going further because I am hoping, not all of them, but some of your issues will be addressed as we discussed them.

But I want to make a few more good points here.

CHAIR BROWN: We're ready to go.

MS. LAWSON-JENKINS: So, this diagram just shows the whole process again, altogether, of how the assessment, determining whether the CDA issue is really important, that's the upper on the right side.

The defensive architecture implementing that is extremely important, then applying the security controls which we do for Milestone 6, which includes looking at the physical security and making sure nothing's being connected through the assets and Milestone 5 and monitoring those security controls.

So, I guess you could say, the big picture for Milestone 1 through 7. Brian, Slide 14?

MEMBER KIRCHNER: Kim, this is Walt Kirchner, the logic, the flow structure of this makes good sense. I don't have anything to add except for I think where Charlie is going in part is this is how you approached it with existing operating plants.

And some of those plants are obviously implementing more and more digital assets and controls. But if you were looking at a new plant starting from scratch, the thing you would really want to do is number three first and then the other parts would follow.

Do you see what I'm saying? So, what you have right now is what you have with an operating fleet.

What could be done to improve the level of cybersecurity protection for new digital INC system for an existing plant or for a new plant would be to

implement the defensive architecture first in the design and then apply everything else that you identify.

MS. LAWSON-JENKINS: Two things, a comment on that. Was that a question that you expect me to respond to? I can.

MEMBER KIRCHNER: I guess it was a statement or just an observation, leave it as an observation.

MS. LAWSON-JENKINS: We'll leave it as an observation now but we'll probably come back to that.

CHAIR BROWN: Kim?

MS. LAWSON-JENKINS: Yes?

CHAIR BROWN: We've gone over the break time. Is there a break point here where we can take a break for everybody? I was looking forward in the slides, the rest will go fairly quickly since we've mouse-milked this on most of these slides.

So, if you want to proceed I think we can get to the overview slide, 18.

MS. LAWSON-JENKINS: Let's go through these because there isn't much more on here. On top of Milestone 1 through 7, we added the full implementation of the cybersecurity program, which is what is shown at the bottom of the screen.

Like I said, you saw this during Jim's presentation in July so I'm not going to add a whole lot of value here. I think we went over the main part, which like I said, everyone has been focusing on, the architecture.

Next slide, Brian, please. And we've discussed this also in a way. I've said we've had inspections, at least for Milestone 1 through 7 I want to give you the information here.

We had 63 inspections and the all of the findings from the inspections were of low safety significance but the areas that we saw the highest number of findings were CDA identification, MMD, handling, and the type of controls that were applied when they said they were applying the protections.

CHAIR BROWN: On identification why is --

(Simultaneous speaking.)

MS. LAWSON-JENKINS: It's this whole issue that I mentioned before when the licensees, some of them said we don't believe this device to be labeled as a CDA.

And the guidance is pretty clear, at least what we had, for the acceptable method of doing this. We were calling CDAs and why and we've actually added clarity to that in this.

If you look at the updates, the difference between what we've said in the original guidance, we talked more about the pathways and how they are to be protected and why they should be labeled as CDAs.

Once again, I really want to emphasize this point, we call these things CDAs for humans, for us, to make sure that we are applying protections consistently with the methodology that makes sense.

And also, that you're protecting the right things, that you have thousands of pieces of equipment, a plant. And this is where the risk-informed, consequence-based security comes into play.

You cannot protect everything when you look at your computers and when you get the updates for virus protection. They do not apply all the virus protections they can to your computer or it would never work.

So, the most important thing is to come up with a methodology, saying these pieces of equipment are the most important things in our plant and we have to protect these functions.

This equipment is associated with these functions and we need to label them as CDAs. But there is no hard and fast rule and when we saw devices

that we said, no, this can affect the safety and security or important safety functions.

Why is it not protected when you called it a CDA or not? That's where we will mark something against Milestone 2, because if it had been labeled a CDA, some protection would have been applied.

So, we bin these things based on the actions we saw. If things were not even labeled as a CDA, it wasn't identified as a CDA and if you don't identify the CDA, then most certainly you won't apply the protection.

So, that was the issue.

MEMBER KIRCHNER: Kim, this is Walt Kirchner again. We often, all of us, I think too loosely throw out this phraseology risk-informed. So, let me ask you a rather pointed question.

You're inspecting existing plants, most of these plants have a full PRA.

Do you use the PRA as the arbiter -- let's put aside physical security for the moment and just talk about safety functions. So, more the classical safety side of the FSAR rather than the physical security side.

Do you use the PRA has a means to inform what are the critical digital assets? Because if it's

just a question of everything that's digital, you could get into a number of honest professional disagreements about whether it's a critical digital asset.

If you fell back on your PRA to demonstrate that this is of no serious consequence in terms of our licensing basis with regards to dose consequences, et cetera, is that a way to arbitrate, so to speak, what's a CDA and what's not?

MS. LAWSON-JENKINS: That could be a way. I support that mechanism to look at a Level 1 PRA to identify scenarios that lead to catastrophic consequence that would be a method of doing that.

But at the end of the day, it's the licensee that has to apply the methodology and they have to explain it to us of why things were chosen.

To me, using something like a PRA would be great for consistency when they were making the explanation. So, I would very much support that mechanism but we don't tell them how to do it.

We give guidance and like I said, I absolutely agree that a PRA would be one mechanism of doing that.

But it really, and this is what I don't think a lot of people understand about risk-informed

security, comparing it with compliance-based security, the onus is on the regulator or whomever is doing the compliance when you're doing compliance-based.

Because you're saying you must do this, this, this, and this, a list of things and they have to comply with it and they check off a list.

With risk-based security the onus really shifts more now to the people who are operating the network or the plant, where you give the evidence of why you chose whatever you believe is important to protect and that you did it adequately.

So, there's more evidence to provide instead of just saying you comply with something. So, there's a balancing act there that I think people didn't recognize.

But to be candid, I think it's necessary because of all the different implementations of cybersecurity plans, different types of equipment they'll have in their network, that it has to be the complexity of the equipment itself.

It would have to move in that direction regardless.

MEMBER KIRCHNER: Thank you.

MEMBER DIMITRIJEVIC: This is Vesna Dimitrijevic. Walt brought something really important

that everybody talks about, risk-informed, but the risk is very different based on what application we are discussing.

So, even you don't really tell them what to do, you should really have some basic definition what the risk they are concerned with, you know?

So, in their application they really know what to looking for. You understand what I'm trying to say, if you are risk-informing something you are measuring that it covers some risk importance.

In that case, what is the risk discussing? This usually consists of likelihood and consequences. So, it should be some general high-level discussion on that.

MS. LAWSON-JENKINS: And we do, if you look at the section of the documentation that discusses how do you identify CDAs? We say some of the considerations you should look at when you're identifying CDAs.

We're pretty explicit, we give general guidance on that and in addition, then we say when you choose a defensive architecture, the things that you have identified have to do with safety and importance of safety and security, have to be protected at the highest levels in your defensive architecture.

So, the technical controls you apply, the operational controls, and the administrative controls should apply to defense in-depth at the highest level to protect those assets.

So, we do give guidance on that and we do talk about the type of functions, safety and security functions, that need to be protected.

The NEI guidance that they are generating go into more detail of how to do that but we do give a guidance on that and I absolutely know that some of the upcoming work, as you keep saying, for the new reactors, we're going to be discussing how you identify these assets.

Let me go on.

(Simultaneous Speaking.)

MS. LAWSON-JENKINS: I'm sorry.

MEMBER DIMITRIJEVIC: Just saying thanks.

MS. LAWSON-JENKINS: Okay, Brian, let's go to Slide 16. We have really discussed a lot of these issues already. We clearly have discussed the deterministic devices.

We've talked about data integrity, which is a huge issue when you're transmitting the data to make sure only the authorized people get access to something and it hasn't been modified by unauthorized

people.

How we move data between security levels and maintain the integrity and the treatment of maintenance and these equipment, we've actually discussed all these issues.

Next slide, Brian. After we finish Milestone 1 through 7, that was the first time the team looked at updating Reg Guide 571, so we started this in 2016 and that was at the beginning of the full implementation inspections.

And in the subsequent years, we finished them actually this year in 2021, we completed all the full implementation inspections of operating licensees. Next slide, Brian, Slide 18.

I guess we can probably have a break because we'll get into more details of the updates. I really want to mention Member Brown and the other Members that we will talk about technical security controls.

I think you'll see that in the slides because as I mentioned before, when security controls were applied, there's a choice of applying them on the device themselves or applying them in their environment.

And for what your concern is, which I

understand, the design of the equipment, that licensees can and they should impose requirements on the people who they're obtaining the equipment from.

That is where those technical security controls are going to be implemented, that they would use just like the kiosk and other devices, the CDAs and here are the controls.

Basically, those controls that are installed actually on the device, on the equipment, the licensee will claim credit for that when they implement their cybersecurity plan.

So, it does all fit together and we do have mechanisms in the guidance that discusses security being sent down to the people who are developing equipment.

CHAIR BROWN: Yes, the secure development environment is what you're talking about I think.

MS. LAWSON-JENKINS: Not just that, there are actually security requirements, as I said. If you have a technical control on the CDA, it didn't just get there.

You may buy the equipment that has it but if the equipment is being designed, it is applicable for the licensee to say to the vendor we need to this security control to be implemented so that we can have

a cybersecurity plan that will meet the regulation.

CHAIR BROWN: This has been a great discussion, I think it's really been illuminating and I hope it helps the Members to understand the overall issue as well.

The thing I'm continuing to struggle with is I don't view a data transmission device coming out of my cabinet as necessarily being cybersecurity.

I look at that as a backstop or control of access issue because I don't have any of what I call the traditional, cybersecurity-type controls, which are virus detections, monitoring and all that other kind of stuff.

I'm just looking at a hardware design and how do I make sure I've got that overall system protected from electronic access through all of its transmission needs.

There are other things cyber-wise that have to be done for the overall plant and the stuff it interfaces with, et cetera. But those will come later.

But some things need to be looked at and they can be used, they help you from the cyber world because they're there but they're also there from the design standpoint of the equipment.

That's just been like sucking blood out of rocks to get through that issue, pardon my example.

MS. LAWSON-JENKINS: So, it's up to you, whenever we can take a break it will be fine.

CHAIR BROWN: We're going to do that right now, we'll take a break. What time is it? It is 11:27 a.m., we'll go until 11:45 a.m., that will give us 18 minutes. Is that enough for you and your dog, Walt?

MEMBER KIRCHNER: Could you afford 20? No, that's enough.

CHAIR BROWN: I'll give you 20. We'll make it 11:47 a.m., I'll give Walt 20 minutes. I've got to take my dog out also so nobody's talking about it. 11:47 a.m., we will recess until then and thank you very much for all your patience, Kim, it's been wonderful.

MEMBER KIRCHNER: Thank you.

(Whereupon, the above-entitled matter went off the record at 11:27 a.m. and resumed at 11:47 a.m.)

CHAIR BROWN: It's Charlie Brown, I see that it is 11:47 a.m. and, Kim, are you there?

MS. LAWSON-JENKINS: Yes, I'm here.

CHAIR BROWN: We will go ahead and

reconvene and you can proceed on.

MS. LAWSON-JENKINS: Thank you. Brian, please go to Slide 19? I don't know if the ACRS is aware or the current Members are aware but we actually issued the draft guidance, a version of the draft guidance, for public comment back in 2018.

And I included that in the package that was shared before this meeting. We clarified the existing interpretation of the regulations based on what we learned from Milestone 1 through 7 inspections.

We updated the guidance to reference the new rule for cybersecurity rent notification. At that time, the current version of NIST Special Publication 85 was Revision 4.

Those are the security controls which, in a way, were the basis of what we had the original reg guide on. I think we used Revision 3 back in 2010.

So, the NIST guidance had been updated in the meantime and we looked at that guidance to make sure our controls were pretty much in alignment, if it made sense. We did it on a case-by-case basis.

At the same time, IAEA came out with new guidance on security. The NRC was actually pretty active in a lot of those Committees when the new

guidance was being generated.

And even though the guidance hadn't been implemented yet, we knew what was coming so we could take those insights and use them in the guidance. And also, the Commission direction regarding the balance of equipment was incorporated into this version of the draft guidance.

So, those were the main changes that we had in there. Next slide, Brian, Slide 20. The guidance was put on hold after we went out for public comment to wait for the completion of the full implemented inspections.

So, that's what occurred and then we started updating the guidance again in 2020. We took good advantage of those two years that we had. Some of the public comments stated that we were not really using risk-informed cybersecurity or we had mentioned it in that last draft guidance.

So we did include text in this current version that you have that discussed risk-informed cybersecurity. We emphasized the need for accurate CDA assessments.

I cannot stress this enough, that the CDA assessments should be living documents. They should reflect the current security posture of that CDA. It

is not something that should be assessed at the beginning of the program and you never look at or touch anymore.

We made that clear in this guidance, that this living document should be accurate and should reflect the current security posture of that CDA. That draft guidance that was coming out of the IAEA actually became standards by 2021.

So, we're referencing those documents and there was another version of the NIST guidance, Revision 5, which we double-checked and clarified to see if there was any area that we weren't in alignment on.

And of course we addressed the public comments we received in 2018. Next slide, Brian. There were 57 cybersecurity inspections completed between 2017 and 2021. The areas that we saw that needed --

Let me stop for a second. Remember back in Milestone 1 through 7 I said there were certain areas that we saw the highest number of findings and you don't see portable media and mobile devices here anymore, right?

Like I said, I believe a great job was done on that. We still were struggling I think, up to

a point, with the quality of the assessments and the systems.

Because a lot of the plans now have moved from being established to being maintained, vulnerability assessments became more important, and also, how often to monitor and verify the effectiveness of the security controls?

That was an issue where we saw we could definitely do some improvements there. Next slide, Brian, Slide 22. This slide and the next slide give an overview of the major changes.

One of the I think comments I received from Christina when I gave her the new version of the draft guidance is she commented on how much bigger it was, how many more pages it was than the original guidance, which is absolutely true.

But that is not to be unexpected for cybersecurity for a document that was being updated that was 10 to 12 years old. And all of the information that we have I really consider value added.

So, I'm not going to go through each slide here because there will be a slide to address each one of these items but this is just an overview for the Members when you look at the slide deck.

MEMBER HALNON: Hey, Kim, this is Greg, are we going to talk about BOP later in the presentation?

MS. LAWSON-JENKINS: A bit, yes. There was a presentation on BOP in July.

MEMBER HALNON: I can go back and look at that.

MS. LAWSON-JENKINS: We can discuss it a bit but I have to admit, I didn't expect for that to be a focus this time. So, at a minimum we can take the questions.

If I cannot answer them all directly or if you don't see it addressed in the guidance, we can provide more information about it.

MEMBER HALNON: I was just interested in how you balanced the risk versus the critical portion given the BOP stuff normally just puts things and the plan in safe condition.

How you can do that in a risk-informed way makes it equal with the risk-informed approach to the safety-related stuff. If that was addressed back in July I'll go back and look at it.

I did not realize that.

MS. LAWSON-JENKINS: We could have Staff support a separate BOP discussion if necessary but

please do look at the information that we had in July because that area was pretty well discussed, I think, then. I was listening in on that phone call.

MEMBER HALNON: And I probably was too.

MS. LAWSON-JENKINS: I know how it is when you aren't specifically thinking of something at that time.

MEMBER HALNON: Yes, let me recover a little bit and go back and look at it and if I have questions, I'll let you know and get the right stuff. Thanks. Brian, why don't we go past the next slide?

And like I said, we'll go through all these, there's a slide for every one of these issues. We'll go right straight to risk-informed.

Risk-informed cybersecurity, as I said, for any computer system you have to make judgments on which vulnerability security threats you address and which ones based on the consequence of something failing and how quickly you apply those things.

For risk-informed security, you have to take into account, and this is the definition we give in the guidance, the threat information, the likelihood of the adversarial success, and most importantly, the resulting consequence of the threat.

And the bullet items you see here are some

aspects that you have to take into account when you are using risk-informed security. For instance, the characterization of the facility functions.

So, as we spoke about earlier, whether you use PRA or some other methodology of identifying what the safety, importance of safety, security and emergency preparedness functions are.

To characterize a threat to the facility, as I mentioned on some of the defenses that were used, I said this defense is only applicable for wire tax, you understand, or wired pathway.

Or it's only applicable for portable media and you have to look at some other things. You have to take all of that into account.

The specification of the requirements including the cybersecurity plan, the defensive architecture, and defense in-depth methodology, all three of those work together to apply risk-informed security.

Implementation of the requirements based on the consequence analysis, a lot of the NEI guidance certainly is based on the consequence. That's how they determine what controls to apply.

And this is a point that isn't well documented often but that we, going forward, are

really going to keep reminding people that there has to be validation and verification of the implementation of the cybersecurity plan and the program as a whole.

You have to make sure the plant, first of all, is doing what you said it's going to do, that you implemented the plan based on the requirements, doing what you said it was going to do.

And then determine whether it's effective. Okay, it's doing what you said it's going to do but is it doing it effectively? Okay, you did something but what it's doing, is it effective?

And what I would say the goal should be of when the licensee implements the cybersecurity plan is that we truly just provide oversight. The NRC comes out and the licensee will provide evidence of what they did, why they did it, and whether it was sufficient.

And then the NRC should comment on it and give our feedback and perform the oversight in that way. With security, we have to get ahead of it, it can't be a whack-a-mole where you find the problem and you fix it, you find the problem and you fix it, you find the problem and you fix it.

You have to understand why you do things

and whether what you're doing is effective. And only once we start moving towards that mentality will we start getting ahead of the game when it comes to security, when you have an active adversary trying to do damage to your facility.

CHAIR BROWN: This is Charlie. I just want to make sure I understand. To me, I'm obviously focused on safeguards, protection systems, reactivity control, starting pumps and valves and all that kind of stuff.

Those are not risk-informed. They either have to start or not, they can't decide that they don't have to start.

MS. LAWSON-JENKINS: Right.

CHAIR BROWN: Therefore we don't have to do anything with them. But what you do with those, we're back to that other question of how do you ensure they actually function?

Those are through design features that you put into the thing, not cyber features of any kind. You make sure, for instance, in a protection system you have four divisions.

You want to make sure at least two of them work so you have redundancy. You make sure they're independent because you don't want them all

interdependent. One failure could take them all out.

You want diversity or defense in-depth within that architecture. So, risk-informing a design of the protection system and safeguard system, I don't think that's what you're talking about here.

MS. LAWSON-JENKINS: No, I said cybersecurity.

CHAIR BROWN: I'm just trying to make sure I'm wrapping my brain around this the right way because to me, it's not like you allow a little bit of risk or a little bit of hiking, as I said earlier. That doesn't work.

MS. LAWSON-JENKINS: Like I said, safety always trumps security. You have to focus on the important things and that's the tricky part. Truly, safety obviously is important and that's what you're doing but how do you do it? And that's what we're debating.

CHAIR BROWN: One of the five major design functions for the protection systems, safeguard systems, are redundancy, independence, deterministic processing of your computer systems, in other words, main operating loops if you can do it.

They don't do it but that's a way to get around that. Diversity in defense in-depth and,

quote, control of access.

And so that's one of the design functions that's called out in 1050.55(a)(h)(2), I think, where there's those functions, that architecture foundation is in the 5055 rule.

MS. LAWSON-JENKINS: Like I said, I don't want to conflate things because as I said, I'm speaking purely from cybersecurity.

CHAIR BROWN: I got that, and I'm just trying to make sure in my own mind that you're confirming what I would hope you were going to say.

Because when we're going through the five principles, fundamentals, as a Committee with the Staff, to ensure that we are comfortable that it's safe and will perform as expected, we think of the cyber stuff that's happening.

