Official Transcript of Proceedings

NUCLEAR REGULATORY COMMISSION

Title:	Joint Plant Operations, Radiation Protection & Fire Protection and Digital I&C Subcommittee
Docket Number:	n/a
Location:	teleconference
Date:	05-17-2023

Work Order No.: NRC-2406 Pages 1-251

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

DISCLAIMER

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

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

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

UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

+ + + + +

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

(ACRS)

+ + + + +

JOINT PLANT OPERATIONS, RADIATION PROTECTION & FIRE PROTECTION AND DIGITAL I&C SUBCOMMITTEE

+ + + + +

WEDNESDAY

MAY 17, 2023

+ + + + +

The Subcommittee met via hybrid in-person and Video Teleconference, at 8:30 a.m. EDT, Gregory Halnon, Chairman, presiding.

COMMITTEE MEMBERS:

GREGORY HALNON, Chair

RONALD G. BALLINGER, Member

CHARLES H. BROWN, JR., Member

VICKI BIER, Member

VESNA DIMITRIJEVIC, Member

WALT KIRCHNER, Member

JOSE MARCH-LEUBA, Member

DAVID PETTI, Member

JOY L. REMPE, Member
MATTHEW SUNSERI, Member

ACRS CONSULTANT:
DENNIS BLEY

DESIGNATED FEDERAL OFFICIAL:
CHRISTINA ANTONESCU

ALSO PRESENT:
RYAN BECHTEL, DHS/CISA
JORGE CINTRON-RIVERA
CHRISTOPHER COOK, RES
DOUG ESKINS, RES
ISMAEL GARCIA, NSIR
ANYA KIM, RES
GURCHARAN MATHARU, NRR
KENNETH SEE, NRR
DANIEL WARNER, NSIR
BRIAN YIP, NSIR

CONTENTS

P R O C E E D I N G S

8:30 a.m.

CHAIR HALNON: Good morning. This meeting will now come to order.

This is a joint meeting of the Plant Operations Radiation Protection and Fire Protection and the Digital I&C Subcommittee.

I'm Greg Halnon, Chairman of this subcommittee meeting. ACRS members in attendance are Charlie Brown, Matt Sunseri, Jose March-Leuba, Vesna Dimitrijevic, Joy Rempe, Vicki Bier, Ron Ballinger, Dave Petti, Walt Kirchner, and our consultant, Dennis Bley.

Christina Antonescu is the ACRS staff, and is the designated federal official for this meeting.

I believe I did see the court reporter on, correct?

Okay, the purpose of this meeting is for the staff to brief the subcommittee on the status of grid reliability, in the relation to cybersecurity and nuclear power plants.

In addition, Department of Homeland Security, welcome Ryan, thank you for coming, Cybersecurity & Infrastructure Security Agency, or CISA, is able to provide a briefing later, also.

This is a very important topic, one the committee has been seeking more information for existing programs, and potential impacts to our reviews of new and advanced reactors.

Cybersecurity seems to be a topic of discussions every day, given the advancement of technology and most recently, artificial intelligence.

We look forward to our discussions today with the various federal agencies overseeing the cybersecurity of nuclear power plants.

The ACRS was established by statute and is governed by the Federal Advisory Committee Act, or 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've set aside 15 minutes or more if needed, for comments from members of the public, attending or listening to our meetings.

Written comments are also welcome.

The meeting agenda for today's meeting is 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 request for making a statement to the subcommittee has been received from the public.

We reserved the entire day for this meeting, however, we may not need the entire time, but we do not want to leave any questions on the table today.

We are conducting today's meeting as a hybrid meeting. A transcript of the meeting is being capped, and will be made available on our website.

Therefore, we will request that participants in this meeting should first identify themselves, and speak with sufficient clarity and volume, so they can be readily heard.

All presenters, please pause from time to time, to allow members to ask questions. Please also indicate the slide number you are on when moving around in your presentation.

We have the MS Team phone line audio established for the public to listen to the meeting.

Based on our experience with previous virtual and hybrid meetings, I would like to remind the speakers and presenters to speak slowly.

We will take a short break after each presentation to allow time for screen sharing, as well as the chairman, as my discretion during longer presentations, we may take intermediate breaks.

Lastly, please do not use any virtual meeting features from the MS Teams to conduct sidebar technical discussions.

Rather, contact the DFO if you have any technical questions so we can bring those to the floor.

We will now proceed with the meeting. I'll ask Mr. Brian Yip, the Branch Chief of the Cybersecurity Branch, Division of Physical and Cybersecurity Policy, in the Office of Nuclear Security and Incident Response, to make some introductory remarks on today's presentations.

Brian?

MR. YIP: Thank you.

Good morning everybody. Again, I'm Brian Yip. I'm the Chief to the Cybersecurity Branch in NSR.

My branch is primarily responsible for the regulations and oversight programs for cybersecurity, for nuclear power plants.

And we also lead the agency's engagement with industry, and the interagency on cyber issues in general.

So for this briefing today, like most issues in cybersecurity, we do work closely with some partners within the agency, and also the interagencies.

So we brought in partners from NRR, and also from DHS, CISA to, to give these presentations with us.

Today we have presentations by Dan Warner first from the Cybersecurity branch. His presentation will kind of lay the groundwork for the rest of the day, talking about the general cybersecurity posture for nuclear power plants today.

And, then we'll move on from that. Dan will also give a presentation about our interagency engagement with FERC, on some of the balance of planned cybersecurity issues over the past 10 years, and how we resolved those issues between our cybersecurity regulations and the regulations established by FERC, using the NERC critical infrastructure protection standards.

Dan is also going to talk about a bit of our engagement with the interagency, when it comes to cyber incident response.

Next, we'll have Jorge Cintron-Rivera talking about the NRC's, a broad overview of the NRC's relationship with FERC as it pertains to some general grid protection, and balance of plan issues.

And then finally, in the morning we have Ryan Bechtel, from DHS CISA. He's here to talk about CISA's engagement with the nuclear sector, both with the NRC, but then also CISA's direct engagement as the sector risk management agency, and their engagement with the nuclear sector directly.

In the afternoon session, we'll start with Ishmael Garcia, our senior level adviser, for digital I&C and cybersecurity.

He'll provide you an overview with a briefing on the proposed cybersecurity approach in the Part 53 rulemaking, that's now with the Commission for review.

And then finally, we have Dr. Anya Kim and Doug Eskins from the Office of Nuclear Regulatory Research, to discuss some of our research activities related to cybersecurity, and how their branch is helping to prepare the NSIR staff to review some of the novel, and emerging cybersecurity issues that we see both in the near term, and that are rising.

And with that, we can start the first presentation, and I'll turn it over to Dan.

Thank you.

MR. WARNER: Good morning everybody. My name is Dan Warner. I am also in the Cybersecurity branch in the Division of Physical and Cybersecurity Policy, in the Office of Nuclear Security and Incident Response.

And for this first presentation, I'm going to discuss the cybersecurity current status and contemporary events at nuclear power plant licensees.

So I know many members have seen this information before, so just briefly. We started our full implementation inspections in 2017.

And basically what that was, is once the rule was issued in 2009, we allowed licensees a number of milestones to get the programs in place.

2017 is when we went and were confirming they had actually implemented the program, as outlined in the Regulations. And those inspections wrapped up in early 2021.

There was a little bit of gap in the beginning of 2022. We started the baseline biannual inspections, and that is the program that we're currently in now moving forward.

MEMBER SUNSERI: Could you maybe position that microphone a little closer?

MR. WARNER: Is that a little better?

So, the key messages for today's presentation, cybersecurity controls in place at nuclear power plants provide defense against attack pathways of concern.

Programmatic controls ensure that the cyber program is positioned to address the ever-changing threat environment, and ensuring defense-in-depth is maintained.

And the inspection program verified licensee implementation of the cybersecurity program. And now we are looking at maintenance for the cybersecurity program, with the current inspection program.

So, I'm going to go over a couple definitions just to make sure everybody's on the same page.

A critical system is any analog or digital technology-based system in or outside of the plant, that performs or is associated with a safety related, important to safety, security, or emergency preparedness function.

We typically will refer to these as SSEP functions, in short.

A critical digital asset is a digital computer, communication system, or network that is a component of a critical system, or is a support system asset where the failure or compromise by a cyberattack result in an adverse impact to SSEP functions.

MEMBER MARCH-LEUBA: Just so we don't make it boring -- yes, so we don't make it boring.

We will be interrupting you continuously, especially me. In my mind, the most famous cybersecurity attack, at least in my mind, was the famous casino that was attacked via the aquarium thermometer computer.

And there are no definitions that I see here, aquarium thermometer, is critical system.

There is too much emphasis, I mean, it's true that you need to protect the safe where all the chips are, maybe to higher level than the aquarium.

But if you don't protect the aquarium, you get into the safe.

So, by focusing and the other problem is in this building, your boss and everybody else is concentrated on regulations. What does the regulation say. And as long as you meet the regulations, you're fine.

This cybersecurity threat is changing not daily, it's changing hourly. Regulations, even if you passed them last month, they're old.

MR. WARNER: Uh huh.

MEMBER MARCH-LEUBA: So this focusing, especially in Part 53 on only CDAs, it scares me.

MR. WARNER: And I understand the concern because as you said, the threat environment is ever evolving, and is something that day-to-day, we don't know what's coming next.

The focus of this presentation I think actually might kind of help with that. Because really, we're focusing on the attack pathways.

Not specific CDAs, but how are each of the pathways that an adversary could use to attack a system, protect it.

So, I can't speak much to the Part 53 because we'll have that later today. But hopefully my presentation will at least help with the concerns you have with the current fleet.

CHAIR HALNON: And Dan, that second sub-bullet under CDA, it's pretty broad when you don't have a succinct definition of adverse impact.

Can you kind of give us a sense of the range of adverse impacts? Because that kind of speaks to Jose's issues that that could, depending on how you define adverse impact, you could aquarium temperature all the way up to you know, core melt.

So, in your experience, could you kind of click on that letter that we're in and kind of expand that for us?

MR. WARNER: What I'll say for this, is this is not the first time that question has come up. Because obviously like you said --

(Simultaneous speaking.)

CHAIR HALNON: I hope not.

MR. WARNER: -- adverse impact is a very broad term.

And again, I just want to emphasize that for this, I'm speaking from my own position.

There are a lot of areas where when we say adverse impact. In my mind, it has to be broad because I feel like that's the conservative approach to trying to capture everything.

Like you said, then the problem becomes if you have to try and plan for everything, how do you focus on what really needs to be protected.

And that in general with cybersecurity, that's always the question. Because like you say, sorry about that.

Like you were saying, I mean, the thermometer in a completely unconnected, I mean, obviously connected but unrelated system causing an issue.

So, with the cybersecurity program, we're trying to balance the ability to protect with reasonable assurance from the concerns that are out there, but also ensuring that as we move forward, any future new attacks, threats, are able to be dealt with.

So, I know that's not quite the best answer for the question, but.

CHAIR HALNON: No, I think it is. I mean, the answer in my mind, is that just yes, you protect your critical digital assets.

But if you have an impact that may not fall into the regulation if you will, that doesn't preclude you from protecting it.

MR. WARNER: Correct.

CHAIR HALNON: So, you know, the whole process we're going to talk through today with the assessments and everything that was done, caused a lot of the utilities and users of technology, to understand better their vulnerabilities, and how far that will go.

As opposed to only drawing a hard circle around things that could really affect the core. So, I think that that's how I see it anyway.

MR. WARNER: Yes. And like I said, the program really what I'm talking about today, is focusing on how we're protecting the different pathways, but also talking about defense-in-depth.

And that's one of the key components that we're really using here is I mean, everybody likes to use the example of the Swiss cheese. It's like everything has holes in it.

The key is to line up the holes so that if you get through one, there's something else blocking you on the other side.

And that's one of the key components of the program that we want to make sure is in place, to offer as much protection as we reasonably can.

CHAIR HALNON: Well, we got to the third slide before we jumped in there so that's actually better than I thought.

MEMBER BROWN: No, we're not.

Yes, this is Charlie Brown. Are you familiar with my general approach relative to the reactor safety systems and safeguard systems, et cetera, and the main control room, and the communications from systems to that control room.

And I guess one of the focuses I guess, I've been emphasizing for numerous approaches, applications we've seen, is not so much going out and looking at every water fountain, and every cell phone, and whatever it is. Not necessarily the cell phones but the connected systems, not the ones you carry around.

There's boundary conditions. If you focus on the piece parts, you're never going to get there to a closed system.

And the committee has always tried to draw a dotted line around the main control room, down through the whatever networks you have, within the plant.

All around all the safeguards and safety systems, and say everything's, there's no doors. If it's a data, if you send data all you want to out to NRC, out to the venders, whatever you want, it's got to go through a hardware type data transmission device that can't be compromised.

Sets aside the guy that comes into the plant, which now he burrows his way in and somehow gets into some piece of equipment.

And we've tried, we've incorporated some of that thought process, also into 5.71, which is pretty extensive.

So, I just wanted to emphasize that again. I don't like, it's like trying to evaluate a reactor safety system by evaluating every position, and every IEEE standard, every Reg Guide. All those piece parts.

It's the architecture that counts. So, you want to boundary the architecture. And that, that is hard to, that's hard to drag out.

When you see Part 53 and the new risk informed thought process, we're, it's like a crapshoot. You're just throwing everything up in the air and we're going to reevaluate what's, what's really necessary.

And maybe you don't have to follow our regulations, even though they, we do have boundary condition set ups.

I just want to emphasize that. I just think the focus somewhere along this line, needs to lay out as opposed to CDAs, boundary conditions for overall plant electronic access, which is now just a, as Jose said, it's just a terrible threat we have to deal with.

So anyway, I'll --

(Simultaneous speaking.)

