Official Transcript of Proceedings

NUCLEAR REGULATORY COMMISSION

Title: Advisory Committee on Reactor Safeguards
Digital Instrumentation and Control Systems

Docket Number: (n/a)

Location: teleconference

Date: Thursday, July 22, 2021

Work Order No.: NRC-1598 Pages 1-119

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

DISCLAIMER

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

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

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

UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

+ + + + +

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

(ACRS)

+ + + + +

DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS

SUBCOMMITTEE

+ + + + +

THURSDAY, JULY 22, 2021

+ + + + +

The Subcommittee met via Video Teleconference, at 2:00 p.m. EDT, Charles H. Brown, Chairman, presiding.

COMMITTEE MEMBERS:

CHARLES H. BROWN, Chair

RON BALLINGER, Member

DENNIS BLEY, Member

VICKI BIER, Member

GREG HALNON, Member

WALTER KIRCHNER, Member

JOSE MARCH-LEUBA, Member

DAVE PETTI, Member

JOY REMPE, Member

MATT SUNSERI, Member

ACRS CONSULTANT:

MYRON HECHT

DESIGNATED FEDERAL OFFICIAL:

CHRISTINA ANTONESCU

ALSO PRESENT:

SCOTT MOORE, ACRS Executive Director

JIM BEARDSLEY, NSIR

TOM DASHIELL, ACRS

MARIO FERNANDEZ, NSIR

JURIS JAUNTIRANS, NSIR

ERIC LEE, NSIR

MICHELE SAMPSON, NSIR

DAN WARNER, NSIR

BRIAN YIP, NSIR

C-O-N-T-E-N-T-S

P R O C E E D I N G S

2:01 p.m.

CHAIR BROWN: Okay. Good afternoon, everyone. Sorry for the slight delay. I was counting noses. The meeting will now come to order.

This is a meeting of the Digital I&C Subcommittee. I am Charles Brown, Chairman of the Subcommittee meeting. ACRS members in attendance are Dennis Bley, Matt Sunseri, Jose March-Leuba, Joy Rempe, Ron Ballinger, Dave Petti, Walter Kirchner, Vicki Bier and our consultant Myron Hecht.

A couple may show up. I will let them come as they are able to get in.

MEMBER HALNON: Charlie, this is Greg Halnon. I'm in.

CHAIR BROWN: Oh, okay. Greg Halnon is also now here. Christina Antonescu of the ACRS staff is the designated federal official for this meeting. The purpose of this meeting is for the staff to brief the Subcommittee on the status of the cyber security program.

The ACRS was established by statute and is 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 for members of the public attending or listening to our meetings. Written comments are also welcome.

The meeting agenda for today's meeting was published in the NRC's public meeting notice 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 requests 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 all participants in this meeting should first identify themselves and speak with sufficient clarity and volume so that they can be readily heard.

All presenters must 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 a bridge line established for the

public to listen to the meeting. The public line will be kept open in a listen-only mode until the time for public comment. To avoid audio interference, I request all attendees to make sure that they are muted while not speaking.

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 or when it's relevant to allow time for screen sharing as well as the Chairman's discretion during longer presentations.

We do have a backup call in number should Skype go down -- excuse me, should Teams go down, and it has been provided to the ACRS members. If we need to go to the backup number, the public line will also be connected to the backup line.

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 we can bring those to the floor.

We'll now proceed with this meeting, and I'll ask Jim Beardsley to share his screen with us while Ms. Michele Sampson, the Deputy Director, Division of Physical and Cyber security Policy, Office

of Nuclear Security and Incident Response for any introductory remarks for today's meeting before we begin today's presentation by Mr. Jim Beardsley, the Branch Chief in the Cyber Security Branch. Michele?

MR. MOORE: Can the members on the public line, you need to mute your phones, you need to mute your phones. We're getting carryover.

MS. SAMPSON: Thank you and good afternoon. I'm Michele Sampson, Deputy Director for the Division of Physical and Cyber security Policy in the Office of Nuclear Security and Incident Response.

I want to express my appreciation for the opportunity to brief on the Agency's cyber security program with the ACRS Digital I&C Subcommittee.

We last briefed the Subcommittee in March of 2019. There have been several significant accomplishments since that last meeting. We will highlight a few, including the completion of the Milestone 8 inspections, a full cyber security program implementation at the operating power reactors and the results of the staff's cyber security program assessment.

We will also touch on some of the exciting future work in cyber security, including the development of a new technology-inclusive graded

approach to cyber security regulations as a part of the advanced reactor rulemaking effort.

The cyber security staff routinely interface with our federal partners and domestic and international stakeholders to share operating experience and best practices.

We are committed to maintaining an efficient, robust cyber security program that can adequately protect against the dynamic cyber threat environment.

I would like to recognize the work of Jim Beardsley, Chief of the Cyber Security Branch and his staff, to prepare for today's briefing. And I look forward to the opportunity to hear from him and several members of his branch.

With that, I'd like to turn it over to Jim to begin the presentation.

MR. BEARDSLEY: Thank you, Michelle. As Michelle stated, I am Jim Beardsley, Chief of the Cyber Security Branch in the Office of Nuclear Security and Incident Response.

Today's brief is an update to a program brief that staff provided to the Subcommittee in March of 2019. Today I will be joined by the following team from the Cyber Security Branch, Mario Fernandez, Dan

Warner, Eric Lee, Brian Yip and Juris Jauntirans.

Slide Number 2. Today's brief will discuss the status of the NRC cyber security program, including successful completion of our oversight inspections for the industry's cyber security full implementation.

The program found with reasonable assurance that industry has implemented their programs to meet the requirements of the Cyber Security Rule and the Cyber Security Plans, which are license conditions for each licensee.

The staff has learned a number of lessons on the oversight program from the full implementation inspections, the staff self-assessment of the oversight program and an NRC Office of Inspector General audit of the inspection program in 2019.

As a result, the staff has been working with industry to further implement the graded approach to cyber security to digital asset protection, to further performance inform our cyber security inspection program, to update cyber security guidance in Regulatory Guide 5.71 and to develop a graded approach to cyber security for future applicants and licensees.

Slide Number 3.

CHAIR BROWN: Jim? This is Charlie.

MR. BEARDSLEY: Yes.

CHAIR BROWN: When you talk about a graded approach, I presume in your later slides you will be giving us a detailed discussion of what that means?

MR. BEARDSLEY: I intend to, yes, yes.

CHAIR BROWN: Okay. Thank you. I just wanted to make sure. Thank you.

MR. BEARDSLEY: Absolutely. In our March 2019 brief to the Subcommittee, the staff discussed the power reactor cyber security program history.

Today, I will briefly review some of that history and talk to in particular our future plans as we move forward.

This slide shows the progression of the program from implementation of the Cyber Security Rule in 2009 through industry's cyber security program full implementation, which occurred at the end of 2017.

As a result of lessons learned during the initial implementation inspections between 2013 and 2015, the staff and industry have developed a series of guidance documents for the cyber security program implementation and NRC's inspection program.

Those improvements proved to be a vital element in the successful completion of both the

licensee implementation and the staff's inspection of their implementation following the 2017 full implementation date.

In 2010, the NRC issued Regulatory Guide 5.71, Cyber Security Programs for Nuclear Facilities. This document provides the licensees a methodology or framework that can be used to meet the requirements of the Cyber Security Rule.

As a review, this slide shows the primary principles of a cyber security program as listed in the Regulatory Guide.

The first step would be for a licensee to establish a multidisciplinary cyber security assessment team. That team would then be instrumental in implementing the remainder of the program.

The next step would be for licensees to review all of their digital assets and determine which of those assets need to be protected in accordance with the Cyber Security Rule and their Cyber Security Plan.

The next step is for the licensees to implement a defensive architecture. And my following slide will discuss the defensive architecture in more detail.

Finally, the licensees would apply cyber

security controls in accordance with their Cyber Security Plan to each of the critical digital assets that they determined needed to be protected in an earlier step.

The final steps of full implementation are for licensees to implement overwriting programs that support the protection, operation and continuing maintenance of their cyber security programs and a number of those elements are listed at the bottom of the slide.

MEMBER HALNON: Hey, Jim, this is Greg Halnon. Do you have a feel, since Reg Guides are voluntary, do you have a feel for how many licensees actually implemented the program for this Reg Guide 5.71?

MR. BEARDSLEY: That's a great question. When the staff published Regulatory Guide 5.71, industry also developed a guidance document, NEI 08-09, which was very, very similar to Reg Guide 5.71.

Most of the operating fleet, in fact all but Vogtle 3 and 4 committed to the NEI document, which has a Cyber Security Plan template that is virtually identical to that in Regulatory Guide 5.71

So only one of our licensees committed to Reg Guide 5.71. But the guidance in the document is

enduring and the staff uses it as part of our assessment and licensees do use it as a reference.

MEMBER HALNON: So it wasn't endorsed, but it was found acceptable through your process?

MR. BEARDSLEY: The NEI guidance document was found acceptable for use by the staff, correct.

MEMBER HALNON: Okay.

MR. BEARDSLEY: It was found to be an acceptable method to implement a cyber security program.

MEMBER HALNON: All right.

CHAIR BROWN: How did that happen?

MR. BEARDSLEY: How did the staff make that determination?

CHAIR BROWN: Yes. I don't remember -- I wrote the letter on 5.71 back in 2009 and '10. And I don't remember this NEI document. What's the date of that?

MR. BEARDSLEY: I don't know exactly. We'll have to get back to you. But it came out right about the same time as the Regulatory Guide. It may have been a little earlier. It may have been a little later. But we'll get you an answer to that.

CHAIR BROWN: The purpose of the question is you say it's virtually identical. The rule is

fairly specific, you know, the 73 point whatever 54 or whatever the right number is. I probably got it wrong. And I just wondered how this NEI document tracked. I don't remember us ever seeing it. That's why I asked the question.

MR. BEARDSLEY: The format in the document is very similar to Reg Guide 5.71. It's not exact. But the template for a Cyber Security Plan follows the same set of controls, the approximately 160 controls, that the staff had included in Regulatory Guide 5.71.

The industry then used that template to develop and submit to the staff for approval a Cyber Security Plan. And each individual licensee had their Cyber Security Plan reviewed and approved back in 2010.

CHAIR BROWN: There were some sections, if you go back into the appendices for 5.71, I think it was Appendix C where it talked about unidirectional data diode-type connections from the Level 4 to 3 and 3 to anything above that, and did it mirror those types of things as well?

MR. BEARDSLEY: It did. And I'm going to talk about that on the next slide.

CHAIR BROWN: Okay. Thank you.

MR. BEARDSLEY: Sure. Any other questions

on the Reg Guide? Okay. Moving on to Slide Number 5.

MR. LEE: Hey, Jim?

MR. BEARDSLEY: Yes.

MR. LEE: The NEI 08-09 was dated April 2010.

MR. BEARDSLEY: Okay. And when was the Reg Guide published?

MR. LEE: I believe that was -- similar time, 2010 or so, I believe.

MR. BEARDSLEY: Right. Well, we'll get an exact answer for the members following the meeting.

MEMBER BALLINGER: It was January 2010.

CHAIR BROWN: Yes, January, thank you.

MR. BEARDSLEY: Okay.

CHAIR BROWN: You got a hit on that.

MR. BEARDSLEY: So the Regulatory Guide was published about three months before the staff accepted NEI's document for use.

So talking about the -- I'm sorry.

MR. HECHT: This is Myron Hecht. You stated -- just a clarification question. You said that all but Vogtle had committed to NEI 08-09. Did Vogtle commit to 5.71? Is that the difference or --

MR. BEARDSLEY: They did.

MR. HECHT: -- did they not commit to

anything? I see.

MR. BEARDSLEY: They committed to Reg Guide 5.71, and they elected to use the template in Reg Guide 5.71 for the Cyber Security Plan. So that was how they -- that's how the commitment was made.

And the reason was at that time, NEI -- at the time that Vogtle 3 and 4 submitted their Cyber Security Plan as part of their combined license, the NEI guidance document hadn't been completed yet. So the only template that existed was the one in Reg Guide 5.71.

MR. HECHT: Thanks.

MR. BEARDSLEY: So to go to the question that Member Brown asked, all of the licensees have implemented a topology that's similar to that shown on this slide.

And on the slide Level 0 is the Internet all the way on the right. And as you move from right to left, the systems are more sensitive and are receiving more protection.

So Level 1 would be a corporate network for a licensee that's part of a larger corporation. Level 2 would be a site-wide network and that's the administrative network for training and administration of the site.

And then the licensee is committed to a one-way deterministic device in their Cyber Security Plan. All of our licensees elected to use a data diode to meet that requirement. And that is a digital device that prevents any digital information from being transferred from Level 2 to Level 3. So the laws of physics will not allow data to be transferred over the network from Level 2 to Level 3.

CHAIR BROWN: So Level 3 would be the area where you had, like, the reactor control systems, trip systems, ESFAS, et cetera, safety systems?

MR. BEARDSLEY: Right.

CHAIR BROWN: -- up to Level 4.

MR. BEARDSLEY: Right. Level 3 and Level 4 are not consistently implemented across the various licensees. So each licensee made a determination on where they wanted to put their critical digital assets in Level 3 and/or Level 4.

So I can't say that they all put a certain system in Level 3 and/or Level 4. But beyond the data diode boundary in Level 3 and Level 4, they have all of their safety and security and many of their emergency preparedness digital assets.

CHAIR BROWN: So I was just trying to figure out when I looked at the slides what

constituted in NRC's mind the Level 4 and Level 3. Cyber security is one set of words. I wasn't sure what that meant inside of this barrier of the data diode. And I also saw a firewall there.

MR. BEARDSLEY: There is a firewall. In fact, some licensees implemented multiple firewalls to partition different parts of Level 3 and Level 4. And some of them have used additional data diodes to partition various different systems.

So from a security point of view, that's the physical security system, the computers that they use to manage the physical security program and then from the safety systems, that's the balance of plant systems. That's the safety systems. That's any other system that the licensee has determined was a critical digital asset and needed to be protected.

CHAIR BROWN: Okay. So I was thinking that when you say security that kind of -- you're talking about all the -- I call them admins. But they're not really admin relative to being admin-admin. They're not part of the business systems.

In other words, that's where you have all the spyware, whatever you want to call it, to make sure people don't intrude into the site, alarms, all the systems that generate that would be back most in

the Level 4 area based on your all's -- whereas Level 3 -- based on your all's categorization would roughly be plant systems, roughly.

MR. BEARDSLEY: I'm not going to disagree with what you're saying, but I can't commit that every licensee elected to put on those systems in one or the other.

CHAIR BROWN: I totally understand, totally. The reason I'm asking the question is because in a couple of the applications we went through, new design plants for the last two or three, we actually ended up with -- you talk about reactor trip in the ESFAS systems which feed, you know, plant control stuff, like reactivity control pumps, valves, whatever you have necessary for your emergency core cooling, et cetera, we largely ended up with unidirectional data diode-type transmissions from those systems to the other ones.

In other words, they were within the Level 3 area, but they were also protected from one safety system, what I would call to maybe a safety -- I don't know what the difference is for the actual components that do the job themselves because you never know what's going to be on some of these pumps, valves whether they have computer controlled controllers or

not, et cetera. So we did not want any interaction backwards into those other systems.

So I presume this allows -- that's not a firewall. That was a hard data diode. Other systems could handle a firewall type approach. So I presume that's flexible definition in that 4 and 3 and then within the 3 routine?

MR. BEARDSLEY: It is. And it's really -- the licensee has to determine what systems should be protected and the appropriate level of protection and then they'll partition their networks as such.

CHAIR BROWN: Okay. And for the operating plants, you obviously have to figure that out for the -- you know, we've obviously emphasized that we needed to do that as a design decision in subsequent plant designs, you know, the applications we've dealt with over the past few years. All right. Thank you. You've answered my question. Thank you very much.

MR. BEARDSLEY: Okay. Anybody else have any questions?

MEMBER MARCH-LEUBA: Yes.

MR. BEARDSLEY: Go ahead.

MEMBER MARCH-LEUBA: This is Jose March-Leuba. Something you just said I wanted to hop on it in a previous slide, but I was having silent problems.

You said the licensee is responsible for defining the critical assets that they have to protect, which is the Step Number 2 on this slide.

MR. BEARDSLEY: Correct.