We're trying to slam a door so nothing can get in, recognizing there are other things that have to be thought about physically from access.

MS. LAWSON-JENKINS: Eric Lee, who you know, as he always says, cybersecurity ensures the reliability of the safety function to make sure that the adversary cannot adversely impact the safety functions. That's the rule.

CHAIR BROWN: I got it, but the 7354 rule

is not part of our design, it's not in the initial design application part of the thing. It's literally supposed to trip or not trip and so you have to have enough redundancy and independence to make sure it does.

I think I understand this is pretty benign relative to what we're doing. From a risk-informed, I can see how you have to look at every asset and say, look, if that thing fails or gets compromised, is that going to cause a design basis transient?

And if the answer is no, then you don't have to do as much. You don't want to go overboard on the site.

MS. LAWSON-JENKINS: You really want to put your resources where it's going to matter.

CHAIR BROWN: That's the way I read this and I just want you to confirm for me that I'm reading that the right way. Go on.

MS. LAWSON-JENKINS: Next slide, Slide 25, please. So, this was the discussion about balance of plans where we consider that important to safety equipment. So, one of the considerations are whether or not you identify certain equipment as CDAs.

So we added a diagram and lots of text. This is only one example of the text that we applied

there. But you'll see that all throughout this Section 3, you see the same information multiple times, where we're talking about balance of plans.

As I would suggest, if you have any questions, please look at the transcript and I don't know if there's a recording of the presentation that was made in July, if there are additional questions, obviously the Cybersecurity Staff would be more than willing to answer the questions.

But we updated this space on guidance from the Commission.

MEMBER KIRCHNER: Kim, this is Walt Kirchner, I will go back and look at that but at a very high level, how do you draw the line on defining balance of plant important to safety?

It goes back to my comment about do you use the PRA and demonstrate that you've got, I'll say this, the design basis accident envelope, it covered?

What's the metric? In the field, how does an inspector determine what's important to safety in the balance of plant?

MS. LAWSON-JENKINS: Basically, like I said, based on the safety rule, in the guidance that, really, the licensees that NEI put out, we gave guidance on what equipment was considered balance of

plant.

And it says it right there on number 6, equipment that can affect reactivity or result in an unplanned reactor shutdown or transient. So, it should be labeled as a CDA based on that.

Now, what controls you apply after that is another story. We aren't talking about that here. We're talking about just identifying the equipment.

MEMBER KIRCHNER: There's a large universe of things that could result in an unplanned shutdown or transient for the plant, that was my concern.

In practice in the field when you do your inspections, do you find that your track record is a general alignment between your inspectors and the operating plants and their estimation of what's important here?

MS. LAWSON-JENKINS: I have seen very few, if any, violations based on this equipment should have been identified as protection for balance of plant. Usually, that is pretty clear-cut.

The actual controls that are applied may be debatable, that's when we usually have some discussions based on that. I generally look at all of the inspection reports. The issue hasn't been usually identifying the equipment or balance of plant.

Normally, that is pretty clear-cut, it's a matter of what controls were applied.

MEMBER MARCH-LEUBA: This is Jose.

This applies obviously to operating reactors because those are the only ones that are operating now, but have you been following the Part 53 developments, especially the Tier 1 and Tier 2 separation, where only Tier 1 items are safety grade?

Will this have any repercussions on cybersecurity that you will not require cybersecurity on Tier 2 things?

MS. LAWSON-JENKINS: I remember Member Brown mentioning in an earlier meeting weasel words. I don't want to speak for someone else.

We are absolutely following the discussion on this and you'll see that in the slide later on, that we are actively -- we haven't completed the Part 53 work yet so I am not the person to even speak on that.

MEMBER MARCH-LEUBA: I know you don't like to --

MEMBER PETTI: Jose, the Staff has changed, they're not using Tier 1 and Tier 2 anymore.

MEMBER MARCH-LEUBA: They call it something else but it's still Tier 1 and Tier 2, they

call it something else.

MEMBER PETTI: There are two sets of requirements now.

MEMBER MARCH-LEUBA: Yes, what used to be Tier 1, which now is called something else goes in tech specs as safety grade. What used to be in Tier 2, which now is called something else, is still not in tech specs because it's still not safety grade.

And what I'm suggesting here is that it should not be out of the cybersecurity platform just because it's in Tier 2. You tell me what the name is that they're giving it today but it's still Tier 2, not tech specs, not safety grade.

MS. LAWSON-JENKINS: There will be a totally different presentation on that. I do understand what you're addressing but I can't speak to that at all.

MEMBER MARCH-LEUBA: First, I have to apologize, I was late but earlier I wanted to put in a word but everybody was talking and it was impossible to break in.

I wanted to support something, Kim, you said during that talk, that if there is a place where defense in-depth fits, it's in cybersecurity. You can put all the one-dimensional diodes you want, I can

find you a way I can bypass them.

I may have to have a SolarWinds attack or something like that. So, there is going to be a tendency, the same way we got rid of safety-grade systems and we are going to relax cybersecurity on what used to be called Tier 2 items.

I hope you defend us on this. Cybersecurity needs defense in-depth and needs to be everywhere. Thank you.

MS. LAWSON-JENKINS: Like I said, we can have some follow-up discussions if you want more information but when we were updating guidance based on the plans, we were in contact with FERC and they gave input.

And like I said, through the inspections we haven't had too many issues on what's been identified as balance of plan, there's general agreement on that. But there has been discussions on what would be adequate protection of that equipment.

But like I said, hopefully this new guidance will clarify that. And Brian, please go to Slide 26? Okay, so again, we're talking about identification of critical digital assets.

And one of the obvious things we added was a diamond at the beginning that you have these

critical systems that have been identified. Does any of the digital equipment contain digital components or firmware or software?

So, we brought firmware into that, which wasn't quite clear from the original guidance. There's a diamond that was there that talked about pathways but we clarified it more to say does this device affect critical assets, functions, and/or pathways?

Because it really matters that we know a possible attack that's approaching, not only when it gets to the target. And we added a diamond to talk about balance of plant, which we didn't have before.

So, we enhanced some of the guidance that has to do with identification of critical assets. And we talked more about protecting the critical digital systems and assets.

That led into the discussion, like I said, about the kiosks or any other device that's protecting especially more than one asset, how actually the protection of that device itself that's providing that function, it has to protect itself.

And we made that pretty clear and it should be identified as a CDA. Next slide, Brian, Slide 27.

We expanded the discussion on defense in-depth-protected strategies and this is a long sentence but it incorporates everything we needed that it employs multiple diverse and mutually supported tools, techniques, and processes to effectively perform timely detection of protection against, and a response to cybersecurity attack.

Too often on the inspections we saw one or two mechanisms that were there, you have a data diode, you have the portable media program, as I said, the Milestones 1 through 7s, they're were great starting points.

But it has to be defense in-depth that's directly from the rule. And it won't always be processes or it won't always be operational things. Technology is very important.

For the older plants there was a heavy reliance on physical security, operational procedures, which is understandable but they also had a smaller attack surface.

As you get more digital equipment in, I think technology is going to play a bigger part, which is why licensees probably need to be proactive in having these discussions with vendors and manufacturers of security features that they would

need to have an effective cybersecurity plan.

Next slide, Brian. Defensive architecture protecting the SSEP function.

We've actually discussed this quite a bit, that functions that are protected when they have to do with safety and security should be protected at the highest levels and the functions that affect safety and security and importance of safety may apply to more than one critical system.

But those critical systems should be allocated at their appropriate security level, whether you call it Security Level 3 or 4. Some licensees only have one security level behind their data diaode, it's whatever they feel is affected but it should be protected in that architecture.

And as I stressed, they must understand the attack pathways for their architecture. Most diagrams will show the wired access into the network and into the systems, which is very important, clearly.

But as I said, we have to be aware of portable media and mobile devices. If other pathways eventually possibly, not necessarily behind the data diaode but it's wireless to see how that's affecting where it is in your architecture.

Supply chain, which is very challenging, to say the least. We did only a limited amount of changes to supply chain in this version because the standards and recommendations are still in flux.

But at a minimum, that's why I keep harping on the detection capability, there has to be a detection capability behind the data diaode to understand when something is different, some new function is being performed, some new communication is occurring.

Which may have been introduced, could have been introduced through the supply chain.

The licensees need to understand the communication paths that you have in the architecture and that should be discussed during the licensing phase when they're giving us the template or whatever they're going to do for their cybersecurity plan.

So, when they talk about their cybersecurity plan, every licensee talks about their defensive architecture, everyone. Next slide, Brian.

CHAIR BROWN: Not next slide yet.

MS. LAWSON-JENKINS: Okay, back to Slide 27, Brian, thank you.

CHAIR BROWN: This is 28. 27 is fine. I'm looking at 28, and I was looking at your comment

right now. Behind the data diode you have to have something monitoring what's going on behind it in order to ensure there's nothing wrong.

And so I translate right into my reactor protection system. I'm not going to go back into the other discussion, I just wanted to clarify. We designed a protection system to a set of I'll say give principles.

It's redundant, independent, deterministic. If not, how do we fix it? Control of access and diversity in defense in-depth. And we have been insisting that all data transmissions out of that system be through a data diaode, hardware-based.

But on the back side of that, within the protection system, we don't see any other monitoring function that is interrupting operations and determining whether there's something else going on that shouldn't be there.

That would totally disrupt the operation of the safety system. In other words, it's a desert back there, it's just what it is, hardware-wise, and the way it's designed and the way the computer system is designed.

You may come back in later and decide you have to change the operating system software because

there was an error in it. That becomes a control of access and monitoring at the vendor level and making sure there's no malware incorporated in that design change.

But you don't have a permanent function constantly interrupting the operation to monitor various subroutines and other routines that the protection system is going through --

MS. LAWSON-JENKINS: Let me clarify something, I think there's a miscommunication on this. There's something called a host intrusion detection system, that's when you have something actually on a device saying this process is running, this process is sending information.

We're not talking about a host intrusion detection system. If anything, we're talking about a network intrusion detection system, where information comes from a device. We're looking on the pipe to see that information come across it.

And it goes all the way it's supposed to go. So, we aren't doing anything to the reaction protection system. We're just looking at information that's coming out of it if you were using an intrusion detection system.

CHAIR BROWN: So, the point you're making

is that, in other words, the data, it's coming out via the one-way --

MS. LAWSON-JENKINS: Yes.

CHAIR BROWN: It goes to a network maybe before it's processed?

MS. LAWSON-JENKINS: It goes to a device that monitors it and then forwards it on somewhere else but there's no communication --

CHAIR BROWN: Let me finish. That one-way input into the network would be residing in the protection system, but before that network sends anything out somewhere else, it might be a deterministic device.

But that network you were talking about would have something sitting within it that's making sure all of its functions are operating as they should and haven't been invaded by something else on the back side of the diode before it sends anything out?

Because there's nothing in the protection system, I've got data coming out of that, it goes to a network then goes to the main control room.

MS. LAWSON-JENKINS: Right, and it's just the same information that's coming to this firewall or whatever is in monitoring. It isn't sending anything back, it's just looking at what comes out of it.

CHAIR BROWN: But I'm just saying, you're not implying -- excuse me, that's the wrong word. The system is delivered, nobody is going to be looking on the backside of that terminal board protection system --

MS. LAWSON-JENKINS: No.

(Simultaneous speaking.)

CHAIR BROWN: -- putting anything in there?

MS. LAWSON-JENKINS: No.

CHAIR BROWN: That's all I wanted to make sure I understood.

MS. LAWSON-JENKINS: It's monitoring communication and like I said, what you refer to is more, like I said, it's a host.

It's sitting on the host and that's something that whoever manufactured that reaction protection system, they did that, that's outside of our control.

We don't do that.

CHAIR BROWN: Let me make one other observation then because one thing we do do in the protection system, there are a set of self-checks that are built into that software to make sure it is doing what it is supposed to do.

They are relative to the protection functions themselves and if they're tripping at the right points or if their set point hadn't changed, et cetera. So, I got it, we can go on, I just wanted to make sure I understood context.

MS. LAWSON-JENKINS: We're just monitoring the information and the communication that's expected. Nothing looks unusual. It would be still forwarded onto wherever it's supposed to be forwarded to. We are not interrupting anything that should be happening on the safety side.

CHAIR BROWN: Okay, thank you.

MR. HECHT: This is Myron Hecht, can I ask --

MS. LAWSON-JENKINS: Yes.

MR. HECHT: So, you spoke about network monitoring of if it were benign. But, in fact the network monitoring equipment, even though it's supposed to be just listening, can interfere with the network communications if it's malfunctioning.

MS. LAWSON-JENKINS: If it's malfunctioning. Which is --

(Simultaneous speaking.)

MR. HECHT: Right. But now they did this -- you might say well, if it's malfunctioning, it's

not within the cyber security provenance.

But, how is that considered? I mean, balancing the risk of, or ensuring that the network monitoring function is actually always fail silent, and doesn't fail so that it starts a jabbering and causing interference with the safety function from the -- through the network?

MS. LAWSON-JENKINS: That's really, I believe incumbent on any piece of equipment that you have. I'm not trying to be fictitious.

But, you have to have some way of verifying that it is functioning correctly. And this is an issue that I said we actually had with a kiosk. Okay.

The -- if an equipment man -- okay, if this is, we're talking about an intrusion detection system, okay. If it fails, it's going to fail securely.

It will not interfere -- that would be a requirement. That's one of the requirements that we have in the, in our cyber security plan.

That if it fails, it's going to fail securely. So, it should not start --

MR. HECHT: Well, --

MS. LAWSON-JENKINS: Okay, jabbering, as

you said.

MR. HECHT: I get it.

MS. LAWSON-JENKINS: Okay. So, that's a requirement of the cyber security plan.

MR. HECHT: Well, you said fail securely. I just -- but not necessarily fail safely. I could envision fail securely --

(Simultaneous speaking.)

MS. LAWSON-JENKINS: So, and that -- and that requirement is still there. We don't replace a requirement. There's an additional requirement.

It must fail securely already, based on the crimes that NRR, you know, has, in their documentation. In fact, that is one of the issues that NEI 08-09, their version of a cyber security plan, they claim credit for that fail safely.

They said that we didn't need the fail secure -- failing in a known state. And you'll see that later in a slide. So, we'll just jump to that now. And I'll skip it later.

That we said that we -- the device needs to fail in a known state so we can understand whether it failed securely and safely.

They substituted a command saying -- or sorry, a control saying it need -- we already do that,

it fails safely.

So, like I said, we -- that is not getting, that is not being eliminated. And the point that why we kept it in Reg Guide 5.71, is that addition to the existing Reg guidance and regulations where it must fail safely, it must fail securely.

And those two things are not necessarily identical. Because you need to understand --

MR. HECHT: Okay.

MS. LAWSON-JENKINS: That that device is performing its security function adequately.

MR. HECHT: Okay. Thank you for that. But, what you're saying is that a failure mode where the security devices might affect safety is handled by NRR. And that the failure modes where they might fail insecurely are handled by NSIR, and served by that --

MS. LAWSON-JENKINS: That's at least piping it that way. I'm saying that if it's going to fail securely, that's a requirement we have in the CST. That we have.

And as I said before, that just safety always trumps the security. Always. So, there's nothing that the security device would introduce that would make that safety system not operate.

MR. HECHT: Well, is there some kind of

poll, because NRR may not know about network intrusion monitoring devices and TAPs, and fiber optic TAPs and things like that?

But, NRR -- NSIR is really worried about the security out there the most. And nobody's worried about the fact that the security devices might fail in a way that impacts a safety or controls traffic.

MS. LAWSON-JENKINS: I'm not quite sure how you can make that last statement. I don't agree with strongly.

I don't agree with -- that is not true. As I keep saying that we always have security so that it doesn't affect, negatively affect the safety function. Always.

Okay. So, that's a requirement.

MR. HECHT: Well, that's a philosophy statement. But, in terms of the actual implementation, in terms of understanding how devices work, and how device fails work together and --

(Simultaneous speaking.)

MS. LAWSON-JENKINS: If you look at security controls -- please look at the details of the security controls in Appendix B and C that are implemented in the cyber security plan.

It isn't just a philosophy. There are

actual requirements in there that it cannot negatively impact the safety function.

That's not in the guidance in the front matter in the staff position. That's actually in the controls also.

MR. HECHT: And how does somebody know that something fails in a way that cannot affect the safety function? How is that verified?

MS. LAWSON-JENKINS: If the device -- I'm sorry, can you give me a specific of what are you -- I guess I'm trying to get clarity on what's your --

MR. HECHT: Okay. Well, we spoke about a network intrusion device. But, how many times have you tried to log onto a system maybe with two-factor authentication, and your second factor, displaying the secret number, or something like that, failed. Or there was a loss of synchronicity and you couldn't log in?

I'm not sure what the analogous failure modes are for network intrusion equipment or for fiber optic TAPs that could cause that. But, it seems to me that you're putting stuff now in series in that communication link that might fail in such a way.

In other words, it's not completely benign. And this requires that technical expertise.

And this regards people who know about these things.

And I understand that NSIR knows about them from the security perspective. But who knows about them from the, I guess I'll call it the electronic perspective, or from the actual device perspective, and those that know the devices don't negatively impact the safety systems of the client?

In other words, there's a requirement there. But, somebody might be overlooking something in verification.

MS. LAWSON-JENKINS: Okay. As I said, that we are not talking about a host detection system. And we also are not discussing an intrusion protection system where it actually may take an action.

Now, I understand you're saying if it fails, well, with the requirement to fail securely, it should leave the -- leave the system in the same state as if it was not operating.

It should not --

MR. HECHT: Yes, that --

MS. LAWSON-JENKINS: Make things worse. So, I'm pretty sure that when we look at the requirements and outputs and things that will occur, that those scenarios will take into account that it doesn't have to be in -- you can have TAPs that don't

affect even when you're possibly just monitoring what's going on.

And it doesn't even have to be on the same communication network. You can have things go off in two directions.

One can go off in the operational. And then you have the other information go off to the device itself that's doing the monitoring.

It's the same. It's just making a copy and sending it. Okay. And you don't have to be right in band.

MR. HECHT: Again --

MS. LAWSON-JENKINS: So, there is definitely a different way to doing this.

CHAIR BROWN: Myron, let me --

MEMBER KIRCHNER: Again, this is Walt Kirchner. I want to -- I'm following up on Myron's point.

I am not, again, I'll say not well versed in this. But, I -- from an architectural standpoint, going back to Charlie's initial point, the pick up that you would use to see, look at whether it's functioning properly, let's pick on the reactor protection system.

In the final analysis what does it do? It

sends a trip signal to some voting logic. We don't have to go into the details.

But, you're monitoring, I would hope, in an architectural sense, would be serially downstream of that function, that trip signal and the equipment that is tripped, the control rods.

Down -- and downstream of a diode that protects that equipment from any back feed because of the monitoring system.

MS. LAWSON-JENKINS: It would definitely --

MEMBER KIRCHNER: Do you see where I'm going?

MS. LAWSON-JENKINS: It would definitely be downstream for sure. And like I said, it doesn't have to be in banded between whatever's being sent.

It could literally be a copy of something that's sent over. So, --

MEMBER KIRCHNER: No, that would be dangerous to put it upstream.

(Simultaneous speaking.)

MEMBER KIRCHNER: I mean, it was my --

MS. LAWSON-JENKINS: There's no upstream because of the diode. There's no upstream anywhere. It's monitoring.

There's no communication. So --

MEMBER KIRCHNER: Right. So, as long as -- as long as you're doing the monitoring downstream of the reactor protection system function, and downstream isolated by a hardware diode, a digital diode, then I would see it okay.