MEMBER BROWN: -- that's just another thought process.

MEMBER MARCH-LEUBA: Yes, I mean, I was the instigator for this meeting. If you didn't know, now you know even though these two guys were going to ask it from me.

CHAIR HALNON: I tried to run interference for you.

(Laughter.)

MEMBER MARCH-LEUBA: Yes. But my goal here is not to learn what you're doing. I'm sure you guys follow regulations, and you have programs and you do audits.

And but there's some ideas in your mind that maybe there is something else we need to discuss.

I personally, my wife has a company and I'm her IT tech. So, I'm there trying to protect her from, from the bad guys.

And if you concentrate on ransom ware and you back up, and you back up, or you back up, I have back ups of older files in different states. I'm not connected to the Web.

But you concentrate on that, and then suddenly they go and they steal your Coca-Cola files and sell them to Pepsi.

So if you put all your eggs into the don't encrypt my files, they'll attack you somewhere else. And I'm concerned that because of regulation, because our mission is to protect the safety, the nuclear safety of the reactor, we may be making the utilities spend too much money on that.

So, they even get the false sense of security that they're protecting the safety very well. And they're not protecting that other thing that they're going to get attacked on, because they don't have enough budget in the program to do the other things.

And one thing that came up into our mind when we reviewing this recent reactor, SHINE, it's a facility to produce molybdenum-99 for, for hospitals.

It came to my realization and I some members agree with me, that the SHINE reactor is more safe when it's running, than when it is not.

If you shut down the molybdenum producing great isotopes for medical production, you kill more people statistically, than if you keep it running.

So, we put all our eggs in the basket of make sure the reactor stays running.

So, there is more than one goal that you need to, and you have to be in a generalist. I'm scared to death.

MR. WARNER: I understand the concern. I was actually part of that SHINE ACRS meeting, because I reviewed the cybersecurity for SHINE. So, I understand where this is coming from.

What I will say is the agency mission, I don't know at least for existing power reactors obviously, isn't really interpreted that way.

We are protecting public health and safety, and that's from the use of the material itself.

I don't know how much I can provide about the production aspect of --

(Simultaneous speaking.)

MEMBER MARCH-LEUBA: Yes, and remember that this is an open, open meeting. So let's, yes.

CHAIR HALNON: We tried to design this meeting to start with the basics, and to spread out into the rest of the world so that we could try to encompass that.

I don't know if we're going to get all of it because it kind of sometimes, we may go outside of our mission.

But as we go through the day, and Dan

we'll let you put your wheels back on here on your presentation in just a second, hopefully you'll find other areas that your can interject some of the wisdom that you've --

(Simultaneous speaking.)

MEMBER MARCH-LEUBA: Sometimes the ACRS value is to provide ammunition for the staff to do their job, or an incentive for the staff to do their job better.

Give you guys ideas on what, oh, gee, I wasn't doing that. Instead of us complaining about paragraph 3.2, or this or that.

Okay, I will promise to leave you off for two more slides.

MR. WARNER: All right, thank you, appreciate it.

CHAIR HALNON: Thank you.

Dan, go ahead.

MR. WARNER: And just to confirm, we are on slide 5 at the moment.

So, I wanted to kind of go over the different types of CDAs that are part of the controls that we'll find in the power plants.

So we have emergency preparedness CDAs, which are those CDAs associated with EP functions, that do not have an independent and diverse alternate method to perform the EP function.

And those will have to have either the baseline controls, or a full, direct CDA assessment with controls in place.

There are bounds of plant CDAs, where those added to the cybersecurity rule scope during the resolution of FERC Order 706 bravo.

And these will be addressed in, actually in the next presentation. We'll go into more detail on those.

Then we have indirect CDAs, which are those that cannot have adverse impact on safety or security functions, prior to detection compensation, or compromise of failure was implemented.

And those get the baseline cybersecurity controls, and I'll be discussing what those are in the next slide.

And then anything non-assessed as indirect VOP or EP as direct, and then they get a control assessment, and that's where you determine what controls need to be applied.

Next slide, please.

So, the baseline cybersecurity controls listed here, for EP indirect and BOP SCRAM/Trip CDAs, they must be located within the protected area or the vital area, or have the NEI 0809 section echo 5 controls applied.

No active wireless internet communication on CDAs, or any interconnected asset. CDA and interconnected assets are air gapped, or isolated, by a deterministic device.

Portable media use is controlled. Changes to CDAs are evaluated and documented, prior to implementation.

And then CDAs or interconnected equipment affected by the compromise of CDAs, are periodically checked to ensure that they can perform their intended functions.

And there's ongoing monitoring and assessment that's performed, to verify baseline security criteria remains in place.

MEMBER BROWN: Did you say no wireless, no active wireless internet communication, yet on the next slide you, couple of slides later you said gee, you have to evaluate all the wireless.

That seems to be an oxy.

MR. WARNER: So, kind of --

(Simultaneous speaking.)

MEMBER BROWN: That's not a negative

comment about.

MR. WARNER: Right, right.

MEMBER BROWN: It's an observation.

MR. WARNER: Understand.

MEMBER BROWN: Don't take that the wrong way.

MR. WARNER: Yes. So, what I will say is that you cannot have an active wireless connection on a CDA, or something directly connected to it.

We're currently doing evaluations on wireless, and will have more discussions in the advanced reactor section this afternoon.

But what we've kind of heard is the potential is basically have a separate set of like wireless sensors monitoring equipment, that prevent operators from having to go into contaminated or high rad areas as often.

So they would be independently installed. And they can discuss more later, but the actual CDAs are not allowed to have wireless --

MEMBER BROWN: They could have a wired connection coming out to wherever you want to monitor, as opposed to a wireless, and that still prevents people from having to go into a contaminated, or high radiation area.

There are ways to solve that without giving in to the mantra that we love wireless and it's the sweetest thing that ever walked, you know, into the plant.

I'm very, if it hadn't been clear in other meetings, I have no, I am not a friend of wireless anywhere inside the plant.

MR. WARNER: And that is something that we are also very concerned about. There's a lot of evaluation going on about that because we also are concerned, and want to make sure that if it's implemented, it's implemented safely and won't impact the cybersecurity program.

MR. BLEY: Dan?

MR. WARNER: Yes.

MR. BLEY: This is Dennis Bley. Your third bullet is very clear. CDAs and interconnected assets are air gapped, or isolated by deterministic devices.

This isn't so much a question for you as for the digital guys when we talk later. We've had a little trouble being able to say essentially, the same thing.

And I'm, this is a requirement for cyber so maybe we'll talk about that some time later, but thank you.

MR. WARNER: Yes.

MEMBER MARCH-LEUBA: Yes, two things. I mean, we're not going to let you go, we can hold you.

MR. WARNER: I'm prepared for it.

MEMBER MARCH-LEUBA: And most people enjoy when they're sitting in your seat, when there is more interaction of the, bless you, instead of yes and reading your prepared slides. It's far more fun.

So, I disagree with my esteemed colleague Charlie on the wireless.

MEMBER BROWN: I knew that, that's why I let Jose object first.

MEMBER MARCH-LEUBA: You need to protect against attacks by both wireless, and non-wireless. Because that aquarium is on the cable.

So the attack came through, through a corporate wire. So, you need to make sure that all your pathways, which you're going to get into, are protected.

I'm going to bring it now. Just a moment ago, I check with the NIST CVE database, it's the vulnerability database. It has 200,000 known vulnerabilities. Those are the known ones.

And I check the last three months, how many have been reported on virtual private networks, VPNs. Twenty-seven in the last three months.

If we continue at the same rate that every time I put this on the record, every three days somebody discovers a vulnerability with a VPN.

And everybody say oh, I have a VPN, how can somebody break into it. Well, let me tell you. We have a VPN right here inside this building, and I personally detected an intrusion inside of the building.

I mean, there was something running sideways trying to infect my laptop.

I shut it down and ran to the phone. I call IT and they say huh?

MR. YIP: Excuse me, we shouldn't talk about vulnerabilities on an open.

MEMBER MARCH-LEUBA: This is not a vulnerability.

So, this has happened. It happened through the wire. So, just, just to put a little bit of the scare of, on your, on you.

I mean, this is very difficult to control. Have to be on your toes.

MR. WARNER: So, like I said, we're going to look at the different attack pathways, and just go through a sampling of controls that protect each of those attack pathways.

And the attack pathways we are going to look at are physical access, wired connectivity or communications, wireless connectivity or communications, the supply chain, and then portable media and mobile devices, which we shortened to PMMD.

So, physical access ensures only the appropriate personnel are able to interface physically with a CDA.

Some of the controls that help protect are access control policies and procedures, account management, access enforcement, which is basically just enforcing your access control policies and procedures.

Physical access controls, such as locked cabinets, USB port blockers, least privilege. Just making sure that the person's account is using the least necessary amount of privileges, to be able to do the work performed.

And then logging. So everything that's being done. Whether it's accessing keys, accessing cabinets, or actually logging into devices, is monitored and identified.

CHAIR HALNON: Dan, just recently, we've had you know, in the news confidential information leak from someone who was in an IT department.

IT folks typically have wide ranging access because of their need to get throughout, throughout the systems.

Is that covered under some of these bullets, like account management and other things? Are the IT people held to a higher standard of background check, and physical access?

MR. WARNER: Yes, so licensees have an insider mitigation program because obviously, one of the most dangerous attacks you can have is an insider who actually knows your system, is coming in and messing with it.

So, the insider mitigation program ensures that only those allowed have the access levels, and they have the background check.

And then also if you're able to access CDAs, you have to go a step further and be in the critical group, which has further restrictions and background checks, to make sure that the people who are accessing your most sensitive equipment are those that are most trusted.

So, wired access controls ensure only the appropriate personnel are able to interface with the CDA, using a wired network.

Some of those controls are, you can see below. I mean, we've got the first six are essentially the first ones that we had for the other one. You see those frequently.

Network access control. Basically making sure that what's on the network, is what's supposed to be on the network.

Any open or insecure protocols are not allowed and blocked, to ensure they're not able to be used to bypass security controls.

Insecure and rogue connections are constantly being monitored and searched for, to ensure that none are on the network.

And then use of external systems is restricted so that any information that's flowing, it's through a protected device like the data diode.

MEMBER MARCH-LEUBA: Your regulations are not written too constrictive. They don't force you into an old technology, right?

I'm thinking right now everybody's moving to what they call pass keys, to replace passwords. And I hope our regulations do say you're required to have a password, and you allow pass keys.

Just keep that in mind that by writing a prescriptive regulation, you might lock yourself into an old technology.

And in this area, all technology is three months old.

MR. WARNER: Yes, and the regulation is like all, most of our regulations, are written at a fairly high level.

That's one of the reasons in the IO 809 and Reg Guide 571 were developed to be able to provide so much more detail on how to implement the actual regulation itself, so.

And then in addition to all the previous controls, wireless access controls ensure the implementation of adequate protection and procedures, to minimize the cyber risk associated with the use of wireless technologies.

Some of those controls include only allowing wireless access through a boundary security control device, such as a firewall.

Prohibiting use of wireless for CDAs associated with safety related and important safety functions.

Disabling wireless when not used. And then conducting scans for employing a wireless intrusion detection system for any unauthorized wireless access points, and disabling them if they are discovered.

MEMBER BROWN: The disabling of the wireless when not used, is that a physical, I mean, or is software? Because anything that can be disabled, the software can be re-enabled.

MR. WARNER: Right. In most cases, it is software based. So, you would have to go in and disable it.

There's a lot, big push both in the general critical infrastructure and where you're looking at here, the agency, for zero trust.

And part of that is basically that devices are secure by default, which would mean that like anything that would potentially allow extra access like wireless, would be disabled upon the vender shipping out the part in the beginning.

And that's to help for when people maybe don't check all the settings, and don't turn off what they need to turn off, so.

MEMBER BROWN: So it's disabled by software, then it can be re-enabled by software.

MR. WARNER: That is correct.

MEMBER BROWN: So, that's kind of a useless.

MR. WARNER: You can say that, but at the same time, I mean, most of these you have to be physically at the device, or physically connected to the device to be able to flip that switch.

With the insider mitigation program, the access authorization program, with the physical security controls in place, with the architecture defense-in-depth, there are a lot of barriers that would prevent that switch from being placed.

MR. YIP: And if I could, that's also one of the reasons why we require periodic baseline configuration audits for CDAs.

To ensure that the settings that were initially put in place, are, are maintained throughout the life cycle of the CDA.

CHAIR HALNON: That was Brian Yin. When you jump in there Brian, make sure you say your name.

So I'm going to ask, Charlie, are you finished because I have Vicki, and then Walt's online who has a question.

Okay, Vicki?

MEMBER BIER: Okay, I'm actually going to sound a lot like Charlie on this question.

Disabling wireless when not used, I guess I have a couple of questions. First of all, is that something that could be automated, or is that a procedural control where the person has to remember oh, I'm done with this task, now I should disable?

MR. WARNER: I mean, it's procedural. I mean, it's going to have to be done by somebody.

MEMBER BIER: Yes.

MR. WARNER: But once it's turned off, it should stay off.

MEMBER BIER: Yes.

CHAIR HALNON: Unless somebody actually turns it back on. So, it just needs to be done.

And that would be part of the process when procurement is done by the licensee, and then the actual it's tested, and then installed.

They do have to do like Brian said, the baseline configuration in the very first place so they know what they have installed and everything.

And part of that should be verifying that your wireless is disabled, if it's part of the component.

MEMBER BIER: Yes. Because I just worry that procedural controls are known to not be very robust.

And if you can't do it, it's a lot harder to do than if you can mess up and you're supposed to not mess up.

I guess the other thing is how much flexibility is there, or just finding another way to do it that doesn't require wireless in the component?

You know, are there functions that really depend on that, or is that just a choice of convenience, or whatever for the designer?