MEMBER MARCH-LEUBA: Do you have an ongoing evaluation of how this changes with time? And what I'm coming to is first, we have had to protect against hackers, which are in the top 0.0001 percent of the smartest people in the world. And some of them have state support and even money. So you have to be extremely careful.

And in the last five years, we have seen an explosion of Internet-connected devices, what we call IoT devices, Internet of Things, something like smart lights, smart thermostats, you know, smart TVs, microwaves.

MR. BEARDSLEY: Right.

MEMBER MARCH-LEUBA: So is there an ongoing re-evaluation of how I can attack my system? And I'm not talking monthly, yearly or bi-yearly but an ongoing one? Something changing my plant, do I need to do something different?

MR. BEARDSLEY: So that's a great question. When we inspected the licensees back between 2013 and 2015, we reviewed their methodology

for determining what assets had to be protected, what were critical digit assets, and also inspected their change control processes.

During the subsequent inspection program that started in 2017, we again reviewed that list and the changes that they had made. So any changes to the program, any changes to the list of critical digital assets, is something the staff will look at it in the inspection space to make sure the licensee has appropriately characterized the assets and made sure that they are appropriately protected.

MEMBER MARCH-LEUBA: You know, I'm more concerned with their changing the hardware in the plant. Somebody plugs in an Alexa in his office. Does that get evaluated?

If you change your protection system and you go from computer type A to computer type B for the protection system, of course, they're evaluated.

What I'm saying is the famous example of the aquarium in the casino. Is there an aquarium somewhere in the plant that has changed the configuration?

MR. BEARDSLEY: Okay. So for the most part, you know, the licensee has their own corporate configuration management program and controls on the

Level 1 and Level 2 network. So that's the administrative network that will be sitting in someone's office.

Level 3 and Level 4 are those assets that have to be protected in accordance with the Cyber Security Rule. And there are very specific requirements on what assets have to be protected and the controls associated with those assets.

So the licensees not only have systems in place, they have to do vulnerability assessments, and they have to do assessments of their digital assets to make sure they're protected, you know, on an ongoing basis.

So they do have, you know, a regular program of periodic review, as is stated on the slide, to look at their systems.

So if someone tried to plug something into an asset, the licensee is responsible to identify that either through log reviews or through an automated system that would monitor whether something had been plugged in.

Also, the licensees are expected to mitigate any potential things plugged into their critical digit assets through configuration management and blocking of ports or a number of other defensive

methodologies.

MEMBER BALLINGER: This is Ron Ballinger. Let me know if I'm getting too security conscious here. But other organizations which I will not name have teams whose business is to compromise a network. Do you folks have such an organization that goes around and tries to compromise a network to test it?

MR. BEARDSLEY: At the current time, the NRC Inspection Program does not include that type of activity. And there's a couple reasons for that.

One, we would never want to try and mess with an operating nuclear power plant. That would be very risky, and it's been determined to be not an appropriate activity.

The other aspect of it is with the data diode, it would be very difficult for an adversary to reach the protected systems. They would have to bypass the data diode, either through the portal media program, which has a very specific set of requirements and the staff has inspected or through supply chain or some other threat vector.

So it is not likely that a penetration type test, which is what I think you're talking about, would add any value to the program at this time.

MEMBER MARCH-LEUBA: This is Jose again.

I am concerned that people will give too much credit to the little diode, which is a great thing to have. But these guys can figure out ways to get past it. You can have a wireless network at Level 4. It's called the cell phone tower. You already have a wireless network inside a plant. You just need a little chip to assist.

So if you have -- you need to have an inside threat, somebody that goes physically as an extra thing with a button that you can bypass. So let's give the credit where the credit is due but don't give it 100 percent credit. It's only 99 percent effective.

MR. BEARDSLEY: And we don't give 100 percent credit. The staff has focused the last four years of inspection on potential methods for bypassing the data diode. Now the licensees do have limitations, and they have committed to not having wireless systems. They scan for wireless networks that are unexpected. So from a wireless point of view, the licensees understand very clearly what their requirements and limitations are.

So we have focused on those areas that can be used to bypass the data diode and that it will continue to be one of the focuses of the industry and

the staff's oversight inspections.

CHAIR CHARLIE: Thank you, Jim.

MEMBER KIRCHNER: This is Walt Kirchner. Just following up on Jose's points, and you live this so it's not my particular line of business.

But with the evolving threats, without getting into any kind of actual threat scenario or mechanism, is it safe to say that line of defense with the data diode, assuming that it's more than a data diode. It's all portable media, et cetera, et cetera. Are you finding that more and more things have to be pulled inside the Level 4 or 3 envelope?

Do you see where I'm going with this? In other words, you actually have to move your fence out further in the plant in terms of balance of plant and other support systems to protect against the evolving threat and the technologies that could represent a threat. Is that a safe assumption?

Are you finding as your licensees get into this and do a continual review, you're pushing more and more stuff? Either you can say it one way, you're putting more and more on Level 4 and 3 or you're moving that boundary out or both.

MR. BEARDSLEY: Actually, the staff and industry have found that the industry may have over

included the number of digital assets and the level of digital assets that need to be protected. So we have and, you know, Member Brown asked me about the graded approach earlier.

One of the things we've looked at in the graded approach is to make sure that the right assets are being protected at the right level. And in some cases, we found that the licensee may have overprotected some of their assets. And in doing so by reducing the protection on some, it helps them focus the protections they need on the most critical asset.

So we have not seen extensions in the barrier. In fact, we believe the barrier is sound and is pretty well implemented right now. But let me --

MEMBER KIRCHNER: Okay. Thank you.

MR. BEARDSLEY: -- to your question, let me just add one quick thing. So the staff has -- in answer, we have a branch that does intelligence and threat analysis. Through that branch and through our interagency counterparts, the staff does monitor any evolving threats and continuously is looking at the potential for a threat that could bypass the systems and the controls the licensees have in place. So that's an ongoing effort that we have. I'm sorry. I

cut somebody off.

MEMBER KIRCHNER: No, thank you. I was just trying to say thank you.

MR. BEARDSLEY: Okay.

CHAIR BROWN: Jim, the data diodes that you all have observed or seen them install or have in place, I presume those are literally hardware-based data diodes. In other words, their direction, that single directionality is not configured with software processes?

MR. BEARDSLEY: It is a physical data diode. It is a laser-based tool. And the laser only fires from the Level 3 side down to the Level 2 side or from the higher side to the lower side.

So you cannot physically -- the laws of physics won't allow data to travel back on the network.

CHAIR BROWN: Okay. I thought that was the case, but I always worried about advertising from some people that make these things so.

MR. BEARDSLEY: It's a pretty small market. I'll tell you that.

CHAIR BROWN: Okay. You haven't gotten to your graded stuff yet. So I'll wait. I'll save my questions for that until you get there.

MR. BEARDSLEY: Okay.

CHAIR BROWN: I have a question on that. I just don't want to interrupt your thought process here.

MR. BEARDSLEY: All right. All right. We'll get there.

MR. HECHT: This is Myron Hecht. Can I just go back to the last thing that Jim has said. You said that there's a diode which allows a transmission only from Level 3 to Level 2. Shouldn't it be the other way?

MR. BEARDSLEY: No. You only want data to travel from the secure level to the less secure level. In other words, the licensees are doing diagnostics on the systems in Level 3 and Level 4. They will pass that down to the lower level so they can aggregate and understand whether or not there are any issues.

MR. HECHT: Yes, yes, of course. Thank you.

MR. BEARDSLEY: Okay. So this slide focuses on our inspection program. The inspections started out in the summer of 2017. And the staff conducted a full implementation inspection at every operating nuclear site in the country.

We completed all 58 of those inspections

in June of 2021. The inspections were a two week inspection program conducted by two inspectors from the appropriate region and two subject matter expect contractors who supported them during the inspections.

We also have a team at headquarters in the Cyber Security Branch that provides the inspection teams technical backup on any questions that arise during the inspections.

Although the inspections did identify a number of very low safety significance findings, the industry demonstrated with reasonable assurance an understanding of the Cyber Security Plan requirements and effective program implementation.

The staff observed at a high level some of the following observations. The quality of critical digital asset and system assessments was challenged at some of the licensee sites. And the staff provided feedback to the industry on that.

It didn't impact their ability to protect the assets, but it may impact their ability to do continuing analysis or change control in the future.

In addition, the licensees were challenged conducting vulnerability assessments on their programs. And the challenge there is they have a large number of digital assets, and there's a

significantly large number of vulnerabilities that are identified by industry and the government on an ongoing basis. And the licensees did have some challenges in collecting and evaluating those vulnerabilities. The staff did cite some violations in this area. And industry has made strides to improve that process.

Another area that the staff found was in the licensee's implement of their cyber security defense in-depth, there were times when the licensees had not fully implemented their defense in-depth programs. The staff again cited that and the industry has continued to improve those over time. Any questions about the inspection program?

CHAIR BROWN: Jim, I have to backtrack one more time on the previous slide. If you could go back to that. Talking about physical security, did you -- you talked about being, you know, the outfit monitors, making sure the overall site is safe.

MR. BEARDSLEY: Correct.

CHAIR BROWN: All the guard information, all the detecting type information for intruders, all that kind of stuff, that generally has an evolving nature if stuff gets upgraded. I mean, people always want to make it better.

I note you were talking about in one of your later slides, and you mentioned wireless. A lot of the stuff in this physical security world is wireless associated. And I guess have you all looked at that relative to systems?

Maybe the right way to say it is those responsible for physical security are not allowing any wireless type connections back down in that Level 4 area or the security world?

MR. BEARDSLEY: That is correct.

CHAIR BROWN: Okay.

MR. BEARDSLEY: The licensees are not at the time by their Cyber Security Plan allowed to connect wireless systems to their critical digital assets. They could in the future do that. But they would have to do significant analysis and the staff would be inspecting that to make sure that it meets the appropriate requirements.

CHAIR BROWN: Yes. One of my concerns was if you -- you don't have it now, but somebody brings in a piece of new equipment. It's a real super whamadyne. Everybody loves it because it's going to simplify all the work. And it's got something buried in it that's wireless and now all of a sudden you've got a path.

I don't know how you monitor that. You know, I'm not a radio engineer anymore. But I guess I'm always worried about new stuff coming in because it seems like the world, as it operates today, as Jose noted, the Internet of Things is now also in the air all the time, its connectivity, so.

MR. BEARDSLEY: Right. Through the licensee's change control program, they have to do a very robust evaluation to include their cyber security requirements. And we inspect those changes, both through cyber security inspections and through the NRC's routine change control inspections.

So we are looking at that. And industry is aware that the implementation of wireless is something that will be a challenge for them. And we do have a discussion on that topic later in the presentation.

CHAIR BROWN: Okay. Thank you.

MEMBER HALNON: Hey, Jim. This is Greg Halnon. On the inspection program, you mentioned challenges in several areas, and those are pretty much downstream of the initial identification of CDAs, which is real documentation intensive.

Did you get a sense that the overidentification of CDAs was taxing the resources

such that those challenges manifested downstream of the process or were those challenges just pretty much specific to the licensee issues?

MR. BEARDSLEY: I would say the answer is both. You know, any time you're trying to manage thousands of digital assets, that's a pretty significant effort.

So if through evaluation the staff and industry find that we can reduce that overall effort and allow them to focus on the assets that are found to be of higher importance, and I'll just characterize it as that, arguably, that would help them focus on their program.

So I can't say, you know, explicitly one way or the other because each licensee is different and each case was different. But that was one of the areas that was identified during our self-assessment that I'll talk about in a moment and one of the things that we've worked on over the past few years.

MEMBER HALNON: Okay. It seems like a graded approach then would try to reduce the front end piece as well so that resources could be not so tied up on the initial discussion.

I know that piece is past this. But it's still, you know, what you mentioned overidentification

of CDAs is still there. And there's still a lot of ornaments that go around that to manage that.

So some resources, I know, is a key issue throughout the industry. I would be interested down the road of seeing how the graded approach might help alleviate some of the resource issues that we have.

MR. BEARDSLEY: Sure. As I stated earlier, we have learned a significant number of lessons since 2012. And one of the things that we're looking at in our future cyber security rulemaking is making sure we've right-sized that assessment process and the identification of digital assets. And we'll talk some more about that in the presentation as well.

MEMBER HALNON: Very well. Thanks.

CHAIR BROWN: Jim, when you get to your graded approach, that's just another word for risk-informed and not personal thought processes. Are you going to be able to provide some information on criteria that will allow you to even think about a graded approach as to not -- is there some partitioning that some things will never get there but others are because of some circumstances or some characteristics?

MR. BEARDSLEY: Well, you're --

CHAIR BROWN: If you do that later, that's

fine. I just wanted -- that's one of the questions I had for later.

MR. BEARDSLEY: That's a great segue. So what I'm going to talk about now is the self-assessment that the staff conducted of our cyber security oversight program and every element in it, from the rule through the implementation, through licensee implementation and our inspection program.

We conducted that assessment in 2019. Staff provided management with a report on the results of that assessment. The assessment included significant engagement with stakeholders, multiple public meetings. And on the next slide, I'm going to talk about our action plan that we put together to address a number of the areas that were identified during the assessment.

Some of those areas are systems where we have looked at a graded approach and the staff will talk about that and talk about those particular areas and how we've approached it. So hold the question for a second. We're going to give you some specifics here in just minute.

CHAIR BROWN: Okay. I don't want you to take it -- I'm pretty overbearing it seems like sometimes as you've probably figured out over the last

few years. I'm very concerned about this particular area. So that's why -- I'm not against that.

My concern is we overdo the classification of what stuff needs to be, you know, really wrapped up tight with millions of sheets of paper and which ones don't. It's just a matter -- I like to see certain criteria type stuff. You throw it off to the side, stuff that there's no way you can put virus software in, you know, plant control systems, trips, et cetera, et cetera.

There's other things that don't meet that criteria. They're not in that category. And it just seems to me to make it easy, it's nice to put things in little -- different rice bowls if you want to call it that, put the stuff that you don't care about and so that you don't beat the licensees to death on this stuff.

MR. BEARDSLEY: Right.

CHAIR BROWN: But it can be overbearing. So don't think I'm just, you know, give me a data diode on every piece of equipment that's in there. That's not the way I think. I just really would like to see how we get to the point and make sure our really important systems don't even get tested. So that's --

(Simultaneous speaking.)

CHAIR BROWN: Okay? Thanks.

MR. BEARDSLEY: Right. Absolutely. So after we completed our interim inspections in 2015, the staff and industry identified the fact that there were some challenges in the area that you're talking to.

NEI developed a guidance document, Document NEI 13-10, that was used by industry and the staff to develop the graded approach to digital asset protection.

So there are classes of digital assets that have full protection, 160 odd controls. And there are other classes of digital assets that have a significantly lower number, somewhere around 15, you know, a dozen to 15 controls.

So we have tried to do that and tried to look at the total group of digital assets. And what the staff is going to talk about in a minute is how we're further evaluating that and further looking at how we can grade that.

So the staff conducted the assessment in 2019, provided an action plan to management in the fall of 2019. And the action plan identified a number of areas that the staff felt were worthy to be

evaluated as part of our program.

Those areas are listed on this slide. And we broke -- and we further broke them down into prioritization of things that we would look at.

Our initial focus areas were primarily looking at digital asset identification, analysis and protection in the areas of emergency preparedness, balance of plant, safety-related and important safety systems and -- did the slides just drop?

CHAIR BROWN: Yes. You're okay. I just compared it to mine on my other computer so.

MR. BEARDSLEY: All right. They just dropped from my computer but hopefully they're still there.

CHAIR BROWN: It just stayed.

MR. BEARDSLEY: So the staff is going to speak to each one of those four areas in detail on the following slides. In addition, the staff and industry identified -- or excuse me. The staff and the Office of Inspector General during their audit of our inspection program identified opportunities to performance inform our inspection program. And the staff is actively developing a new inspection procedure that we believe is focused on licensee performance and performance informing our oversight.

There we go. The next area the staff focused on was the best practices for digital asset assessment. And those best practices have been incorporated into the current revision of Regulatory Guide 5.71 that is in the review process. Finally --

MEMBER HALNON: Jim.

MR. BEARDSLEY: -- I'm sorry, yes.

MEMBER HALNON: Jim, on 5.71 is the NEI document keeping pace with it since 99.9 percent of the plants are committed to the NEI document?

MR. BEARDSLEY: At this time, NEI has not decided whether or not they're going to update NEI 08-09, which is the document that they based their cyber security plans on. So that will be a question that industry evaluates once the Regulatory Guide is complete.