But, if that monitoring is upstream of a diode, you could get feedback into that system theoretically.

MS. LAWSON-JENKINS: No -- no disagreement. No disagreement on that.

But, I have to admit, in the architectural diagrams I have seen, there's no -- if you have a data diode, you don't usually put something, especially in front, right in front of a safety system.

You don't put --

MEMBER KIRCHNER: That was my point earlier in the morning about where you had the diode on the diagram.

MS. LAWSON-JENKINS: And as I said, there are usually multiple, because these networks are so vital.

MEMBER KIRCHNER: Of course. Yeah, of course they would be.

MS. LAWSON-JENKINS: That's all I'm

saying. That it really, and this is why when we -- you get down to the details, all these things are considered.

I'm not dismissing any of it. Because that is what you have to look at. You know, how do you meet all these requirements, not just to do the, obviously do the protection.

But that malfunctions won't affect it. That -- you're still -- but you'll still be able to detect when something's going wrong, and recover from it.

So, it does take, I agree, a lot of expertise. We have the safety and secure -- the safety engineers need to talk to the security engineers, who need to talk to the vendors, who understand.

And this was a big issue that we're constantly working with the licensees on. That they must, must communicate with the vendors who make this equipment, so that we can understand the normal operating functions of this equipment.

So that when anything, and this is with security devices also, when anything is different, when it starts to act differently, we need to understand why.

I really, I feel like there's no disagreement here, really what we're talking about. But, obviously the implementation details matter a lot.

And the questions that are being asked, and the discussion we're having is the exact same thing that should be happening with the licensees and their vendors.

MR. HECHT: Okay. Thank you.

MS. LAWSON-JENKINS: Thank you.

CHAIR BROWN: If I could -- this is Charlie again, Kim. Trying to think of this, I've listened to both.

I recognize you all wouldn't put anything close, in the reactor protection system, you know, upstream of the data diode, sending the data out of the protection system.

But, there's no monitoring. So, that's built into the design, whatever they want to do. So, there's no host -- that's the host, I guess you would call it.

But, if you look at a network where the data goes to, and then gets sent some place else, I was trying to integrate how you do something securely and safely. And I understand the need to monitor

network functions.

So, something that monitors, to me the ideal monitor has to be unintrusive to the network operation. And the only way it could really do that would be to take data in.

And that data has to be received via unidirectional type devices so that nothing can go back out the other way.

And as the monitor determines based on that input that something scurrilous or nasty is going on, its output should not go back into the network system. It should be an independent transmission to another system, or people, or control center.

That hey look, part of your network is not working right. In other words, it should not put itself back and let the network communicate that.

And that's, I think that's what Myron and Walt were both probably talking about. These are designed, hardware designed details.

MS. LAWSON-JENKINS: System -- they're system designed, yes.

CHAIR BROWN: Yes, system designed.

MS. LAWSON-JENKINS: So, I would say for system designed detail.

CHAIR BROWN: That to me is the ideal

monitoring system. Number one, it obtains data in a unidirectional input manner such that it can't go back the other way and affect something.

And it does -- and it communicates a problem out without using the thing that it's monitoring. Okay. That's the simplest way I can phrase it.

In Section 3.2, I guess I had one other just, it's a little bit of a bone to pick. But, I'll pick it anyway.

And this was in the preamble part of 3.2, the input part. One of the paragraphs talks about, and it says, while a data diode can be an important element of an acceptable defensive architecture, use of a data diode alone does not provide adequate protection to comply with the defense in-depth strategies required by 73.54.

Exploits of vulnerabilities associated with supply protection, supply chain PMMD, wireless, physical presence -- physical presence pathways, can allow an attacker to circumvent those protections by the diode implementation.

All true. That's written in a format that implies that the data diode is -- is not a very good protection from the overall standpoint.

And what's lost in the way this is put out, it sounds like the other supply side stuff with this -- that you put in place, is the important part.

But, that's -- that issue we've had to deal with for the last 60 years, of supply side PMMD whatever, when you made changes in the analog world.

The real point is, when we introduced computers, we have now bypassed that physical protection capability. It's the one that's been damaged.

And the data diode saves the day on the -- on the data, you know, the communications aspect of it, on the electronic communication.

So, I mean, the way I would have written this was, hey, in the old days we protected ourselves this way. But, it wasn't good enough to handle the electronics. And now the data diode rides in on its white horse, and protects us from the electronic intrusion.

So, I'm kind of bent around the axile on terms of the way this is performed. Because it's -- it's inverted relative to the actual path and the development of the technology as we went forward.

But new -- new problems were introduced electronically by the introduction of digital data,

digital computer type circumstances.

In other words, the only way you can provide a new virus is via these other physical means now. Okay?

But the data diode prevents it from happening electronically. I just think it's written kind of convoluted where, you know, I don't know what, whether you ever want to do anything with that.

But, I'm aggravated. Not aggravated, that's the wrong word. I was a little concerned that the message comes out that the data diode is the new thing that has come in here to provide a protection that we did not have now with the electronic.

And it's still subject to people getting in, like you say, behind, back into the host via other means. And that should have been emphasized instead.

But, I think we're probably ready to go onto the next slide.

MS. LAWSON-JENKINS: Okay. I do -- I would like, and I know you didn't ask a question, and I do want to address that, because we spent a lot of time on that text.

And the reason was because we have seen in systems where there has been, in a way, an over reliance on the protection of a data diode. Where

that was deemed sufficient.

CHAIR BROWN: Oh, absolutely. I agree with you. You can't do that. It only protects you from the operation of a system and getting data out to other things.

It does not protect you from physical access to the system with other problems. And I still can't figure out why anybody would ever want to use wireless.

MS. LAWSON-JENKINS: And we would never get rid of this. We aren't saying we're going to replace this with something newer and shiny or better. We are not saying that.

But, we want to build on this. And just -- and I'm not going to comment on the wireless in that way.

But, I'm really saying that if you look at what you're doing today in your regular life, as far as the -- and that's you, and I, everyone, as far as communication, I don't know anyone who has a plain old telephone system anymore that's wired.

CHAIR BROWN: I do. I do.

MS. LAWSON-JENKINS: Very few. And I used to work at Motorola. So, there's very few who do. I have with -- I really miss it, because there were, you

know, issues that I don't -- I wouldn't have had with that old phone.

My point is, especially for this guidance, we want to build and keep what we did that worked well. There's no doubt that introducing the actual requirements of a data diode in our architectural plan we had for in 2010, you know, it was -- it really met the mark.

And it will continue to meet the mark for wired communication where the proper analysis has been done and you know the pathways in.

CHAIR BROWN: Let me interrupt you just for a second. All I'm saying is that this little for example paragraph, which I agree is a very important paragraph. The point gets across, okay?

So, I'm not complaining that you don't get the point across. But, the lead in really ought to be that our protection of these plant systems, the critical safety systems and safeguard systems and other systems as well, okay, really consist of two pieces.

One is the physical protection of access where things can get discombobulated. And the second is now the introduction of an electronic data transmission path that was not -- has not had to be

considered before.

And requires both data diodes and these other vul -- you know, physical protection pathways to be protected in order to achieve total security.

That's the way that it makes much more sense to write this paragraph, the lead in. If you understand what I'm saying. It's a couple of sentences.

So, I'm leaving it up to -- hey, I can't force you to do anything. I just think the point is not made that it takes two pieces since we introduced the other.

It used to be one, physical only. Now it's two. And one is enhanced with the data diodes and the other still is maintained with physical protection. All the list of other stuff you talk about for those physical pathways.

MS. LAWSON-JENKINS: Okay.

CHAIR BROWN: So, I would just introduce it in a slightly different manner. But we -- I'm not going to go any further on this.

Hopefully you will take this under advisement.

MS. LAWSON-JENKINS: Oh, I will. And I will.

CHAIR BROWN: Okay.

MS. LAWSON-JENKINS: I will. I'll look at -- and if you ask --

(Simultaneous speaking.)

CHAIR BROWN: I agree with the concept of what you said in it. Okay? It's totally okay.

MS. LAWSON-JENKINS: Okay. So, the actual words I used, we used. Okay. I understand.

CHAIR BROWN: Okay?

MS. LAWSON-JENKINS: Yes.

CHAIR BROWN: And let's go onto the next slide, which I think is 29.

MS. LAWSON-JENKINS: Twenty-nine. This was the wiggly room I think you referred to.

CHAIR BROWN: Oh, yeah.

(Laughter.)

MS. LAWSON-JENKINS: One of the other meetings where we had to have a communication path that will allow for vulnerability updates.

Because in the existing, in the original guidance, we said you had -- we had these separate security levels. And that you could not communicate from lower to higher security levels.

CHAIR BROWN: Prohibited. It was very specific.

MS. LAWSON-JENKINS: Yes. We prohibited. But, at the same time, was have the var -- a requirement that you had to do vulnerability updates.

CHAIR BROWN: Well, what do you -- let's explore that a minute. What do you mean?

I mean, what -- vulnerability updates from what standpoint?

A deny all permits by exception is a bidirectional data communication device that's software controlled. And by command, can be allowed to input from a lower level to a higher level.

MS. LAWSON-JENKINS: Okay. We -- I'm not talking about a wired communication. Because you've discussed diversity and things like that already for safety.

Okay. So, what has been approved on the mechanisms that we've seen implemented at plants, it's not wired communication to install an update.

No plant has that. And no plant is using that, because that would bypass the data diode in an unacceptable way.

What we have seen are processes and procedures, as I mentioned, with a kiosk and approved media that's been received from a vendor that will be scanned to make sure there's no known vulner -- no

known malware on that media that we're getting ready to install on the CDA that's located behind the data diode.

So, if everyone who does the vulnerability update is a portable media. They are not using wired connections.

CHAIR BROWN: Okay. That does not come across. And in the way that's written into the Reg Guide right now, does not do what you just said.

MS. LAWSON-JENKINS: How does it --

CHAIR BROWN: That does not -- that does not preclude a wired bidirectional device to be installed so that you can do vulnerability updates, not by some other physical means, but by electronic means.

And that ought to be clarified. That's all I'm saying. And what you just said -- and I understand what you just said. That's very clear.

MS. LAWSON-JENKINS: Um-hum.

CHAIR BROWN: But, that's not what this says. This is an open -- this is an open -- when we're reviewing a design, you know, and its structure, okay, from a one line diagram and architecture standpoint, we would see this, this could be implemented and say hold it, the Reg Guide allows

that.

Because it's -- we got it processed. We'll have controls when we tell it. It can process and input to all these software systems on a permit by exception basis.

And that's as soon as it's -- that's the way that reads. You really ought to clear that up. Because that's --

(Simultaneous speaking.)

CHAIR BROWN: That's like an open cesspool type to destroy everything.

MEMBER PETTI: Kim, this is Dave. When I saw these words, I, you know, knew it would trip Charlie.

But, what I thought was exactly how you answered it, is exactly how I thought it should be done. So, there is a disconnect between what these words mean and what most of the plants seem to be doing, which is the right thing.

So, I would support that somehow some words need to change here so that it doesn't look as open as the words could imply.

MS. LAWSON-JENKINS: Point taken.

MEMBER PETTI: Thanks.

MS. LAWSON-JENKINS: I will. I will.

But, to be -- just to clarify, there was, not as serious, but there was a suggestion about, you know, when we were coming up with the procedures, on how would you do vulnerability updates? And immediately the staff said no to wired communication. No.

And we were like, -- I said, with physical security, you don't have a door open for 20 minutes just to have someone do these updates. You don't do that. And you wouldn't do the same for -- for wired communication.

And like I said, there's a lot of procedures and technical controls that we are using to implement this. So, I will -- I can understand why this needs to be clarified more.

And since what I said is actually the way it's being implemented in the plants, we -- like I said, we don't like to, the staff prefers not to say how to implement something.

Okay. And keeping in mind that this maybe the basis of future work, we don't like to dig ourselves into a hole on something like that.

At least a new guidance will have to say, maybe take exception to something we're saying. We try to give the licensees and the vendors enough flexibility that they can still implement things in a

secure manner.

But, your point is taken that because we didn't specifically mention wired, that people may think that's a justifiable way of doing it. When absolutely everyone we've discussed this with knows -- has agreed and we don't have that.

So, I will make sure that we update the text regarding that point. I agree.

CHAIR BROWN: Yes. I make one observation on part of your comment about, we try not to tell people how to do it.

You are the regulator. You are the safety oversight. And sometimes, you have to tell people what's absolutely acceptable to you, and what's not.

MS. LAWSON-JENKINS: Yes. We're the security oversight. And honestly, I'll be candid, only with physical security, with -- well not physical.

With physical -- how can I say it, chemistry, physics, a lot of those disciplines, we -- there are axioms, this is the way it operates, things generally don't change.

With security, especially with cyber security, change is the constant. That's the only thing you can rely on.

And you have to have ways of adapting just as the attacker adapts. Okay. So, that's why we tried to give guidelines.

We tried to -- and on some things, when we introduced the data diode, they said, if you really want to do one way, you must use a hard way mechanism. So, we don't totally avoid it.

CHAIR BROWN: That's right.

MS. LAWSON-JENKINS: But that is the preference. We don't totally avoid it. But, when we don't want any miscommunication on it, which is clearly what we have here, on this vulnerability update.

And that preferred method is not to do wireless. You've got to do wired absolutely. Because -- and then we've come up with a better way of doing it with portable media.

CHAIR BROWN: Yeah, that's --

MEMBER KIRCHNER: But Kim, this is Walt Kirchner. May I ask a question about what is actually in practice?

For those plants that you've inspected that have implemented digital INC on critical assets, say you come in with a computer. The computer is scanned in this kiosk or whatever means.

And it's clean. It has no malware and such. But, it has a wifi connection.

So, say the maintenance guy or gal is working on a piece, a CDA and needs to reference the home base for the latest and greatest update or ancillary information, whatever, that person -- if that person does it through wifi and the internet, doesn't that present a vulnerability to that CDA?

So, how do you deal with that part? Because you know, when you have technicians in your home, more often than not, they don't have printed material anymore. They're on the internet pulling down things, et cetera, et cetera.

So, how does the, in practice in the industry, how are they dealing with that potential vulnerability when they're working on CDAs?

MS. LAWSON-JENKINS: Okay. I can't speak for every, clearly every licensee. But, I can give some, those guidelines here.

That first of all, almost every security plan that I know of, says that for safety and security devices that -- that there is no wireless for those devices.

Now, that can be changed. They can put in an LAR and say we want to use wireless. That's a

totally different story, okay.

And they will have to have strong justification or whatever. But, right now for existing operating plants, there should not be an attack surface there.

And this --

MEMBER HALNON: Hey, Charlie, this is Greg. And Kim, it's Greg.

(Simultaneous speaking.)

MEMBER KIRCHNER: Okay, again, also that pertains to maintenance as well?

MEMBER HALNON: Yes. Charlie, this is Greg.

MEMBER KIRCHNER: Do you see where I'm going?

MEMBER HALNON: Yeah. It's -- it's similar to, go back to the old language. If you bring something out of the cal lab that's calibrated and you drop it or you do something to it, it invalidates its ability to be used.

So, these laptops and other potential issues that you might plug in, first and foremost will have either the wireless modules removed or disabled so that you cannot connect it.

And that's a pretty standard portion, not

just with cyber, but with normal security. A normal security laptop will have a label on it saying, this cannot be connected to any other things.

Same thing with printers or copy machines similarly.

MS. LAWSON-JENKINS: Yes.

MEMBER HALNON: They are not connected to the LAN. And so those are -- that's a pretty standard practice in the operating forum.

MEMBER KIRCHNER: Okay. Thanks Greg. I wasn't sure whether that was part of the procedural practice or not. Thank you.

MS. LAWSON-JENKINS: Yeah. If you get, like I said, take a look at the access controls in Appendix B, and you'll see the wireless communication and the information that we just relayed.

Okay. Next slide, Brian. And this what we were just talking about. Minimizing the attack surfaces and pathways.

CHAIR BROWN: Okay. You can probably go on then, right? Or you -- we're falling behind a little bit. And I want to get to lunch at some point here.

(Laughter.)

MS. LAWSON-JENKINS: Yes. Okay.

CHAIR BROWN: But, I think then -- I think we've kind of been through this stuff. Am I right?

MS. LAWSON-JENKINS: Yes. But, I -- let me make one statement.

CHAIR BROWN: Okay.

MS. LAWSON-JENKINS: A couple of statements on this, because this is huge.

CHAIR BROWN: Okay.

MS. LAWSON-JENKINS: This is big. Because with all the things with telling the licensees you've got to monitor what you have.

You have to understand what you have. You need to minimize the attack surface and pathways. If you don't want to maintain it, if you don't want to put vulnerability updates on for something, don't -- and you don't need it, don't have it on the device.

Okay. If you don't want to -- if it -- if you have so many protocols, like when you're in the lower defensive levels and you have IT equipment that talks all these different applications and things, you don't have that normally, the industrial control system.

You should have the minimum set of functions that you need to operate that plant safely and -- securely and safely. Okay.

Don't have extra software on it. Don't have protocols running that you don't need. You have the minimum number of things there.

And at the same time, anytime you're using new technologies, make sure those new technologies cannot be used to circumvent or bypass the architecture that you put in place.

This was really important. Because when people do digital upgrades, and as you said, you bring in new maintenance equipment to do something, it has to be locked down.

It has to have the minimum functionality. And if you do it, at least do it, and get out. And you have to understand how the device is, your devices are affected by it.

So, we put a lot of information in about minimizing the attack surface and the pathway. Next slide, Brian. Slide 31. Okay.

Use of alternate controls. One of the big things we had, in 2018 we added the intent of every security control that we had in Appendix B and C.

Because sometimes licensees said they would use different controls, alternate controls compared to -- instead of using the ones that were in our Appendix.

Like they would use physical security, or something that's been done in a safety system, we're going to take credit for that. Or the maintenance program.

We said look at the intent of the control. Okay. It should meet that intent. And so we made it clear on what the control, why the control was there.

There's lots of additional information about that. Which is why the look of the guidance really increased. Next slide, Brian.

Consequence based graded approach. You look at the consequence of if a device fails, you know, and based on that, that's what determines how you're going to apply security controls.

And it should be consistent. It should be repeatable. It should be understandable. And it shouldn't change based on different, you know, things. That was really important. Like I said, just to understand why things were done.

And 13.10, we cite that in the new guidance that 13.10 is one acceptable way of doing this. Next slide, Brian.

Okay. This is an important one obviously. This is where we mention that technical security controls, things that you are installing on that

device, okay, that that could be a part of the design certification list.

The licensee said, for this part of our cyber security plans, we're depending on these controls that were implemented in this device. This is where they take credit for it.

And also, that's -- obviously that's based on them giving requirements, like I said, to the vendors. And the vendors demonstrating that they have fulfilled those requirements.

We added text to the sections that talk about technical security controls. Because as I said, sometimes licensees would use physical security or other operational security, something else to take credit for technical control.

And we wanted to be clear why these technical controls, what it means to fulfill these things. So, next slide, Brian.

I think we -- did I give one example? I didn't give an example of that. But, if you look at those sections, the previous sections, that will discuss it.

But, technical controls are very important. They weren't installed a lot, like you said, we -- for the cyber security plans, we added

that. That was added after the plants were built.

So, that's why they didn't take on the significance, is what -- I would have thought as cyber security. But, absolutely for the newer plants, for new designs, technical security controls will be vital.

Incident response, we updated based on the use of cyber security event notification rule that has been added. And we updated guidance based on some references we had for this and the DHS CISA Cybersecurity and Infrastructure Security Agency. Next slide, Brian.