MR. WARNER: To my knowledge, there is not active wireless being used within the plants. Definitely not within the actual, the higher security levels that are behind the data diode typically.

MEMBER BIER: Okay.

So this is conceptually a possibility, but to your knowledge, people are not currently relying on this option?

MR. WARNER: Right, because we're still working with industry to try and figure out how vested --

MEMBER BIER: Okay, thank you.

CHAIR HALNON: And just remind everybody, the techniques are unknown to us, because our security program, physical security programs, have been using these for a while on the laptops and whatnot that they use.

Walt, you're online. Go ahead.

MEMBER KIRCHNER: Thank you, Greg.

Good morning everyone. Dan, one of my questions would be the following. On your second sub-bullet under applicable controls prohibiting use of wireless for CDAs associated with safety related.

That part I see as relatively straightforward, at least determining which are in that category because safety related typically is the reactor protection system, engineering safeguard systems, passive systems like the primary coolant pressure boundary, et cetera.

Important to safety gets into the probabilistic world actually, in my mind. Or maybe that, that definition becomes, or that terminology comes from that word.

To what extent are you using PRA techniques to really examine vulnerabilities? Because I'll just, I'll come up with a set of systems that I think can be very important to safety for many designs.

And, it would be something like feed water control because you can use that to, to remove decay heat.

So, how do you draw the boundary, and how do you systematically search for what functions are important to safety?

MR. WARNER: That's a tough one. I come from the digital I&C world before I came into the cybersecurity, so I know how when you start talking important to safety, the definitions get a little nebulous.

So basically, anything that's going to be, okay. So, as part of some of the changes that were made with the NEI guidance documentation, safety related, important to safety did have some changes that were done.

And, I think the real primary part of that was because licensees were overly conservative in how many assets they were kind of lumping into that category.

I will be perfectly honest, I'm not as familiar with the actual changes that were made. So, that is a concern.

Obviously, licensees tend to be more conservative because it's better to have too many CDAs, than not have the appropriate CDAs bounded.

Yes, so I don't know if I'm really able to answer your question.

MR. YIP: And, this is Brian Yip. If I could, I think that the short answer would be we recognize the same, same challenge that you just identified that important to safety is not as clear cut as safety related.

And the staff did do a review of the Nuclear Energy Institute's document NEI 10-04, revision 3, which we just proofed for use about a year ago.

A part of the discussion and the reason for revising that document by NEI, was to address and provide additional guidance on important to safety.

So I don't know that we can get into the specific details of it without having it in front of us, but just to say that was something that we considered and addressed in recent guidance changes.

MR. WARNER: Thank you, Brian.

MEMBER KIRCHNER: Well, let me if I may, just Greg, elaborate with a few examples. I mean, for many, many reactor concepts as well as plants, your ultimate heat sake is certainly important to safety.

And so you get into a large swath of the balance of plant so to speak. And, then you have the dilemma that much of that part of the plant can be compromised by wireless, or internet connections, and so on.

So, I'm just concerned there because important to safety can be a lot broader class, or swath of a power plant than, than more readily, not easily, readily determined safety related functions.

Just an observation.

MR. WARNER: Thank you.

CHAIR HALNON: Thanks, Walt.

Charlie?

MEMBER BROWN: I want to segue back to, not to the what I said before; different, different, slightly different subject.

A lot of controllers now, you know, for pumps, valves, et cetera, et cetera, were moving away from relays and contactors and stuff like that, to programmable logic devices.

You can argue whether throwing in a software based PLD is a good idea, or not. The other one was a coil, the contacts closed and it worked.

Now you've got all kinds of stuff. But the argument generally is that you can monitor that component much better if you can get data on whether it's currents are changing, is it overheating. It's doing a lot of different things.

Then we get into the world that we just finished with, the commercial dedication of some of these programmable logic devices.

So now it's another step down the path on the, what did I call it, the 1E, or NQA type certification via NRC standard.

That's just another layer of these things, of having to deal with. But that's a more complex issue.

And is there anything in your all's world where you're starting to look at how these are being used, and how they work into this not necessarily wireless even connected because it doesn't really matter which, which one you do.

MR. WARNER: Yes, I mean, FPGAs are obviously starting to be used in a lot of the newer designs. That's a concern along those lines.

MEMBER BROWN: But FPGAs are almost, once you program it, depending on what type of device you store it from the FPGA.

But if it's a volatile FPGA, you have to reboot it every time you lose power. You're setting yourself up to having something happen under those circumstances.

If it's a non-volatile FPGA, once you program it, theoretically, I'm not a programmer, okay, I'm not a designer, you can't go in and change where those, those various logic units are switched on and off.

That's the theory.

MR. WARNER: Yes.

MEMBER BROWN: I used to block stuff with having a UV-type where you, they weren't e-squared like accessible whether they're FPGAs or anything else. And, that's pretty good.

Once you UV it, you can't touch them from a programmable read only memory.

Anyway, the PLD starting to me after our last rounds, when you can see them, people wanting to back some of those.

And they're not in the plants now, but they may want to for plant monitoring and reliability assessment. Particularly as they get older.

CHAIR HALNON: Yes, and as we get into the part, the afternoon session, I think we're going to dig into this wireless since the trend is to go more wireless, and more automated, we're going to dig into this.

And I think a lot of these comments on the wireless are probably more appropriate for the research and other folks.

MEMBER BROWN: I'll wait.

CHAIR HALNON: Well, but that was my way of saying to Charlie, wait, but I was trying to be more professional than just yell it.

(Simultaneous speaking.)

MR. WARNER: What I will say, and that's kind of the, what we wanted to emphasize with this presentation.

Technology is obviously ever-evolving. Nuclear plants are way behind everybody else who's been using these newer devices for many years.

But as far as cybersecurity goes, especially since I've been involved with some of those critical infrastructure activities coming out of CISA, I think we're ahead of the game.

Part of that is because we're really, besides all the controls, checking baseline configurations, ensuring that vulnerabilities are identified and mitigated, we're also protecting the pathways that ensure that hey, if somebody can't get to the devices that are of concern, then they can't mess with it.

So, it's belts and suspenders because making sure, and that's the whole point of the defense-in-depth.

So I understand where the concerns come from because we obviously we're getting reports, seeing all this stuff coming out about the new threats and vulnerabilities.

So, we have to make sure they're protected. That's what we, in the firms do.

MEMBER BROWN: To me, it's nice to see, I remember 10, 12 years ago when I first got here and I addressed the data diode hardware based. It was not received very gently in terms of the need for that type of stuff.

And now, I see you know, if you go back several slides you emphasize the deterministic isolation values, the hardware based stuff.

Air gaps are really becoming into play, which so maybe all that political palaver that we went through 10 years ago and on, ongoing over the last few years, is starting to pay off. So good to see that.

CHAIR HALNON: Exactly.

So then the next type of pathway we're going to talk about is the supply chain. So, supply chain controls ensure that cybersecurity risks throughout the supply chain are identified, assessed, and mitigated.

And some of those include policies for systems and services acquisition, supply chain protections, trustworthiness, basically ensuring that the, from the development of the device to the time it was delivered onsite, that the device is protected and you're sure that the, you're getting what you ordered.

Developer security testing and evaluation, and then licensee applicant testing. Basically do, have the developer do their testing, and then when you get the device, you do the site acceptance, and factory acceptance testing to ensure that what you got is what was ordered, and what was you were told.

CHAIR HALNON: And, is what we learned about the counterfeit issue intertwined in all those?

MR. WARNER: Yes. The counterfeits are obviously a big concern. And then part of this is definitely making sure that you are getting legitimate components.

MEMBER BIER: Are there any restrictions or requirements regarding country of origin for components?

MR. WARNER: I don't know.

MEMBER BIER: Okay.

MR. WARNER: I have not delved too much into this.

MEMBER BIER: All right.

MR. WARNER: So, I don't want to answer that question.

MEMBER BIER: Yes.

MR. WARNER: That's something that I can go back and ask.

MEMBER BIER: My guess is no, but it would be nice to know if you know, what the true situation is.

The other thing on acceptance testing, it's unclear to me how far that goes, because acceptance testing can verify that the component does what it's supposed to do in it's intended application.

But I'm not sure how one would acceptance test for kind of hidden code, that can be activated under the right circumstances. It's really hard to know what's in that black box when you test it, so.

MR. WARNER: And that's one of the reasons when we have vender inspections, and ensuring that the venders are trustworthy. There are a secure development and operational environments in place.

A lot of that's more on the digital I&C side than here in cyber, but that is definitely a concern.

And when you're doing your site acceptance testing, it's important to test what you're supposed to have, but also test what you don't want, so.

MEMBER MARCH-LEUBA: Yes, put this little bug in your head. You guys are familiar with legacy

APIs where you -- code and you put an include, and there goes something that a graduate student wrote in 1972, and it's still being carried on.

And the order attack similar to this, is when you have included code, and goes and gets it automatically from a get hub.

And bad actors have gone to the get hub and put a newer version on top of the old one, so they, you just flipped it for them and send it to the power plant.

So, we have to be careful. There are so many ways to get in.

MR. WARNER: Yes, but I will say if a licensee is going to get hub to get updates for a device instead of going back to the vender, that's a problem.

And that's something that they shouldn't be doing just as a company doing smart business.

MEMBER MARCH-LEUBA: I need to send you a study they made on the Israeli company that gets into iPhones, how they got into the iPhone.

I don't know if you've read it, it's really interesting. It's incredibly sophisticated. And, they using a grad student work from '99 is to do that.

MR. WARNER: Yes.

MR. BLEY: Hey, Dennis Bley again. Charlie brought up commercial dedication. We went through that a lot with the I&C folks a while back.

My memory's not complete on that, but a lot of the things such as monitoring at the factories kind of goes away when you have commercial dedication, I believe.

Have you folks in cyber, are you in sync with what's been going on on the I&C side for, for that issue?

MR. WARNER: So, no, that would typically reside again in the digital I&C realm. I mean, we're more concerned on the cybersecurity side that once it's installed, protecting pathways, and ensuring it's doing what it's supposed to be doing.

But when you get down to the commercial grade dedication, that's kind of our of our purview.

MR. BLEY: Yes, but I, but if something goes wrong through that path, it will be back in your purview. So, it seems there ought to be some coordination on that issue.

MR. WARNER: And there is. We do have some interaction with the I&C branches in NRR. In fact, we've got some members here that I hope for the next presentation.

So, there is coordination. Doesn't mean that never is there opportunities for more.

MR. BLEY: But I guess what I'm getting at, some of the, some of the things that are routine to do from the cyber side using the previous sources, kind of disappear I think, unless I'm missing something when you go to commercial dedication.

Maybe some of the other guys can talk about that later.

CHAIR HALNON: Yes, if we don't pick it up, Dennis, reinvigorate the question.

Walter, you're online, go ahead.

MEMBER KIRCHNER: Thank you, Greg.

Dennis asked a more detailed version of my very same question. This all looks a lot, you know, the drive, the desire, let me back myself up.

At a very high level, there's certainly the economic factors, particularly this afternoon if we talk about advance reactors, that were, they want to partition systems and limit the, the number of quote/unquote safety related systems in a sense as they used digital I&C, they're going to want to limit the number of critical digital assets.

But this list of applicable controls looks a lot like NQA-1. Which we hear a lot of pushback on because of economic reasons, not necessarily others.

What kind of, as Dennis pointed out, if we go to commercial dedication and sources, yes, what kind of controls or quality assurance regime are these, these, is the supply chain going to be monitored under?

MR. WARNER: I mean, so as part of the inspection process when we're onsite, we're looking at the commitments that the licensee has made in their cybersecurity plan.

And then we are also looking at policies and procedures that they have in place, to ensure that they're addressing those commitments.

As part of that, there are supply chain procedures and policies that we'll look at, see how they're being implemented.

And then determine if we feel that they're meeting the commitments they've made, in their cybersecurity plans.

So, we make sure that they are ordering them in a manner to ensure the appropriate controls are in place.

That they're stored. That they're, when they're accessed, they're necessary. Making sure that the protectors are in place.

Or they're tested to ensure that the device is what they want to install, and that it's got all the necessary controls in place.

And I know that really does kind of dovetail what's really done on the procurement just on the engineering side.

But yes, we tend to focus more on the security controls, as opposed to security development and ensuring that the site acceptance testing was performed, and the engineering side of things.

CHAIR HALNON: So, Dan, more specifically, the question and I want to try to help to answer here.

In the process of the utility developing an approved suppliers list, ASL, the cyber controls and stuff that you have in the cyber plans for approving a supplier includes the requirements of the cyber trustworthiness, and material testing, and those types of things, as well.

So, it's not like you have an approved supplier and then you have to apply security, cybersecurity controls on it.

They're intertwined in the development, just like they would be in a digital I&C design. They're intertwined in that.

And the cyber plan sets those requirements that people have to design with, not necessarily in isolation of. I guess that's my point.

So, while from same thing with the dedication, commercial dedication. The requirements are built in to the dedication process, and then the cyber plans verify inspections, make that verification documented.

So, yes, is anything I said off, or is that correct?

MR. WARNER: No, that sounds good. Thank you for the assistance, so, yes. Not really handled by us, but we are part of that process.

CHAIR HALNON: Well, yes, you're the technology piece that sets, set the rules or sets the parameters of what they have to do to make their systems work.

Anybody else as we go forward?

Okay, Dan, go ahead.

MR. WARNER: All right, thank you.

And then the last pathway we're looking at is the portable media and mobile device. Release controls ensure the implementation of adequate protection and procedures, to minimize the cyber risk associated with the use of unapproved PMMD.

And some of the controls for that include uses and restrictions, and implementation guidance for controlling the PMMD.

Authorizing, monitoring, and controlling PMMD access to CDAs. PMMD security integrity are maintained at a level consistent with the CDAs they support.