MEMBER HALNON: Okay.

CHAIR BROWN: Well, they are updated. I guess, it looks like you have all interacted with them on what, 13-10 and --

MR. BEARDSLEY: 10-04.

CHAIR BROWN: -- conditional 4.

MR. BEARDSLEY: Right.

CHAIR BROWN: But yet, I had never seen 08-09 even referenced. So I'm not familiar with that

one at all. But that's the primary one. I guess we need to find that one.

MR. BEARDSLEY: Okay. We can make that available to you as well.

CHAIR BROWN: That would be much appreciated.

MR. BEARDSLEY: Okay. The other two areas, clarification of program definitions and terms was identified by both industry and the staff because there are a number of guidance documents. There's an NEI guidance document and there's a staff guidance document. And what we found was in some cases our definitions and terms weren't the same.

So we're working with industry to try and clarify that and make sure we're all speaking to the same definitions. And that's an ongoing effort as we update various different documents.

And finally the area of risk-informing control sets for digital assets, that's really looking at the future and how do we potentially come up with other methodologies that are different from that laid out in Reg Guide 5.71 or potentially the NEI 08-09 for implementation of cyber security programs in the future? Again, that's an ongoing effort that includes the Part 53 rulemaking and other areas that industry

is evaluating.

Now I'm going to turn it over to Mario Fernandez, who is going to discuss our changes to the emergency preparedness digital assets. If I can change the slide, oh, went too far. There we go.

MR. FERNANDEZ: Thank you, Jim. This is Mario Fernandez, Cyber Security Specialist in the Cyber Security Branch. As Jim Beardsley stated in the most recent assessment of the program, several areas were identified as areas for further risk informing to improve the efficiency and effectiveness of the power reactor cyber security program.

One of those areas identified is the emergency preparedness critical digital asset determination or what we call for a short term, EP CDAs.

Recognizing that an evolving program can benefit from lessons learned, the cyber security staff evaluated the proposed changes by the industry through EP CDA determination and the NEI guidance, which is related to Section Bravo 1 of 10 CFR 73.54, which requires licensees to analyze digital computer communication assistance and networks and identify those assets that must be protected against cyber-attacks.

The review and evaluation process required two public meetings. One public meeting that took place in November of 2019 and another meeting that took place in August of 2020.

Many iterations of the proposed changes, various reviews and evaluations by the NRC staff, reaching alignment into the NRC industry to ensure the proposed changes meet the requirements of 10 CFR 73.54 and finally a tabletop workshop conducted in August of 2020 to ensure implementation of the guidance is consistent with NRC approved implementation, strategies or approaches.

The new and improved guidance for EP DA screening, or digital asset screening, accomplishes the following.

It adopts a more risk-informed approach, that is an asset is identified for protection commensurate with the risk significance of that asset. And this approach is aligned with NRC emergency preparedness requirements and emergency plans, licensee emergency plans.

The enhanced EP DA screening methodology is more granular and considers methods and criteria that gives licensees the flexibility to take credit for methods that are required in the EP regulations

and the licensee's emergency plans.

This screening methodology provides efficiency and effectiveness to the power reactor cyber security program because it reduces the number of digital assets incorrectly identified for protection thus allowing licensees to reallocate its resources to the safety and security areas.

The Cyber Security Branch staff evaluated these changes and determined that this proposal is consistent with NRC approved implementation strategies or approaches described in NRC Regulatory Guide 5.71, Cyber Security Program for Nuclear Facilities.

These changes will be incorporated in future revisions of NEI 10-04, Revision 2, titled, Identifying Systems and Assets Subject to the Cyber Security Rule and NEI 13-10, Revision 6, titled, Cyber Security Control Assessments.

CHAIR BROWN: Can I ask a question on this, on the 13-10 and 10-04?

MR. FERNANDEZ: Yes, Member Brown, please.

CHAIR BROWN: You all had -- part of the -- thank you. As part of the documentation you sent, there were two submittals to the NRC from NEI that covered changes to both 10-04 and 13-10. And there were subsequent letters which went back to NEI which

said that they were -- and I've read it as best I could on your terminology, they were consistent with what you all thought. In other words, you didn't disagree with them.

Let me finish my thought process a little bit. I'm a little bit slow here. With that thought in mind, correct me if I'm wrong, the emergency planning efforts are largely carried out -- correct me if I'm wrong, from the emergency support center. If there was a program, it's outside of the plant boundaries. Am I correct on that?

Normally, we see an ESC that's not within the plant, but it's out on the site within the boundary conditions. And you need to communicate bi-directionally in many, many different ways. So it would seem to me that this is a pretty strong area to have to pay attention to since you don't want guidance or requests to do certain things to be compromised in those interchanges.

I just -- this seems to me a big threat problem to me. That's why I'm asking the question. Is that part of the overall -- I mean, obviously you've got to do bidirectional communications all over the place. You've got to let NRC know. You've got to let these people know. The governor has got to know,

et cetera.

That seems to be a tough challenge today. Do you do it independently? Do you segregate some systems or is it a combination of those?

MR. FERNANDEZ: Member Brown, you are partially correct. Licensees, depending on where the EP digital asset is located, its function, they perform the analysis and then they make the determination whether the EP function can be performed or not.

If the EP function cannot be performed because the digital asset is cyber compromised, let's say, then the licensee is required to provide protections for that particular digital asset. That's the granularity that exists in the enhanced methodology. Does that answer your question, Member Brown?

CHAIR BROWN: Well sort of. I mean, it's my impression if you look at what's been going on in other industries today, hackers have been getting in and turning things around and starting stuff that shouldn't be started. Shutting down stuff that shouldn't be shut down.

And so all of your -- my feeling is most of the cyber protection functions are reactive. All

your virus protections are basically reactive. So you're fighting the last battle. In other words, you're fighting the last war that tried to get through, not the current war that may come and get you.

Are there any what I call hardened data communication pathways which implement using a data diode or hard-wired type stuff as a backup? It doesn't have to be as extensive, but something what I call a backup to the more flexible digital approach.

MR. FERNANDEZ: Yes, Member Brown, you are correct. So there are digital assets as you have mentioned that are hardened, and they may be behind the data diode. Those digital assets are required to be fully protected.

And, therefore, throughout inspections we have verified that the licensee is putting all the appropriate security controls, physical as well as logical, in those EP digital assets that are supposed to be fully protected. And all the digital assets that required a certain level of protection, they also rely upon performing the EP function with other means, which the methodology allows licensee -- and provides the flexibility to do so.

CHAIR BROWN: Okay. Thank you very much.

I appreciate it.

MR. FERNANDEZ: Yes, Member Brown. And now I will introduce my colleague, Dan Warner, who is going to speak about the balance of plant digital asset determination. I turn it over to you, Dan.

MR. WARNER: Thank you, Mario. Good afternoon. And for those participating, we are on Slide 10. My name is Dan Warner. And I'm an IT Specialist Cyber in the Cyber Security Branch. And I'm here to discuss changes to balance of plant, or BoP, CDA determination guidance. BoP CDAs -- I'm sorry.

CHAIR BROWN: This is Charlie Brown again. I'm sorry to interrupt -- well, I'm not sorry to interrupt. I actually have a question so.

MR. WARNER: Sure. Please go ahead.

CHAIR BROWN: I'm not quite as versed in all the nomenclature inside the plants, balance of, I think, in terms of, you know, rod control systems and ESFAS systems, reactor trip, I call those reactor safety systems.

But you've obviously got switch gear, turbine generators. Is that balance of plant or miscellaneous other pumps and valves that have to be operated? I don't know where the dividing line is

between what I traditionally deal with and what people refer to as balance. Do you have an example of what balance of plant stuff is for poor little me?

MR. WARNER: So your balance of plant stuff is pretty much the power generating portion of the plant. So past any safety systems on the turbine, essentially from the generator outward to the first inter tiebreaker to the grid.

CHAIR BROWN: Okay. Okay. So it's right after the generator to connect again to the grid then. It's all that stuff.

MR. WARNER: Yes. And there are systems that would be associated with the turbine that are non-safety related or generator as well that would be included in that.

CHAIR BROWN: You mean, like voltage regulators and governors, I mean, those type of support that actually make them run and operate or is it the cooling systems for the turbine generator? Is it all that stuff?

MR. WARNER: Yes. Some of the plants, I think, define the area a little differently. But in general, we typically call it the stuff that's used to just actually make the power as opposed to the main steam system with the reactor --

CHAIR BROWN: Okay.

MR. WARNER: -- and through there.

MEMBER HALNON: Charlie, think turbine building.

CHAIR BROWN: I got it. That's a nice definition. Thank you very much. Okay.

MR. WARNER: Thank you.

CHAIR BROWN: You're welcome.

MR. WARNER: So BoP CDAs are those CDAs that were added to the scope of the Cyber Security Rule during the resolution of FERC Order 706-B. Industry proposed aligning the BoP CDA evaluation criteria with the review NERC CIP standards, which are based on impact to the bulk electric system.

What this means is that BoP digital assets that can result in a loss of power to the bulk electric system of 1,500 megawatts or less are low impact and have a reduced set of cyber security requirements.

BoP digital assets that can result in a loss of power to the bulk electric system of greater than 1,500 megawatts are medium impact and have a greater set of controls which are similar to our current BoP CDAs.

The grid operator can also indicate a

plant as medium impact under specific circumstances to maintain grid operation and reliability.

Most BoP CDAs will end up in the low impact category. This will allow licensees to reduce the number of controls on a significant number of CDAs and instead focus their resources on those assets with a higher safety significance.

As you can see on the slide, we had a number of public meetings to discuss the document.

The initial public meeting occurred in January 2020 and then NEI first submitted the paper in April of 2020. We addressed concerns and fed them back to NEI. And they submitted a revised paper to address those concerns in July of 2020.

FERC staff were involved throughout the review of the proposed guidance changes, and they were satisfied with the final document.

In August of 2020, NRC staff included the proposed changes in the paper are consistent with the requirements of 10 CFR 73.54 as well as the NRC approved implementation strategies or approaches described in Reg Guide 5.71 and NEI 08-09, Rev. 6.

And as Mario mentioned previously, these changes we are discussing will all be rolled up into future revisions in NEI 10-04 and NEI 13-10. And if

there's no questions, here's Eric Lee to talk about the safety-related and important to safety white paper.

MEMBER HALNON: Hey, Dan, this is Greg Halnon.

MEMBER KIRCHNER: This is Walt Kirchner.

MR. WARNER: Okay.

MEMBER KIRCHNER: You are implementing a FERC order. So I'm not asking you to comment on this. I would just observe that the threshold of 1,500 megawatts is very high. I guess FERC doesn't rule over ERCOT, but events in Houston would suggest a lower threshold in terms of the critical importance of nuclear power. You don't have to comment.

MR. WARNER: Okay. Thank you.

MEMBER HALNON: Dan, this is Greg Halnon. Did you guys -- I mean, early on, there was a concern that FERC and the NRC might be onsite doing different types of oversight on the same systems. Did you guys get an MOU or something with FERC to cover their systems?

MR. WARNER: That is correct. When this order was initially issued back in 2009, they put together a Memorandum of Agreement between FERC and the NRC that documents that NRC is going to be

cognizant of everything from the first inter-tiebreaker into the plant that maintains one regulator within the plant.

MEMBER HALNON: What ongoing discussions did you guys have at FERC? Do you have incoming reports that you give them or any kind of assurances or anything relative to your inspection process?

MR. WARNER: I'm going to ask Jim to chime in. I know there are commission meetings between FERC and the NRC, and I'm not sure if these are involved. So I'll let him weigh in on that.

MR. BEARDSLEY: During the every two year FERC and NRC Joint Commission meeting, the staff does provide an update on the inspection program and what we've found, but we do not have a routine reporting process for FERC. If we did find significant issues in a licensee site, the staff does have routine communications with FERC staff, and we would inform them thereof.

MEMBER HALNON: And I was really interested in vice versa, where non-nuclear facilities may come up with some issue or lessons learned or other issues that may have happened from a cyber perspective. How do you guys get word of that?

MR. BEARDSLEY: The staff has a number of

different liaisons with the Department of Homeland Security in particular. And we're establishing various lines of communication with the new Department of Energy agency that's responsible for cyber, and I can't remember what their acronym is.

And so that's really where we would do our interagency liaison. We also have a full branch in NSIR whose primary responsibility is intelligence analysis and interagency liaison. So we have multiple different lines of communication.

MEMBER HALNON: Okay. So is there no one national clearing house that accepts all the cyber issues or is that DHS?

MR. BEARDSLEY: That's DHS CISA, that's Cyber and Infrastructure Security Agency.

MEMBER HALNON: Okay. And then it all feeds out from that.

MR. BEARDSLEY: Correct.

MEMBER HALNON: It feeds in and feeds out from there. Okay.

MR. BEARDSLEY: Correct.

MEMBER HALNON: Thanks.

MR. WARNER: Okay. If there are no more questions then Eric, take it away.

MR. LEE: Thank you, Dan and good

afternoon. My name is Eric Lee from the Cyber Security Branch. And I'm a Senior Cyber Security Specialist. And I'm on Slide Number 11.

This white paper does safety-related and important to safety white paper is a sister paper to the BoP white paper that my colleague, Dan, just explained.

Like the BoP white paper, safety-related and important to safety white paper provides proposed changes to NEI 10-04 and NEI 13-10.

As stated previously, the focus of the BoP white paper is providing guidance for identifying BoP CDAs that were added to the scope of the Cyber Security Rule as an important to safety CDA during the resolution of FERC Order 706-B.

However, the focus of the safety-related and important to safety white paper is providing guidance for identifying those digital assets that the Cyber Security Rule originally intended to identify as safety-related and important to safety CDAs.

The term safety-related is defined in the regulations. However, the term important to safety is not even though the term is used in the NRC regulations and used throughout the history of the NRC.

As a result, everyone seemed to have a picture or an idea of what important to safety systems and equipment should be. But the picture that everyone draws in their mind may not be the same.

So guidance provided in the white paper aligned the term safety-related to the definition provided in 10 CFR 50.2 and closely aligned the term important to safety to how the NRC historically used this term.

This ties safety-related and important to safety systems and equipment for the purpose of identifying safety-related and important to safety CDAs to those systems and equipment that are accredited to meet the licensees current licensing basis to shut down the reactor, maintain it in a shutdown condition and prevent the release of a radioactive material during the event and accidents to meet its current licensing commitments or its current design basis.

Additionally, any systems and equipment that meets the following two conditions are protected as safety-related or important to safety CDAs. One, any system or equipment that functionally interfaces with the safety-related or important to safety equipment that I mentioned earlier.

Two, if a compromise of a cyber attack of a subsystem and equipment interfacing with the safety-related and important to safety equipment could adversely impact the safety-related or important to safety function, if that is so, then they are protected in the same manner as the safety-related or important to safety CDA.

This white paper took a year to develop. It began in August of 2019 when NEI and the NRC met to discuss the concept of safety-related and important to safety system and equipment for the purpose of identifying CDAs.

A year later in August of 2020, the NRC accepted the white paper after NEI addressed the staff's comments on its white paper that NEI submitted in May of 2020.

Staff provided its comment in a public meeting in June 2020. This allowed licensees to use the guidance provided in the white paper before NEI updates 10-04 and NEI 13-10. Any questions?

MEMBER HALNON: This is Greg Halnon. I have a question. It may be more for the Branch Chiefs. But is this the typical regulatory process? I thought typically that NEI would write a document. The NRC would endorse it through a Reg Guide. But it

appears that we're kind of paralleling that with white papers and NEI documents that are agreed to and a Reg Guide that's only being used by one licensee.

Is that the way that we have planned this? Was there some other thing behind the scenes that's going on?

MR. BEARDSLEY: Greg, that's a good question. Planning it is a little bit challenging. Because we knew there were a series of changes that were going to happen to these guidance documents, but through the assessment process and the feedback we received from stakeholders, we recognize that these were areas that we felt were important to be addressed.

The industry elected to submit a series of white papers while it's trying to update the documents in a sort of parallel fashion, which would have been very challenging.

So it does seem a little strange the way it played out. But it provided the industry the feedback in these areas more quickly than they would have had we had to wait until the guidance documents had been updated for each one individually.

When they're done, which we are done now with all four of the white papers, industry is

preparing a comprehensive update to each of these guidance documents. And the staff will have the opportunity to review that in total.