There's an error on this slide and on -- in Section 3, C.3.3.3.1. That just say updates, the updates site Section 2.1 through 2.5 of Reg Guide 1.1.5.2.

That it -- there is no Section 2.6. But, it references that for secure development of equipment.

So, it talks about the concept requirements, design, implementation, and testing. Those are the five sections that are up front.

So, then after this meeting, that will be updated before it goes out for public comment. That will say 2.5 instead of 2.6. Next slide, Brian.

We've talked a lot about continuous monitoring. We added more examples to say what we consider acceptable.

And I expanded -- we expanded the text that talks about the importance of anomaly detection. They need to understand what's normal in the network.

Which is why minimizing the software, what you need in that network to have that minimized to be able to detect something different. New activity that's unexpected is probably the first signs of a cyber security attack.

So, we added more text on that. Next slide, Brian.

Effectiveness analysis of security controls. I drafted almost all that text. So, and that it was -- it isn't mandatory, but this is a method that they can use to explain why they -- what they did was effective.

So, we talk about how to come up with objectives. What are good metrics? What are metrics they want to capture?

How to build on the log files and all the requisites they're currently doing in the cyber security plans. How to establish benchmarks and targets for metrics.

And how to review, keep reviewing. Are you getting the data you expected? Are you missing any data?

Or did you -- are you getting more data from different types of devices? There's a whole section that was added on this in 2018. Next slide, Brian.

CHAIR BROWN: So Kim, is this a convenient -- we're looking like we're changing subjects a little bit.

This is the --

MS. LAWSON-JENKINS: Do you -- no, do you want to go back to the metrics part?

CHAIR BROWN: No. I would -- I'm looking for a convenient place to --

MS. LAWSON-JENKINS: Break?

CHAIR BROWN: Stop for lunch.

MS. LAWSON-JENKINS: Okay. We only have a few more slides. But, let's go ahead and break for lunch.

Because this -- the part that talks about where we're going and what we're going to be doing, is very short. That's not going to take more than ten minutes or something like that, 15.

CHAIR BROWN: And that's ten, you're

talking about the next ten slides or what?

MS. LAWSON-JENKINS: No. It won't take long, I believe, to go through those. So, if you want to break here, that's acceptable. That's fine with me.

CHAIR BROWN: Is -- does anybody have any comments? Walt? Greg?

MEMBER HALNON: No, I'm good Charlie, so far.

MEMBER KIRCHNER: I'm fine. Thanks, Charlie.

CHAIR BROWN: Do you all want to finish?

MEMBER HALNON: I hate to place that back on your Charlie, but.

CHAIR BROWN: I can't -- I can't -- we could take ten minutes. Okay. I was -- we've got this scheduled out to about three o'clock.

So, we've got time. I figured we could go ahead and take a lunch break until about 2:15. And then use that ten minutes to wrap up the last 45.

MEMBER PETTI: Charlie, I tend to agree with you. I mean, you've still got to go for public comment.

CHAIR BROWN: Yeah.

MEMBER PETTI: So, yeah.

MEMBER KIRCHNER: Yeah.

MEMBER HALNON: Yeah.

CHAIR BROWN: All right. We'll go ahead and take a break right now. It is 1:07. We'll come back at 2:15.

I'll give Walt an extra little time with his dog and give my time for my dog. Is that suitable? Okay. So, we are, I can't say adjourned. We are recessed, that's the right word, until 2:15, Eastern Standard Time.

(Whereupon, the above-entitled matter went off the record at 1:07 p.m. and resumed at 2:15 p.m.)

CHAIR BROWN: Okay. Good afternoon, everyone. It is 2:15. I will now reconvene the meeting. And, Kim --

MS. LAWSON-JENKINS: Yes, I'm here.

CHAIR BROWN: Okay. I wanted to make sure we got back safely here. You can proceed. And we will start on slide 39 I guess. Is that right?

MS. LAWSON-JENKINS: That's correct. Thank you.

I'm leaving my camera off for the moment because earlier during the presentation I ran into bandwidth issue. And it was, I was afraid I was going to get cut off. So I'll probably leave the camera off

until the end of the presentation just to --

CHAIR BROWN: You can't see us either. So --

(Laughter.)

MS. LAWSON-JENKINS: Assets, sorry, security assessments and plant assets. Unlike the previous section where I briefly discussed metrics, the updates regarding quality security assessments are not a separate section in the updates but made throughout the whole document, both the security assessments of the equipment and the effectiveness analysis of the control supply, knowing this information is critical in providing evidence that the assets and the SSEP functions are protected from cyber attacks.

We spoke earlier about requirements, going to vendors and, you know, that the vendors should implement the technical security requirements, and that will be reflected in the plan. That's the asset procurement and identification. That's where that kind of interaction should occur.

We discussed earlier about maintenance of the equipment and how that could possibly be used to, as a segue to go to a network. So that's why asset management is very important, asset maintenance is

very important as far as the security of the device.

We spoke about vulnerability assessments. That's included in here.

The whole point of this diagram is to show that these activities don't operate by themselves isolated, you know, in a silo as we've been saying, that they all have to interact, and they all affect the security of the device.

The licensee should understand the plant functions that's affected by the technology that's being used. They need to understand the minimum capabilities of the technology to support the identified plant functions.

And they need to constantly evaluate the risks, the attack surfaces, the vulnerability, and the mitigations that are applied to protect the devices. Next slide, please, Brian. Okay.

So, for CDA security assessments, as I said, we updated text all throughout the document to really drive home the point that the security assessments should reflect the lifecycle of the equipment.

It's not just done at the beginning. It may not even be just done once a year. It should be constant monitoring, assessing to understand the

security posture of that equipment.

You have the initial assessments and the reviews when you decide what controls you want to apply. You need to verify that the controls that are applied are effective.

We need to keep, the licensee needs to keep track of the vulnerability notices that the, issues for the devices in their plant and under the control of their plans, and be able to discuss what mitigations they applied based on that.

And very important, they need to fold in their configuration management, which they already do for safety, but to make sure that this configuration management program is somehow associated with the security, because a lot of times with cyber security attacks we see that something has changed on the device, whether it's escalated privileges or some process turns on. And that's configuration management. You should know what's running on your device and keep track of those things. Next slide, please, Brian, 41.

And as I said at the beginning and throughout this presentation, we apply, for every security control in Appendix B and Appendix C, we listed the intent of the control so it will be clear

why that control is needed for certain devices, why it's applicable, and how to then hopefully, if you want to use an alternate, apply one that meets the intent of the control.

The text added, we added text regarding reducing or eliminating attack surfaces and pathways, as I said, going for that minimum functionality.

If the licensee, I would mention to the licensees, if you don't want to track it, if you don't want to worry about vulnerabilities being reported on something, if you don't need that service, remove the service. It makes it much simpler to maintain and keep a security posture for it.

And as I said, the last two to three years, there's been a new version of NIST 800-53. So the latest updates reflect those changes that were applicable for our guidance. Next slide, Brian, slide 42.

This is actually a slide that I pulled from the 2018 presentation. As I mentioned, there are some differences between NEI 08-09 and the draft reg guide that we're establishing.

Sometimes, we actually removed a few controls that were still in this, sorry, in NEI 08-09 after reviewing the NIST guidance and deciding that we

really didn't need this because it was covered by some other controls.

A few of the controls that you see in the middle we agreed that we can remove this. And I gave the reasons.

But there were a few controls at the end I said that remain in the NRC guidance that has been removed from the NEI guidance. It usually had to do with the intent for security is different from safety, where they were trying to basically credit the security plan with a safety function. And it really depends on how that's being used. And that's why we kept those controls in.

One of the issues that was just brought up during this discussion was for vulnerability updates how during my explanation I said we use the PMMD program not wired connections to implement the security for that. That's the diversity. We need to have a different way of doing something.

So that's going to be an example of that. And it's probably what's going to be in the justification when I update the text that has to do with vulnerability updates.

And I already mentioned about filling in a known state which deals with security and safety.

Next slide --

CHAIR BROWN: Can I ask hopefully a quick question?

MS. LAWSON-JENKINS: Sure, no problem.

CHAIR BROWN: And it's relative to your, the diversity, B.3.20. I guess I'm trying to find it again. I thought I wrote a note in the computer. I'm not used to doing this. So I have a hard time. What was that, B.2.20 or B.3.20?

MS. LAWSON-JENKINS: B.3.20 in NEI, sorry, in the Reg Guide 5.71, the revision that we're doing.

CHAIR BROWN: Okay. Well, let me -- I'm looking to see if I did write a note on that. I thought I did. Maybe I didn't.

MS. LAWSON-JENKINS: Okay.

CHAIR BROWN: Oh, yeah, here it is. It's B.3.21 actually.

MS. LAWSON-JENKINS: Oh, it's the one that we've been discussing a lot actually. Okay.

CHAIR BROWN: I guess my question on this is diversity is nice, but also a multiplicity of different types of virus systems, cyber systems adds to the complexity and difficulty of maintaining your assurance that you're doing stuff okay.

You can have too much diversity. And it

complicates. And how --

MS. LAWSON-JENKINS: Agreed.

CHAIR BROWN: -- balance with that?

MS. LAWSON-JENKINS: That's the word that I was going to use. You have to balance it. And that is, no doubt about that.

If you have Windows software in your control room and other places, one vulnerability there could be spread in various systems.

So, but at the same time, it takes effort to maintain different types of systems. It might be untenable to be able to have different types of software everywhere. So there is a balancing there.

And once again, that's risk-informed security. You have to be able to understand what is the risk on having several different types of ways of doing something, because you have to have procedures and processes and keep people trained on how to do that, okay, or having the same software or the same technology everywhere.

There is a tradeoff on that. And that has to be discussed. And it's going to be different depending on the circumstances. So we won't be able to make a blanket statement on that.

I mean, usually when we actually get

through the licensing aspect and they talk a bit about their plans and they get specific about the technology and what's being used, then we can give more informed guidance or ask them more informed questions. But it's something they have to keep in mind.

CHAIR BROWN: How come you don't get involved in the Mac versus Windows issues, because you can't -- there's a lot of stuff done in Windows you can't move over to a Mac environment and vice versa. And you have to maintain both of them under the -- it just seems to me that this -- and I'm not trying to side with industry by, you know, safety or anything. That's not the point.

It seems to me this would become fairly complex for licensees to manage if -- you know, what defines the balance or the reasonable approach? And it depends on person to person.

I mean, you have one definition when you're doing this kind of stuff, and then somebody else in your section or you retire and somebody else does it, and they've got another interpretation of what it means. That's --

MS. LAWSON-JENKINS: Well --

CHAIR BROWN: We've been trying to avoid that kind of stuff for years.

MS. LAWSON-JENKINS: No, but at the end of the day, it is the case that needs to be made by the licensee based on what decisions they made and to justify the decisions they made.

Personally, I would limit the amount of Windows --

CHAIR BROWN: I agree with you there.

MS. LAWSON-JENKINS: -- devices that you have and the data diode. For Windows, we don't know a lot of the details. It's a lot of proprietary software. That's why a lot of systems use Linux because you get the source codes with that, and you can look in detail.

But to be honest, you know, most people who are system users, they aren't going to go into that kind of detail. The people who supply the equipment may do it maybe, you know. And sometimes even they don't know what they're procuring, you know.

So supply chain and managing, deciding what type of access and what type of technology will be used at a nuclear facility is going to be, it always has been and it will continue to be challenging, especially with supply chain and that we don't manufacture.

We don't know exactly. You know,

sometimes you don't know exactly what you have in that black box. And it's been certified, whatever. But it's going to be a challenge.

And that's why, like I said, I keep going back to we have to have those dialogues and a discussion with the people who are supplying the technology --

CHAIR BROWN: So you're going to --

MS. LAWSON-JENKINS: -- and have them explain what's normal operation.

CHAIR BROWN: Okay.

(Simultaneous speaking.)

CHAIR BROWN: You're going to rely on a balance of common sense in other words. I'm trying to characterize this in some common --

(Simultaneous speaking.)

CHAIR BROWN: It's just seems to me that this was kind of a black hole that we could go down, and also it complicates things in terms of the ability, transferability of information from one system to another and everything else.

There's a good basis for having the same stuff everywhere, whereas there's a good basis for not having the same --

MS. LAWSON-JENKINS: Right. And it really

is going to be on a case by case basis --

CHAIR BROWN: Okay.

MS. LAWSON-JENKINS: -- how well you know the technology --

CHAIR BROWN: Yes.

MS. LAWSON-JENKINS: -- and things like that. So it's, they have to make their case on that.

CHAIR BROWN: All right.

MS. LAWSON-JENKINS: That's why I say we don't have, we can't just -- we shouldn't dictate in my opinion on that because it is one of those it depends. And there may be a good justification for what they did. And we need to hear it.

CHAIR BROWN: Okay. That's good.

MEMBER HALNON: Kim, this is Greg Halnon. I just have a quick question. I'm trying to follow the path here. In the Rev. 1 that we got delivered, A.3.21 is the heterogeneity. Is that just a typo in your slide?

MS. LAWSON-JENKINS: Let me --

MEMBER HALNON: I think you get -- it looks like the numbers are like one off. But that's not the real question.

In the Reg Guide, it's relatively sparse on the information. And I'll have to confess I didn't

know, I don't think I've ever seen the word heterogeneity before. But I followed it through. Then I opened up the NIST document. There's a lot more information.

Is the path that designers and people are trying to get through is to go from the Reg Guide to the much larger and more detailed NIST document? Is that how you expect people to comply with this to ensure that all the aspects are in the plan itself?

MS. LAWSON-JENKINS: The guidance that we have in Reg Guide 5.71 in the draft guidance for this revision is a tailored version of what's in this 800-53.

MEMBER HALNON: Okay. So that's --

MS. LAWSON-JENKINS: 800-53 is applicable for all types of IT systems, like we said, systems that have lots of Windows computers in there and lots of unrestricted or a lot more people accessing the system, and they're all connected to the internet. And there's a lot more things that are going on in networks.

And that's a very generic, you know, systems they're talking about. We have a tailored version of that for what we're doing for nuclear.

MEMBER HALNON: All right. But you

mentioned earlier that the text align so that if someone went to the NIST document to comply with B.3.21 --

MS. LAWSON-JENKINS: Okay. So these or the B, that is for the Reg Guide. So that's the NIST standards. That's a totally different numbering that you --

MEMBER HALNON: Well, I understand that. But I'm just trying to get the pathway. If I looked at, just in my lack of experience, looked at that in the Reg Guide I would have not understood what it meant. Then I went to the NIST document --

MS. LAWSON-JENKINS: Okay, okay. I understand.

MEMBER HALNON: -- and I understand it a lot better because there's a lot more verbiage. And I was wondering --

MS. LAWSON-JENKINS: Yes.

MEMBER HALNON: -- if that was the expectation is that the Reg Guide is a pointer in a sense to the --

MS. LAWSON-JENKINS: You could. We could do that.

MEMBER HALNON: I mean, that's okay. I mean, that's what you want. There's nothing in the

--

MS. LAWSON-JENKINS: There's nothing wrong with that.

MEMBER HALNON: -- NIST document that is wrong. It's that --

MS. LAWSON-JENKINS: Nothing's wrong with that. But not everything that's in the NIST document is going to be applicable for --

MEMBER HALNON: I understand.

MS. LAWSON-JENKINS: -- nuclear security.

MEMBER HALNON: I understand.

MS. LAWSON-JENKINS: Especially when they talk about privacy. We don't -- there is no privacy. So things like that, it just won't be applicable for our systems.

MEMBER HALNON: All right. I got it. Thank you.

MS. LAWSON-JENKINS: Next slide, Brian, please. Okay. Slide 43, supply chain. Sorry.

So, and supply chain for a few of the controls we removed the prescriptive guidance. It really was like how you -- it was too prescriptive.

If you look at the, you'll see what's been deleted. Lots of those things have not been changed, or they've just been deleted.

And we say that we should look for known vulnerabilities. The licensee has, sorry, the supplier has to demonstrate that there are no known vulnerabilities. And it has to be placed in the system in a secure manner, that we've added a lot of text about evaluating attack surfaces and attack pathways, because that's how you know how to put that securely in your system. Okay.

So we definitely made it more -- we got away from saying you must do this, you must do that, you know, a checklist of things, and said how you need to do due diligence and understanding what you're putting in your network and how to put it in there securely.

The glossary has expanded. We tried to balance on putting in just enough and not too much. In most cases, we tried to use existing definitions that came from NIST or DoD or somewhere that's, you know, more applicable rather than coming up with our own definition. But you'll see that.

Obviously, we updated the guidance, sorry, the reference sections to more up-to-date things since 2010.

And also we had numerous editorial changes when we had different people reviewing from public

comments, from OGC. And now we're going to put in more changes based on the discussion today absolutely for clearer guidance. Next slide, please. Okay.

So that is the overview of what we did or the changes we actually made in the document. Do we have any final questions on that before I go to the next steps?

CHAIR BROWN: Just one, and it's just a cross referencing type thing. I had looked back through B and C. Where's the direct reference to NIST for those items? I must have missed it.

I've seen NIST in some of the earlier parts of the Reg Guide. I mean, you know, when I keyworded that, I came up with a bunch. But I couldn't get a direct tie to how you tied in the Section B stuff we've been talking about, the -- all those, you know --

MS. LAWSON-JENKINS: Right. All right. I can provide you with a spreadsheet.

(Simultaneous speaking.)

CHAIR BROWN: No, I don't want that.

(Simultaneous speaking.)

CHAIR BROWN: How does the Reg Guide connect those things back to NIST? You reference not all the NIST stuff is in there, but these are based on

NIST. How does --

MS. LAWSON-JENKINS: There --

CHAIR BROWN: -- the Reg Guide translate that or connect the dots on that?

MS. LAWSON-JENKINS: Okay. There are tailored controls that you will find in NIST. So there is -- for every control in there --

CHAIR BROWN: Where are they told that? I'm sorry to -- but where in the Reg Guide are people told that all these tie to NIST? Are they based on the same numerical thing --

MS. LAWSON-JENKINS: No, it's a different numbering. I mean, NIST has something like 800 -- they had a lot of controls, a lot more than we have. So we took a subset of those controls. And then we made them very tailored for the nuclear security.

CHAIR BROWN: Okay. Let me ask the question --

MS. LAWSON-JENKINS: And that was in the original Reg Guide. So that was done on the very first Reg Guide.

So all we did for the update is to look at the controls. And we don't have a mapping if that's what -- there was a, I believe, and we could find that in one of the references. In one of the references,

and I could look it up in the minute before we close, there was a NUREG that was put out that did do the cross referencing between NIST and the guidance that we put out --

CHAIR BROWN: Okay. Let me phrase it again a different way. Okay. That's another document that nobody knows about.

I'll look at Appendix B, technical security controls. You reference all these things are derived from NIST.

But if I look at the lead-in of that overall Section B or Appendix B, it doesn't say that these, all these controls are derived from NIST and the document and the revision level.

It's referenced. I mean, NIST is referenced in this thing somewhere in the references. But it doesn't -- when I read this I didn't see it -- I didn't get that.

Let me -- I looked at these, and I said, uh-oh, they came up with all kinds of stuff. There was a lot of stuff in the last document.

MS. LAWSON-JENKINS: Okay. I think that if you look at Section 3.3 in the front matter before where we talk about security controls, you know, in the staff guidance at the beginning and Section 3.3

that talks about security controls, we say that we did a tailored version of the NIST controls. That's how we came up with those.

MEMBER HALNON: The bottom paragraph on page 7 in Rev. 1 also kind of goes through exactly what you just said, Kim.

CHAIR BROWN: It does? Okay. I missed that then.