And then PMMD can only be used on one security level, and not be moved between security levels.

MEMBER MARCH-LEUBA: This kind of ties with the wireless, because it's fairly easy with physical access to prevent somebody from plugging in a USB port.

But more and more, all the maintenance people in power plants work in there with a tablet to do their job.

And those tablets somehow, if you have a possible wireless path, somehow they become PMMDs. So, and that's a nightmare.

MR. WARNER: Well --

(Simultaneous speaking.)

MEMBER MARCH-LEUBA: That's why you have to, you have to attack it from the wireless point of view. The CDA cannot accept an unknown device.

MR. WARNER: Right. And that's one of the reasons the baseline configuration controls also ensure that no wireless is active so they can't connect.

MEMBER MARCH-LEUBA: Yes, but yes, but you.

MR. WARNER: Yes.

MEMBER MARCH-LEUBA: Every instrument technicians that walks into a power plant, has a tablet in their hands.

MR. WARNER: Or phone in their pocket, I mean, yes.

MEMBER MARCH-LEUBA: Yes.

MR. WARNER: We understand.

CHAIR HALNON: Dan, there's constant software updates on our equipment. And it's usually done wirelessly for us laymen people.

But, so how do you control a vender coming in and saying I need to update the software on your system, which is a critical digital asset?

Could you just walk us through how that would work to ensure that it's protected?

MR. WARNER: Yes. So, in many cases, venders have a laptop. And, the laptop they use is specific to the equipment they have installed.

And licensees will typically have that

laptop. It will be part of their PMMD program. It's basically an engineer can like, test equipment essentially.

That PMMD, depending on what level it is, is protected in a cabinet. It's secured, it's ensured that nobody's messed with it.

They will also do scans on it right before actually using it, to connect to equipment to make sure there's no malware or anything on there.

And then usage is logged and tracked from when it's pulled out of the cabinet, it's used. The vender, if they're the one actually doing the work, will have to be escorted by somebody who's in the critical group.

Basically, there's a lot of protections in place to make sure that the test equipment, or just being used, is not infected with any sort of malware, so we don't transfer it to the device.

And that there are protections in place to ensure the person who is actually doing the work, is also being monitored and show no malicious activity.

CHAIR HALNON: Okay, thanks.

MEMBER PETTI: So, I'm just a little confused. The computer sits at the plant and the guy comes in. Is that what you basically said?

MR. WARNER: So, I'm, I have not dealt with this as much, so that I have dealt with is that venders will leave equipment there onsite, or it will be a licensee device that has the appropriate software necessary to interface with the system.

MEMBER PETTI: But if they have to update something, they're bringing something in. They're bringing some additional software.

So, how do you protect, how is that protected?

MR. WARNER: The kiosks are basically used as scanning devices for any media transferring from one level to the next.

So if you're bringing in something from the outside, it has to get plugged in, scanned, transferred to a level appropriate device, and then that device is what's actually connected to the equipment.

So there should never be anything that's bringing, been brought in from the outside and not been scanned, before it actually interfaces with any devices.

Then we also have a host of programmatic controls that are in place. These programmatic controls are necessary to maintain security throughout the life cycle of CDAs.

One of the primary purposes of these controls is to ensure that as the threat environment evolves, the licensee systems remain secure from cyberattack.

We obviously discussed that, that significant amount this morning.

Some of these controls include continuous monitoring and assessment. Licensees must do periodic assessment of security controls.

They must perform effectiveness analysis, which basically is a review of their program to ensure it's still meeting the intent.

Vulnerability assessments and scans on devices. Configuration management. You want to know what's going in and out of the plant.

Change control. Security impact analysis of any changes in the environment, and then obviously, cybersecurity program reviews.

And, a lot of this stuff is also being assessed when we come in for our inspections.

CHAIR HALNON: Back on the when you say continuous monitoring assessments, it gives you the visual that there's somebody sitting in front of a computer screen watching a bunch of graphs, and spikes, and whatnot.

Is this basically software monitoring the software and flagging it, and giving somebody a text or something to that effect that there's an issue?

MR. WARNER: So, that is in place, so, just to get the actual, the definition for the continuous monitoring, so, ensures that period review and testing of security controls, processes, and procedures are conducted to confirm that the established security controls remain in place, and that changes in the system network environment or emerging threats do not diminish the effectiveness of these controls, processes, or procedures.

This is more the programmatic controls. It's more talking about actually the overall administrative aspects more than it is the technical monitoring of logs and networks.

CHAIR HALNON: In other words, you have dedicated folks running the program essentially. Thanks.

MR. WARNER: And then vulnerability management, so to protect against the ever-changing threat environment, nuclear licensees are required by their established security plans to address ongoing threats and vulnerabilities.

CDAs are performing vulnerability assessments or scans and evaluations to identify applicable corrective actions required to mitigate or remediate vulnerabilities to maintain an adequate defense-in-depth and prevent CDA compromise or exploitation. Yeah, that was a long one.

So, here are some of the controls that are used for vulnerability management. The most basic is obviously installing any operating system, application, and third-party software updates, remediating any flaws that are identified, reviewing security alerts and advisories to determine if there are any new vulnerabilities that impact your systems, contacts with security groups and associations which helps ensure that lessons learned are being distributed, and then evaluating and continuing to manage cyber risk.

Then, of course, defense-in-depth, so as stated in 10 CFR 73.54(c)(2), a licensee must design a cybersecurity program to apply and maintain an integrated defense-in-depth protective strategy to ensure the capability to detect, prevent, respond to, mitigate, and recover from a cyberattack.

So, an acceptable defense-in-depth protective strategy includes a defense architecture that describes a physical and logical network design that implements successive security levels separated by boundary control devices with segmentation with any security level. I have a diagram on the next slide that kind of helps show that a little bit better.

And then also employs multiple diverse and mutually supporting tools, technologies, and processes to effectively perform timely detective of, protection against, and response to a cyberattack.

As you can see here, this is the typical drawing that we like to include in many of our presentations. On the left, you see key components of creating a cybersecurity assessment team, identifying your critical digital assets, implementing the defensive architecture.

In this case, level zero is your least secure, and as you're moving down through the levels, you're going through boundary control devices, and then as you can see between level two and three, we have demonstrated here a data diode that prevents communication going from a lower security level into a higher security level, and then applying the security controls to CDAs.

And then the bottom part really talks about different aspects of the program that support all of this. Obviously, we have defense-in-depth, applying security controls, and that's typically done using NEI 13-10, mitigation strategies, training, managing your cyber risk, periodic reviews, evaluations of any modifications to components, incident response, and then having procedures in place, and then, of course, recording. Any records are being retained for the future.

MEMBER BROWN: Just to be parochial, level four is something like the reactor protection system, safeguard systems, et cetera, et cetera, and I've never been comfortable with just a firewall sending data from a protection system to the main control room or any place else other than tripping the breakers or starting a pump, you know, but those are isolated controls.

But sending that information anywhere else just with a firewall, and depending on then the level three, which I would view as that's communications out of a control room, or technical support center, or something -- yeah, that's just hypothetical, but that's one way to view this.

So, I've really never liked this diagram. It used to have a data diode. If you went back when we talked ten years ago, 12 years ago, 2008 or '09, we were arguing that that ought to be from a system standpoint, not necessarily from a diagrammatic standpoint. There are other things in level four that a firewall would work just fine for, but there are some that you ought to draw a harder line.

MR. WARNER: So, are you saying an additional data diode between level four and level three?

MEMBER BROWN: For specific systems like all of the RPS stuff, reactor protection system data should be a level four, I mean, should be a data diode type of thing. So, that's what we've actually been able to accomplish in most of the applicants.

They've either recognized that it's good advice to get it through the NRC and the committee, so they do it, or whatever, but it's been a struggle in some cases to discuss it because it's a hole and it gets very prescriptive when you do that, mention it.

The NRC, I forget, and I'm not trying to pick on particular people, but the NRC is very reluctant now to tell people how to keep their plant safe. They're more reluctant than they used to be. That's my impression. That's not the committee's impression.

CHAIR HALNON: Have you found the level

three, level four barrier hasn't been effective?

MR. WARNER: I mean, I will say we have not had an incident on a system that's behind the data diode at a nuclear facility.

CHAIR HALNON: Okay.

MEMBER BROWN: I would have expected that to be. It's going to be an exception rather than a rule, having general problems. There's going to be this specific problem that comes up that you don't anticipate some circumstances.

MEMBER MARCH-LEUBA: Meanwhile, on this drawing, you still have a firewall. You should put Gruyere cheese because that firewall has a bunch of holes that are open.

MEMBER BROWN: It's like an open cesspool.

MEMBER MARCH-LEUBA: So, well, no, it's not that bad --

(Laughter.)

MEMBER MARCH-LEUBA: -- not that bad, but honestly, you put the firewall because you do need communication flowing that way.

MEMBER BROWN: Yes, I agree with that, but a data diode would work also, or --

MEMBER MARCH-LEUBA: No, the diode would not allow you to communicate from three to four.

MEMBER BROWN: Well, that's -- a wire is a data diode when you trip something, so you can get from three to four fairly easy if you've got a switch and cables.

MEMBER MARCH-LEUBA: Simple --

(Simultaneous speaking.)

MEMBER BROWN: That's a detailed design issue. I'm just saying that that makes it look like that's the only thing you have to have is the software-based fire walls, which are easily, pretty easily compromisable by very, very confident hackers, but now they've got another wall to go through to get there, so that's the good news. So, all right, I just wanted Dan to slow down on this, obviously.

MR. WARNER: Understood.

MEMBER BROWN: Sorry about that, Greg.

CHAIR HALNON: That's okay. Back on the defense-in-depth slide, those items in number five, the bottom portion, we're pretty good at coming up with additional stuff.

Is there other things under consideration there from a defense-in-depth perspective given the advancement in technology that we are right now or is that pretty much the bounding list of stuff that we're doing for the lower end of it?

MR. WARNER: I mean, we're always looking at the program and looking to evolve the program to address threats. I mean, as Charlie mentioned, so most licensees use a data diode, but it's not required. That is just an easy way they've found to do this. So, and as Jose said earlier, the regulation is not prescriptive because we want to allow licensees to address the requirements how they feel.

So, I would say at this point, especially for all of the operating plants, I mean, they have a program that seems to work, so we're happy with what's there. Advanced reactors, maybe things will be a little different, but that will have to be a discussion for this afternoon.

CHAIR HALNON: Yeah, you know, part of me gets this picture of Muhammad Ali sitting in the corner just taking the punches with his fists up and waiting for the time to take the punch back.

It feels like we're in the corner, you know, just taking the punches, so maybe down the road, CISA, when we talk about that, Ryan, and the other things we can talk, is there anything proactive going on with defensive stuff?

And we don't need to answer that now. It's just a thought that came to my mind and, you know, we're kind of taking it in the chin looking for different ways of protecting ourselves as opposed to, you know, the other way around, and it may be something we can't talk about in an open meeting.

MR. WARNER: I mean, again, the whole point of the program is to ensure that we don't know what's coming, so we're trying to be as prepared as we can. We're trying to get as many layers of defense as possible to ensure that critical systems remain protected.

CHAIR HALNON: Yeah, okay, thanks. Go on, please.

MR. WARNER: And then for my last couple of slides, I'm just going to kind of give a brief overview of the two types of implementation inspection and the current inspection program.

So, the full implementation inspection program ran from 2017 to 2021. It used a preliminary version of the inspection procedure 711030.10, which is what's used currently. Teams consisted of two regional inspectors and then contractor subject matter experts.

They were completed in 2021 and they focused on ensuring that licensees were in compliance with the requirements for establishing a cybersecurity program, and these consisted of a week onsite, followed by an offsite week, and then there was a second week onsite, and then the CSB staff supports remotely will sometimes go out in person just to kind of keep fresh on things, but we're there to answer any questions that the inspection team has.

CHAIR HALNON: So, early on in the program development back in the '11, '12, '13 time frame, '14, it was difficult to find SMEs. Is the community much larger now or is it still real exclusive?

MR. WARNER: The community is much larger, but the need is even greater. I mean, I was at a conference last week and they were talking about it, and it's -- licensees and just in general, cybersecurity staff is difficult to come by --

CHAIR HALNON: It's still very --

MR. WARNER: -- and that's something that's a very big challenge to all industries, especially with how cyber-focused things are moving forward.

CHAIR HALNON: Okay, Jose?

MEMBER MARCH-LEUBA: Yeah, we were making a tour when we were talking about the inspection of pipes, that you find yourself -- in terms of pipes. The problem is the money. These other people are stealing the little guys.

But my question on the audit, on the inspections, is the focus on paperwork or how is it implemented?

MR. WARNER: It's how it's implemented and I'm going by personal experience. I mean, when we go out onsite, we'll sit there and we have prep beforehand where we are looking at documentation. Just to make sure I'm just raising this right, we're looking at the current inspection program now.

So, what we'll see is we'll look at any changes that are made and we're trying to basically ensure that the changes are being appropriately implemented.

We'll go out and we'll look at what's actually installed, make sure the protections are in place that need to be in place. We'll review the modification packages to ensure that any cybersecurity criteria were addressed as part of the modification.

We look at storage of CDAs. We look at procurement of CDAs. So, there's a lot of paper we do review, but we're also out there looking at the physical components and ensuring that they actually implemented things appropriately.

MEMBER MARCH-LEUBA: Yeah, the concern is when you are an inspector, you see there are good licensees and there are bad licensees, and so there are guys that are really concerned about it and they may make a mistake, and there are others that say, hey, I want to save money, and those are the ones you have to look at more carefully.

MR. WARNER: And typically, then you will see more findings as a result of the inspections because of that.

MEMBER MARCH-LEUBA: Typically, the ones that save money, they do their paperwork right.