MEMBER HALNON: Do you anticipate you'll endorse those through a Reg Guide or some other more established mechanism?

MR. BEARDSLEY: As a general practice, we have not endorsed the NEI guidance documents for cyber through Reg Guide. We have accepted them for use by letter.

MEMBER HALNON: Okay. That seems like a one-off as well but maybe it's been done in the past. I just didn't know.

CHAIR BROWN: If you've accepted those -- I tried to look at some of these white papers. I couldn't define everything. I was looking for the ones that defined these safety-related and important to safety functions. And I was trying to get a definition of what that was. I didn't see a clear definition of what somebody claimed to be safety-related or any examples. Was that deliberately left out in terms of providing examples for what that means? It's pretty wordsmithed in most of the places I was able to find.

MR. BEARDSLEY: So just for context, this

particular white paper is different than the other three in that we wrote a number of inspection findings in this area because the licensees had underprotected the systems. So they had classified systems that we felt should have had a full suite of controls as having a lesser suite of controls.

And so the goal of this effort was to be very clear to industry on what needed to be protected more and what needed to be protected less. And I think Eric would agree with me that the result is more systems will be protected as a result of this part of the initiative.

MR. LEE: And certainly, Member Brown, to your point, to help the licensees and the inspectors understand what systems and equipment should be considered safety-related and important to safety for the purposes of identifying critical digital assets, we have provided the 10 steps to identify what systems are considered safety-related and what systems are considered important to safety CDAs.

CHAIR BROWN: Are those in the white papers? One white paper I found on safety-related versus and affected -- I guess, it was an NEI document dated July 17, 2020, and it showed changes to NEI 10-04 and 13-10. And it was all related to the -- let me

get the title correct so I don't mess that up -- safety-related and items important to safety.

But they refer to things like integrity, the reactor coolant boundary, the capability to shut down. Some of that didn't change. But then a lot -- there were a lot of red markups when you got to the changes which didn't seem to relate.

I'm kind of echoing Greg's thought process. It seemed backwards. I would have expected instead of these things showing up in industry documents, I would have thought that they would have ended up being categorized within, you know, 5.71 or something like that to categorize this particular terminology to make sure there was one consistent NRC document that told people what was what, what was safety-related and what qualified as important to safety. But as opposed to that, you have to now go to all these other documents.

I haven't read any of the revisions. I've tried to look through parts of the new 5.71, but it's increased considerably in size from 114 pages to 144 or something like that. So it got a little bit difficult to go side-by-side and compare them.

So it just seemed a little bit backwards. I guess that's a little bit of a concern is how well

is this stuff defined?

MEMBER KIRCHNER: This is Walt. Eric, is this defined in your white paper?

MR. LEE: Yes, sir.

MEMBER KIRCHNER: Did you see any of that, Charlie?

CHAIR BROWN: The only paper I had that I saw was a white paper on this was an NEI Document E200-717-TE040841 dated 7/17/20, changes to the NEI documents. And I didn't see another white paper in anything we got. I saw then there was a response to that.

MEMBER KIRCHNER: Well, Charlie, this is a side observation, but this is very important and useful for 10 CFR 53 deliberations because clearly in 10 CFR 53 draft rule language, they're going to have to deal with definitions.

This approach that Eric has described strikes me as a functional approach that could be, you know, getting beyond the 10 CFR 50.2 definition of safety-related to a more generic technology inclusive definition. What the staff has done here might be very relevant to the 10 CFR 53 development.

MR. BEARDSLEY: Yes, we'll be discussing at a high level our first 10 CFR 53 cyber security.

But I think that -- I agree that the appearance of just looking at the white papers can be confusing. We will be receiving a markup of the guidance documents from NEI in the next few months. And I think that once you see all of the changes associated with the document, it will be much clearer how this all works.

And so what industry is going to do is they take the white paper that Eric addressed and then they'll go implement the changes in the white paper to their own implementing procedures, which are based on the NEI guidance documents.

So it's clearer to the user than it is to maybe the casual reader.

MEMBER KIRCHNER: Yes. But for our purposes put the NEI aside that's more of an industry position. It's the staff's position that I'm the most interested in. Is this white paper available to us?

MR. BEARDSLEY: Yes. It's the paper that Member Brown mentioned a moment ago.

CHAIR BROWN: If that's the July -- that's the July 23 -- that letter number that I wrote or referenced? I think it was the E200-717-T040841 of 7/17/20?

MR. BEARDSLEY: We'll verify that for you and make sure that you have the right one. I believe

that is correct.

CHAIR BROWN: It was about 19 pages long. And it had a lot of red inside the document. And those changes were to NEI 10-04 and then I think at the very end, they got into 13- --

MR. BEARDSLEY: 13-10, correct.

CHAIR BROWN: -- 13-10, correct. But they referenced, I guess, one of the sets of words that I had highlighted where they had talked about stuff that could be thrown in to some other category. I couldn't figure it out.

It was examples of equipment that does something. It would be electrical equipment powered from the 1E tire supplies and are classified under the 1.97. So it started tossing around Reg Guides like candy at a child's party. I lost track of what was going on.

I wasn't able to read that entire white paper and understand it relative -- I just got the NEI document a day or so ago. So it just seems --

(Simultaneous speaking.)

MEMBER KIRCHNER: Well, Charlie, I'm just repeating myself, but the staff's position is what I'm interested in --

CHAIR BROWN: Yes.

MEMBER KIRCHNER: -- not a markup by NEI.

CHAIR BROWN: This is NEI's document. I agree with you.

MEMBER KIRCHNER: This is a fundamental important thing in developing the10 CFR 53 rule.

CHAIR BROWN: I agree with you. It's just a matter of how do you get these things integrated together? And you don't want to develop another rule that has another set of terminology that you have to deal with so. Okay. So we're informed of what you're doing. Any other questions before we move on? Okay. Eric.

MR. LEE: Thank you. Now, here is Brian Yip to talk about the security white paper. Brian?

MR. YIP: All right. Thanks, Eric. Good afternoon. My name is Brian Yip. I'm a Cyber Security Specialist in the Cyber Security Branch in NSIR. And I'm going to talk about the final white paper for this afternoon, which addresses critical digital assets related to physical security systems.

And like the others, it proposes changes to NEI 10-04 and NEI 13-10 to clarify guidance on how to identify physical security critical digital assets and the appropriate controls to apply to them. And I focused on four areas.

First, it tied the definition of a physical security function, you know, when we talk about safety security and emergency preparedness functions, it tied the physical security functions to the physical security regulations in 10 CFR 73.55(b).

So, for example, access control systems, physical barriers, you know, alarm intrusion detection systems, assessment systems, so it makes clear the list of physical security functions that need to be protected from a cyber perspective.

The paper also provides guidance on what it refers to as digital security tools. And these are devices that licensees in some instances use such as like a digital range finger or a digital rifle scope. These are things that may be used from a security perspective but don't really meet the intent of performing a security function.

So the paper gives licensees a guidance that if they evaluate these devices, they would still need to evaluate them. And they confirm that the device does not perform a security function and that it cannot adversely impact -- the compromise of it could not adversely impact a safety security or emergency preparedness function, then they don't need to consider those devices to be critical digital

assets.

The paper also gives licensees an alternative means to address security support systems. An example of that would be an HVAC system that provides cooling to the central alarm station or the security computers.

And similar to the approach taken with emergency preparedness, if licensees establish procedures and training to implement alternate means to provide that support function and they do it in a way that prevents an adverse impact to the security function that it's supporting, then that device performing a support function does not need to be protected as a CDA.

And lastly the paper provided additional guidance on the protection of digital assets used for access authorization. So computers used for background checking programs, granting access to the plant, et cetera.

And it addressed a number of different configurations and scenarios that we see with licensees in the field. Some licensees protect their digital assets for access authorization at the highest levels of their network. Others rely on offsite corporate assets to perform some access authorization

functions. So this paper provides additional guidance on how licensees should classify and protect those digital assets in each case.

It also describes how licensees must verify the data integrity if they take access authorization data, such as somebody was approved for plant access, all that badging information, when it's transferred onsite to the plant security computer, it gives licensee's requirements that they have to perform a secondary verification to make sure that data integrity was maintained when that data was transferred to the plant security computer.

On further review of this white paper, we had some initial discussions with NEI in mid to late 2020 and then NEI submitted a draft in December 2020.

We held a public meeting in January 2021, and provided NEI with comments, staff comments in April of 2021.

Our comments centered around ensuring that there was sufficient detail in the access authorization section to ensure proper implementation that covered all of the various licensee configurations that we've seen and also ensured that there was sufficient detail in the security support system guidance to ensure that it protected against

adverse impact to the security functions that it's supporting.

NEI submitted another revision that we reviewed and found consistent with the NEI 08-09 in June of this year. And as with the other white papers, licensees can implement these changes now or they can, you know, wait for the full revision to NEI 10-04 or NEI 13-10 if they wish.

Any questions on physical security? Okay. With that, I'll turn it back over to Jim. Thank you.

MR. LEE: Jim, you are muted.

MR. BEARDSLEY: That was going to happen eventually. As I noted earlier, when the staff performed our program assessment in 2019, the Office of Inspector General also conducted an audit of the cyber security inspection program at the same time. And both of those processes identified opportunities to further performance inform our inspection program.

The staff has taken the lessons learned from our full implementation inspections conducted from 2017 through 2021 and developed a new inspection procedure that will be incorporated into the reactor oversight process inspection cycle.

The inspections have been shortened from two weeks to one week and will be conducted on a two

year basis versus a three year basis.

The inspections will be based on having two regional inspectors and two subject matter expert contractors similar to the inspections we've conducted to date.

We are providing opportunities in the inspection procedure for licensees to provide the staff with performance metrics information or potentially performance testing information on replicas of their systems. If they do that, the staff will evaluate the information and may reduce the resources assigned to the inspections.

The staff hopes to have this inspection procedure approved in August and plans to conduct a series of public meetings with industry and stakeholders to discuss implementation of the inspection procedure prior to the start of inspections in January of 2022.

Are there any questions about our future inspection program? Okay. I will be followed by Juris Jauntirans, who will discuss our cyber security efforts associated with the Part 53 rulemaking program.

MR. JAUNTIRANS: Good afternoon. As Jim said, my name is Juris Jauntirans. I'm a Cyber

Security Specialist within the Cyber Security Branch. During my portion of the brief, we will be on Slide 14.

In Part 53, NSIR staff aims to develop a technology inclusive regulatory program for advanced reactors that applies a performance-based graded approach for a comprehensive range of security areas, including physical security, cyber security, information security, fitness for duty and access authorization.

This proposed regulatory framework will offer applicants flexibility to rightsize the program by providing performance-based requirements that are commensurate with the risk to public health and safety. Both of the physical security and the cyber security sections in Part 53 are going to point to new sections within Part 73 and for cyber security, that's going to be Part 73.110.

In this new section of Part 73, the staff specifies cyber security requirements for the protection of digital computers, communication systems and networks for advanced reactors. And we presented the proposed language at a June 10 public meeting.

While 10 CFR 73.54 provides a good framework for cyber security operating reactors, the

staff feels that advanced reactors require a more flexible approach to adapt to the wide variety of technology that advanced reactors could potentially represent.

CHAIR BROWN: Why?

MR. JAUNTIRANS: With that in mind -- I'm sorry.

CHAIR BROWN: Why? I mean, a reactor is a reactor. Why does an advanced reactor -- why does it need more flexibility than the regular reactor plants that we have today?

MR. JAUNTIRANS: We were given the task --

CHAIR BROWN: That's the next statement.

MR. JAUNTIRANS: Okay. That's a good point, sir. We were given the task to develop a graded approach because of the variety of technologies.

We can go from a very, very small source term, very, very small reactors all the way to something that's as big or larger than the current light-water fleet and because the varied types of control systems that a cookie-cutter approach from 73.54 would not necessarily be the best approach. And we are currently in a draft. And we would be happy to accept any other --

CHAIR BROWN: Did we lose you?

MR. JAUNTIRANS: -- on the draft rule.

CHAIR BROWN: Why in the world would the cyber security requirements be worried about whether you had a low source? I mean, you don't want a reactor plant regardless of the source term to be hacked, destroyed, rendered, you know, unusable or be dangerous in any way, shape or form than it regularly would. Just because it may not contaminate as large of an area, we let guys freewheel in and do what they -- I'm being facetious a little bit with my statement. I'm overstating the point just to make the point.

It just doesn't seem to make sense that source term would be used to define the level of cyber security or the allowance for less or a more penetrable type cyber security then you would involve on a large light-water reactor.

MR. JAUNTIRANS: So source term is not the only criteria. And I believe Michele Sampson here has appeared on the screen. I think she's got something to add here.

MS. SAMPSON: Thanks so much, Juris. I just wanted to make the point that our intent in the Part 53 rulemaking effort is to provide an equivalent level of safety and to develop regulations that are

technology inclusive.

So we certainly are not looking to provide anything that would be a lower level of safety. The regulations will provide an equivalent level of safety but also provide a performance-based approach that will enable or ensure that applicants consider the range of, you know, potential hazards that may exist with the different technology designs.

So, you know, it's certainly not our intent that the regulation is lesser. It is just technology inclusive and very performance based.

CHAIR BROWN: Well, all of these were performance based. I mean, the stuff we are putting in today are performance based. They are technology inclusive, and they are technology neutral. You can do them multiple different ways. So those words, pardon my French, seem to be injected into a lot of these different conversations these days relative to what we're doing.

The connection we have in general is stuff that's going to be the same across platforms, we shouldn't make them different or think they should be -- this is a personal opinion now. This is not a committee opinion. I want to make that clear.

I just have a hard time understanding why

we can allow a wireless connection into a plant where it can be totally hacked and melted down because it's an advanced reactor, because it's got a little source term, I'm saying that speculatively, when we wouldn't allow that type of stuff in a large light-water reactor.

It's just the thought process. I think we have to -- there are some things you have to protect against. And cyber is a very vulnerable area on any plant that we put out in the field that NRC puts their name behind.

MEMBER BLEY: Charlie?

CHAIR BROWN: Yes.

MEMBER BLEY: They haven't said they are going to allow wireless on a new plant. They said they're going to maintain the same level of safety. And I'll take you back to a meeting we had a couple years ago on this topic when you very much, and I was with you, were worried that the level of effort we were forcing people into and looking at critical assets was going to cost more than is reasonable.

And I personally see if there's a low chance of harm, we don't need to pour as much effort in as if there's a high chance of harm. And I'd give them the chance to come up with something. Now

they're saying they will maintain the same level of safety. We've got to see what that means. But dismissing that as not possible at least to me doesn't seem reasonable.

CHAIR BROWN: I'm thinking more of access than I am anything else. And I agree with you. I've always worried that we can overdo the CDA routine and beat the licensees to death. You're correct. I've said that before, and I will say that again right now. I don't want to impose.

I like to categorize systems, those that really are related to safety. And those that aren't -- so they get compromised, you can recover and don't worry about it because you just may lose some data. You may lose some of this. But the world is not going to end.

And I've always worried that we've applied too many rules to stuff that don't need a lot of rules. So it's a double-edged sword, but I don't like -- I'm just worried about people thinking access can be maybe a little bit easier because the outcome or the results may not be as bad.

And I just think it's bad for any reactor plant to be viewed as a potential hazard. It's hard enough getting them built these days without adding

impressions to people that they're just not as safe as they used to be. It's just a thought -- that's just my thoughts. That's all. I'm not trying to -- I'm just trying to make this to be thoughtful and not get carried away. That's my only thrust.

MEMBER HALNON: So, Charlie, this is Greg. I understand where you're going with that. And I'm kind of looking at it from a different perspective that the new look at it from this performance based, maybe we'll have a conversation in the future how that could apply based on lessons learned and higher levels of knowledge that we had in the '08s and '09s time frame based on, you know, the contemporary cyber knowledge. Maybe we will have a conversation on how this could apply to the large light-waters in the future as opposed to just the smaller reactors.

Kind of like what Dennis said, I'm kind of just anticipating an interesting conversation on the other end, why couldn't this apply to the bigger plants as opposed to, you know, what you're saying is why can't the bigger plants comply to the advanced reactors? So anyway, that's my thoughts. That's what you sparked.

CHAIR BROWN: I don't disagree with you from that thought process. My fundamental thought

when we do our design reviews, primarily my focus is on the reactor trip, safeguards, ECCS and the functions that they control to ensure the plant is safe. And there's a plethora of other equipment out there that don't really require that level of protection.