MEMBER HALNON: It's in the background section of the --

MS. LAWSON-JENKINS: Okay. But it's -- and then I say this also, if you look in the section that talks about controls in general, how you apply security controls, we say that we tailored the version.

CHAIR BROWN: Okay. I got it. I see it now. I just totally missed that when I read it.

MS. LAWSON-JENKINS: Out of 160 pages, I'm not surprised.

(Laughter.)

CHAIR BROWN: At 11:00 or 12:00 at night, it's easy.

MEMBER HALNON: Charlie, this is Greg. I got one. I think it's just a housekeeping issue.

CHAIR BROWN: Yeah, go ahead.

MEMBER HALNON: Kim, when you referenced NEI 10-04, you said it was based on the current version. And then later on, you referenced NEI 13-10. And you actually put the Revision 6 in there with the same version or the same verbiage saying it's based on the current version.

Did you do that intentionally to leave out the rev number in 10-04, or was that just a housekeeping issue?

MS. LAWSON-JENKINS: I have to double check. I can't -- I have to look at this because --

MEMBER HALNON: I think it's around page 20. I don't --

MS. LAWSON-JENKINS: Okay. I know for NEI 13-10 there were several versions. And you see up to six. There were several versions of the document. And so I wanted to be clear on which one we were using.

10-04 and also for NEI 08-09 there were not multiple versions usually of the document. Once we approved it that was it.

MEMBER HALNON: Okay.

MS. LAWSON-JENKINS: Okay, okay. So --

(Simultaneous speaking.)

MS. LAWSON-JENKINS: But definitely go by

the references in the back.

MEMBER HALNON: Yeah, make sure it's intentional. I would just say for consistency either leave both of them the same or not.

MS. LAWSON-JENKINS: Okay. I understand.

MEMBER BIER: Charlie, this is Vicki.

CHAIR BROWN: Yes.

MEMBER BIER: I have one a little more philosophical point that I want to raise kind of to make sure that I understand things correctly and other people understand things correctly. I don't think there's been anything wrong implied, but just to clarify a possible confusion.

When we talk about risk-informed cyber security, I think what is meant is look at the eventual outcome, like is this affecting a pressure transducer which is not essential for safe operation or is this affecting a scram function or whatever.

And the reason I want to ask this is it seems easy, you know, both in my own mind and potentially for licensees to fall into the sort of pitfall of having, viewing the attack paths from a risk-informed point of view of like, oh, this one is more difficult and less likely to succeed or less likely to be used so we don't have to protect against

it.

And I don't think that's accurate, because if you protect against the easy ones then somebody is going to choose that harder one at the end of the day.

So I just wanted to clarify. Am I interpreting things correctly as to what's intended?

MS. LAWSON-JENKINS: First, one of the basis of risk-informed security is to look at the consequence of the failure of that SSEP function. That's probably one of the overriding issues. Okay.

As far as applying controls or mitigations to ensure that that function doesn't fail, there has to be, you have to meet the security architecture that you've established. And that architecture may change, you never know, depending on what the type of technology you're introducing.

And most certainly, it's in the rule that you have to have defense in depth. So you have to have, as we said, the preventive functions, the detection function, assume they get in, how do you recover from the cyber attack.

So it's not just one thing or a few things that they do. And then you can't just rely on, as I said, physical security or operational security. You need -- on some things that may not be sufficient.

And the reason I guess we're calling it risk-informed, because it takes, you're looking at multiple things. And you're trying to -- the licensee will have to determine what is going to be the appropriate level of mitigation based on what you're trying to prevent. Okay.

So you're using multiple avenues of trying to protect this asset and the pathways to make sure that you can have timely detection and respond to a cyber attack.

MEMBER BIER: So I guess my interpretation of your answer is it's defense in depth which kind of tells you, no, you cannot just dismiss some attack path and say it's unimportant because --

MS. LAWSON-JENKINS: No. And there was a question earlier about what methodology do you use to decide what's important. So they have to make their case on whether they use PRA or something else to say this is important, okay, and this is why we have protected it accordingly. Okay.

MEMBER BIER: Okay. Thank you.

MEMBER DIMITRIJEVIC: I would like to -- this is Vesna. I would like to add something to this, because Vicki brings up the important question. And this is why I make my previews come and show it,

because this is such a complex problem because you have so many different aspects.

Obviously, consequences, you know, they're very important. And maybe they can be measured through the PRA and maybe not. The PRA is not exactly positioned to measure importance of the factions and, you know, or you cannot really compare easily transients versus impacts on the systems, components, human actions. So PRA is already, if you have a complex issue, how to address the consequences.

And then we have to decide the aspect Vicki just brought, and this is what is likelihood of that cyber attack, I mean, how complex is, how likely it is to happen, and also what is extremely important from the consequence point of view, how likely is the recovery, you know, because importance of that, if it ever was the same of a certain system, is how long will that system be out of function.

So this is such a complex problem that when we can really maybe through that we can just really give only this very general, you know, directions. But as it's being applied, we will learn more.

I mean, you know, it is, this risk is very complex and consists of multiple parts, you know, and

they both contribute to this side. And really, I mean, you know, maybe even I really very much against anything this general, this is risk-informed, this is risk-informed. And we don't really know what risk we are talking about. In this moment, we are just learning more. So I have no any idea how to make this more specific. Okay. That's it.

MS. LAWSON-JENKINS: We'll probably talk about this a little bit more in the wrap-up. But I wanted to go on to the next slide, so if, no objections.

CHAIR BROWN: Go ahead.

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

So we started, as I said, updating the Reg Guide in 2016. We released it for public comment in 2018. And we delayed the work because we wanted to finish some industry initiatives and the post-assessment work and also the oversight program. We wanted to get through the full implementation inspections, which we did.

So we resumed the work on the Reg Guide now. And we received the last comments, no legal objections from OGC in July. Next slide, please, Brian. Okay.

I want to give you an idea just -- this is not all the cyber security branch does. But we are involved with the inspections for units, Vogtle Units 3 and 4. We are engaging with NRR and Region II and Region IV staff who are performing digital upgrade reviews. And we're talking to them and participating.

As we mentioned, we are engaged on the Part 53 rulemaking and guidance. And some of that work that they're doing may leverage what we are doing in this upgrade of the Reg Guide.

And we work a lot with research, the Office of Research and the DOE labs on different technologies of things that are coming up the pike or things that we see coming.

So it isn't a matter that the work we are doing is all reactive. We do the -- you're saying we wait till the inspections, and then we start looking at what's been implemented all the time. That is not what we're just doing. We are actually looking at the development of guidance and how certain technologies may be used possibly in the future.

I know we see websites of licensees talking about some of these things such as supply chain, obviously, and drones, artificial intelligence.

I've worked on security models, how to

revalidate that the equipment, the security postures, what they're doing is actually effective. We are actively involved in all these issues.

So we're laying the groundwork I guess for the next revision of the document. But it is important that we get this one out. It's important we get this one out, because the last version of the Reg Guide that was out was the original version, which was in 2010.

I did a quick Google search for some reason for the draft guidance that we put out in 2018. And DOE and, what was the other one, DOE and there was -- oh, NIST actually, they actually referenced the draft guidance that we put out in 2018 because they couldn't or didn't want to reference the 2010 version.

It is really important that we give, you know, us, where we get it to the point that we feel that it's adding value we need to get this published. That's just the goal.

MEMBER HALNON: Kim, this is Greg Halnon. It was my understanding that there's no licensees even using this right now. Is that right?

MS. LAWSON-JENKINS: The licensees are using, the current licensees, almost all of them are using NEI 08-09. Okay. Both 5.71 and NEI 08-09 are

acceptable ways of implementing a cyber security program. But they are not, as we keep saying, are not identical. Okay.

In addition to the updates that we are doing based on the lessons learned from the cyber inspections, this updated guidance will be used by stakeholders, including vendors and equipment manufacturers. Okay.

If you look at the comments that we received during the public comment period, some of the best comments -- all of the comments are helpful. But the really, really the best comments came from vendors, because they wanted more guidance on how to implement things, not to say you must do it this way. Okay.

But they were very good comments. And we -- you could see on some of the responses, we said we accepted those comments, and we incorporated those things.

MEMBER HALNON: So I think my misunderstanding was your urgency was not for licensees. It's for the vendors and supply chain piece.

MS. LAWSON-JENKINS: And you never -- in the end of the day, the guidance is valid. It will

not be the basis for inspections for the currently operating plants. Okay.

But if they do digital upgrades, they will probably look at the latest guidance, because the guidance that was put out in 2010 won't reflect all the lessons learned.

So it would be good to update this guidance and not have the NRC's guidance still based on what we knew in 2010.

MEMBER HALNON: Thank you.

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

CHAIR BROWN: Not quite.

MS. LAWSON-JENKINS: Okay. Back.

CHAIR BROWN: I keep seeing the wireless thing pop up. What in the world are we doing looking at wireless, trying to figure out how to use wireless, or why not just say no?

MS. LAWSON-JENKINS: The staff position has not changed on this. As I've said throughout the presentation on a lot of things, if wireless is ever introduced, there would have to be an LAR for the currently operating plants, okay, to do anything.

The case has to be made how to do it securely. And that's probably why we haven't seen a

lot of guidance yet on that.

Clearly, wireless can be done. I came from the Department of Defense. We do wireless. But we have unlimited resources. And you could do that.

CHAIR BROWN: Well, the Department of Defense is, you know, is sad they did that. They got hit through that source.

MS. LAWSON-JENKINS: Well, but, you know, there are some places, when you fly in a plane you have to use wireless.

CHAIR BROWN: No question about if you're in an airplane you can't drag a wire behind you.

MS. LAWSON-JENKINS: So --

CHAIR BROWN: I'm just hoping that nobody is sitting around trying to do research and figure out how we can use wireless. Let the industry figure out how to do that and tell us that it's good. That's --

MS. LAWSON-JENKINS: I agree. We should be in oversight mode on that absolutely.

CHAIR BROWN: Yeah. Okay. That's it. Thank you. You can go on now, yeah.

MS. LAWSON-JENKINS: Okay. I just want, I want to make a clarification on something, that we are doing research. We are actively looking -- how can I say this?

I know you just said to let the industry figure this out. As I kind of, as I'm trying to say in this slide, we are being a little bit more proactive because we don't want to be in a reactive mode all the time. We need to come up and understand what's coming ahead and see and try to develop a staff position at the same time. So I want to be clear on that.

While I agree we are not advocating and pushing for something, we don't want to wait until a decision is made that we're going to do something and then it's on us to say, no, you cannot do, you know, do it.

So we are still -- we have a research office that is looking at this. They collaborate with the, our group to talk about what we've seen and the possible pitfalls.

So I don't want to get down the rabbit hole on wireless. And the industry may be using it for non-safety, okay, and non, you know, security functions, because there's no real restriction on that because there's no impact on their cyber security plan.

But we're taking a we'll see attitude. We are actively looking at this on our own because we

don't want to be caught unaware, and we want to have our own positions when the proposal is made. Okay.

CHAIR BROWN: Okay.

MS. LAWSON-JENKINS: I do believe in being proactive on some of these things.

So back to the timeline. Okay. So we would like, okay, now that we've had this opportunity to have this engagement with the ACRS to possibly get this Reg Guide out for public comment in 2022, in January.

And the reason I'm mentioning January is that it would actually get it published this year if we can do that. Every month that we wait it's going to delay getting it out.

The ACRS will have another brief. You'll see me again if we let it go in January before the end of the year to say the final language that's in there and to get a resolution before --

CHAIR BROWN: Okay.

MS. LAWSON-JENKINS: -- published --

CHAIR BROWN: Let me give you the game plan so you'll know.

MS. LAWSON-JENKINS: Okay.

CHAIR BROWN: We are going to, as a result of this meeting, we will have a full committee

meeting. And I think it's scheduled for December. And we will prepare, I will prepare a report for, you know, which gets the consensus of the committee.

We may have suggestions. I've made comments, you know, along the way. You know, I've written some stuff down there, observations, suggestions, to think about.

And then you can, you've had suggestions via the meeting. Remember there's no, they are individual member's suggestions or thoughts, some you might want to consider in preparation for clarifications.

And we'll go through those in the December meeting. We'll have a report. And then you should be able to get it out sometime after that.

MS. LAWSON-JENKINS: Okay.

CHAIR BROWN: I think that's sort of consistent with your timeline, within a few weeks anyway.

MS. LAWSON-JENKINS: Okay. That would be wonderful. Okay. Thank you. And --

CHAIR BROWN: Christina, was I right, that we do have this scheduled for the December meeting, don't we?

MS. ANTONESCU: Yes, sir. We do in

December, first week of December, the full committee meeting.

CHAIR BROWN: Okay, thank you. All right, go ahead, Kim. I'm sorry.

MS. LAWSON-JENKINS: No, I think -- Brian, the next slide, please. Okay.

So basically I'm restating what I said at the beginning for key messages. Everything that is actually in this guidance, it isn't an academic exercise. We have actually seen programs implemented. We've seen what works. We've seen better ways of giving -- of writing guidance. We've pulled this from IAEA, from NIST. There's a lot of lessons learned in here.

There is no change in the staff's position. There are only clarifications. And we have one new regulation which is the cyber security notification. And the world has changed since 2010 and the technology and it's going to continue to change. And we'd like to get this updated guidance out as the basis for new guidance that will be from Part 53 that they might leverage. And as I said, also for the vendors to see the best practices that they can incorporate and for the licensees who want to upgrade digital equipment also. They can look at

this.

And I believe we have final, any final closing questions and answers if anybody has any more questions.

Brian, I think the next slide is Q&A, yes. So any last questions.

CHAIR BROWN: Members, this is the -- before I go to the public comments, does anybody want to add anything other than what they've already said or do they want to clarify or amplify? This is the opportunity before we go out for public comments.

MEMBER KIRCHNER: Charlie, this is Walt. May I ask Kim one question?

CHAIR BROWN: Yes.

MEMBER KIRCHNER: Kim, under vu-graphs, you mentioned Vogtle 3 and 4. I think you've got a number of plants, too, like Limerick and others that are proposing much more expansive use of digital I&C.

As a result of those interactions, are you testing this against those reviews or interactions or inspections? Because now we're in the situation with those newer plants or new digital I&C. It's not -- I'll say it's not backfitting in dealing with it in an older plant that's primarily analog, but you're now seeing much more expansive use of digital. Is that

impacting your thinking in any way?

MS. LAWSON-JENKINS: We are clearly basing this based on lessons learned that licensees have experienced now with implementing fiber security plans, so they are aware that we will be looking at the impact of adding the new equipment and technology to their plants.

There is a security control, like I said, obviously, 140 controls, but there's one that's called security impact analysis where the licensee has to say what is the impact of adding the new features or equipment to the plant and they have to have a detailed analysis that shows that they looked at this.

I have participated or I have observed factory acceptance testing, so I can see the requirements that went to the developer, the system developers and could see the responses that came back. I will probably be participating in a site acceptance testing to get an understanding of how they're going to introduce the new equipment into their cyber security program.

So we are, like I said, very involved in these things. It isn't that we have a hands off and don't look at it until we have another formal inspection. And so they have to explain to us how

they understand the attacks purpose, how they understand the pathways of communication paths, how those are being protected and they will show that when they actually implement the equipment in their plant.

Did I answer your question?

MEMBER KIRCHNER: Thank you. I was just curious whether or not you were seeing, as we go more digital, as I was saying -- different strategies like in architecture or in hardware space to minimize vulnerabilities and attack services.

MS. LAWSON-JENKINS: Yes. You know, when it is using new technology, you're using more embedded systems. You have ways. You limit the amount of interaction and updates you'll have to do, the type of equipment they're using for manual -- sorry, maintenance and testing is very controlled, that you know, and we see a lot of security controls applied there and under what conditions they're being used. So they are very aware of the security aspect of their equipment now when maybe 20 years ago they wouldn't have been. So there is thought of doing that well by the systems supplier, not just the operator who is going to install the equipment. They understand that they need to address security earlier in the life cycle.

MEMBER KIRCHNER: I was just searching to see if you were seeing, for example, design approaches that are used for reactor protection systems being also implemented in control or balance of plant and other systems such that it's much more, how shall I say, burned in software than free-form software so to speak so that the device, the individual CDAs are much more resilient and less vulnerable to all the issues of cyber attack.

MS. LAWSON-JENKINS: I can't -- because we -- like I say, we observed the processes that they used for the secure development of the device, so that's why I said we can participate in the factory acceptance testing and the site acceptance testing. We won't get that kind of information what you're asking for which, I believe, until we actually see the implementation of the equipment. Like said, that's the realm we operate in, okay? For better or worse, when we actually have regulatory oversight, is when the equipment is actually installed.

And then at that point the licensee will take credit for whatever changes -- whatever they did for the -- in the actual system. So it would probably be more clear then, so not yet because a lot of things we haven't discussed yet with them. We are definitely

in an observation mode at this point and no formal requests or answers are made at this point.

CHAIR BROWN: Walt, we're planning -- Christina, correct me if I'm wrong, right now, I think Limerick and Turkey Point are planning on replacing their existing analog systems with digital systems, safeguards and reactor protection. I don't know the extent, but that's the general. And we'll be seeing those now as part of the design reviews.

MEMBER KIRCHNER: Yes, so maybe my question -- I'll just hold these and that's probably the more appropriate venue to ask these kinds of questions. Thank you.

CHAIR BROWN: What Kim is dealing with is after the fact, the systems designed and then they have to deal with how the vendor took care to protect it. It's a different -- they're in a different pocket here.

Okay, I heard somebody else about to say something and if you're still -- members, you still wanted to say something go ahead. Hearing nothing --

MR. HECHT: Charlie, this is Myron.

CHAIR BROWN: Yes, go ahead.

MR. HECHT: Just a -- you made a side comment back on chart 27 and I'm not sure how

seriously you meant it, but it's not on the chart, it's based on what Kim said. But you said you haven't come up with clear supply chain guidance yet.

There is some guidance as you pointed out later in the presentation and I don't want to try to find it now, but there is some. Of course, NIST has a 400-page publication, 800-161, on that subject.

And so you come from DoD which has been dealing with it for a long time. Why -- and I guess the other part of it is that we do know that supply chains can -- are an attack path, so the wins taught us that.

So I guess is more needed and if so, why are you not considering using available sources to both do that section and if it's not needed, why not?

CHAIR BROWN: Do you remember which section it was? You said Slide 27. That was defense in depth and I'm just looking at that now and I don't see supply in there.

MS. LAWSON-JENKINS: Go forward, Brian, because I did talk about supply chain later on towards the end. Keep going. There. And maybe -- two more slides, keep going. Keep going. Two more. Another one. Another one. There. Okay.

Please do look at that section and

Appendix C that talks about supply chain. And like I said, we added information that talks about attack surfaces of pathways. We can -- I think eventually we need guidance and even IAEA hasn't come up with this yet, guidance on supply chain. They're in the process of doing that, but did not want to -- we do need additional guidance.

I think we've provided some clarity on this one and this guidance, but I'll be the first to agree it doesn't go as far as I think it needs to go, but because those recommendations are still in flux, that was a design decision on my part. I did not want to put information there that hadn't been generally vetted or at least accepted by the community yet. So I'd be the first to agree that we need more information on supply chain.

And right now, like I said, the best defense of supply chain is to minimize the attack surface and to know what should be going on in the network and be in close contact with the suppliers.

This has been a big issue with -- obviously, the supply chain is not just nuclear security. It's all of the areas. But I do feel that for critical infrastructure that's going to be a special case. I think if we won't have the level of

protections, possibly we won't be at the exact same level that we have in the Department of Defense because like I said there's more resources and things like that there where they have to be above what you have in normally commercial equipment, commercial grade equipment. It has to be higher than that.