CHAIR HALNON: Vicki, did you have a question or anything? No?

MR. WARNER: And I've kind of covered this a little bit, but now we're talking about the current inspection program, similar IP, similar team composition, two inspectors and then two contractor subject matter experts, and again, focusing on reviewing changes to the program and ensuring that the licensees are implementing their programs to ensure cybersecurity throughout the life cycle for any newly-installed CDAs, and this inspector program currently consists of a prep week offsite and then one week onsite.

CHAIR HALNON: And you said that's a

biennial?

MR. WARNER: Correct.

CHAIR HALNON: Every two years? So, have you looked back given the, what, couple, three years that we've been doing this? Is that frequent enough for the way that things are changing?

MR. WARNER: There are some discussions going on regarding basically we wanted some runtime with the program and then look at it and see if there's anything that needs to be changed.

CHAIR HALNON: Or maybe more frequent, too frequent? I mean, it's possible it could be a three-year program given the fact that we're not changing out plants all that much, but threats are obviously evolving, so you're talking about internally.

MR. WARNER: I believe that's my last slide. I'd say I'd ask for questions, but --

CHAIR HALNON: Yeah, well, I was going to ask if, and I don't know if this is the right spot for any recent -- I know that you have a reporting structure and there's a report out back to the plants as well with the CSAT response.

Could you talk a little bit or maybe go down the road about the incident response and how that works, and then any interesting stories you might have relative that you can talk in an open session?

MR. WARNER: And I assume you're talking more about like the agency Cyber Assessment Team and how we handle licensee reporting of events?

CHAIR HALNON: Yeah, well, just take an incident with someone that has -- I know that even in an RPS, a reactor protection system actuation requires at least a question whether or not it was a potential cyberattack. How does that work that you guys get involved in something like that?

MR. WARNER: So, we'll discuss that more in the next presentation.

CHAIR HALNON: Okay, yeah, I just wanted to make sure we don't lose that because I think that's important as we get into the advanced reactor world with the smaller staffs and more autonomous, not completely autonomous operation.

I know that we're going to talk about that down the road, but that comes up quite often. And, you know, Jose, he's sort of our conscience. He rakes over the news and sends us articles all the time about potential cyber issues out there.

MEMBER MARCH-LEUBA: There are 30,000, more than 30,000 vulnerabilities that have been identified this year and we're in May. Most of these are identified by ethical researchers, but 30,000. Okay, I wanted to make a couple of comments.

MR. WARNER: Sure.

MEMBER MARCH-LEUBA: Okay, I wanted to make a couple of comments on a high level because the way I see it, I'm not going to make any plant safer. You are. So, I'm trying to put ideas in your mind, but, so I'm going to make two comments. One is positive and one is, let's call it forward thinking.

The positive one comes from the news, CNN. I've been following the Ukrainian War and you have the brightest minds in the Russian security forces trying to attack all the Ukrainian power plants and they have not succeeded because they're sending bombs.

They cannot go through the cable and make them fail, so something is working right. Maybe they're in such a cocoon that they don't let anything in and that's why they're succeeding, but maybe that's the norm -- we need to operate normally.

The second forward thinking comment is I am uneasy about this concentration of critical digital assets. Our guys are always attacked where you are not looking. And I also told when I used to work on safeguards to my DOE boss that we need to have our meeting in Las Vegas.

And we should go to see all the magic shows, because if I control the scenario, I can make an elephant disappear, and that's the attitude you guys have to have when you're doing this. If a bad guy controls the scenario, don't let him control it because an elephant can disappear.

Thank you. That's very good. I think we're doing a great job, but it is your job to keep the plants safe, not mine. I can only complaint.

CHAIR HALNON: Thank you, Jose. Any other comments or questions on this presentation from the members or members online? Okay, Dan, thank you.

MEMBER BROWN: Yeah, let me ask one question.

CHAIR HALNON: Sure, go ahead, Charlie.

MEMBER BROWN: And it may be applicable to the I&C part which is this afternoon.

CHAIR HALNON: Yeah, go ahead, please.

MEMBER BROWN: In one of the earlier projects that we reviewed, this is eight years ago or so, there was a network where a lot of data went into and they talked about how some of that data was critical data, but yet it went into the overall network in a partitioned or segmented manner.

In other words, it didn't get run

routinely as the network operated. It was only queued. If something came up from behind, you know, the other, up through into that system that asked it to be run.

I was never comfortable with that. I'm not a programmer, so partitioning and how you do that and prevent access during the routine operation of the network for doing everything else that you're doing within the plant, even the non-critical operations.

Do you all get involved in that or do you try to work with -- or do you see that as the I&C guys ensuring that the software development that's done for that network has adequate protections within it?

It's like a giant server farm in a way, but having little compartments that you can't get into unless you're, you know, queued to get into it from the more safe systems within the plant. Am I clear on that question or --

MR. WARNER: Yeah, I think I understand what you're saying. So, actually, just let me ask one question.

MEMBER BROWN: Commingling software fundamentally, but saying hey --

MR. WARNER: Right.

MEMBER BROWN: -- you can't get to this

little packet over here because we never ask for it unless.

MR. WARNER: We don't really get too in-depth in that. If that was something that was being done at a licensee, what I imagine would be we want to ensure that, I mean, if it's data just speeding out for monitoring purposes, then obviously, we want it filtered through like a data diode to ensure there's no communication back to your critical systems.

Beyond that, I don't want to speculate too much more because just pulling something out of thin air.

MEMBER BROWN: Okay, well, obviously, this was overall a much larger range of thought processes without all of the details of how it was going to be utilized. This was a long time ago and we never -- I'm not sure we even finished the application on that. It's been a while. It's just a software thought process that I wanted to ask.

CHAIR HALNON: Thanks, Charlie. Any other questions? Okay, we're a little bit ahead of schedule. I'm going to go ahead and call the break now and we'll be back at 10:15.

When we come back, we're going to expand out a little bit and get into the inter-NRC coordination between the offices and also the intergovernmental agency coordination as we expand out from the reactor going towards the grid. So, we'll recess until 10:15.

(Whereupon, the above-entitled matter went off the record at 9:52 a.m. and resumed at 10:15 a.m.)

CHAIR HALNON: Okay, this is the cybersecurity presentations we're having for our subcommittee. We're back in session and Dan, you're up.

MR. WARNER: Good morning. I am back. This is Dan Warner from the Cybersecurity Branch in the Division of Physical and Cybersecurity Policy in the Office of Nuclear Security and Incident Response, and for this presentation, we're going to talk about government interaction and coordination between the NRC, NERC, and FERC, and then the role of DOE and DHS CISA.

So, the key messages for this presentation, the NRC has a long history of engagement and cooperation with FERC, DHS CISA, and other federal partners on cybersecurity and other issues.

The NRC's engagement with FERC on cybersecurity ensured appropriate protection for bounds of plant CDAs, and the Cyber Assessment Team processes design both to coordinate internal response to issues, as well as support early engagement with interagency partners.

MEMBER BROWN: What is CISA?

MR. WARNER: It's the Cybersecurity and Infrastructure Security Agency.

MEMBER BROWN: Oh, okay.

MR. WARNER: Ryan is our representative and he'll be talking a little bit later.

MEMBER BROWN: Okay, sorry about that. I actually read that, but thought I'd ask.

MR. WARNER: So, just a brief background on bounds of plant. In January 2008, FERC issued Order 706 which specified critical infrastructure protection and reliability standards to safeguard critical cyber assets, and it specifically exempted facilities that are regulated by the NRC.

In March 2009, the NRC issued 10 CFR 73.54, protection of digital computer communications and networks to NRC power reactor licensees, and that also did not cover all bounds of plant equipment at NRC power reactor facilities, which created a potential gap between NRC and FERC regulation.

Then in March 2009, FERC issued Order 706(b) which clarified that BOP systems and equipment not within the scope of 73.54 is subject to NERC standards, and then nuclear facilities were allowed to seek an exemption from those standards on a case by case basis for digital assets they believed were subject to the NRC's cybersecurity requirements.

Then in December of 2009, the NRC and NERC signed a memorandum of understanding basically addressing how they would handle their respective authorities over the nuclear power plant cybersecurity.

In 2010, NERC sent a survey called the Bright Line Survey to power plants requesting them to determine which of their components were potentially subject to NERC standards and which ones were subject to cybersecurity regulation under the NRC.

Then in August, NERC confirmed to the NRC that based on the response to the survey, that NERC had concluded the assignment of regulatory authority for the BOP components was subject to the NRC cybersecurity authority.

And then a memorandum between the NRC and NERC and FERC will be discussed in more detail, will be discussed actually in Jorge's slides which will be after this presentation.

MEMBER BROWN: Is NERC a government agency or is that a commercial industrial thing for the electrical world?

MR. WARNER: So, NERC is the North American Electric Reliability Corporation.

MEMBER BROWN: Right.

MR. WARNER: They are a non-government entity that has been ceded authority for developing standards and regulatory authority for power plants by FERC.

MEMBER BROWN: When you say ceded?

MR. WARNER: So, basically FERC has authorized them to act on their behalf with the development of reliability standards and enforcement.

MEMBER BROWN: Can they do that independent of keeping back -- I've looked at this grouping of three different organizations and how does anything ever get done?

MR. CINTRON-RIVERA: So, this is Jorge Cintron. So, FERC provides oversight over NERC. Pretty much NERC develops the reliability standards that are able to ensure they are able to meet the regulations for FERC. So, they do provide inspections of the reliability of the grid.

MEMBER BROWN: Do they have to get FERC approval for what they're doing or can they, do they have the ability to take action with the industry in terms of utilities, grip support, all that type of stuff, or are they -- is there a leash? They always have to come back, well, we want, we're going to be doing this? We need -- that's a firefight. I mean, people that run electrical stuff ought to be able to fix things.

MR. CINTRON-RIVERA: My understanding is that they have to go through FERC. Singh Matharu is on the line, I don't know if he has more information on that, but FERC has the oversight over NERC in these aspects.

MEMBER BROWN: So, NERC only has a limited, when you say ceded, they only have a limited amount of things they can do independently based on what is in whatever this memorandum of agreement is or whatever document that's been signed. Is that correct? Is there a document that cedes that?

MR. CINTRON-RIVERA: I can double-check that. I don't know. Singh Matharu, are you on the line?

MR. MATHARU: Yes, good morning. My name is Singh Matharu. I'm in the electrical branch and I've been coordinating our efforts with NERC and FERC for a long time.

So, to answer your question in a simple manner, I think it would be easy to compare how the standards' committees for nuclear power plants like IEEE write standards and then the NRC issues a reg guide that either takes exceptions or approves the standards and says this meets our requirements and regulations.

There's a similar relationship between FERC and NERC where the FERC has the authority to issue what we would call regulations and NERC would write the corresponding standard to meet the regulation. Does that help?

MEMBER BROWN: Okay, yeah, somewhat, but IEEE, they change their standards without getting approval from the NRC, but they then, the NRC then makes a decision as to whether they're going to adopt those standards. Is that --

MR. MATHARU: Correct.

MEMBER BROWN: -- the same?

MR. MATHARU: Correct.

MEMBER BROWN: So, NERC can develop standards on their own for doing things which can be followed by the utilities if they want to, but NERC can then incorporate them into their regulations. Is that -- that's kind of the way IEEE standards and --

MR. MATHARU: Correct, correct.

(Simultaneous speaking.)

MR. MATHARU: Very similar relationship, yes.

MEMBER BROWN: Okay, similar relationship, okay, so they are independent, but their standards are adopted or not adopted by NERC?

MR. MATHARU: Correct.

MEMBER BROWN: But industry can still use some of those standards if they want to?

MR. MATHARU: And NERC --

MEMBER BROWN: In areas where they have the authority to do it?

MR. MATHARU: Yes.

MEMBER BROWN: Okay, thank you. I'm sorry. I just had to get a handle on this.

MR. MATHARU: To give you an example, after the breakup of the electrical utilities, the nuclear power plants needed some assurance that the grid would be maintained in a certain manner as far as offsite power requirements would go.

So, FERC made the regulation and then NERC told the utilities and the independent power producers and the transmission systems how to maintain adequate wattage, frequency, whatever our requirements are to the levels that would satisfy the nuclear power plant.

MEMBER BROWN: Okay, thank you.

MR. WARNER: In November of 2012, NERC adopted CIP-002-5, which basically indicated how to identify and categorize bulk electric systems, cyber systems, and associated cyber assets based on the adverse impact that loss, compromise or misuse could have on the reliable operation of the bulk electric system.

Essentially, what that did is it kind of allotted a graded approach depending on some factors which we'll go into a little bit further down the line.

In 2022, the NRC approved for use revisions to NEI 10-04 and 13-10, which incorporated this graded approach in the latest versions of the NERC standards.

This approach uses a number of criteria, primarily the electrical output of a facility, to determine if they were low impact, which is an impact to the grade of 1,500 megawatts electric or less, or medium impact, which is greater than 1,500 megawatts electric, to the bulk electric system and the required cybersecurity controls that need to be applied.

MEMBER BROWN: So, excuse me again. Now,

to me, what that means is the grid is controlled external to the plants, okay. They put it out there. They either open or close the breakers. They adjust, you know, and then our plants respond as a normal generator would on a grid, okay, with all its reactive, real power, et cetera, et cetera, et cetera.

So, the operation then, the paralleling of our plants with the grid is controlled external to the plant? Is that -- am I saying that correctly, or is there an operator on the plant that then connects to the grid under the influence of the controls --

(Simultaneous speaking.)

MEMBER BROWN: I'm just trying to get that.

MR. CINTRON-RIVERA: Each nuclear power plant has their internal memorandums of understanding between the utility and the plant, so every activity, if there is a severe weather event, if there is maintenance of the lines, everything has to be coordinated between the utility and the plant.