MEMBER HALNON: Okay. Yes, I agree, and, you know, clearly the balance of plant stuff for the smaller reactors will be in a different neighborhood --

CHAIR BROWN: Absolutely.

MEMBER HALNON: -- so.

CHAIR BROWN: Absolutely. But yet one of the big concerns in the power supply type world is with operators going to Internet controls of their remote stations, you have just set yourself up for a massive grid shutdown because it's very difficult to protect those assets cyber-wise. I mean it's a continuing threat. And you're always fighting yesterday's battle.

MEMBER HALNON: Well, and this brings us back to the potential discussion of autonomous operation. You're talking about wanting to be fearful of something that could happen bad is no one would even be watching it.

CHAIR BROWN: Yes. Yes, we mentioned that before. It's another one of my big concerns.

MEMBER HALNON: Yes.

CHAIR BROWN: All right. I'm sorry I just -- you can tell that this stuff is dear to my heart so.

(Simultaneous speaking.)

MEMBER KIRCHNER: I think, Charlie, this conversation sooner or later is going to have to include a conversation about operators and where they're located and how they're licensed, et cetera, et cetera, and physical security.

I kind of view it as kind of like a Venn diagram of sorts because for those micro reactor concepts and other concepts that aren't likely to be large megawatt plants, what they are envisioning is entirely different than what we expect of, you know, a large power plant in terms of are there operators or physical security and the cyber security aspects, especially if they're "to be remote operated."

MEMBER MARCH-LEUBA: Yes. But let's not relax the requirements for the 3,000-megawatt plant because there is an assumed 1 megawatt plant out there that may want to do something different.

We tend to write our regulations to the

lowest common denominator, which is the best plant, which is the 1 megawatt plant. But we still have to deal with the 3,000. That was just a comment.

I wanted to bring back to the discussion this line, which is Part 53. In my opinion, the biggest qualitative change in Part 53 is the interaction of Tier 1 and Tier 2 safety goals. Okay.

And what we've done is move all of the safety off to Tier 2. And anything that is in Tier 2 is non-safety grade. So you guys have the experience of operating reactors with almost all SSCs are safety grade, and you have to protect them.

When you look at that 53 license plant, they may not have a single safety grade component, not one, because of the way they have it under Tier 1 and Tier 2. And you need to think about it because I don't like it. I'll put it on the record. You guys please do think about --

MEMBER PETTI: Jose, I really wish you'd stop interpreting and reading into 53 things that aren't there. I've seen a ton of plants. They all have safety systems. Okay? To say that they would have no safety systems is an exaggeration and doesn't affect the operation.

MEMBER MARCH-LEUBA: I will go to the

transcript and say where the staff said that. I will find it for you.

MEMBER MARCH-LEUBA: The staff said some of this is more than one --

MEMBER PETTI: The staff is recommending getting rid of the concept of Tier 2, which means that all of the requirements would just be there so.

MEMBER MARCH-LEUBA: And I don't know. And we are, too, ACRS put it on the record.

MEMBER PETTI: Yes. So that's just not --

MEMBER MARCH-LEUBA: So right now it is there. Okay? So if you are writing a cyber security policy for Part 53, you have to assume, today, that there's a Tier 1 and a Tier 2. And a very small low power reactor with very good fuel cannot possibly produce 25 rem at the boundary. Under 4, you don't need anything for safety grade. And they told us that yesterday.

MEMBER KIRCHNER: So you're throwing that position, Jose, that I don't think is a likely outcome from a staff review of an application.

MEMBER MARCH-LEUBA: They told us that yesterday.

MEMBER KIRCHNER: Remember, you still have to, as a previous presenter today said, you have to

shut down the reactor and maintain it in a shutdown condition and you have to protect efficient product --

MEMBER MARCH-LEUBA: Nope, nope, nope, nope, nope, nope, nope. Control reactivity is Tier 2.

MEMBER KIRCHNER: No. It is not.

MEMBER MARCH-LEUBA: It is. Look at it. Check it out. Tier 1, and we'll discuss it in Part 53. I apologize to these other guys. Tier 1 is only control of heat ventilation (phonetic).

CHAIR BROWN: That's okay. Can we resolve that and get on with this particular discussion? I think we ought to get that one cleared up so we all understand that, Jose and Walt so and Dave. So I agree. We ought to --

MEMBER PETTI: Let's table that and keep going, Charlie.

CHAIR BROWN: Yes. That's what I'm planning on doing that right now. Okay. Go ahead. I'm sorry about that.

MR. JAUNTIRANS: No worries. Thank you. I think it's a good valuable discussion for everybody to hear. Thank you.

So with the flexibility that we've previously discussed, in lieu of requiring advanced reactor licensees to protect against cyber-attacks up

to and including the design basis threat as required for power reactors in 10 CFR 73.54, the proposed new section implements a graded approach at the cyber security program and security controls implementation level.

A greater approach based on consequences is intended to account for the differing risk levels within advanced reactor technologies. Specifically, the new section requires licensees to demonstrate reasonable assurance of cyber security protection against cyber-attacks only if such attacks would lead to a consequence as defined in the proposed rule.

The proposed new section leverages the operating experience from power reactors. The proposed regulations for fuel cycle facilities as well as 10 CFR 73.54 framework as it contains some of the basic requirements needed for cyber security regardless of reactor type.

It's also informed by the NRC's Office of Nuclear Security's Incident Response Interagency interface efforts associated with cyber security.

Differences between the 10 CFR 73.54 requirements and those discussed in the proposed new section are primarily based on the implementation of the graded approach used in the Part 53 construct to

accommodate the wide range of technologies to be assessed by the NRC.

The proposed new section currently includes two consequences which are related to advanced reactors physical security requirements in Part 53.

The first consequence seen here on the left side, the second box from the top, deals with the topic of radiological sabotage. Specifically, it deals with the scenario where the cyber-attack leads to offsite radiation hazards that would endanger public health and safety.

CHAIR BROWN: We lost you or you're muted.

MR. JAUNTIRANS: Yes. Somebody muted me there. Okay.

CHAIR BROWN: Yes.

MR. JAUNTIRANS: All right, anyway. So it specifically deals with -- it's the consequence exceeding specific dose value criteria from Part 53. At the current time, it's tied to Part 53 first tier safety and criteria.

The second one, which would be the bottom box on the left side, that consequence deals with the topic of theft or diversion. Specifically, it deals with the scenario where the cyber-attack adversely

impacts digital assets used by the licensee for implementing the physical security requirements for special nuclear material, source material and byproduct material in Part 53. This is tied to the Part 53 physical security rules for advanced reactors. And that is linked with Part 37.

As a part of the Part 53 rulemaking efforts, the staff is seeking formal feedback from all stakeholders on whether any additional consequences should be included in the new section. And as of present, we have not received any feedback in that regard.

The primary feedback we've received has been about the Tier 1 safety criteria. I don't have that at this present time. But that's the most feedback we've gotten at this time.

The remainder of the rule resembles 10 CFR 73.54 in many ways while implementing the graded approach as previously discussed. And are there any more questions? Okay. I'd like to turn it back to Jim for discussion on the PRM.

MR. BEARDSLEY: Thank you, Juris. In 2019, when the staff briefed the Subcommittee -- there we go -- we noted the fact that NEI had submitted a Petition for Rulemaking to change the Cyber Security

Rule in 2014.

The staff has reviewed that rule over the course of the last few years. And in 2019, a decision was made to hold off on a decision until the staff had completed the efforts associated with our internal self-assessment and the action plan that we discussed earlier in this presentation.

The staff has since made a recommendation to the Commission and the Commission has yet to complete their decision-making on the petition. And we expect to hear from the Commission sometime this month or early next month. Any questions about the Petition for Rulemaking?

CHAIR BROWN: Yes, Jim. Is that the 73.54 rule or --

MR. BEARDSLEY: It is. It was a petition -- PRM 73.18 dealt with the content and construct of 73.54.

CHAIR BROWN: We haven't been involved in that, at least I haven't been at that point. Can you give us a little bit of the thrust of the NEI? I know we've got the Petition here, but I didn't get to that part. I was looking at the other parts.

MR. BEARDSLEY: Sure. Big picture, NEI's point was that the industry had overincluded digital

assets in their cyber security programs, which could potentially distract them from focusing on those assets with a higher risk or a higher significance. And they believe that the rule should be rewritten to reduce the overall scope.

The staff reviewed that in light of the fact that it is a performance-based rule. The staff has, you know, done evaluations and in particular, as a result of the action plan, has been working with industry to try and look hard at the decision-making process on what digital assets need to be included in the program and those that have not. And those are the areas we talked about earlier in our presentation.

MEMBER KIRCHNER: Jim --

CHAIR BROWN: Have you provided a recommendation -- just a minute, Walt. Have you provided a recommendation to the Commission or --

MR. BEARDSLEY: The Petition Review Board did provide a recommendation to the Commission. And the Commission has yet to respond to the staff.

CHAIR BROWN: Was the staff involved in that? I mean, like --

MR. BEARDSLEY: The Petition Review Board was made up of staff, yes.

CHAIR BROWN: Okay. Folks that were

familiar with the cyber security requirements in 5.71 and what fell out of the rule in terms of actual execution?

MR. BEARDSLEY: Right. As with all petitions, you have a multidisciplinary team that makes up the overall evaluation.

CHAIR BROWN: All right. Thank you. Yes, Walt, I interrupted somebody.

MEMBER KIRCHNER: No. It was along the same lines, Charlie. I was just thinking 2014 is a long time ago. Both the industry and the staff have come a long way, the staff, in implementing its program plan. Does the industry still feel like the rulemaking is necessary given where we are in 2021?

MR. BEARDSLEY: I couldn't say. You would have to ask industry.

CHAIR BROWN: Okay. Any other questions on this subject? All right. Why don't we roll on, Jim.

MR. BEARDSLEY: Absolutely. We talked about Regulatory Guide 5.71 a number of times over the course of the brief. Just to point out, the Reg Guide was published in 2010. In 2016, the staff initiated an update to the Reg Guide.

And in 2018 and 2019, it was recognized

that the staff and industry, through our assessment and as a result of inspection lessons learned, had found a number of areas that probably should be included in the draft guide or the Revision 1 to the Reg Guide. So we put that draft on hold in 2018 and picked it up again just this past year in 2021.

The staff has completed the update of the Reg Guide based on the information they had to date. And that update included the implementation of the industry white papers, which we talked about earlier in this presentation, clarification on insights gained from operating experience in both national and international cyber security standards, updated text to discuss risk-informed cyber security evaluation methodologies and updated texts based on the resolution of public comments that were received when the draft guide was last released publicly in 2018.

The staff intends to release this version of the draft guide for public comment in the near future and will hold multiple public meetings associated with that public review process.

The current schedule has the Revision 1 to Reg Guide 5.71 being published sometime in the spring of 2022. Any questions about the revision to the Reg Guide 5.71?

MEMBER HALNON: Jim, this is Greg Halnon. I realize that it looks like a lot of effort for revising a Reg Guide that one licensee is using for one plant that's not even operating yet. What is the industry looking at?

Are they looking at helping you get this to where it needs to be so we can use 5.71 consistently across the country and satisfy our earlier concerns about so many documents with so many different definitions and whatnot or is this going to just be a continuing saga of just one licensee using it?

MR. BEARDSLEY: So based on the feedback I received from industry, I don't believe that the licensees are going to change their Cyber Security Plans because the draft guide isn't changing the template for the Cyber Security Plan significantly.

Our goal with updating the Reg Guide is to incorporate the lessons that we've learned over the years and really look hard at both national and international standards and make that information available to future licensees.

So the Rev 1 to Reg Guide 5.71 is arguably tailored towards the information for future licensees.

MEMBER HALNON: So future Part 50 and 52,

right.

MR. BEARDSLEY: Future Part 50 and 52, right. We are engaged in a parallel Regulatory Guide development as part of Part 53, which will also include a significant amount of the information we've included in Reg Guide 5.71.

MEMBER HALNON: Okay. I think my concern is that there's just a lot of parallel efforts going forward and a lot of parallel documents. You know, there are multiply different licensees using them in different ways.

I mean, ultimately, they're all getting to where you want to be. I get that. But the concern is that it's a lot of effort when there's, I mean, both on your side and the industry side to get this document updated.

And I agree it's for future licensees. But I'm not sure how many more there's going to be under Part 50 and 52 that it would make all this effort worth it.

So anyway, I got to go back and look at the whole plethora of documents again and just see how it all fits together. So thanks. And I'll hold my comments until later.

MR. BEARDSLEY: Any other questions on our

Regulatory Guide 5.71 update?

CHAIR BROWN: Yes.

MR. BEARDSLEY: Okay.

CHAIR BROWN: I don't want to do a detailed -- I'm not trying to do a detailed -- I'm always curious about 5.71 so I did take some time and compare the original revision from 2010 to the new update.

The new update has some good stuff in it, okay, some references to unidirectional, hardware based, non-software controlled, et cetera, et cetera. Good lessons learned from all the design applications we've gone through.

It also has some stuff that's not so good. And you probably knew I was going to say that somewhere. For instance, the old one, and I'm not going to go through a lot. It's just an example. The old one prohibited bidirectional communications or any communications from lower levels of security to the more secure levels, in other words from Level 2 to Level 3 or 4.

MR. BEARDSLEY: Mm-hmm.

CHAIR BROWN: And they do it on a denial, permit by exception basis. It's just all kinds of weasel words whereas before you weren't able to do

that with bidirectional or even unidirectional from the lower safety to the higher safety systems. That's not good.

But like I said, is that countered by some of the other good stuff? I don't know what else is in there. It would certainly behoove to get us and you all on the same page before you go out with this. That's all. I don't know what your overall plans are but --

MR. BEARDSLEY: Sure.

CHAIR BROWN: -- we really probably ought to -- and it's also about -- let me see. It's at least 55 pages or 45 pages longer than it used to be. So I'm worried about complexity being added into it now as well. Does that mean more requirements or what? So what you --

MR. BEARDSLEY: So the section of the regulatory guide that details the licensee's cyber security plan has not changed very much at all. There are a few changes that we approved for industry over time that are incorporated. So the majority of the new information is program level guidance on sort of how you would look at a program.

And also the initial Reg Guide was based on the National Institute of Standards, cyber security

standards, at the time in 2009, 2008. Those standards have changed significantly over the last 10 years. And so we've looked at those and tried to incorporate the lessons from those standards as well in addition to look at some international standards.

So there's a lot of information there, I agree. And it is a significant change. But there is good information in there for users.

CHAIR BROWN: I saw some. I told you all right up front, I saw some stuff that was much better than the previous words. But I'm also -- every time somebody says we've updated the new standards, and the new standards are more what I would call less safe, like communicating from low level to high level, high security level stuff, that was totally prohibited and was looked at, you wouldn't do that before and now it's allowed, fundamentally allowed, although you say they're going to have to jump through hoops to do it.

I don't know what else is in there like that. That's why I think a little bit of another eyeball on it before we get all enhanced with the industry and public standpoint would probably be useful. We need to look at that just to give you a heads-up.

MR. BEARDSLEY: Got it.

CHAIR BROWN: Go ahead. You can move on unless --

MR. BEARDSLEY: Okay.

CHAIR BROWN: -- somebody else has something.

MR. BEARDSLEY: Okay. The NSIR staff over the last year or so have engaged with our colleagues in the Office of Research on a number of research projects to look at different aspects of cyber security, both current and future.

This list shows the high level four areas that we currently have cyber security research going on and our colleagues in research will be briefing, I believe, the full committee tomorrow. So if there's any questions from a research point of view, you'll have an opportunity to ask then.

Just a quick look at what these are, attack surfaces for cyber security monitoring and oversight. One of the things that we've looked as we've inspected industry over the years is trying to understand and help industry understand what are the, you know, attack surfaces or the ways that an adversary could attack them?

And the staff is engaged with research on a project to help us define what are a clear set of

attack surfaces that we can use as a model when we're evaluating the licensees and the licensees' programs?

The staff is looking at developing a replica of licensees' networks that we could use for research to look to evaluate different techniques that the industry has implemented and also for training for the staff themselves.

MEMBER BLEY: Can you explain that one a little bit to me?

MR. BEARDSLEY: Sure. So the licensees have multiple different methodologies for developing and implementing their networks. And what the staff would like to do is put together a network training tool that would allow staff to go evaluate those implementations and better understand them.