So hopefully, CISA out of DHS for critical infrastructure will start helping and leading in the guidance on that, but I don't believe this will be solely tied to nuclear security. It should be definitely infrastructure, critical infrastructure. We may get additional guidance and are working. We have people involved with the guidance out of IAEA also.

CHAIR BROWN: When you talk about supply chain, do you mean qualified suppliers or are you talking about replacement parts or both?

MS. LAWSON-JENKINS: Both, both. I mean at the end of the day, any of that can affect the security of your system, so we have to have everything in there. Yes.

CHAIR BROWN: Okay.

MEMBER HALNON: Charlie, this is Greg. I guess I'm confused. I thought that the urgency to get this out was primarily for the supply chains because

no licensees are using it. And now you're saying that we have to continue to add information for the supply chain?

MS. LAWSON-JENKINS: Well, we have more information than just supply chain. However, and I'll be candid about this, this is what any guidance, you won't -- it won't be finished. It will never be finished.

Okay, there's information in here that is useful currently to the vendors and the licensees who might want to upgrade systems. I absolutely agree that more information that can be added or should be added, but there's no consensus on it yet. So that's why I prefer not to add it today. But it should not take candidly another ten years to get another revision of this document out, not for cyber security.

MEMBER HALNON: Okay. Thanks, Kim.

CHAIR BROWN: Okay, I don't hear anything else from members.

Christina, how does the phone line work now? They're patched in? They don't have to be connected. They're there now.

MS. ANTONESCU: They don't have to be patched in. Whoever is on line from the public can make a comment.

CHAIR BROWN: Okay. All right, I'm inquiring of the public right now, whoever is on the line, this is your opportunity to make a comment. If you would speak up, give your name, and then go ahead and provide your comment and organization.

MR. MOORE: Members of the public may have to press star-6 to unmute themselves.

CHAIR BROWN: Oh, okay. Thank you. I hope you heard that. You might have to press star-6 in order to unmute yourself.

I don't hear anything, so we will come on back. I think this kind of wraps up --

MS. ANTONESCU: Member Brown, I have a question.

CHAIR BROWN: Go ahead.

MS. ANTONESCU: Can you let the staff know what to prefer for the full committee meeting, what your thoughts are, what they should present at the meeting?

CHAIR BROWN: Well, they should present -- obviously, we'll have what, about two hours or two and a half hours at the meeting, full committee meeting?

MS. ANTONESCU: Yes, about two and a half hours, yes.

CHAIR BROWN: Between the two meetings, I

think most of them -- how many members do we have? We have about six members here today? Did I count right? About the same. We had a few more, I think at the other one.

I would abbreviate the first few, what I call the stuff you did the last time with no more than intro part of it. And then I would try to focus on some of the issues we brought up on some of the slides, those that didn't draw much response, you can probably reduce those.

MEMBER HALNON: Charlie, this is Greg. I suggest that you give it some thought first and work through it methodically as opposed to doing it on the fly. I think for two and a half hours it deserves some reflection on what you want done. Just my suggestion.

CHAIR BROWN: No, that's a good point. I have some -- if anybody has got some questions or items they would like to be covered, please send them to me and we'll get those wrapped into the presentation.

MEMBER PETTI: Charlie, it just seems to me the obvious questions that we raised about new plants and how to get those people to know that there's stuff over here that's important for them to

consider, how did that work? To me -- I still don't have in my mind don't have a clear understanding of how that works. It's really not their purview and you know, what's the right answer? Are we looking for work around? What are the options, those sorts of things. And that may require Kim's management to be involved or something because their focus is existing plants, but we've got this other concern.

CHAIR BROWN: Yes, that's the thing I want primarily to be able to address. It's wired in with the change to this particular Reg. Guide.

MEMBER HALNON: And that can could segue into how they're connected with the Part 53 effort, too.

CHAIR BROWN: And also -- yes. Because the design issues are going to come up. These things are complex and to me there's a number of things we do in the design space that we have to do in the beginning and even though we know there's all these other ancillary issues that we cover by other cyber security type approaches to doing things. But there are certain design items we have to cover. Just like we do with how do we evaluate a system relative to the principal -- the framework, the principal design criteria. And this gets cranked into that as well

because it's one of their concerns, the control of access issue.

We can feed that back. I agree with you, Greg. I've got to go back and look, but if you notice the primary thrust of most of my -- most of the stuff I address was how do we get to the resolution of getting people not to push back during the design phase.

MEMBER HALNON: I agree. I think if you can get the transcripts, you can probably walk through it and come up with a present decent list for presentations' format.

Vicki has got her hand up, too, just to let you know.

CHAIR BROWN: Go ahead, Vicki.

MEMBER BIER: Sorry, I had to unmute. I would say that probably the risk-informed aspect of this should be at least a little bit of time in that presentation. As Vesna said, it's kind of complex and sort of a work in progress or a work of art or something to figure out how to do that best. So other people on the committee may have good comments on that.

CHAIR BROWN: Okay. Any others? How did you phrase yours, Dave, the same thing I was talking

about. I'm trying to remember. I think you said something that tweaked my memory and now I don't have it any more.

MEMBER PETTI: Yes, how do we in a process sense get the advance reactor folks to look at this?

CHAIR BROWN: Well, it's not just advanced reactors. It's backfit equipment into the operating plants.

MEMBER PETTI: Right, right.

CHAIR BROWN: At the design stage.

MEMBER PETTI: Yes, right.

CHAIR BROWN: Design phase I should say. And ditto for operating plant backfits.

MEMBER BALLINGER: This is Ron. Aren't the advance reactor people by definition going to have to deal with the risk-informed aspect of this?

CHAIR BROWN: Well, you're still going to have to have a protection systems. It's got to have some type of instrumentation and control. It just depends on the characterization of them.

MEMBER BALLINGER: But since risk informing is a bit subjective, that's going to get to be pretty important I think. No?

CHAIR BROWN: I don't know. I have a hard time risk informing my safety protection systems.

MEMBER BALLINGER: Yes, but that's just the starting point, right? I mean it's the key point, but it's a starting point.

CHAIR BROWN: Well, they're applying risk informing to see how hard do they have to go after certain quote digital assets. I mean if their failure doesn't create a problem, then it's a don't care. You don't do anything. If it creates a little problem, then it's not much -- you do a little bit, but no more. And then if it's a big problem, then you do more.

MEMBER BALLINGER: But this implies there's some kind of figure of merit, you know, people have suggested using the PRA.

CHAIR BROWN: Yes, well a PRA doesn't address what these components look like.

MEMBER BALLINGER: Yes, yes.

CHAIR BROWN: It's more of a direct result of things not working or other design aspects from materials or other stuff not working, whatever it is. I don't want to convolute it too much.

MEMBER DIMITRIJEVIC: We have sort of like different components, like you know, the cyber security, the plant safety, I mean and all getting mixed in the big pot. So I mean -- but this should --

I think it deserves to be discussed again.

CHAIR BROWN: Kim, you made the observation that hey, you're all in your world and NRR is in their world. And the real problem is as I think we envision it, there's not a coming together on how certain pieces of your world need to be addressed in the design world because that's part of the equipment and overall functional architecture. They're separate from the stuff you deal with in the more abstract cyber world.

I think it would be a really good idea if you all and NRR would -- you know what the issue is. We discussed it ad nauseam for the first hour and a half of the meeting. And somehow, you all have to get together. We are in between and it's -- we're kind of getting hammered from both sides. And we know what we're going to do from the design standpoint, the certification standpoint, but it's making it very difficult to get there without a lot of angst on the part of the staff and thinking that they're getting into other people's turf, if you want to call it that.

So I don't think I'm speaking out of turn, but I think it would be useful if NRR and NSER would -- hey, look guys, we've got an issue we're dealing with. How do we help resolve this because the

committee is going to continue to address making sure there's adequate control of access, not being allowed in that architecture that we have evaluated when the staff presents the new design architectures and frameworks.

MS. LAWSON-JENKINS: I want to be clear on my earlier comment. I didn't -- I don't want to give the impression that we don't look at the NRR documentation or the recommendations or specifications they put out. We do work together and one of the later slides kind of alluded to that, especially on things such as digital upgrades and other areas. So we work with research. We work with NRR. In some circumstances, we work with NMSS. I don't believe in operating in different silos because as you said, security can cut across all of those areas.

But at the same time, we have our own areas of expertise. I feel comfortable talking about security.

CHAIR BROWN: I understand that. I understand that. But when we're in a design certification phase and we're looking at an architecture and we look for how do we prevent data transmissions and other access into the reactor safeguards, protection systems, and the other critical

safety systems that those feed or that -- and we look for where are the protections from a data transmission and we get pushback that they can't do it because that doesn't get covered until the COL. And that's for new design, you know, that's for brand new design plans. The same thing is going to be similar, not quite as bad for the backfits. And that's a difficulty. So that's the pushback we're dealing with.

I would just hope that -- and they're pointing at you all, not pointing -- that's the wrong word. They're saying they're not allowed based on the rule and I don't agree with that. I think that's short sighted to say the least. That's my words, not the committee's words. Recognize that, okay?

MEMBER PETTI: To me, my concern is that the right people are at the full committee meeting to address this issue. What I don't want to see happen which happens all the time is that's not us. That's so and so's responsibility. This is an issue that's cutting across. And so it's not necessarily Kim. The message back to us is get the right people in the full committee meeting so that we can address this and get this resolved.

And so it may not be you, Kim. You may have to go your management. They may have to walk

across to NRR management, but that's one of our biggest issues and we just want to get it on the table and get the right people in the room, so we can figure out how to get there because personally, I'm not an expert, but I don't think this is a big ask. We basically identified sort of a hole, if you will, in the way the processes link up that we think just isn't in the best interest of the Agency or the applicant. And how do we put it all back together so that we don't have the problems that we've identified in our letters.

Is that fair, Charlie?

CHAIR BROWN: That's very good. You said it exactly right. We've been dealing with this for several years. We did it on AP1000. We were successful on APR1400. We finally got there. And NuScale, it came out okay although there was a little bit of pushback, but it came out okay also.

But it was brutal. It was hard to deal with. It was always we really can't do that. And the vendor, the licensee just decided to do it anyway. And once he decides, we're home free. So Dave, you phrased that very, very well. Hopefully, that's in the transcript.

MEMBER PETTI: You can take it back to

wherever we have to take it back to.

CHAIR BROWN: So he phrased that right. Somehow management, you guys have to get together. We're going to keep working on this and all it does is cause more work for both NSER and NRR to keep having to deal with this issue as it comes up from us.

You would see a little bit of our frustration in some of the reports we've written recently.

MR. MOORE: Member Brown, Jim Beardsley who is Kim's branch chief, I believe, is on representing management and he also has had his hand up and patiently waiting, so you may want to call on him.

CHAIR BROWN: I didn't see it. I'm sorry. There's no hand up on my computer.

MR. BEARDSLEY: Thank you, Scott. I actually took my hand down because I was going to make the same point that was made before, that we hear your concern and we understand and we look forward to getting any other information you'd like to have addressed at the December meeting so we have the right people at the table to do so.

CHAIR BROWN: Okay. I have a few observations or suggestions based on some stuff I saw

and it's similar to the one on the deny whatever. That one particular thing that everybody and Kim picked up on and she's going to think about. I had a few comments and thoughts about how some stuff ought to be I guess clarified. I'll pass those on. Those are mine. They're not recommendations. They're not committee things that you all can decide what you want to do with them. I'm just passing them on. Those are things that I think you might want to address in part of the meeting as well. And I did discuss them here.

And then I'll think about some other stuff. But Dave and Greg, they hit on -- the big issue is the -- I don't want to call it confrontation, the interactions on this other issue. We've just got to get through this so that people are working together and we're not always at loggerheads.

So Dave, Greg, you've got any other side comment on that?>

MEMBER PETTI: No, you did it. Thanks.

MS. ANTONESCU: Member Brown, all the staff and management from all the offices were invited at this meeting and previous meeting.

CHAIR BROWN: Okay. Well, they've heard it. They know what's going to it. Now they've heard it again.

All right, if there's no other -- if I'm not missing anything else, I think we are done and I guess have a good weekend to everybody and the meeting is now adjourned.

No, don't go. It's not adjourned yet, I'm sorry. One thing I want to make sure is clear. You can take the share down.

I want to thank Kim for a very good job of giving us the presentation and explanations, her patience with our repeated questions. So I just wanted to make sure that Kim understood that, that this was a good session and I thought it was very valuable.

MS. LAWSON-JENKINS: I appreciate the opportunity to discuss why we have what we have in the document. No, really, and I appreciate the comments and your comments and input will help make it a better document. Thank you very much.

CHAIR BROWN: Okay, Kim.

MEMBER DIMITRIJEVIC: Thank you, Kim. It was a wonderful presentation. Thank you.

MS. LAWSON-JENKINS: Thank you.

CHAIR BROWN: All right, so with that -- did I miss anybody?

I didn't invite Michele. Did you have

anything else you wanted to say at the end of the meeting, Michele?

MS. SAMPSON: No, I think Kim has so wonderfully covered everything. Thank you very much. We appreciate the opportunity for this meeting.

CHAIR BROWN: Okay, and thank you. All right, see you all at the full committee meeting and hopefully we'll drag ourselves through this again with a little bit more clarity. So the meeting is now adjourned.

(Whereupon, the above-entitled matter went off the record at 3:30 p.m.)

U.S.NRC
Protecting People and the Environment

# Revision of RG 5.71
# (Draft Guidance 5061)

Kim Lawson-Jenkins
Cyber Security Branch
Division of Physical and Cyber Security Policy
Office of Nuclear Security and Incident Response

U.S.NRC
Protecting People and the Environment

# Overview

- Key Messages
- Background
- Updates
- Conclusion
- Q/A

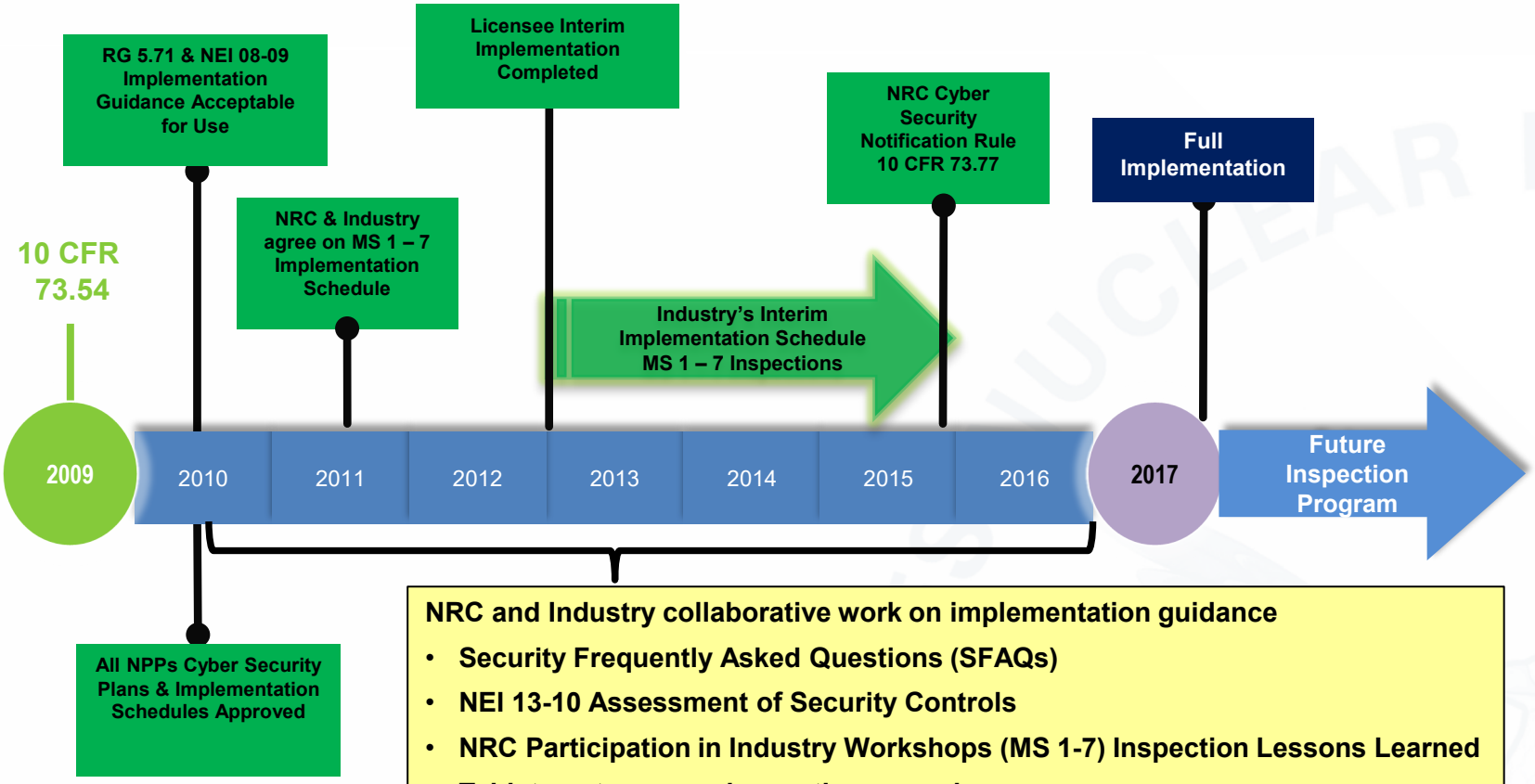
U.S.NRC
Protecting People and the Environment

# Key Messages

- Since 2012, operating nuclear power plant (NPP) licensees have implemented cyber security programs and the NRC has implemented effective oversight of the licensee's CSPs.
- No changes in staff's position, only clarifications and one new NRC regulation 10 CFR 73.77, "Cyber Security Event Notifications".
- DG-5061 reflects the lessons learned since the issuance of RG 5.71 and prepares for the future.