So, each plant has their own agreement with the utility, the grid operator, to ensure that all of those activities don't affect either the grid or the operations of the power plant.

CHAIR HALNON: Charlie, you'll hear the

term TSO, transmission system operator.

MEMBER BROWN: Yeah.

CHAIR HALNON: And those agreements were forced, I don't want to say forced, they were -- during this period of time, they were put in place, and INPO got involved with it as well, to make sure that the TSO, utility, memorandums of understanding and agreements were memorialized in some document.

So, that's pretty established that the control room and TSO are in pretty frequent conversations about --

MEMBER BROWN: Okay.

CHAIR HALNON: -- power changes and stuff. I'm sorry, go ahead, Vicki.

MEMBER BIER: I have quick question. My understanding, which may be incorrect, is that the impact that a plant has on grid stability may not be entirely based on megawatts, but also kind of where it's located in the grid, and that, you know, certain locations may be vulnerable even if there's only a small amount of power generated at that location. Can you talk about whether or how that's taken into account?

MR. WARNER: So, I will say that some of the other considerations, I didn't list everything, one of them is basically the grid operator can come to a facility and say hey, because of condition X, Y, Z, we need you to run, and then in the case of nuclear plants, we're base load, so the anticipation is we're always running.

MEMBER BIER: Sure.

MR. WARNER: So, this may apply more to facilities that, for example, like in Texas, when they had issues with the freezing a couple of years ago, so that is one of the considerations that is taken into account when looking at the impact to the grid and how that impact what controls need to be applied to your components.

MEMBER BIER: But this categorization of low impact or high impact --

CHAIR HALNON: Vicki, your mic isn't on.

MEMBER BIER: Sorry, I thought I turned it on. The categorization of low impact or high impact is done ahead of time, correct, before there's an event, so some things that are identified as low impact early on because of megawatt rating may actually turn out to be high impact in the situations?

MR. WARNER: Yeah, when we were doing the reviews of the documentation, we had extensive interactions with FERC's Office of Electric

Reliability and that was a question that did come up. Is a licensee expected basically to increase their protections if suddenly they are bumped from low impact to medium impact due to some sort of exigent circumstances?

And in that case, basically, no, they don't have to apply the extra controls. For example, the letter I was kind of talking about, I believe, is a one-year time frame is as long as that can be in effect, and then theoretically, conditions have cleared up so that you can go back down.

And those circumstances are not typically used for, like, weather events because of just the immediacy of those, but are more established ahead of time on a longer time scale to address, like you said, maybe there's a power plant that's going through significant work and it's going to be out, so they need extra support on the grid.

MEMBER BROWN: Where are the grid operators located?

CHAIR HALNON: So, there's multiple --

MEMBER BROWN: I know there's got to be multiple --

CHAIR HALNON: Yes.

MEMBER BROWN: -- because we've got a

number of grid --

CHAIR HALNON: Right.

MEMBER BROWN: -- agencies, not only the connect, or disconnect, or what have you. I understand there's not a cohesive, totally cohesive setup. So, they're in different -- they're not in the plants is all I'm saying.

CHAIR HALNON: No.

MEMBER BROWN: They're in separate locations and they control the general interactions, the interface with other grids --

CHAIR HALNON: Right.

MEMBER BROWN: -- they interact with, et cetera. My next question is because I'm ignorant on this, all right? I come from the Naval side of the thing and we tended to operate our electric plants independently, so that the generators were not parallel just because we don't want them both to go away due to sudden power shifts.

And it's not the load. It can be reactive current where all of a sudden, you overload something, you overheat stuff, and you trip everything. That's not a good idea for a submarine when they're in the water somewhere.

So, aircraft carriers are a little bit

different. They do stuff differently. So, how does that control of the general excitation systems in the plant and its interface with the grid get controlled? Is that done by the, what do you call it, the transmission, the local operator in the plant? Do they get told what to do?

CHAIR HALNON: Yes, the TSO will call the plant and say I need more bars, less bars, I need --

MEMBER BROWN: Okay, so there is a direct control back with the excitation control for --

CHAIR HALNON: Correct.

MEMBER BROWN: -- the connection to the grid.

CHAIR HALNON: Yeah, and the nuclear plants are pretty autonomous because of the potential impact on the reactor core and reactivity. They won't let anyone offsite control reactivity, so that's why they have the telephone.

MEMBER BROWN: Yeah, I love that.

CHAIR HALNON: A telephone call is necessary. That may not be the same for a gas plant that's on the TSO control.

MEMBER BROWN: So, if you have a giant outage where you lose a whole -- I mean, you hear about blackouts. Many of those are driven by overloading not necessarily the power side, but it could be reactive current drains and what it's doing to the systems and the trip systems.

So, is that still when those suddenly happen? I take it there's a lot of communication with those that in bulk power. Is that correct?

CHAIR HALNON: Yeah.

MR. MATHARU: This is Singh if I may help with that answer.

MEMBER BROWN: Okay.

MR. MATHARU: So, what you're essentially asking is a twofold question. The external entity, which is the TSO, does not have any control over the real or the reactive power that's generated by a nuclear power plant.

MEMBER BROWN: Okay, that's what I thought, so they've got to communicate.

MR. MATHARU: So, they've got to communicate, number one. Number two, part of our regulation, NRC regulation requires the offsite source to be capable of supporting safe shutdown of the plant.

So, the operability of the offsite source is dependent on the strength of the grid and the voltage that's maintained at the switchyard, and as you know, voltage is a function of the reactive power.

MEMBER BROWN: Yes.

MR. MATHARU: So, one of the requirements that we at the NRC impose on plant operators and they in turn impose it on what we call the TSO would be that the nuclear power plant does not support the grid because if the nuclear power plant were to trip, then the offsite source would not be adequate to support safe shutdown.

MEMBER BROWN: Got it.

MR. MATHARU: So, using that logic, we, at least the plant operators maintain minimum reactive power output or the minimum supports that are required for the grid.

So, we rely on the TSO to ensure that upon loss of a nuclear power plant, the reactive power and the real power demand will not adversely or I should say impact the grid such that it will not be able to support safe shutdown.

MEMBER BROWN: Okay, so then the plant then becomes dependent upon its onsite emergency power sources?

MR. MATHARU: Correct, we want to get them on the backup plan, yes.

CHAIR HALNON: Yeah, in those agreements, there's pretty strict voltage requirements, frequency requirements.

MR. MATHARU: Correct.

MEMBER BROWN: That was a good answer. That was a good clarification. I was wondering who controlled the reactive component to this stuff, and so we do it internally on our plants --

MR. MATHARU: If we do it internally --

MEMBER BROWN: -- so we're not a grid -- recognizing we need the grid to shut down the plant properly and in a stable manner.

MR. MATHARU: Correct.

MEMBER BROWN: Okay.

(Simultaneous speaking.)

MR. MATHARU: Just to elaborate a little bit more, we had an event back in, I think it was circa 1995, where there was, in the summertime, there was an excessive transfer of power from one -- to the other, and in the middle of that was our Callaway Nuclear Power Plant and Callaway was supporting the midpoint of that transmission system.

And we realized once the TSO did some studies and they figured that if Callaway were to trip, then the offsite source would not be operable as such, so we wrote information orders that clarified our position on that.

MEMBER BROWN: Really complex. Okay, thank you very much.

MR. MATHARU: Sure.

CHAIR HALNON: My question was in the first two bullets, there's a decade between the adoption of CIP-002 and NRC's endorsement of 10.04. During that time period, were we in an approving time frame using basically the concepts and making sure that that's what you wanted or was it --

MR. WARNER: So, everything that was in place at the time was really the basic versions of the documents that were issued when we first were addressing these concerns.

The reason I brought this up is basically saying that things kind of changed in how they're assessing what controls need to be applied in the interim between then and when we made revisions to guidance, and in that time frame, we wanted to ensure that we adopted the same approach so that we're protecting the bounds at play.

Because while we are taking regulatory authority for those bounds at play and assets, we're still trying to maintain at least the protections that FERC requires for similar facilities are non-nuclear.

So, that was kind of the point of that, is that we're adopting this new approach to be in line with the current revisions of the NERC CIP standards.

CHAIR HALNON: Okay, thanks. Any other questions? All right, let's roll on.

MR. WARNER: And then just, I've kind of already covered it a little bit, but I'm just saying that when we were doing the review of these documentation changes, we coordinated with FERC's Office of Electrical Reliability to ensure that the changes we made were consistent with the latest NERC CIP documents.

And then kind of giving a brief overview of the controls, and again, these are the ones that were in place when we first started doing the review, there has been a little bit of an addition and I'll cover that in a later side.

So, CIP reliability standard 003-7 defines the cybersecurity controls to be applied to bulk electric system cyber systems for lower impact CDAs, and here at the nuclear plants, they're being referred to as BOP CDAs.

They would need cybersecurity awareness, which is essentially training, physical security controls, electronic access controls, cybersecurity incident response, transient cyber asset, removable media, and malicious code risk mitigation, which is PMMD in the nuclear space, and then declaring and responding to CIP exceptional circumstances.

And then for medium impact controls, and I will say for medium impact CDAs, these will be called BOP-SCRAM/TRIP CDAs, there are not any CDAs currently identified as medium impact at nuclear power plants.

These would have the baseline cybersecurity controls that we discussed in the previous presentation that would basically apply to BOP and indirects.

Similar to the beginning, it has the personnel training, electronic security perimeters, physical security controls, system security management, incident response and response training, recovery plans, configuration management, information protection, and again, that declaring responding to CIP exceptional circumstances.

CHAIR HALNON: I was curious that you said there's nothing, no medium impact at NPPs, but our previous discussion just talked about voltage and frequency controls on the grid, which indirectly, if not directly, can trip.

MR. WARNER: So, all of the additional potential categories that would apply to NPPs don't apply as far as the letters saying they have to run and all of that stuff. So, really the criteria we're looking at for nuclear power plants is whether they meet that 1,500 megawatt electric threshold.

There is no single unit at a U.S. nuclear site currently that operates at greater than 1,500 megawatts electric, so the only potential medium impact CDAs we are thinking that we will see -- this is still fairly new, so a lot of plants haven't even started trying to implement this guidance.

We would basically think that maybe if there's a common system between two units, that could potentially trip both units offline, but the odds of finding that are pretty slim because that's not something you'd want to have happen at your plant.

CHAIR HALNON: Yeah, so the 1,500 megawatts is more geared towards maintaining grid integrity than it is a plant staying online --

(Simultaneous speaking.)

MR. WARNER: Correct, my understanding is --

CHAIR HALNON: The nuclear power plant, we're worried about staying online or at least a controlled shutdown.

MR. WARNER: Yeah, and my understanding is that requirement really is based on how much swing capacity they have on the grid to be able to bring online, because there's a stipulation that the actual reading is a loss of 1,500 megawatts electric within 15 minutes.

So, if it's somehow over a longer time frame, they can easily bring enough swing capacity to cover that loss, so.

CHAIR HALNON: Okay, so that spending reserve is what --

MR. WARNER: Right.

CHAIR HALNON: -- depending on -- when we had the polar freeze way back when, the spending reserve was basically not there, much less than the ten percent they like to have on there. They have to have at least ten percent spending reserve. Okay, so it comes down very specific to the plant versus the operators' --

MR. WARNER: Yeah.

CHAIR HALNON: -- ability to keep the grid up and at frequency and voltage.

MR. WARNER: Correct.

CHAIR HALNON: Okay.

MEMBER BROWN: That's the grid operators.

CHAIR HALNON: Grid operators, sorry.

MEMBER BROWN: I want to fix my understanding of something you said a minute ago. Our plants, the nuclear plants fundamentally supply our, but not reactive current control. Somebody said something like that, but yet the generator operates at some power factor like 0.8 or what have you so you can't overload it, so who controls --

I mean, the loads are the loads. The grid wants power, but it also has to deal with reactive currents which are controlled by the excitation from our generator based on the regulators, voltage regulators.

MR. WARNER: So, I'll take a crack at this. Please feel free to chime in.

MEMBER BROWN: Well, let me --

MR. WARNER: Sorry.

MEMBER BROWN: Let me finish my thought.

MR. WARNER: Sorry.

MEMBER BROWN: No, I think I -- this is another, since we don't really control grid reactive current control. We've got about 20 percent of the normal power that's required in the country, volt power that's required. There's another 80 percent that's controlled by gas, coal, oil, whatever we've got. So, somebody else is taking care of the reactive current on the overall grid.

If you had 500 plants, then we would have to be part of the reactive control. Is that a correct assumption? But if we were nuclear islands where we could do that, it would be okay, but we're not nuclear islands in most circumstances. We depend on the grid to shut the plant down if we lose the generator.

MR. WARNER: And that is my understanding. Basically, because we're base load --

MEMBER BROWN: Yeah, but the power base load, but you --

MR. WARNER: Right.

MEMBER BROWN: The generator has some reactive -- it's supplying reactive current --

MR. WARNER: Right.

MEMBER BROWN: -- to meet its generative requirements. You just can't be all of one and nothing of the other. That's not good for the generator.

MR. WARNER: Right, and my understanding is basically, and when I say basically, like your -- power plants, nuclear power plants are always just producing the same amount, both regular power and reactive power.

MEMBER BROWN: Right.

MR. WARNER: And then everything else on the grid, which can be spun up much quicker and it doesn't have an impact on the reactivity of the core, is used to kind of balance everything else out.

CHAIR HALNON: Charlie, it's not unusual for a system operator to ask a nuclear plant to change reactive power.

MEMBER BROWN: No, I understand that.

CHAIR HALNON: But they have the strict curves they stay within, the generator curves.

MEMBER BROWN: I got that. I was just trying to get a better understanding of the connectivity of the overall control relative to the offsite.