MEMBER BLEY: So this would be like a software model of their network or something to experiment with?

MR. BEARDSLEY: It would be a software model that we could configure to be similar to different licensee networks and then use those for evaluation.

MEMBER BLEY: Interesting. Okay. Thanks.

MR. BEARDSLEY: And this is at the -- we're at very early stages. So we're just going to

investigate the potential for it. We're not ready to move forward with any kind of construct yet. But our colleagues in research are helping us sort of scope out what it would take to go do that.

MEMBER BLEY: So this is kind of like the digital twin stuff we've heard about from research?

MR. BEARDSLEY: It could theoretically be that although we are tapped in with research into the digital twins effort as well.

MEMBER BLEY: Okay. Thanks.

CHAIR BROWN: Jim?

MR. BEARDSLEY: Yes.

CHAIR BROWN: I want to phrase this -- get this stated clearly. I'm trying to remember if we've seen this or not. It seems to me we've seen this somewhere, and I'm not remembering where.

But networks, a couple configurations of networks, you have a bunch of systems out in a plant. Data goes into the network. It gets distributed to a bunch of control systems, emergency support center, technical support center, et cetera, et cetera. And it's distributed via just like a big server if you want to call it that, a distributor.

MR. BEARDSLEY: Mm-hmm.

CHAIR BROWN: But you can also embed

control software in a network so you don't end up building control software for the functions like a motor control or a reactivity control system. And then you go segregate or partition the network so that you've got software barriers between them.

MR. BEARDSLEY: Mm-hmm.

CHAIR BROWN: I'm not sure I'm saying that right. Have you even given that any thought? I'm trying to remember if anybody -- I thought I remembered somebody doing something like that, but I don't think it was in the reactor trip circuit. It wasn't in the safety system area. It was in some other area.

Have you all seen any of that at all? It seems to me that's a dangerous thing to get into when you start burying stuff, control functions for various other, maybe, balance of plant systems or whatever into a network instead of a unique control system for that component.

MR. BEARDSLEY: Yes. I can't speak to the specifics on what we've seen. I mean, we've done 58 inspections. But I will say that the greater majority of the plants in the current operating fleet do not have high functioning digital systems in their safety systems.

They are evaluating digital I&C upgrades. And that's something that the staff is focused on, and we're very involved in the evaluation of.

They have implemented complex digital instrumentation and control in the balance of plant. So there are differences there. And the licensees have used various different tools to, you know, partition their networks to try and keep different levels of protection in different areas. But, again, there's many, many different configurations out there. I mean, virtually every plant is different.

CHAIR BROWN: Okay. Thanks.

MR. BEARDSLEY: We have a whole other slide to talk about wireless. So I'm not going to get into that on this slide, but we are engaged with research looking at different wireless technologies and their impact on the plant systems. Any questions about our interactions with research?

All right. Now, I'm going to turn it over to Mario Fernandez to talk about wireless.

MR. FERNANDEZ: Again, this is Mario Fernandez, and I'm on Slide 18. As Jim mentioned, there was a public meeting that was held with the industry on February 20, 2020.

The industry at this time discussed

opportunities for future implementations of wireless technologies, the benefits of implementing wireless technologies, implementation considerations related to cyber security and the next steps.

At this time, the CSB staff is working with the Office of Research, as Jim mentioned, and also working with the DOE labs under the Light-Water Reactor Sustainability Program to evaluate potential industry implementation so we can better understand all the possible uses of these technologies to ensure the licensee is complying with its Cyber Security Plan.

Specifically, the NRC concern is that we want to have a thorough understanding of how these technologies will be used if the wireless devices or the wireless technologies that the licensees are intending to implement will be critical digital assets. And currently, CDAs are not affected by the use of wireless technologies.

And now I'll turn it back over to Jim.

MEMBER REMPE: Before you do that, I had a question. Could you go into some more detail about specific examples that are being considered? This is just a little too high a level for me.

I'm aware of some examples that they're

doing in Japan at Fukushima that I think might be of interest to U.S. industry for operations and maintenance. And, again, if the plant is shut down where it's applied so you don't adversely affect cyber security. But what kind of examples are being discussed?

MR. FERNANDEZ: That's a very good question, Member Rempe. The industry, for instance, have mentioned in use of wireless technologies to obtain data for different devices in the field.

This data will be collected at some central point. And instead of running wires, the licensee's intend to use wireless technologies to collect this data for analysis or to be able to perform other functions.

There have also been some preliminary information where the use of drones can be used for specific functions to perform some kind of maintenance inspections or to perform maybe some security functions. Because we don't have enough information yet and the industry only has a present desire to use these technologies, we don't have a lot information.

And that's the reason why we are engaging with the Office of Research so we can understand how these technologies can be used, what are the possible

vulnerabilities that can be introduced into the environment that this technology will be used. We want to have a full understanding and then we want to assess and evaluate implementation to ensure the licensees are meeting the requirements in the Cyber Security Plan. Does that answer your question, Member Rempe?

MEMBER REMPE: Yes, it does with respect to the condition between the plant components I'm aware of. I have not heard much discussion yet about the use of drones, which is of interest and how that could be done. Again, it's being used quite effectively in Japan. And so I'm interested in hearing more about that.

MR. FERNANDEZ: Yes, ma'am. So are we.

MEMBER REMPE: Tomorrow, during our research discussion, do you expect that they will be able to provide more details or it's just too preliminary? There's just not enough information coming from industry yet?

MR. FERNANDEZ: Ma'am, I don't know what the Office of Research is going to present. But I believe that it is too preliminary to even go beyond what we are discussing right now.

I'm just providing some examples where the

licensees have expressed were the areas that they can use these kind of technologies for a lot of different reasons. Obviously, some of them are economical reasons. Some of the other reasons are to automate or try to implement a more effective and efficient way of doing business at their sites.

MEMBER MARCH-LEUBA: Hey, Mario, this is Jose March-Leuba. On those examples you've given, I assume you will use wireless for one directional data out not for control in, correct? Is that what you envision?

MR. FERNANDEZ: That's a very good question, sir. We don't know yet. We don't know how this technology will be used. That's the reason why we want to learn how this technology will be implemented, how the licensee intends to implement those technologies. In order for us to provide an answer exactly to the question, that's exactly the question we're asking ourselves, you know, how this would affect your --

(Simultaneous speaking.)

MEMBER MARCH-LEUBA: I'm sure you know more about this than I do but the way I would implement it would be establish a VPN tunnel in the sensor on the receiver. All right? And I would

encrypt all the communications and ensure that both sides are authenticated.

However, I did a search on the NIST database of vulnerabilities this morning again, and I found 39 VPN vulnerabilities reported this year. It turns out to be one VPN vulnerability reported every three days.

And then I extended the search for three years, which is an easy way to do it. And it turns out to be one VPN vulnerability every three days. So just because somebody tells you I have a VPN between my sensor and my receiver, Jesus Christ, every three days there is a VPN, somebody messed up in their parameter on VPN so. But please do be careful. Thank you.

MR. FERNANDEZ: I share your concern. That's our concern, too. And I'm aware that recently there have been a lot of vulnerabilities reported regarding the use of VPNs.

And this is exactly why we're engaging with the Office of Research because we want to thoroughly understand this technology to ensure that when licensees implement this technology or they desire to do so we ensure that they provide the high assurance that this technology is not going to impact

the current cyber security posture or the CDAs that they're already protecting.

MEMBER MARCH-LEUBA: Just for fun, Google NIST vulnerability database. Go in there, click on search and you can type key words. It's scary.

MR. FERNANDEZ: Absolutely, sir.

MEMBER MARCH-LEUBA: It's scary. There are at least 5,000 this year.

MR. FERNANDEZ: Yes, sir. I had looked a little bit into it, and you're right. If you go to the NIST website, you're absolutely correct. VPNs that have vulnerabilities all will be listed there currently where they're having the NIST database.

That's a very good source of information for vulnerability assessments.

CHAIR BROWN: It got it. Jose, there's other ways to do that. You can also send data to a wireless device through a data diode and then it can get transmitted as long as you disconnect at that point.

So you can get the data out if you want. It's cumbersome, but you can do it by isolating. And that way you don't allow something -- and you don't have a way for --

MEMBER MARCH-LEUBA: I understand,

Charlie. I want to make a joke. When you are a hammer, everything looks like a nail. And your nail is your voice. And it's a very good one. It's a very good. It's gets you the 99 percent.

CHAIR BROWN: Yes. I'm a nail person. You're exactly right, along with a hammer. Joy, one other thing when you talked about with the plant shutdown, wireless shouldn't be a concern. The wireless can come in and plant malware into your systems if you start letting it in even with the plant shutdown then it gets you after you're up.

MEMBER REMPE: Yes. I'm talking about the Fukushima plant being shut down. But, yes, I get what you're saying. But it's just something that if there's a way that we could adapt it in a safe way, it would be of interest, I think.

CHAIR BROWN: It hasn't stopped me yet.

MEMBER REMPE: Anyway, it's just something to think about.

MR. FERNANDEZ: Absolutely.

MEMBER REMPE: And I would be interested in how its progressing.

MR. FERNANDEZ: Absolutely. We are very interested, too. That's why we are engaging with the Office of Research and the DOE laboratory so we can

absorb, so to speak, all of this information and be able to assess and evaluate and keep up with the industries if they decide to go down this path.

CHAIR BROWN: Yes. I'm going to interrupt here for a second. We've only got two slides left other than the question mark slide. We were going to have a break. Does anybody have a vote? Should we take a 10 minute break right now, 15 minute break rather and come back?

MR. FERNANDEZ: I'm okay to continue and I think Brian is ready.

CHAIR BROWN: Members, do you all have any voice?

MEMBER MARCH-LEUBA: I vote we continue.

CHAIR BROWN: Okay. All right. Go ahead.

MR. FERNANDEZ: Thank you, members. Now I'm going to turn it over to Brian Yip, who is going to be talking about the cyber security roadmap. Thank you.

MR. YIP: Thanks, Mario. This is Brian Yip, again. This is a real brief update. We were requested to give an update on the cyber security roadmap.

For background, the initial roadmap paper, this is SECY paper that the staff put up in 2012 to

provide the Commission with an update on the staff's plans for implementing the cyber program early on.

We then provided a subsequent SECY paper to the Commission in 2017 with an update to the cyber roadmap. And this gave the Commission some information on what the staff's plans were with regard to the full implementation inspections that Jim mentioned earlier in our briefing.

And it also gave the Commission some additional information about the evaluation and guidance that NRC had issue for other classes of licensees. An example would be the staff put out a best practices guide for non-power reactor cyber security.

So now at this point, we're considering if we were to provide an update to the cyber roadmap what the future format of it should be. We're really at the initial stages at this point. We're taking into consideration what areas of the cyber program we need to inform the Commission of and also any areas where we think that we may need Commission direction. And we're going to use some of those indicators to help us determine what the appropriate vehicle is to communicate that information.

If we did update the cyber roadmap, we

could do another SECY paper as we've done in the past. We may do a Commissioner assistance note or a Commissioner assistance briefing. However at this point, we haven't made any decisions yet in that regard. So we don't have much more that we can provide you on the cyber roadmap other than that at this time. And if there are no questions on that, I can turn it back to Jim.

CHAIR BROWN: Okay. Go on, Jim. Thank you.

MR. BEARDSLEY: Okay. Since the Commission approved the Cyber Security Rule in 2009, the staff and industry have made significant strides in program implementation. The industry has completed their two phase program implementation, and the staff have conducted over 170 cyber security inspections over the last eight years.

Based on those inspections, the staff had found with reasonable assurance that industry has implemented their cyber security programs.

The staff have received considerable stakeholder feedback on the cyber security oversight program through public meetings and our own self-assessment combined with inspection lessons and an audit of the inspection program by the NRC's Office of

Inspector General. That feedback is being used to further develop the NRC's graded approach to cyber security oversight.

In addition, those insights, combined with lessons from the interagency and international partners, are being used to develop our approach to cyber security for future licensees.

This completes our remarks, subject to your questions.

CHAIR BROWN: Okay. Jim, are we done?

MR. BEARDSLEY: We are done.

CHAIR BROWN: Okay. Question mark page. Scott or Tom, is there an issue with the public line or what? Are we good?

MR. MOORE: Tom, this is Scott. I thought the public line had been muted. So should we go to comments after the break?

MR. DASHIELL: Yes, Scott. That would be preferable. Can you hear me now?

MR. MOORE: Yes.

MR. DASHIELL: I just unmuted it using star 6.

CHAIR BROWN: Okay. So you'd like to take a 15 minute break and then we'll go do public comments and then a round around the table.

MR. MOORE: Yes, Chairman, that would be best.

CHAIR BROWN: Okay. We'll come back here at 4:32, make it 4:35 Eastern Standard Time and then we'll resume with the public comments and then any other final comments. Okay? We are recessed until that time.

(Whereupon, the above-entitled matter went off the record at 4:18 p.m. and resumed at 4:36 p.m.)

CHAIR BROWN: Okay. It's 4:35. And we will resume the meeting. At this point, just to confirm, Tom, is the public line open right now?

MR. DASHIELL: Yes, Charlie, it is.

CHAIR BROWN: Okay. Is there anybody on the public line that would like to make any comments relative to this meeting? Okay. Second question, is there anybody on the public line, again, that would like to make any comments? Okay. Hearing none, Thomas?

MR. DASHIELL: The public line is muted.

CHAIR BROWN: Okay. Thank you. At this point, we will go ahead and go around. Do any of the members have any additional comments that they would like to provide or ask, I should say?

MEMBER PETTI: Charlie, I have one.

CHAIR BROWN: Yes, go ahead.

MEMBER PETTI: And, again, I may just be off-base. Before I got the documents, particularly in light of Part 53, I mean, I understand this is all about a process of identifying critical assets that need protection. I'm not talking about that.

What I was looking for was guidance that an advanced reactor designer would need to help them in the designs of some of their systems.

You know, I saw the data diode. It's in there. But I didn't see a concise list of, you know, these are sort of either the design philosophies or actual, you know, for lack of a better term, requirements or guidance that the NRC finds that this is an acceptable set of approaches that would work but these are those that aren't. Is it just that that's somewhere else?

CHAIR BROWN: No.

MEMBER PETTI: And you wouldn't expect to find it here?

CHAIR BROWN: No, you're right. Normally, we have covered that. This is my interpretation of what we've done, and you've got to look at different systems.

We fundamentally look at it from a design

certification standpoint. And we normally deal with the digital I&C systems, which result in a safety monitoring control safeguards, whatever they may be, whatever configuration they may take.

And in the old methodology, there was a Chapter 7, which covered all of the I&C systems. And we normally developed -- or they did develop fundamentally, a functional one line diagram of the basic architecture showing that they meet the frameworks of redundancy, independence, deterministic processing, control of access and diversity and defense in-depth.

And there we have looked at the interrelations of the various systems and what type of communications they make and where they go to and where they don't go to. And so that has been covered in great detail as part of the design certification approvals.

MEMBER PETTI: So there's nothing new that cyber would add on top of that?

CHAIR BROWN: No. Fundamentally, if you look at the words and you go through the document -- and it's hard to find, okay -- system by system and you look and see how does it deliver data someplace else?

For instance, a reactor trip system doesn't have to receive any data. I mean, it just either scrams the plant or it doesn't. So it can send data out, but you want it to do it through a data diode, a type of unidirectional non-software based data circumstance transmission.

So you do that, you evaluate that in that context, bidirectional versus unidirectional, as we have talked about several times.

So you're right. We don't go -- there's nothing that says this is a hard and fast criteria. We try to use our heads as we're looking at the design.

MEMBER PETTI: Okay.

CHAIR BROWN: And it gets difficult sometimes needless to say. Are there any other member comments?

MEMBER MARCH-LEUBA: Yes. This is Jose. This is going to be a little out of character, but I found this presentation really interesting. It's an interesting topic.

Overall, well done. The staff has done a fantastic job trying to do a difficult task. And I want to congratulate you. But stay on top of it because things change daily so don't sleep on your

laurels. Thank you.

CHAIR BROWN: Thank you, Jose. Is there anybody else that would like to say anything?

MR. HECHT: This is Myron. If I could just add a comment with respect to the research initiatives that were being planned.

CHAIR BROWN: Yes.

MR. HECHT: There is a plethora, a huge amount of work, that's been done on industrial controlled cyber security in the ISA standard, ISA 99 Series. There's an awful lot of work that's been done.