# Background

## Cyber Security Program Timeline



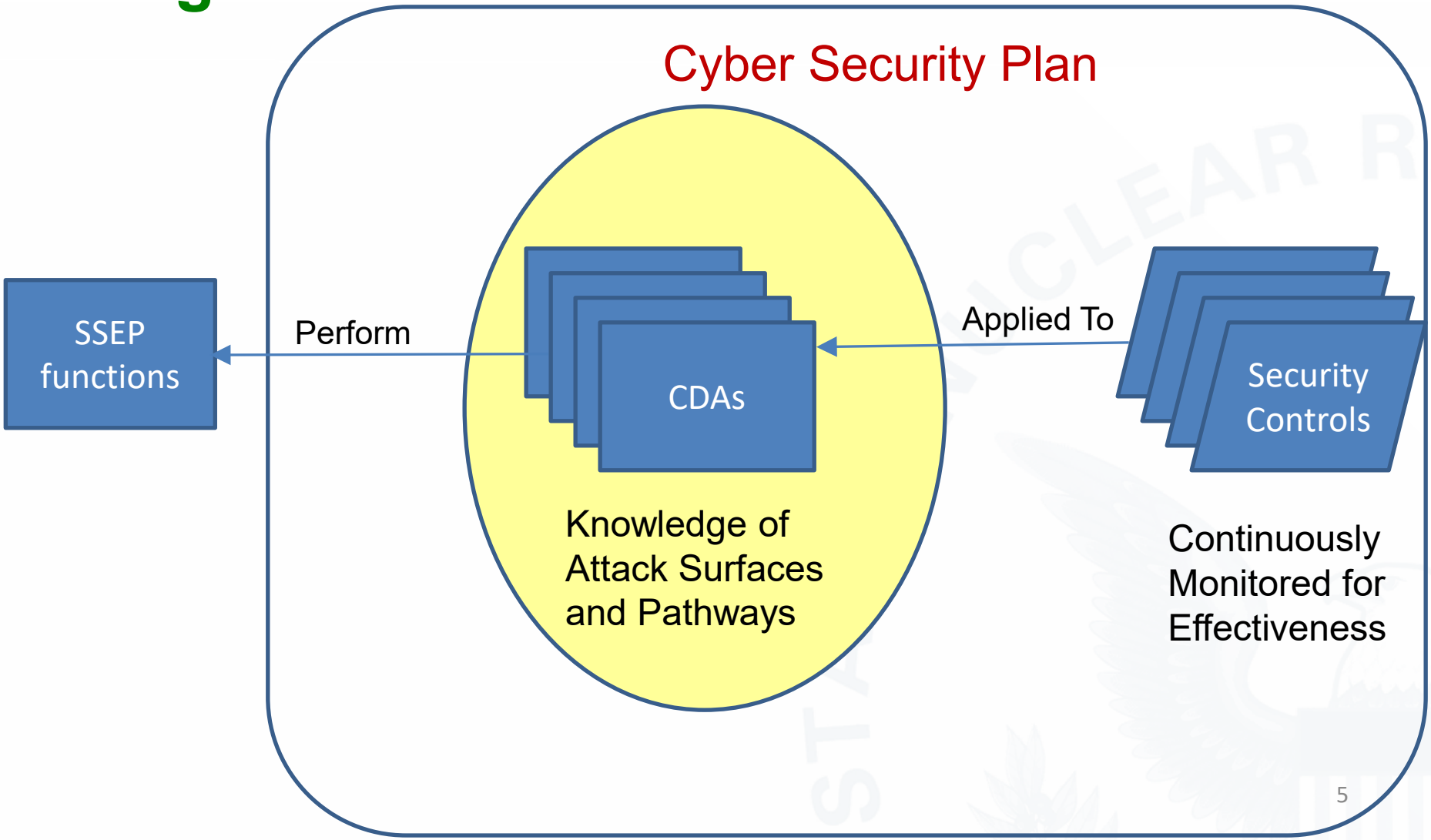

**NRC and Industry collaborative work on implementation guidance**

- **Security Frequently Asked Questions (SFAQs)**
- **NEI 13-10 Assessment of Security Controls**
- **NRC Participation in Industry Workshops (MS 1-7) Inspection Lessons Learned**
- **Tabletops to assess inspection procedure**

RG- Regulatory Guide
NEI - Nuclear Energy Institute
CFR – Code of Federal Regulation
NPP – Nuclear Power Plant

# Background

## The Big Picture



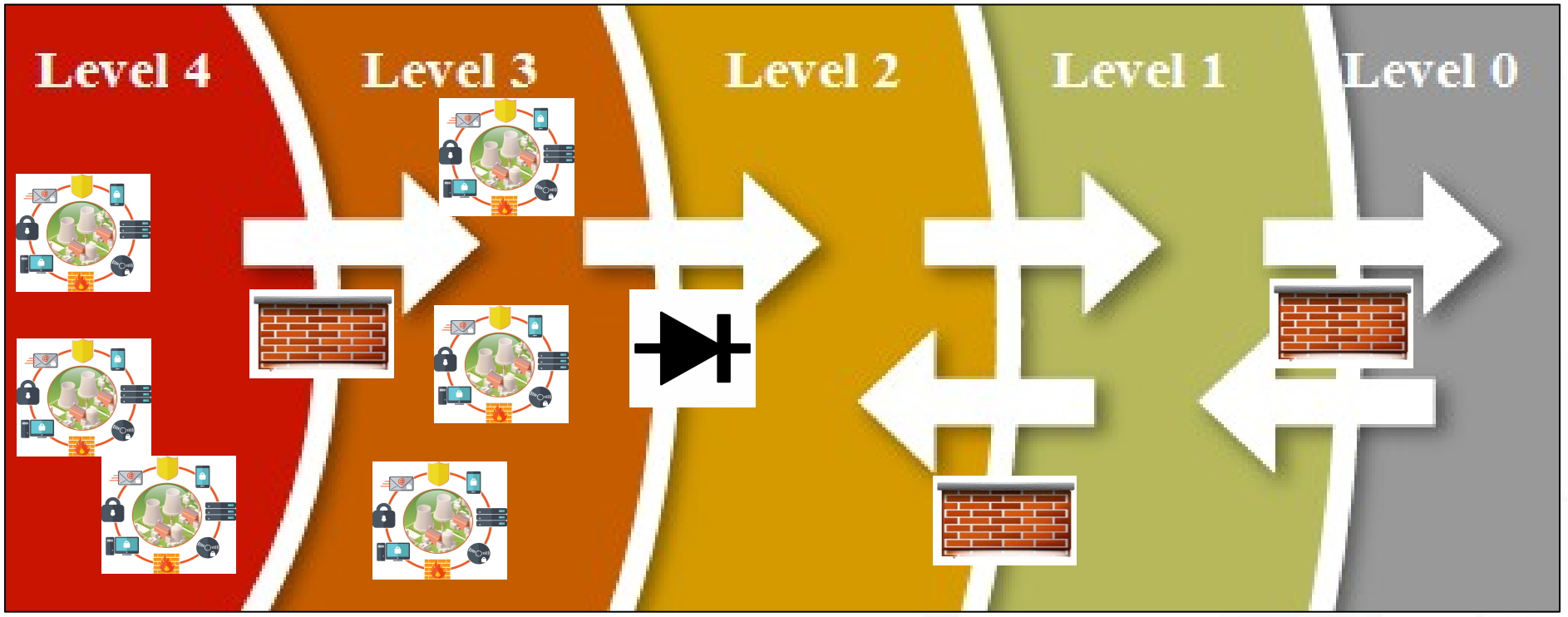
# Background

## Milestone 1 – 7 Inspections

2013 → 2015

| MS 1 | MS 2 | MS 3 | MS 4 | MS 5 | MS 6 | MS 7 |
|---|---|---|---|---|---|---|
| Establish the Cyber Security Assessment Team | Identify Critical Digital Assets | Implement One-way Deterministic Device | Access Control for Portable & Mobile Devices | Implement Observation & Identification of Obvious Cyber Tampering | Apply Security Controls to Most Important Critical Digital Assets | Implement Ongoing Assessment & Activities for Applied Controls |

# Cyber Security Defensive Architecture



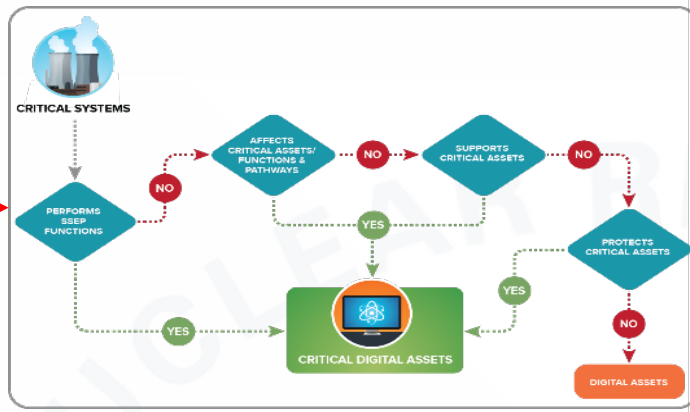

One-way Deterministic Device

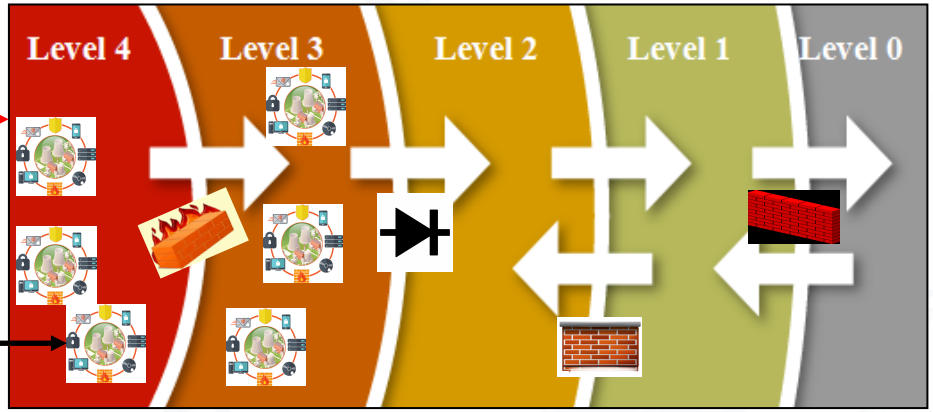
U.S.NRC
Protecting People and the Environment

# Milestones 1 - 7

1. Cyber Security Assessment Team
2. Identify Critical Digital Assets (CDAs)
3. Implement Defensive Architecture
4. Apply Security Controls

Most Risk Significant CDAs

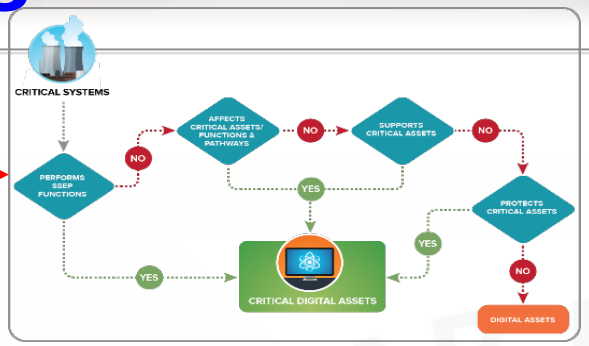


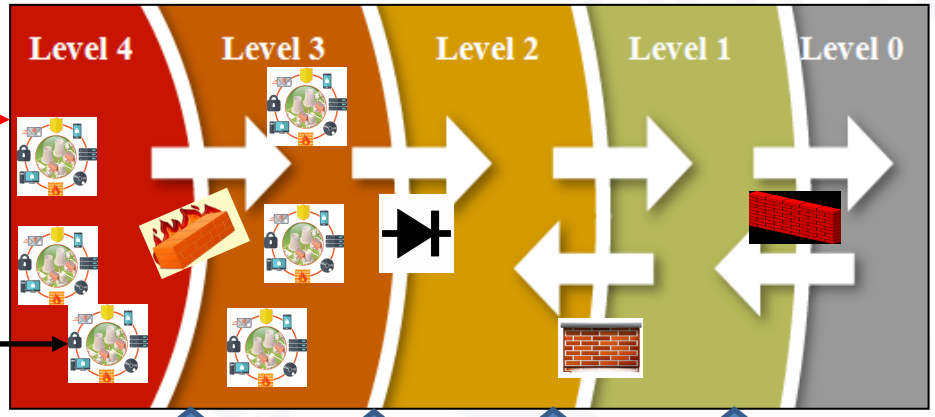



U.S.NRC
Protecting People and the Environment

# Full Program in RG 5.71

1. Cyber Security Assessment Team
2. Identify Critical Digital Assets (CDAs)
3. Implement Defensive Architecture
4. Apply Security Controls




CYBER SECURITY PROGRAM

| | | | | |
|---|---|---|---|---|
| Defense-in-Depth | Security Controls NEI 13-10 | Mitigation Strategies | Training | Manage Cyber Risk |
| Periodic Review | Modification Evaluation | Incident Response | Procedures | Records Retention |

# Milestones 1 – 7 Inspections

| Inspection Year | Number of Inspections |
|---|---|
| 2013 | 20 |
| 2014 | 22 |
| 2015 | 21 |

All of the findings from the inspections were of very low safety significance.

The areas with the highest number of findings were:

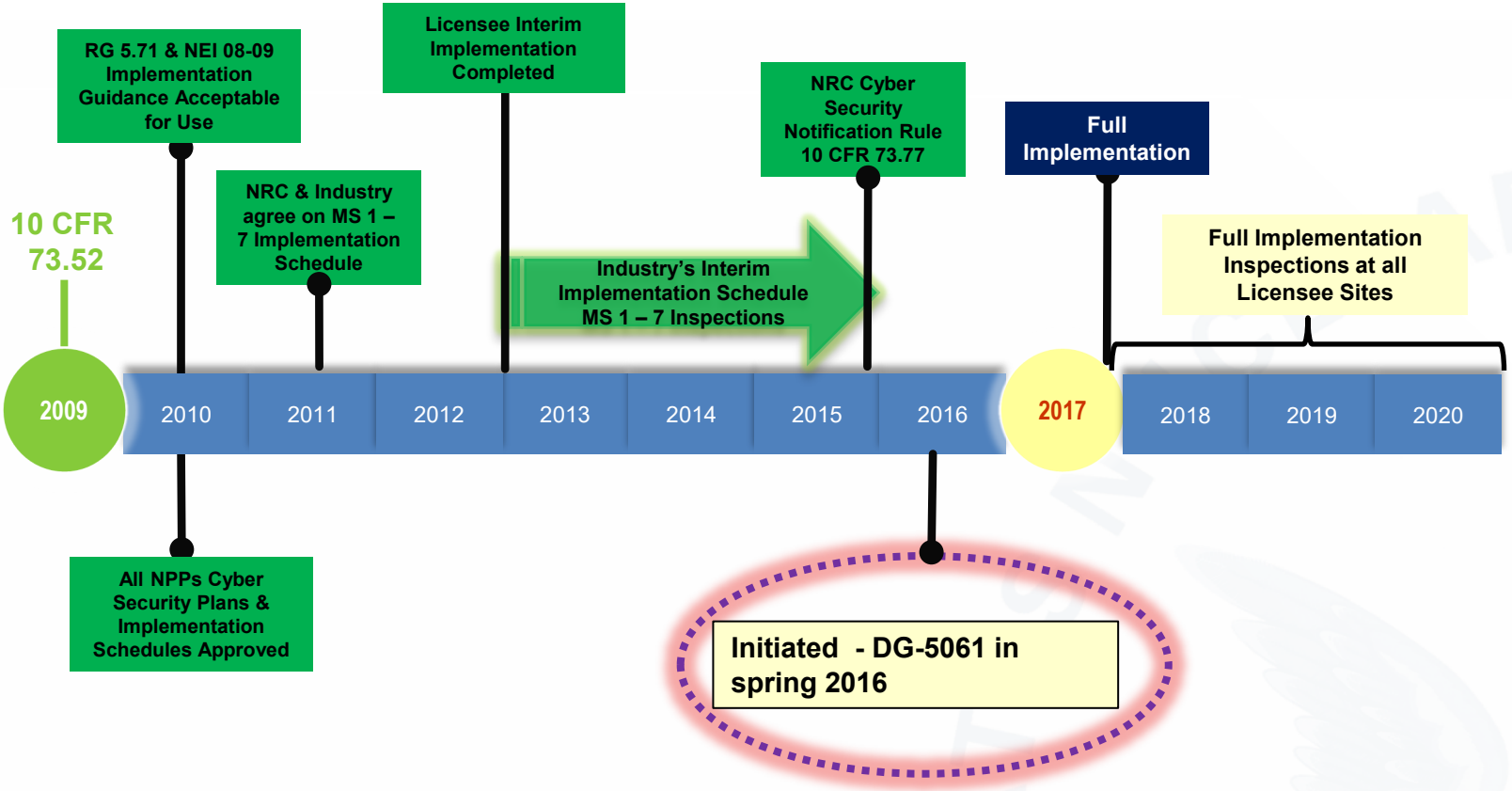
- Milestone 2 – CDA identification
- Milestone 4 – PMMD handling
- Milestone 6 – CDA protection

# Milestone 1-7 issues identified and addressed

- Deterministic Devices
- Data Integrity
- Moving Data Between Security Levels
- Treatment of Maintenance & Test Equipment

U.S.NRC
Protecting People and the Environment

# Timeline with DG-5061 Development



# OVERVIEW OF DG-5061 UPDATES

# Updates in DG-5061 in 2018

- Clarify existing interpretation of regulations based on lessons learned from Milestones 1 –7 inspections
- New regulation since 2010
  - Cyber security event notification
- Changes in NIST SP 800-53 r4 “Recommended Security Controls for Federal Information Systems”
- New IAEA security guidance
- Commission direction regarding Balance of Plant equipment

# Updates in DG-5061 in 2020

- Discussed Risk Informed Cyber Security
- Emphasized the need for accurate CDA assessments
- Leveraged new international standards/guidance and updated NIST guidance on cyber security
- Addressed public comments to 2018 DG-5061

# Lessons Learned from Full Implementation Inspections

57 inspections completed from 2017 - 2021.

Insights on potential areas for improvement:

- Quality of licensee critical digital asset and system assessments
- Vulnerability assessments
- Periodicity for ongoing monitoring & monitoring of security controls.

U.S.NRC
Protecting People and the Environment

# Updates in DG-5061

| Section | Reason for Change |
|---|---|
| C.3 | Added text for Risk Informed Cyber Security |
| C.3.1.3 | Added Balance of Plant asset identification |
| C 3.1.3 | Added new decision points and text for identifying CDAs |
| C 3.2.1 & C 3.3 | Updated text for Defense in Depth protective strategies |
| C 3.2.1 | Updated text for Defensive Architecture for protecting functions, addressing vulnerabilities, and minimizing attack surfaces and pathways |
| C.3.3 | Updated text regarding the use of alternate controls |
| C.3.3 | Updated text to clarify the use of a consequence based, graded approach in applying security controls |
| Background C.3.3.1 | Added text stating technical controls can be incorporated during design certification |
| C.3.3.1.1 to C.3.3.1.5 | Text was added explaining the purpose of various technical security control groups |
| Background C.3.3.2.6 | Text was updated to cited new cyber event notification rule and guidance |

U.S.NRC
Protecting People and the Environment

# Updates in DG-5061

| Section | Reason for Change |
|---|---|
| Background, C.3.3.3.1 | Updated reference to sections of RG 1.152, Rev. 3 |
| C.4.1 | Added more examples of Continuous Monitoring; discussion of anomaly detection |
| C.4.1.2 | Added new text on using metrics for effectiveness analysis |
| C 3.1.3, C.3.3.1.5,C.4.1, C.4.1.3,C.4.2.1,C.4.2.2, multiple sections in Appendix A, various controls in Appendices B & C | Added text regarding quality CDA assessments |
| Appendices B & C | Clarification of all security controls |
| Glossary | Added new terms and definitions; clarified terms in Rev. 0 |
| References | Updated references |
| Throughout document | Editorial changes based on OGC comments, public comments, peer reviews |

# Updates in DG-5061

## Risk Informed Cyber Security

New to section C.3 Establishing and Implementing a Cyber Security Program

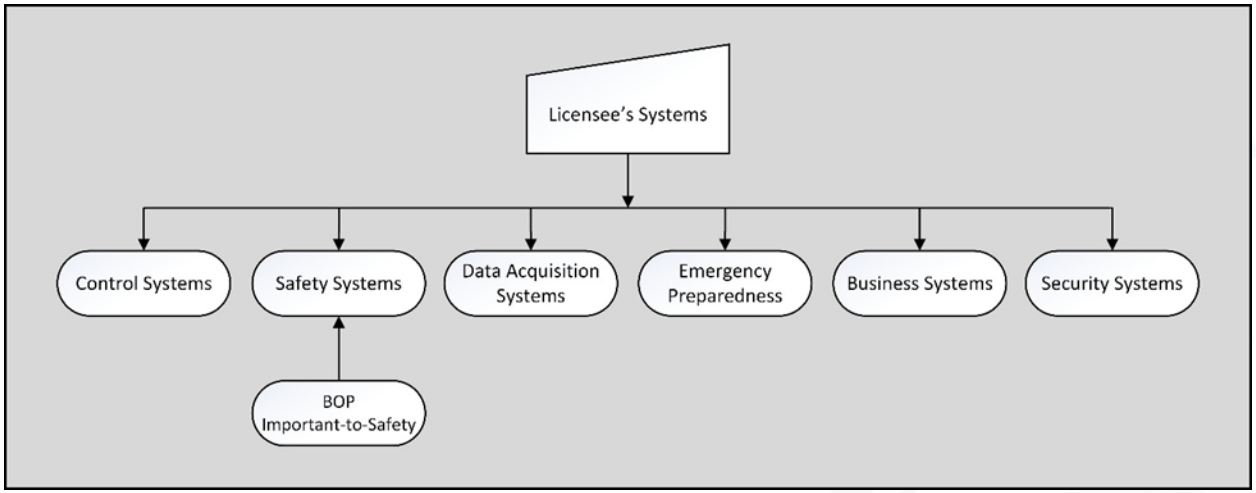
Such a cyber security program can be characterized as risk-informed security in that the development and maintenance of the program makes use of risk insights—including threat information, the likelihood of adversary success, and the resulting level of consequences of the threats—up to and including the DBT described in 10 CFR 73.1. Establishment of a cyber security program could include the following:

- characterization of facility functions, including the identification of SSEP functions
- characterization of threats to the facility
- specification of requirements (including the CSP, the defensive architecture, and defense-in-depth methodology)
- implementation of the requirements based on consequence analyses
- validation and verification of the implementation of the cyber security program

# Updates in DG-5061

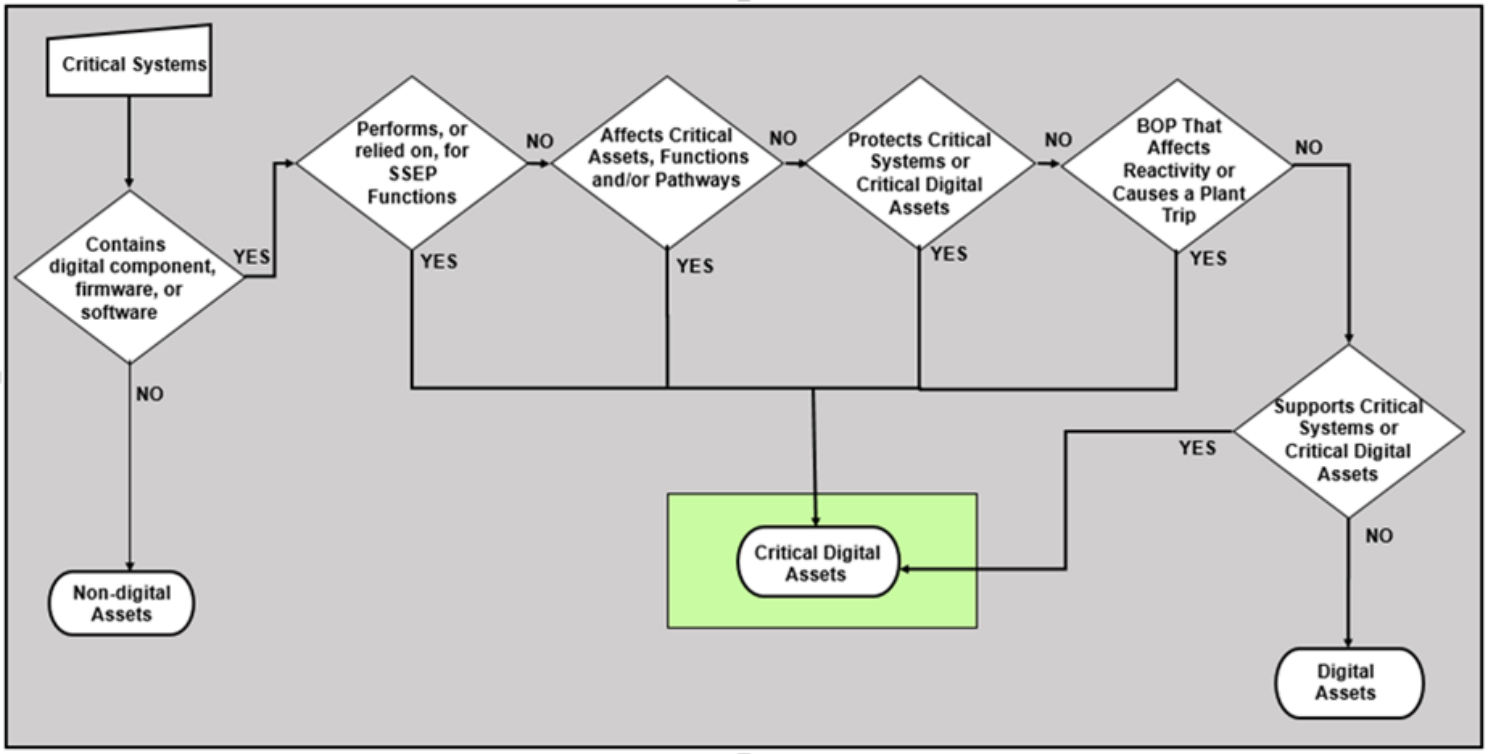
## Balance of Plant

Modification to section C.3 Establishing and Implementing a Cyber Security Program




The identification of CSs should include those systems, equipment, and devices that (1) perform or are relied upon for SSEP functions, (2) affect SSEP functions or affect CSs or CDAs that perform SSEP functions, (3) provide a pathway to a CS or CDA that could be used to compromise, attack, or degrade an SSEP function, (4) support a CS or CDA, (5) protect any of the above from cyber attack up to and including the DBT, or (6) are BOP systems, equipment, and devices that affect reactivity and could result in an unplanned reactor shutdown or transient.

# Identification of Critical Digital Assets



# Updates in DG-5061

## Defense-in-Depth Protective Strategies

New text in section C.3.2 and section 3.3 Security Controls

Defensive strategy that employs multiple, diverse, and mutually-supporting tools, technologies, and processes to effectively perform timely detection of, protection against, and response to a cyber attack.

.

# Updates in DG-5061

## Defensive Architecture – Protect the SSEP function

New text in section C.3.2.1

Functions are protected commensurate with their safety and security significance through the determination and use of appropriate security levels.

.

Each function is implemented by one or more critical systems. A system's allocation to a security level is determined by its associated function with the highest safety or security significance.

.

# Updates in DG-5061

## Defensive Architecture – Communication from lower to higher security levels (vulnerability updates)

New text in section C.3.2.1

Initiation of communications from digital assets at lower security levels to CDAs at higher security levels should be implemented on a “deny-all, permit-by-exception” basis, and the exceptions should be supported by a complete justification and security risk analysis.

.

# Updates in DG-5061

## Defensive Architecture – Minimizing attack surfaces and pathways

New text to section C.3.2.1

- Applications, services, and protocols not necessary to support the design-basis function of the contained CDAs are eliminated.

- Implementation of the multiple, diverse technologies used within the plants addresses the attack surfaces and environments associated with the technologies so that the protections of the defensive architecture are not bypassed or circumvented.

# Updates in DG-5061

## Security Controls – Use of alternate controls

Updated text to section C.3.3

- The various security objectives are explained in detail with examples.

- If a security control cannot be implemented, use alternative controls or countermeasures that provide at least an equivalent level of protection against the threat or attack vectors and vulnerabilities or weaknesses.

# Updates in DG-5061

## Security Controls – Consequence based, graded approach

Updated text to section C.3.3

- Analysis done in support of this consequence-based, graded approach should be rigorous and repeatable by ensuring reproducibility and consistency of the applied security controls posture.

- NEI 13-10 is cited as an approach deemed acceptable for use

# Updates in DG-5061

## Technical Security Controls

Updated text to section C.3.3.1

- Applicants for design certification may incorporate technical security controls as part of the nuclear power reactor.

Added text to sections C.3.3.1.1 to C.3.3.1.5

- Text was added explaining the purpose of access control, audit and accountability, system and communication protection, identification and authentication, and system hardening.

# Updates in DG-5061

## Incident Response

Updated text to Background and section C.3.3.2.6

- Cites 10 CFR 73.77 Cyber security event notifications
- Updated references to incident response documents generated by NIST and DHS Cybersecurity and Infrastructure Security Agency

# Updates in DG-5061

## System and Service Acquisitions

Updated text to Background and section C.3.3.3.1

- Update cites Section 2.1 through Section 2.6 of RG 1.152, Rev. 3

# Updates in DG-5061

## Continuous Monitoring and Assessment

Updated text to section C.4.1

- Added more examples of continuous monitoring
  - continuous monitoring of inbound and outbound network traffic and analysis of event logs;
  - periodic vulnerability scans and assessments;
  - ongoing verification using established baseline configurations that CDAs are being protected commensurate with their safety and security significance
- Expanded text to discuss the importance of anomaly detection

# Updates in DG-5061

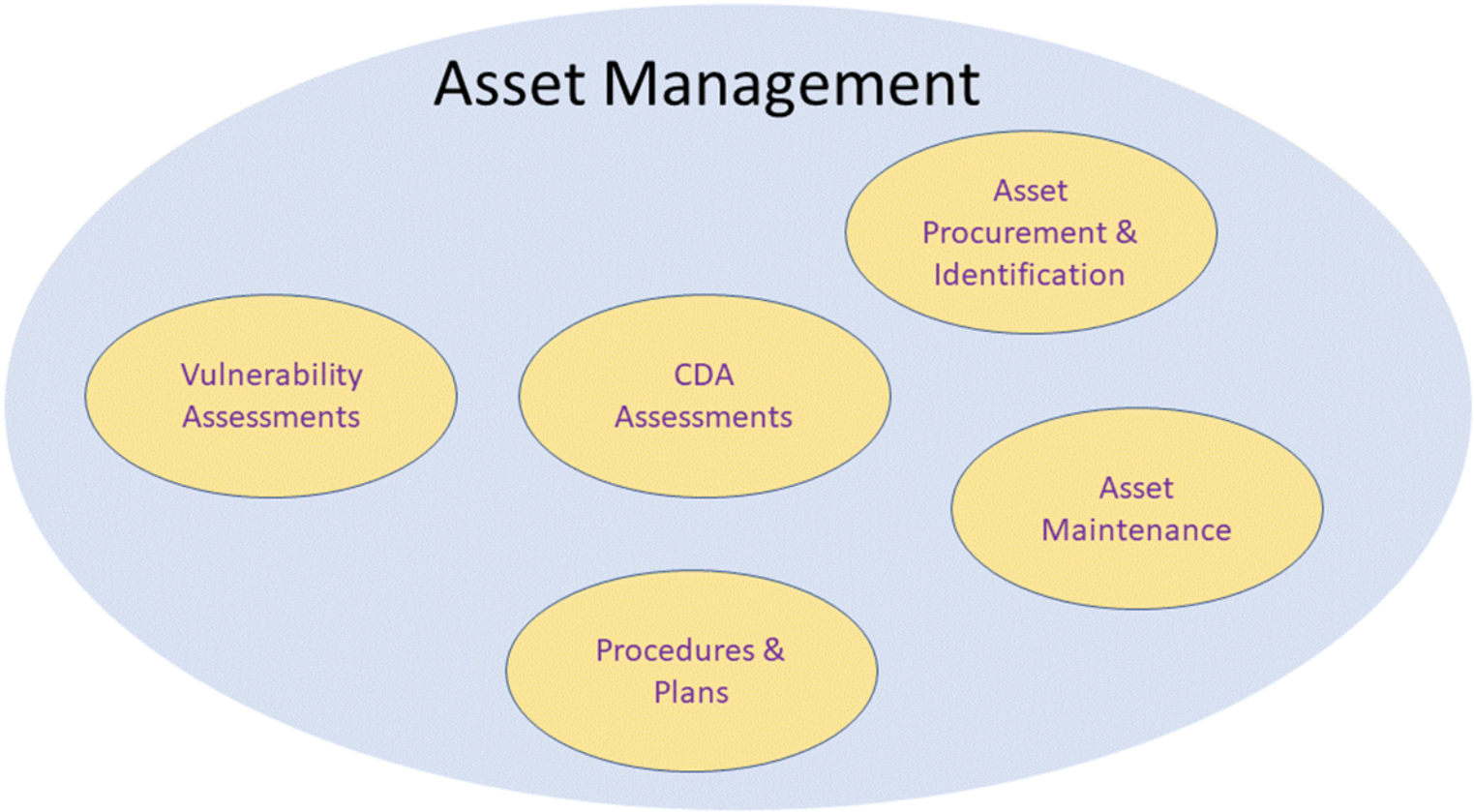
## Effectiveness Analysis of Security Controls

Updated text to section C.4.1.2

Introduced a methodology for defining metrics

- Define measurement goals and objectives as related to the security goals of 10 CFR 73.54
- Define what metrics to capture and track to best measure the effectiveness of the CSP
- Develop strategies for generating and capturing metrics (e.g., log files, audit records).
- Establish benchmarks and targets for metrics
- Establish a formal reporting/review/refinement cycle.

# Assessments and Plant Assets



# Updates in DG-5061

## Maintenance of CDA Security Assessments

Updated text to sections C 3.1.3, C.3.3.1.5,C.4.1,C.4.1.3, C.4.2.1,

C.4.2.2, multiple sections in Appendix A, and various controls in Appendices B & C

Clarified maintaining the accuracy of the security assessments throughout the CDA's product lifecycle

- Initial assessments and reviews
- Application of security controls
- Verification of security control effectiveness
- Vulnerability assessments
- Configuration management

# Updates in DG-5061

## Updates to Security Controls in Appendices B and C

- Control intent added to every security control
- Text added regarding reducing or eliminating attack surfaces and attack pathways
- Aligned with text in NIST 800-53 revision 5

U.S.NRC
Protecting People and the Environment

# Appendices B & C (security controls)

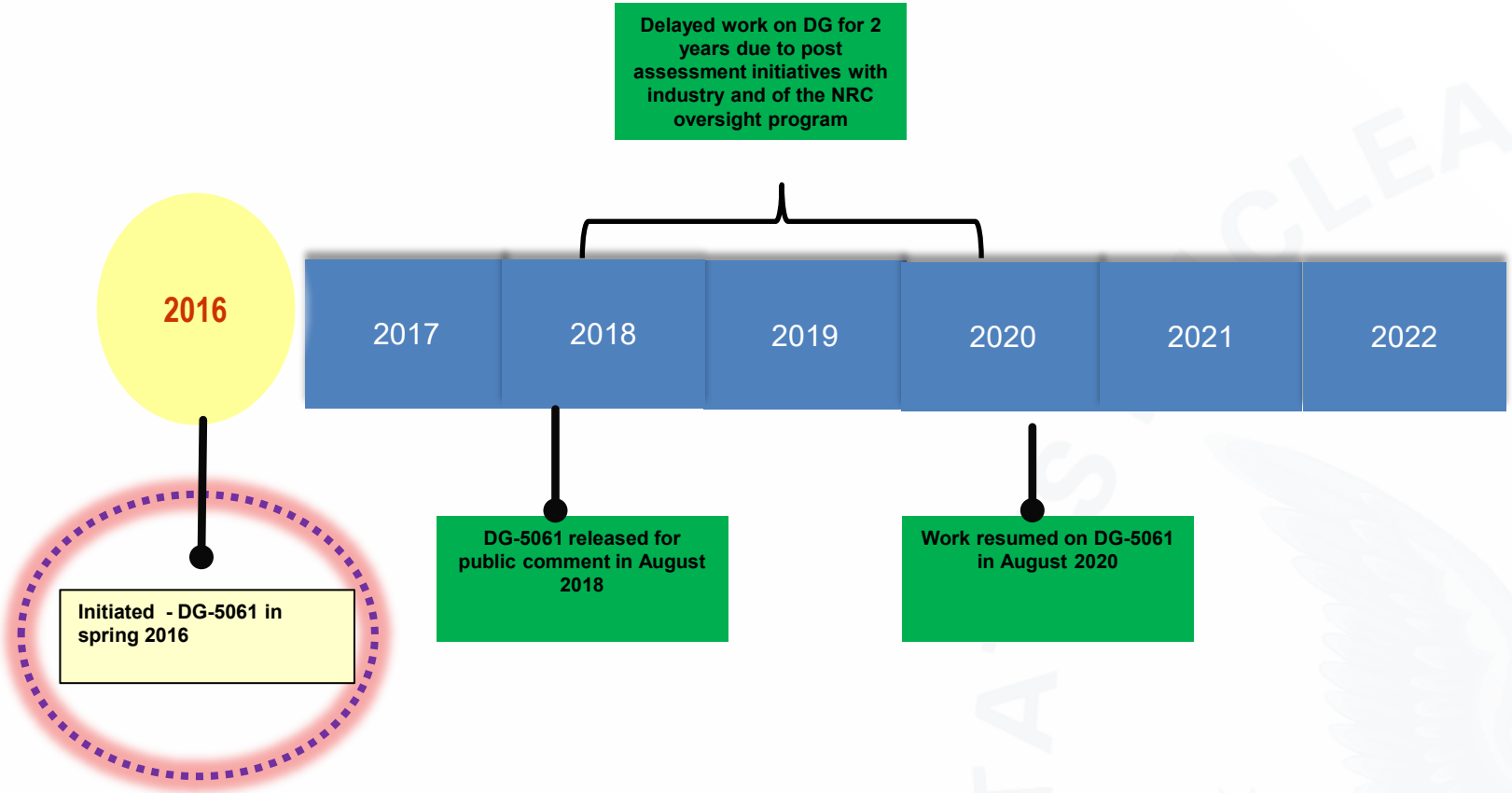
| | DG-5061 | NEI 08-09 | Rationale for change/difference |
|---|---|---|---|
| B.1.9 Previous Logon Notification | Removed control | | Intent covered in covered in logging/audit controls |
| B.1.11 Supervision and Review – Access Control | Removed control | | Intent covered in covered in logging/audit controls |
| B.1.14 Automated Labeling | Removed control | Removed control | Intent is covered in C.1.3 Media Labeling/Marking |
| B.3.5 Resource Priority | Removed control | Removed control | Any safety requirements for resource priority would have precedence. This control is usually applicable in the design phase of a digital device. |
| B.3.19 Thin Nodes | Removed control | Removed control | This control would be covered in the B.5.1 Removal of Unnecessary Services and Programs. |
| B.3.20 Heterogeneity/Diversity | | Removed control | Different depending on safety or security context. |
| B.3.21 Fail in a known state | | Removed control | Important for security |

# Other Changes

- Supply chain
  - Removed prescriptive guidance from Appendix C.12.5 Developer Security Testing and Evaluation and C.12.6 Licensee/Applicant Testing
  - Added text to evaluate attack surfaces and attack pathways
- Glossary
- References
- Numerous editorial changes

# DG-5061 STATUS AND NEXT STEPS

# DG-5061 Timeline



# Some Current CSB Work

- Vogtle 3 and 4 cyber security inspections
- Engaging with NRR, Region II, and Region IV who are performing digital upgrade reviews
- Part 53 rulemaking and guidance
- Work with RES and DOE national labs
  - Wireless
  - Zero Trust Architectures
  - IEC and IAEA nuclear security work
    - Supply chain, Risk Informed Security, Security Models, Artificial Intelligence

# Estimated Timeline

| Task | Date |
|---|---|
| RGGIB issues DG for Public | January 2022 |
| Public Comment Period | 2 months |
| Update and finalize the RG – January through July 2022 | 7 months |
| ACRS brief and comment resolution | 2 months |
| Publish RG | December 2022 |

# Conclusion

- Since 2012, licensees have implemented cyber security programs and the NRC has implemented effective oversight of the licensee's CSPs.
- No changes in staff's position in DG-5061, only clarifications and one new NRC regulation 10 CFR 73.77.
- World has changed since RG 5.71 revision 0 was issued in 2010. DG-5061 reflects the lessons learned and prepares for the future.

# Questions