They're the ones that are controlling other assets that are providing that basic reactive current control, but they are also controlling the switchyard circuits and stuff, and that's where the cyber issue comes in relative to the controls also.

I assume that's part of this whole thing we're looking at and you certainly don't want -- I mean, there are other folks other than our guys are controlling the switchyard, is that correct?

MR. WARNER: Yeah, I mean, we have everything within the first inner tie of the grid is our responsibility and everything outside then falls under --

(Simultaneous speaking.)

MEMBER BROWN: Once our breaker is closed, that's our connection.

MR. WARNER: Yes.

MEMBER BROWN: There's a lot of other breakers out there that can get operated and my concern is their impact on our plants if they get tripped off in the wrong way and screw up the ability to take care of our plants. That's what I was -- that's my cyber issue that I haven't really --

(Simultaneous speaking.)

CHAIR HALNON: That's exactly the interface that we're trying to explore.

MEMBER BROWN: Yeah, okay, and that's -- okay, now that's what I'm looking for and that's the kind of --

CHAIR HALNON: Okay, Charlie's caught up.

MEMBER BROWN: Pardon?

CHAIR HALNON: Charlie's caught up.

MEMBER BROWN: I'm finally caught up. Thank you.

MR. WARNER: So, I just want to emphasize, so when the rule first came out, the bounds of play in assets were not determined to be within scope of NRC regulatory authority because they were not part of safety, security, emergency preparedness, important to safety.

So, that is -- obviously, we do know that those bounds of play in assets can impact reactivity, but when it comes down to it, you don't need them to safely shut down the facility and keep it safety shut down.

So, when we're looking at what we're doing as far as bounds of play in digital assets is we're basically trying to maintain what FERC is doing to protect those assets and ensure grid stability is maintained.

So, and you'll see that even though, if we look at the low impact we looked at, like nuclear power plants exceed what is currently required, and in fact, in the next slide, I'm going to discuss how a new requirement came out that we actually already have determined that we addressed, so we can go to the next slide. Thank you.

So, NERC CIP-003-9 came out recently. It was recently released and it includes an additional control for low-impact facilities. So, we were aware when we were doing the review that there was new guidance that was going to be coming down the pike from our interactions with FERC.

So, we reviewed the document changes and determined what changed from the previous version that's currently incorporated in our guidance and if it impacts bounds of play at CDAs.

So, there's an additional control specific to low-impact power generation facilities which requires facilities to implement vendor electronic mode access security controls.

When we were interacting with FERC during the review process, they also mentioned the only incidents they were seeing were on low-impact facilities.

And as we've seen from a lot of the different attacks that have been publicized lately, especially on like water infrastructure and those kind of things, a lot of it people just using that vendor remote access and being able to get in, whether they got credentials from somebody or were able to find a vulnerability they were able to use to access it.

So, we reviewed the controls that are current in the latest version of NEI 13-10, Rev. 7, and there's already a requirement in there for these low-impact CDAs that they have electronic access controls either air-gapped or isolated by a deterministic device.

So, in that case, even if there is a vendor remote access that should be disabled, there is no pathway to get there, so we've already determined that that control has been addressed and no guidance changes need to be implemented to incorporate the latest version of CIP-003.

MEMBER BROWN: So, the electronic devices that are actuating switchyard devices for whatever purposes are air-gapped or isolated so they can't get into our electric system and then somehow get back into our safety systems or safety-related systems?

MR. WARNER: That is correct. And based on what's required in the document, they need to have physical security controls. If they're out in the switchyard, they need to be protected by physical controls. They need to have --

MEMBER BROWN: Electronic.

MR. WARNER: -- electronic controls. They need to have this isolation behind some sort of device. So, they may be connected to other devices within the plant itself, but then they're subject to all of the same security requirements needed for those types of CDAs.

All right, so this is a busy slide, but this is the one we use and I kind of like it. So, basically, what I wanted to go over here is the various federal agencies that kind of have a touch point to the different aspects of cybersecurity at a nuclear plant and kind of where those roles reside.

Brian will give more detail later, but we'll start with the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency. They are the sector risk management agency for nuclear plants.

They lead the national effort to understand and manage cyber and physical risks to the U.S. critical infrastructure, and that responsibility includes communicating threats, vulnerabilities, and to provide instant response services for that U.S. critical infrastructure.

And we would interface with CISA during a significant cyber event at an NPP licensee. I have an example later on where we talk about the Cyber Assessment Team that will kind of go over that a little bit.

The Department of Energy are responsible for advancing the energy, environmental, and nuclear security of the U.S. The Office of Cybersecurity, Energy Security, and Emergency Response, you'll typically hear that as DOE CESER, is the lead for the DOE's emergency preparedness and coordinating responses to disruptions to the energy sector, including cyberattacks, and the NRC would interface with DOE during a significant cyber incident at a nuclear power plant.

Then, of course, we have FERC, the Federal Energy Regulatory Commission. They regulate the interstate transmission of electricity, natural gas, and oil. They have an MOA between us and FERC that facilitates interaction on matters pertaining to nuclear power plant cybersecurity, and we coordinate activities regarding nuclear power plant cybersecurity such as what we did with reviewing the new guidance changes that are being implemented.

And then we have the Nuclear Regulatory Commission. We have oversight in nuclear reactors. We perform cybersecurity inspections at power plants and then we coordinate with other federal agencies as needed on matters pertaining to nuclear power plant cybersecurity.

So, I'm going on a little bit about the

agency's Cyber Assessment Team. I am the Cyber Assessment Team lead for the agency. So, the CAT is a team of headquarters and regional cyber experts that activates in response to cyber events at NRC licensees.

So, we have NSIR cybersecurity staff, headquarters subject matter experts, and we have regional cybersecurity inspectors that are part of the team.

We evaluate cyber events at licensees, primarily power reactors, and we assess the severity of the event and provide recommendations to agency leadership, and we also assist in internal coordination between headquarters and the regions.

CHAIR HALNON: Dan, how many events do you guys screen on a regular basis? I mean, pick a time period.

MR. WARNER: So, the -- and actually, we'll go into this in a couple of slides, but, so the CAT typically activates in response to any reports that are made under 10 CFR 73.77. Those reports would go to the WHO, and then when they feed to us, to me, then I determine what we need to do as far as activation.

There has never been an incident report

under 73.77 since it was issued in 2015, so the CAT has never officially activated other than to primarily address non-licensee regulated systems, typically licensee business systems. In that case, it's mostly just ensuring that management is aware of what's going on.

CHAIR HALNON: How often do you drill?

MR. WARNER: I've been the CAT lead for over a year and I haven't because the nature of a cyberattack is such that any incident response that would start and activate the ops center won't be identified as a cyberattack until weeks after the incident is addressed.

So, in the actual CAT, like the SME cybersecurity portion of the response has been removed, so ops center and the team there would deal with the issue and make sure the physical consequences of something are dealt with, and then once it's determined to be a cyberattack, that's when we would be brought in, but like I said, that really probably wouldn't be identified until weeks later.

CHAIR HALNON: Okay, so you're looking at a very discrete event that's sort of underneath the radar because the physical impact is more important to establish a stable shutdown plant?

MR. WARNER: Correct, the ops center activates to make sure the plant gets into a safe position and stays there, and then once the forensics start getting on and figuring out what actually happened, then we'd be called.

CHAIR HALNON: So, there's no scenario that you can come up with that would require at least a parallel, after an incident or during, while the incident --

Because, I mean, just take something we know the most about is Three Mile Island took several days to get to the point where we were okay with it from a stability standpoint. You don't see any scenario that that aspect needs to be drilled through the parallel interactions?

MR. WARNER: In that case, I could see us being kind of brought in and brought up to speed if there was some sort of evidence that seemed to indicate that a cyberattack might have been responsible.

CHAIR HALNON: Okay.

MR. WARNER: But even in that case, it would really be awareness, because until we are actually notified that something happened, we can't really act on it. We do have site assessment teams that can go out and help with that, and we're obviously more than willing to provide that assistance if it comes up, but --

CHAIR HALNON: Okay.

MR. WARNER: Yeah.

MEMBER MARCH-LEUBA: So, the CAT will be involved in the postmortem if something like this happens, in analysis of root causes and --

MR. WARNER: Yeah, once we get to a point where they have a reasonable assurance that there is a cyberattack involved, and then any reporting that's made. There has not been an incident on a licensee, NRC regulated system. Everything we've seen, and again, we'll kind of go on it later, has been on the business side.

(Simultaneous speaking.)

MEMBER MARCH-LEUBA: Most people -- Walt, wait a moment. Most people think of cyberattacks as millisecond response, and what I read is that when bad guys penetrate a corporation, on average, they're there for 90 days before they get discovered, so that's where the CAT would come to figure out why they got there and did we get rid of them? Walt wants to go.

CHAIR HALNON: I think Brian was going to jump in there.

MR. YIP: Yeah, this is Brian Yip, if I could just add to that. Looking at the agency's incident response program, we used to have a construct where, on the security team, you would have physical security experts and then also a single cybersecurity expert that would sit on that team.

What we did in the past couple of years working with the Division of Preparedness and Response was instead set up all of the incident response procedures where -- you know, as Dan mentioned, the first indication that something's wrong is going to manifest physically most likely.

So, while the incident response organization is addressing the actual incident onsite, if they have indications that the incident is cyber related, it's built into their procedures to activate the CAT and the CAT would serve as an advisor to them and work in parallel so that we could address the cyber issues as soon as they're identified in coordination with the actual incident response.

CHAIR HALNON: Thank you. Walter?

MEMBER KIRCHNER: Thank you, Greg. I was going to follow up on your question.

Dan, do you -- does the CAT team look at other incidents perhaps not at nuclear plants and just do kind of an assessment of potential vulnerabilities or that -- or reflect on your own programs based on those incidents? And if that's the case, have you made any changes to your guidance as a result of some of the more recent events, whether it's the aquarium or the clean water system in Florida, or any of those attacks? Have you assessed those and then made any changes to your program?

MR. WARNER: So we're on a number of distributions such as like FireEye, which I think has changed to a different name at this point. And then like E-ISAC when they're basically reporting events that are out there, vulnerabilities. So we are looking at those and kind of keeping an eye on things.

In the grand scheme of things the NRC and nuclear power plants are well ahead of the rest of critical infrastructure as far as cybersecurity --

Ryan, chime in if I'm speaking wrong -- part of that being because we've had regulatory authority since 2009 to enforce cybersecurity protections where a lot of the other critical infrastructure just don't have the authority to force people to do things.

And so in a lot of these cases we look at things, but because of the architecture, because of defense-in-depth and the way things are required, most cases we don't have to worry. We're covered.

And, Ryan?

MR. BECHTEL: Yes, I'll just add that --

MEMBER MARCH-LEUBA: Say your name for the record.

MR. BECHTEL: Oh, this is Ryan Bechtel from DHS/CISA. Yes, I'll just add an echo to that that the nuclear sector is pretty unique amongst the 16 critical infrastructure sectors in that it is so well and heavily regulated. There are some sectors that just simply don't have anything resembling a regulatory structure that is seen here. So a lot of nuclear tends to be the one that detects things first amongst these sectors.

MEMBER KIRCHNER: Thank you.

MR. WARNER: So I mean stole my thunder a little bit, but we'll go over the slides anyways.

So CAT is primarily activated by the Ops Center in response to a licensee event, or it's under 10 CFR 73.77. Any reportable cyber event under 73.77(a) will trigger a notification to myself as the CAT lead. There have been no 73.77 reports since the rule took event in 2015. There have been incidents that have been on non-regulated licensee systems such as corporate networks, but a CAT was not activated in part due to privacy concerns.

Management, the CAT lead, or regional staff can request the activation of the CAT based on the information received from or about a licensee or other industry cyber event, and we have activated to leverage the process to assess non-licensee cyber events.

And I think our next slide, if we could go to it, kind of covers that. So this is based on a real event. So I as the CAT lead was notified of an incident involving the licensee's business network and what is speculated maybe as a ransomware attack or some sort of exfiltration of data.

I determined if the incident would have an impact on NRC-regulated systems. If not, then no further activation is needed. I'll work with the chief of the Cybersecurity Branch. We determine if any briefing documents for management need to be prepared and if there's any courtesy notifications that needed to be made to DHS/CISA.

If CISA notification is needed, contact is made with the nuclear sector risk management agency and the threat hunting groups to ensure awareness and provide points of contact for any necessary follow up.

And basically this is the chain of events that happened with a recent event. We made sure that CISA was aware since it was not on an NRC-regulated system and had impact for potential multiple licensees. We wanted to at least ensure that they were aware and this wasn't going to come as a surprise.

DR. BLEY: This is Dennis Bley. This is a minor point. On your last exfiltration, that seems an odd word to me. Usually that's -- we exfiltrate our troops or something or we get the data to go away. You really mean just taking data from the place that's been attacked, right?

MR. WARNER: Correct. Basically it's somebody going in, taking data, and --

DR. BLEY: Okay.

MR. WARNER: -- pulling it out for whatever use.

DR. BLEY: Maybe I'm thinking more sinister here.

MR. WARNER: And then just to kind of wrap things up, talking about more coordination. So the DHS Threat Hunting Group has been receiving some NRC training. Staff are working with staff from the DHS Cybersecurity Division's Threat Hunting Team. They are responsible for responding to cybersecurity incidents at critical infrastructure facilities and want to help familiarize them of nuclear technology.

They went down to the TTC down in Chattanooga, which is our technical training center, and they attended a course of R-105, which is nuclear technology for security. Essentially a streamlined version that gives all the highlights, but not a lot of in-depth into physics and how reactors work and all that fun stuff.

And then the same team will be visiting Millstone just trying to get familiar with the licensee facility. And they will also be participating in a short class on radiation protection later this year. That's all I got.