And many of the questions that have been raised here, what if, you know, what if questions, change control, just new vulnerabilities that are coming up. That's all largely addressed in those standards. And I would advise that research be directed to look at those as part of their activities as well.

CHAIR BROWN: Okay. Thank you very much, Myron. If you can identify some of those and send them to me, I would like to see them.

MR. HECHT: Sure. I can do that.

CHAIR BROWN: If you can identify a few of them, thank you. You all --

MEMBER REMPE: This is Joy, Myron. If you could do this soon, we do have a meeting tomorrow afternoon. And we don't really direct research to do anything. We make recommendations of things they should be considering. But it would very timely if you could get this out to us, you know, before like, I guess, it's what 2 o'clock, the time tomorrow.

CHAIR BROWN: If you could get --

MR. HECHT: I can give you a short list of the major ones, yes.

MEMBER REMPE: It doesn't have to be, yes, everything. But anyway, it would help us out.

CHAIR BROWN: Okay. Yes. Send it to Christina, and she can get it to everybody. Okay?

MEMBER MARCH-LEUBA: I mean, would it be possible to task Myron to be in the meeting tomorrow because he's the one that knows.

MEMBER REMPE: Actually, I just don't think we need that. One, it's kind of late to have to send him all this information. It would just help us if you got us a list. It's not necessary for you to listen to -- we're going to be going through a lot of things that are covered by the Division of Engineering, and it would be a waste of Myron's time to have to sit through the whole meeting for that.

MEMBER MARCH-LEUBA: But, Myron, as an interested member of the public, there is an open line that you can always log in if you are bored on a Friday afternoon. You won't have a voice until at the end of the meeting.

MR. HECHT: Thanks.

CHAIR BROWN: Any other comments from members?

MEMBER KIRCHNER: Yes, Charlie. This is Walt. Thank you to the staff for the presentations. I second Jose's comments on the staff's presentation.

If it's possible, could Christina obtain the white paper that Eric Lee presented? I thought the conceptual approach that he described on safety-related and important to safety of much interest and relevant to our deliberations on 10 CFR 53. Thank you.

MS. ANTONESCU: Yes, Walt, I already sent it to everybody. I'll try to resend it to you, too.

MEMBER KIRCHNER: No, don't resend it. I'm just not monitoring my email in real-time. Thank you.

MS. ANTONESCU: On, you're welcome.

MEMBER SUNSERI: Hey, Charlie, this is Matt.

CHAIR BROWN: Just let me answer Walt. I think it might be in the package that you got for this meeting. If I can -- is it the one on safety, safety-related? There were three of them in there, one on balance of plant, one on security and the other white paper, I think, was on safety and safety-related.

MEMBER KIRCHNER: Okay. I'll look for it, Charlie. I don't want to create extra work for anyone. Thank you.

CHAIR BROWN: I'll try to let you know which ones they are if I can remember that long. Somebody else was speaking up when I interrupted. I apologize for that.

MEMBER SUNSERI: Charlie, it's Matt. I was just curious. From a planning perspective, are you planning on recommending that we write a letter on this topic?

CHAIR BROWN: No. This is strictly an information briefing right now. Our letter would be on 5.71. That's the key point for us to go do. So that's coming up. That revision process is in process. So that's where I've got my focus right now.

MEMBER SUNSERI: Thank you.

CHAIR BROWN: Okay. Anybody else? Okay. I'll wrap-up. Michele and Jim, I want to thank you

all for a very good, well done presentation.

For some reason, these presentations on mass subjects always end up with some very excellent discussion with a wide range of viewpoints, which is also very, very useful.

So I think your presentation engendered some of that. And that was much appreciated. And your ability to respond on the spot is also much appreciated. It certainly is indicative of the good work that you guys are doing.

So I wanted to thank you very much for a very well done presentation and very complete in terms of your ability to describe some details of what you all were doing and what you've seen.

So, Jim, Michele, thank you all. Much appreciated. With no more ado, I guess it's time for me to adjourn the meeting and the rest of the members, we'll re-adjourn tomorrow morning sometime. Everybody take care. The meeting is adjourned.

(Whereupon, the above-entitled matter went off the record at 4:47 p.m.)

NRC Cyber Security Oversight Program Update July 2021

Jim Beardsley, Chief

Cyber Security Branch (CSB)

Division of Physical and Cyber Security Policy (DPCP)

Office of Nuclear Security and Incident Response (NSIR)

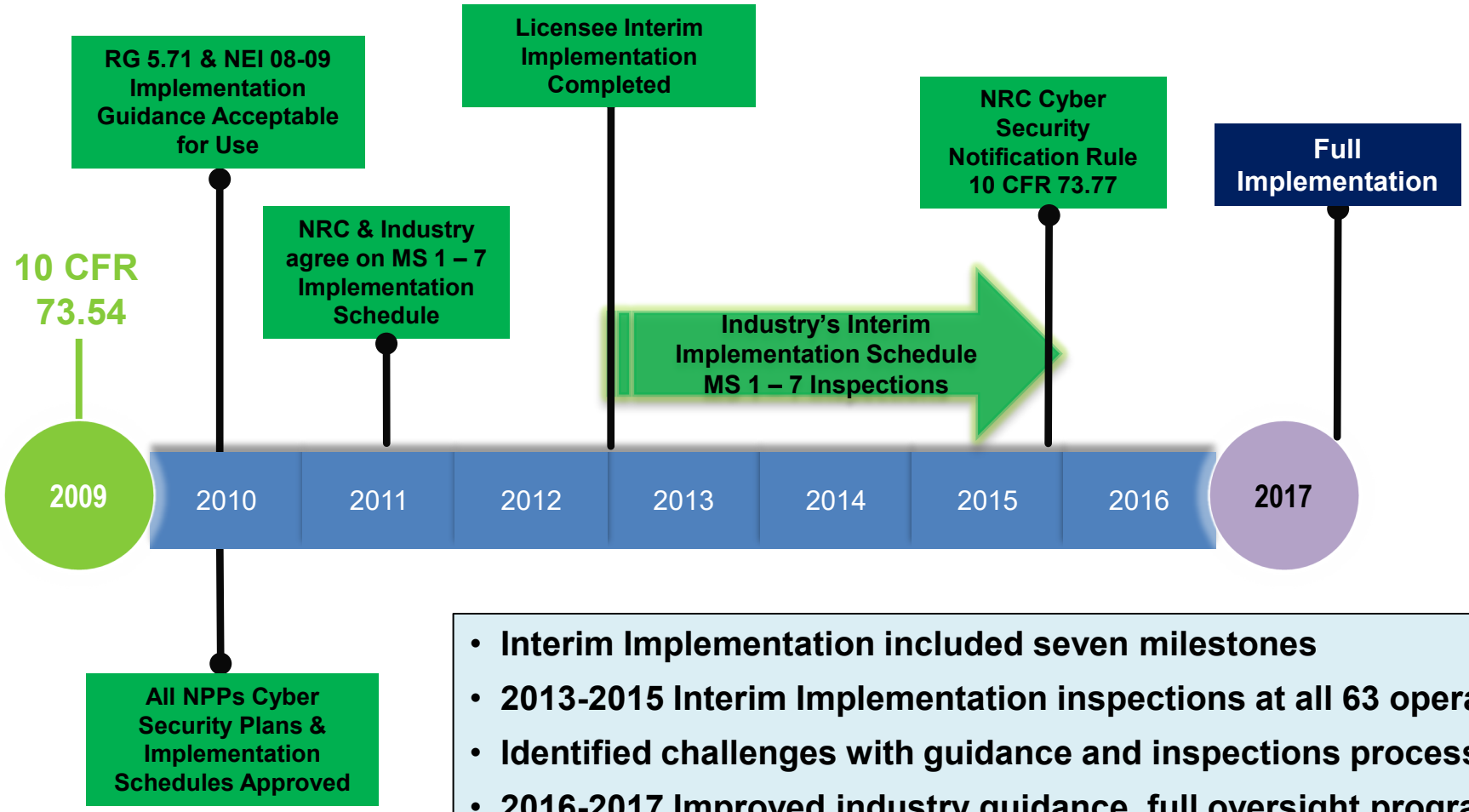
james.beardsley@nrc.gov

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

Key Messages

- The NRC staff is committed to maintaining an efficient, robust cyber security program that can adequately protect against the dynamic cyber threat environment.
- The cyber security inspection program has verified that licensees have adequately implemented the cyber security regulations.
- Lessons learned from the implementation of the cyber security oversight program are being used to implement efficiencies and enhancements to the cyber security program and update RG 5.71.
- Experience gained with the operating reactors oversight provide the NRC staff with insights for implementing appropriate levels of cyber security for other licensees including SMRs and other technologies.

Power Reactor Cyber Security Background



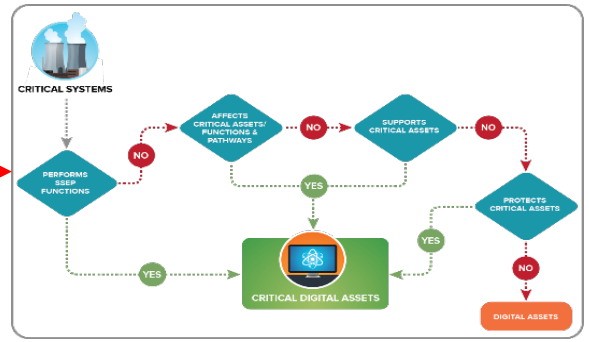
- Interim Implementation included seven milestones
- 2013-2015 Interim Implementation inspections at all 63 operating NPPs
- Identified challenges with guidance and inspections processes
- 2016-2017 Improved industry guidance, full oversight program and improved inspector training implemented.

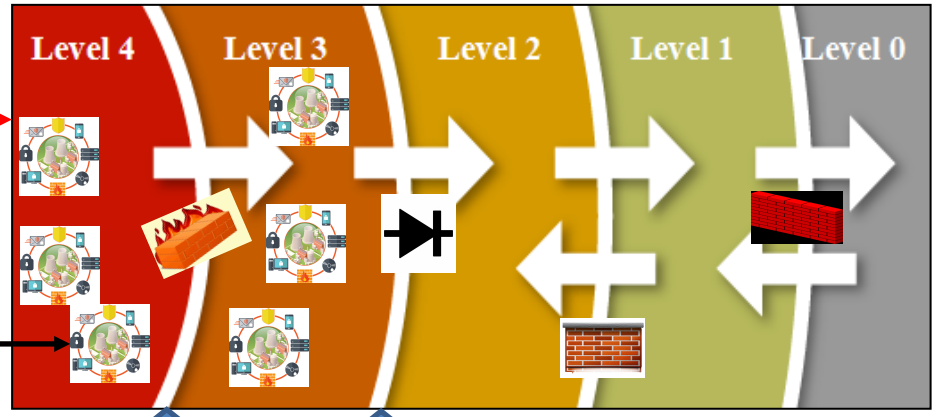
RG- Regulatory Guide
NEI - Nuclear Energy Institute
CFR – Code of Federal Regulation

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

RG 5.71 Cyber Security Program Implementation

1. Cyber Security Assessment Team
2. Identify Critical Digital Assets (CDAs)
3. Implement Defensive Architecture
4. Apply Security Controls



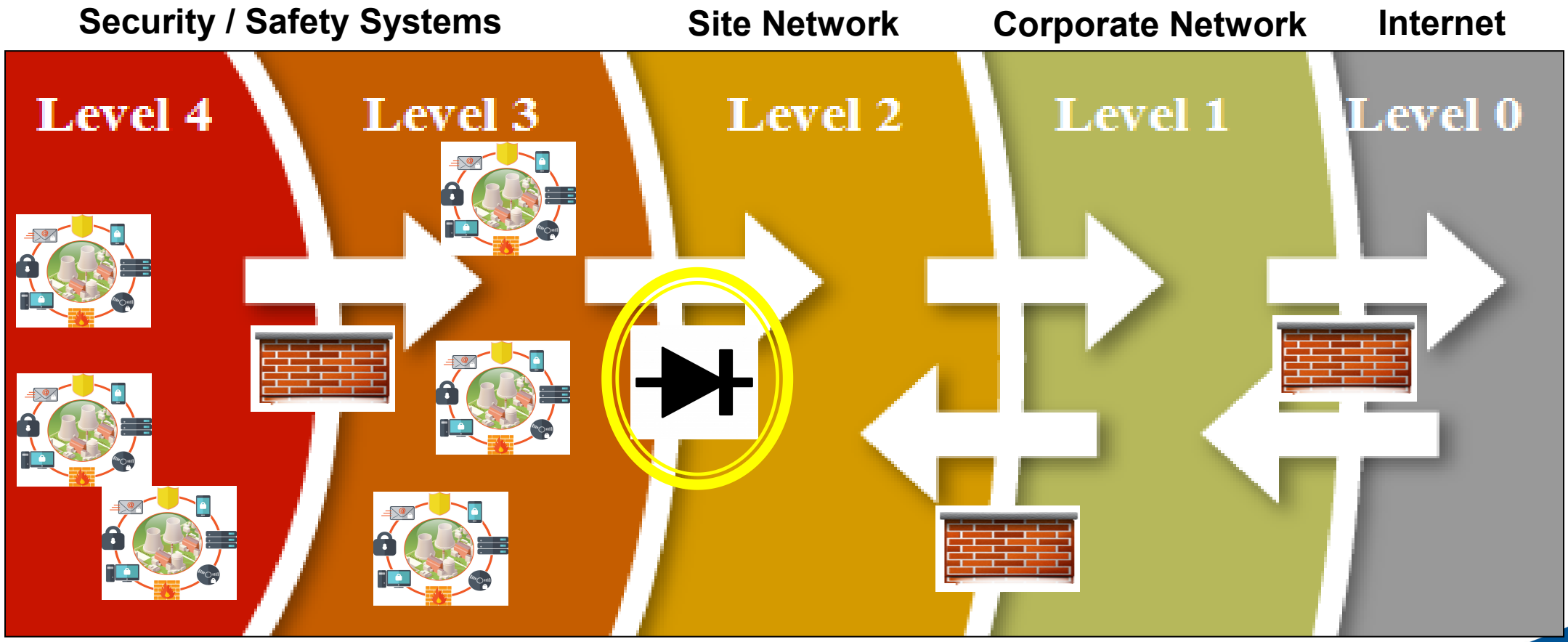


CYBER SECURITY PROGRAM

Defense-in-Depth	Security Controls NEI 13-10	Mitigation Strategies	Training	Manage Cyber Risk
Periodic Review	Modification Evaluation	Incident Response	Procedures	Records Retention

RG- Regulatory Guide
NEI - Nuclear Energy Institute

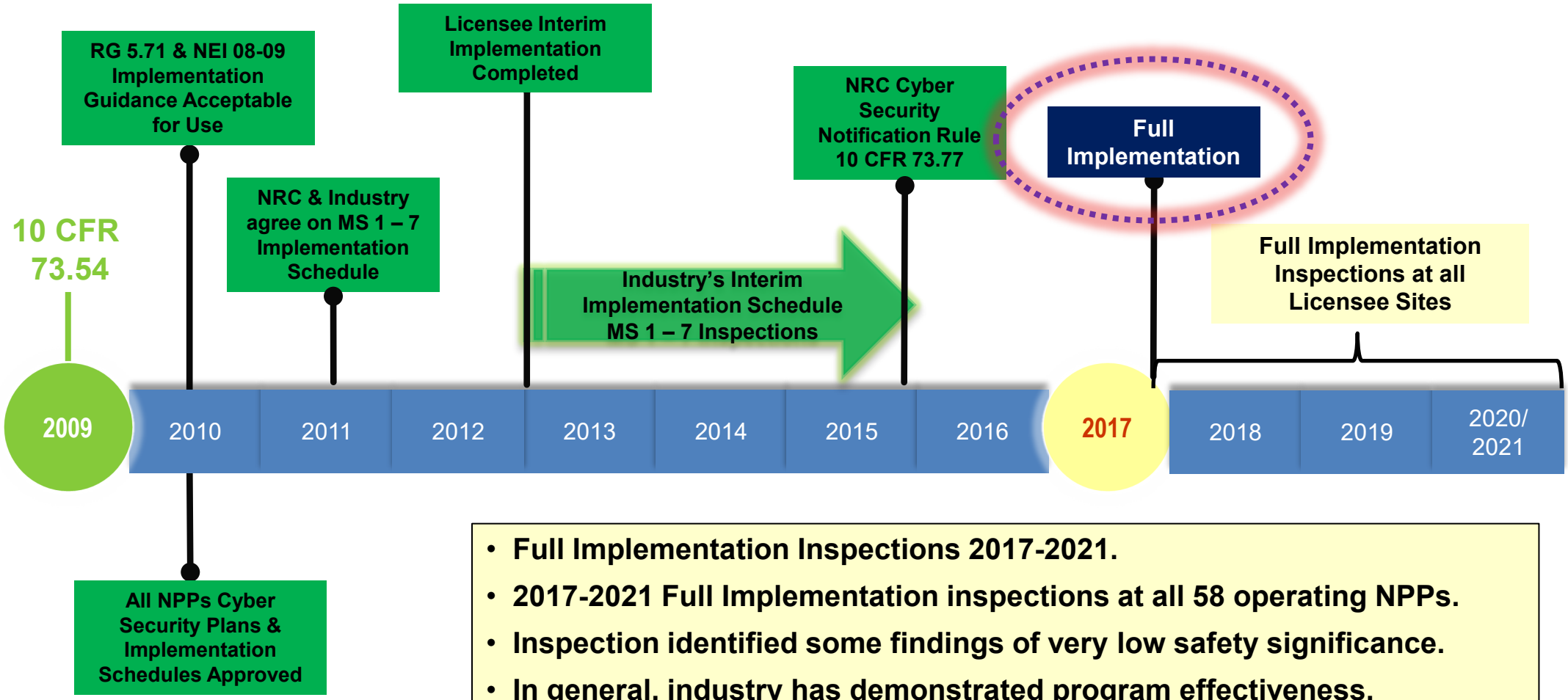
Generic Defensive Architecture



One-way Deterministic Device

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

Power Reactor Cyber Security Background

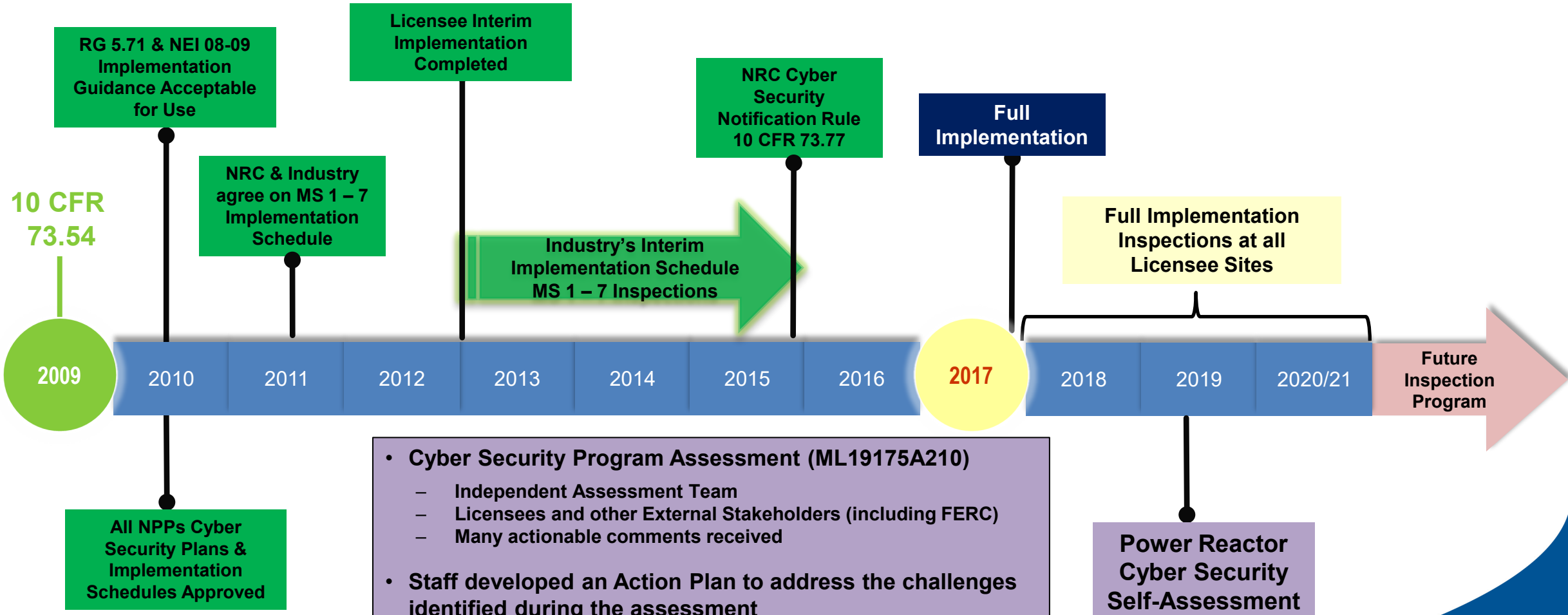


- Full Implementation Inspections 2017-2021.
- 2017-2021 Full Implementation inspections at all 58 operating NPPs.
- Inspection identified some findings of very low safety significance.
- In general, industry has demonstrated program effectiveness.

RG- Regulatory Guide
NEI - Nuclear Energy Institute
CFR – Code of Federal Regulation

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

Future of Power Reactor Cyber Oversight



- **Cyber Security Program Assessment (ML19175A210)**
  - Independent Assessment Team
  - Licensees and other External Stakeholders (including FERC)
  - Many actionable comments received
- **Staff developed an Action Plan to address the challenges identified during the assessment**
  - Phased approach
  - Critical digital asset determination initial focus areas
  - Focus on defense-in-depth

RG- Regulatory Guide
NEI - Nuclear Energy Institute
CFR – Code of Federal Regulation

Cyber Security Action Plan

- Clarifications of program definitions & terms
- Review criteria for digital asset analysis and protection
  - Emergency Preparedness (EP)
  - Balance-of-Plant (BoP)
  - Safety-Related and Important-to-Safety SR/ItS
  - Security
- Best practices for digital asset assessment → RG 5.71
- Risk-inform control set applied to protect digital assets
- Future inspection program
  - Inform oversight with licensee performance metrics
  - Evaluate performance testing as a element in the oversight program

Initial Focus Area

Initial Focus Area

EP CDA Determination Changes

- Industry proposed changes to EP CDA determination guidance
  - Changes are related to 10 CFR 73.54 section (b)(1)
  - Aligns with EP requirements and program implementation.
  - EP DAs classified as CDAs if the DA(s) is compromised and the EP function can't be performed
  - Objective: properly classify the number of EP risk significant CDAs, and reallocate resources for more focus in the Safety & Security Critical Systems.

- Accepted by the NRC in August 2020 following staff review and public meetings
  - Initial public meeting to discuss proposed changes in November 2019
  - NEI first submittal in November 2019
  - NEI submitted revised paper to address staff concerns in April 2020
  - Tabletop workshop conducted to discuss proper implementation August 2020
  - Licensees may implement the changes prior to the revision of NEI 10-04 and NEI 13-10 guidance
  - Changes will be incorporated in future revisions of the NEI guidance (above)

CDA: Critical Digital Asset
DA: Digital Asset
EP: Emergency Preparedness
NEI: Nuclear Energy Institute

BoP CDA Determination

- Industry has proposed changes to BoP CDA determination guidance
  - BoP CDAs are those CDAs that were added to the scope of the cyber security rule during the resolution of FERC Order 706-B
  - Industry proposed aligning the BoP CDA evaluation criteria with the latest NERC CIP standards which are based on impact to the Bulk Electric System (BES) by revising the guidance found in NEI 10-04 and NEI 13-10.
- Accepted by the NRC in August 2020 following staff review and public meetings
  - Initial public meeting to discuss in January 2020
  - NEI first submittal in April 2020
  - NEI submitted revised paper to address staff concerns in July 2020
  - Licensees may implement the changes prior to revision of NEI 10-04 and NEI 13-10 which will roll up all changes.

CDA – Critical Digital Asset	FERC – Federal Energy Regulatory Commission
BoP – Balance of Plant	NERC – North American Electric Reliability Corp.
NEI – Nuclear Energy Institute	CIP – Critical Infrastructure Protection

SR/ItS CDA Determination

- The proposed guidance refined SR/ItS CDA determination criteria
  - Defined terms “safety-related,” and “important-to-safety” functions in the context of cyber security based on how the NRC historically used these terms.
  - Aligned the SR/ItS CDA identification criteria with the NRC’s safety regulations.
- Accepted by NRC in August 2020 following staff review and public meeting.
  - Initial discussion on the subject in August 2019
  - Submitted for review in May 2020: public meeting in June 2020
  - NEI submitted revision that addressed staff concerns in July 2020.
  - Licensees may implement the changes prior to revision of NEI 10-04 and NEI 13-10 which will roll up all changes.

SR – Safety Related
ItS – Important to Safety
CDA – Critical Digital Asset
NEI – Nuclear Energy Institute

Security CDA Determination

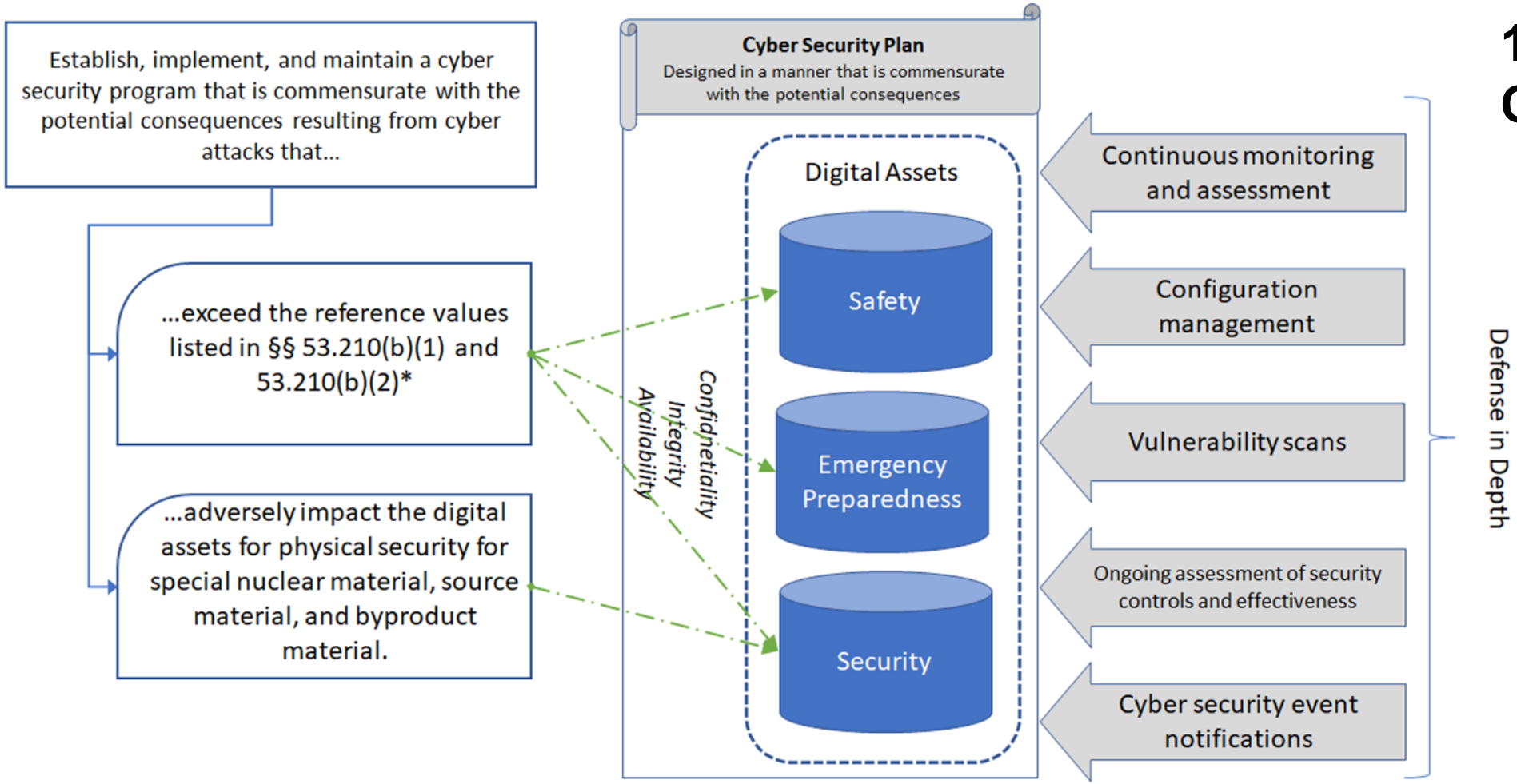
- The effort focused on refining CDA determination and classification criteria for security digital assets.
  - Defines “security function” in the context of cyber security;
  - Addresses digital security tools and security support systems;
  - Clarifies cyber security protection for digital assets used for access authorization.
- Accepted by NRC in June 2021 following staff review and public meeting.
  - Initial draft received in December 2020; public meeting in January 2021.
  - Response to NEI in April 2021: additional guidance needed on security support systems; more clarity in access authorization.
  - NEI submitted revision that addressed staff concerns in June 2021.

CDA – Critical Digital Asset
NEI – Nuclear Energy Institute

Post Full Implementation Inspection Program

- Performance Informing Initiatives
  - Performance Metrics:
    - Staff and industry have conducted two public meetings to discuss the voluntary use of licensee performance metrics to inform future inspections.
  - Performance Testing:
    - Staff and industry have discussed the potential for informing future inspections with licensee performance testing results.
- A structure for review of performance metrics and testing results has been included in the draft inspection procedure.
- Staff conducted a public meetings in February and April 2021 to discuss the proposed inspection process and receive stakeholder feedback.

Part 53 Rulemaking Cyber Security Approach



10 CFR 73.110 Cyber Security

* An individual located at any point on the boundary of the exclusion area for any 2-hour period following the onset of the postulated fission product release would not receive a radiation dose in excess of 25 rem TEDE; and an individual located at any point on the outer boundary of the low population zone who is exposed to the radioactive cloud resulting from the postulated fission product release (during the entire period of its passage) would not receive a radiation dose in excess of 25 rem TEDE.

Cyber Security Rule Petition for Rulemaking

- PRM-73-18 submitted by NEI in 2014.
- Staff assessed the PRM in 2017 and further in 2019.
- Decision on the PRM deferred to evaluate the impact of cyber program assessment action plan activities.
- The Commission is expected to make a decision on the petition in July 2021.

Regulatory Guide 5.71 Update

- Published Regulatory Guide 5.71 (2010)
- 2016 Initiated update to Regulatory Guide 5.71
- Issued DG-5061 for public comment (2018)
- In 2021, staff updated DG-5061 to incorporate the program changes implemented since 2018.
- Plan to issue updated DG-5061 for 2nd public comment in Aug.
- ACRS review of the DG following public comment period, early 2022
- Plan to issue RG 5.71 Revision 1 in Spring 2022

Cyber Security Engagement with RES

- Attack Surface for Cybersecurity Monitoring and Oversight
- Licensee Network Replica for Cybersecurity Training
- Wireless Communication Technologies (Safety & Security)
- Cybersecurity Expert Seminars

Wireless Technology and New Licensees

- Public Meeting on February 20, 2020
  - Current wireless implementations
  - Potential future wireless initiatives
- Future Wireless Technology Engagements
  - Discuss specific examples for potential industry initiatives and how they might fit into the regulatory framework.
  - Staff are working with the DOE laboratories and the Light Water Reactor Sustainability Program to evaluate potential industry wireless implementations

Cyber Security Roadmap Update

- The initial roadmap paper was completed in 2012 (ML12135A050).
- The paper was updated in 2017 (ML16354A258).
- Staff is weighing best approach for future updates:
  - Acknowledging other processes that will keep the Commission informed (e.g., Part 53 rulemaking process).
  - Considering whether there are areas where additional Commission guidance may be necessary.

Conclusion

- The cyber security inspection program has verified that licensees have adequately implemented the cyber security regulations.
- Staff conducted an assessment of the program in 2019 including significant stakeholder feedback, focus areas are being addressed.
- Staff and Industry are further implementing graded-approaches for the CDA selection and protection of EP, BoP, Security and Safety-Related/Important-to-Safety digital assets.
- Staff are performance-informing cyber security oversight.
- Evaluating cyber security implications for wireless connectivity and appropriate cyber security for new licensees.
- Staff are evaluating graded approaches for cyber security for new licensee/applicants.

Questions