CHAIR HALNON: Does anyone have any further follow up or questions?

Okay. Jorge, I think you're up.

MR. CINTRON-RIVERA: Good morning. Can you pull up the slides for --

CHAIR HALNON: My sense is we've talked around your presentation quite a bit. And once you get we up -- well, once people see words on a screen, they tend to come up with new questions.

MR. CINTRON-RIVERA: Well, good morning. My name is Jorge Cintron-Rivera. I work for the Office of Nuclear Reactor Regulations, the Division of Engineering and External Hazards in the Long Term Operations and Modernization Branch. Along with me is Singh Matharu. He's a senior electrical engineer, previous point of contact for NRC and NERC coordinations. And also joining me as well is Kenneth See. He is the dam safety inspector officer in case that we have any questions regarding to the safety inspector program. And today I will be talking to you about the NRC coordination with FERC and NERC.

Next slide, please? Just an outline for the presentation. I will provide some purpose and objectives of the presentation, the background, some background information about how we develop some of the documents that we have in place for communications between the NRC, FERC, and NERC. We will talk a little bit about the NRC and FERC requirements and standards, a common interest, interagency agreements and interactions, multiple of them like a Memorandum of Understanding, the MOA, and the IEA between NRC and FERC regarding safety inspection. We will also cover NRC and FERC's jurisdiction boundaries and we will provide some scenarios of coordinations that we have had during the -- between agencies.

Next slide, please? So the purpose of our objectives is to provide a briefing to the ACRS on the governmental interactions for protecting the grid and power conversion. We will need to familiarize with the agreements that we have in place between NRC and FERC and NERC to facilitate communications between agencies. We will discuss the comparative roles between the NRC, FERC, and NERC and discuss the jurisdictions for each agency to protect the grid.

Next slide? Some background information. The NRC, FERC, and NERC provides regulatory oversight of protecting the grid. The most significant event that influence the level of NRC and FERC coordination occur in August 14, 2003 station blackout. This event has been the largest powers outage in U.S. history occurred in Northeastern United States and parts of Canada.

Approximately 500 generating units experienced shutdown that day including nine U.S. nuclear power plants and seven Canadian nuclear power plants. Nine of those U.S. nuclear power plants experience reactor trips all happening within 1 minute and 23 seconds of the event. The time to the full power was available again to the U.S. nuclear power plant stations ranged from one to six-and-a-half hours. This power outage affected 50 million people in the United States and Canada. This experience highlights the need for formal agreements between the NRC and FERC to ensure that there is sufficient communications or coordinations.

So therefore this pretty much event triggered the development of multiple MOUs and MOAs to facilitate the coordination between agencies. Each agency agreements has established the roles and responsibilities for each agency and provide guidance for the cooperative work through the events of multiple interests.

Next slide, please?

CHAIR HALNON: Jorge, that event was -- now we're 20 years into it. And obviously the energy of the organizations to get together and figure it out right after those types of events are both internally and externally induced to the point where there's a fervor of activity. What gives us confidence that that level of MOU and level of cooperation is still the same level of intensity, if you will, given today's environment 20 years later?

MR. CINTRON-RIVERA: So in terms of ensuring we revise those documents certain amount of time now is I think every five years. We do engage in communication with FERC and NERC with different topics during the year depending of some of the topics -- but, we do have communications between both agencies and right now mostly we try to ensure that what we have there is sufficient and if we need more information.

I understand that, yes, it might seems to be more like a reactive instead of active, but we -- after the Texas weather event I think we have engaged more communication, talking to the regions and talking with FERC to ensure that we are in constant communication. As recently -- last year I think we did a workshop to ensure that each agency knows their roles and responsibilities. The staff as well. And also we have invited FERC as well to talk about us about their activities that they're doing related to -- of common interest.

CHAIR HALNON: Okay. And I think there's an annual NRC commissioner meeting as well, too, that --

(Simultaneous speaking.)

MR. CINTRON-RIVERA: Correct.

CHAIR HALNON: -- a touch point to make sure --

(Simultaneous speaking.)

MR. CINTRON-RIVERA: It's usually biennial. We had it last year, but then because of the COVID the schedules were a little bit shifted. So we're having it as well. It should be -- we are working right now in the development of the setting of the date with both commissions. And even it's going to be this October.

CHAIR HALNON: Okay. So but typically it's biennial?

MR. CINTRON-RIVERA: Biennial.

CHAIR HALNON: Okay.

MR. CINTRON-RIVERA: Correct.

CHAIR HALNON: Thanks.

MR. CINTRON-RIVERA: So NRC and FERC common interest. The NRC and FERC have multiple interests related to the nation's electrical power grid reliability, nuclear power plant safety and security. In summary, the NRC evaluates the design, operation of nuclear power plants and electrical power grid systems. FERC regulates the interstate transmission of electricity and focus on the reliability, integrity, security, and operation of the electrical power grid.

FERC also provides oversight on -- of NERC. NERC's mission is to assure that the effectiveness and efficiency of the risk and the reliability of the security -- the grid is maintained and develops and enforce reliability standards -- not only assess the system on long-term reliability and monitors that both power systems through the systems awareness and educates, train and certify industry personnel.

Next slide, please? Requirements of standards for protecting the grid. The NRC evaluates the design and operation of nuclear power plants and electrical power grid systems. Some of the requirements that we have in place for electrical systems is General Design Criteria 17 which requires that -- to maintain at least to independent circuits from the off-site. 10 CFR 50.65 requiring for monitoring and effective maintenance of nuclear power plants. And we also have tech specs in place for limited conditions of operations in case there is an issue with the grid or a plant as well.

And we also issued the United Letter 2006-02 and which is the agreement reliability and impact on plant risk and reliability of the off-site power plants.

FERC regulates the interstate transmission of electricity. It focus on the reliability, integrity, and security of operation of the bulk of power systems and provides oversight over NERC. And there's been some for sure the effectiveness for those shown on the risk and liability. Develop the standards on risk and long-term reliability and monitors the bulk power awareness.

CHAIR HALNON: How does NERC enforce reliability standards?

MR. CINTRON-RIVERA: So they have the power to provide inspections of the grid to ensure that each of the TSOs are meeting their reliability standards. And those are coordinated between FERC and NERC.

CHAIR HALNON: So they have an inspection branch as well as a standards development --

(Simultaneous speaking.)

MR. CINTRON-RIVERA: Yes, mostly concentrated on security and protection of the systems.

CHAIR HALNON: Okay. Thanks.

Walt?

MEMBER KIRCHNER: Yes, I have a similar question, Greg, on reliability.

Overall robustness of the grid across the nation to a large extent depends on stemming reserves. As we retire coal plants, for good reasons related to climate, we've taken a lot of the hardware or spinning reserves so to speak and hence robustness of the grid. How does NERC deal with the evolving composite parts? We're probably going to get for example less energy out of hydro with the impact of climate change, especially out in the West where I am, et cetera. There's reliability kind of on a piece/part level and then there's reliability and robustness at a much more national level going back to -- your Northeast blackout slide is a good example.

So how does NERC's mission deal with that aspect of maintaining the overall robustness and reliability of the grid?

MR. CINTRON-RIVERA: So -- and, Singh, feel free jump in if I miss something, but as part of the requirements under -- or the development of the reliability standards that they have each individual TSO or ISO has to pretty much predict pretty much what are the -- what are going to be the lows for each day and any work or issue that is affecting the grid. So therefore they usually have a estimate of reserve that they have in place. If the reserve are -- grows not be in -- within the limits of the standards, they have to enter in communications with the operators to ensure that there is no issues between the reserve of the power systems.

So again, it falls more on the -- each of the TSOs to ensure that there is enough capacity and there is enough reserve to provide during the operations of each day. And we -- previously we used to issue a report every day of providing that information on if there's going to be -- how many reserve each of the TSOs have. We look in if there was any sonar -- solar storms that could affect the grid, all -- we used to do a report every day, but because not many people in the agency were -- we were not using it as much. We just rely right now on the TSOs to ensure that they provide the informations and communicate with each of the nuclear power plants in case there is not enough reserves.

MR. MATHARU: Yes, this is Singh, Walt. We don't have a good answer for you, let's put it this way. The question is very valid. What we are doing on the grid is two things: Like he said, we are retiring some of the base load coal plants that we had. In addition to that, we are now adding renewables like wind power, which are not very reliable either as far as maintaining grid frequency because depending on the circumstances we could lose a lot of generation.

The other challenge was after the breakup of the monopolies that the utilities had the intent of every TSO was to maximize their progress. So the spinning reserves, as you know, cost money and nobody's paying for them, as such. So we lost a lot of reserve power that was just running as a spinning reserve. So NERC and FERC have a challenge to meet what you're asking, which is long-term planning of how we're going to maintain reactor power especially during challenging times.

But so far, like Jorge said, we are managing. Going forward we don't have a good answer for you.

CHAIR HALNON: I would just add that a lot of the discussion surrounding the new reactors and the load-following capabilities of those are kind of based in this renewable aspect of, yes, high sun periods, high wind periods and whatnot. And all this is kind of factoring into their challenge of how do you manage this when you really are not in control of what kind of base load you're going to have, or what kind of base load generation you're going might have.

MR. MATHARU: Absolutely. In fact, there were a lot of proposals where the transmission system operators want to engage with controlling the nuclear power plants. And like we discussed earlier on, we were -- shied away from that.

MEMBER KIRCHNER: Thank you. It was a leading question and I knew would be a difficult answer.

CHAIR HALNON: Continue on, Jorge.

MR. CINTRON-RIVERA: So as I mention before, the NRC, FERC, and NERC, we have multiple agreements in place to ensure that all the information that we share is properly handled. Currently with NRC and FERC we have three agreements. We have one MOA for liabilities, cybersecurity, and physical security. We have the dam safety interagency agreement and the security coal energy electrical infrastructure information, or CEEII MOU. And also have NRC and NERC MOU for security and physical security.

Next slide? The reliability, cybersecurity, and physical MOA facilitates interaction between the NRC and FERC on matters of multiple interested related to the reliability of the nation electrical power grid, of the nuclear power plant safety and security. We added cybersecurity, physical protection, and emergency response. The document provides guidance for sharing operational events, information between the NRC and FERC and it provides a agreement to coordinate activities relating to cybersecurity and physical protection of share critical infrastructure assets including sharing of information on threats.

This MOU was issue as a response from the 2003 event and it has been recently revised in 2022. It will be active until 2027 unless there is a required change that triggers the revision of the document.

MEMBER MARCH-LEUBA: So there is sunset on the agreement on 2027, or that you plan to revise it?

MR. CINTRON-RIVERA: There is a termination clause in the agreement.

MEMBER MARCH-LEUBA: It's a sunset?

MR. CINTRON-RIVERA: Yes, which we also revised. Typically we used to go through a complete revision of the document, but sometimes also the information between -- coordination between both agencies is still -- doesn't change as much. So right now we have -- on 2027 if there is no changes needed to the document, what we will do is to issue a memo reissuing the previous MOA unless there is technical changes that we need to provide in the document. Then it will require a major change.

So typically we will start probably a year-and-a-half since it's a multiple-agency document. So they -- we pretty much -- we went through this exercise last year and we pretty much got the input from both agencies and then all the way to the --

(Simultaneous speaking.)

MEMBER MARCH-LEUBA: Certainly above our pay grade, but you have to renew this -- as the government shut down, one of these things that happen regularly, it is best to keep it operational --

(Simultaneous speaking.)

MR. CINTRON-RIVERA: So some of the -- like the dam MOA -- or IAA, sorry, it doesn't have a expiration date as well as the NERC/FERC MOU. Those are in place until change is needed for adding more information. As far as the CEII and the reliability one, there has always been a termination clause. So it might be something to consider as well later on for revisions.

The dam safety interagency agreement, it provide guidance to the NRC and FERC for implementing the NRC Dam Safety Program. Pretty much FERC assists the NRC by providing expertise to conduct inspections at dams. SECY-91-193 established the NRC Dam Safety Program Plan, which provides insurance of compliance of federal guidance for dam safety.

Currently there are eight dams that are under NRC jurisdiction. Seven of the dams are operating power reactors. One of the dams is a uranium recovery facility.

So typically there is a statement of work developed for the planning and implementation of the inspections of the safety dams, and that is handled by our colleagues on the Dam Safety Program following the IAA which was issue in 1992.

The CEII MOU is an agreement between the NRC and FERC to ensure safety and security of the electrical grid by protecting critical energy infrastructure or CEII structures.

The NRC staff responsible for national identifying information that maintains CEII and in consultation with CE -- FERC's, sorry, CEII coordinator. This MOU was issue in 2008 and it was as well as re-signed in 2022 for a five-year extension.

Finally, the cyber and physical security MOU between the NRC and FERC -- and NERC, sorry. It establish the roles and responsibilities between the NRC and NERC as they relate to the application of their respective cyber and physical security requirements for the protection of the assets in the U.S. nuclear power plants. It focus in the prevention of radiological sabotage and the reliability of the bulk of the power system.

The MOU establishes inspection protocols for each agency. Digital assets that can affect the safety and security and the emergency preparedness especially digital assets related to continued power. It provide guidance for sharing all information to carry out of the intent of the MOU and it was -- this MOU was revise in 2015.

CHAIR HALNON: Jorge, does this MOU eliminate or prevent overlap in inspections? I mean, is this the one that gave us the -- for lack of better term, the line between what NERC looks at and what the NRC looks it in a power plant?

MR. CINTRON-RIVERA: I don't believe it's the MOU. It was mostly -- and, Dan, you can elaborate on this.

MR. WARNER: Yes, I believe the MOA between NRC and FERC is what really divided that line and basically said, hey, you guys can regulate everything within that first intertie of the breaker at the NRC facilities.

CHAIR HALNON: Okay.

MR. CINTRON-RIVERA: This is just a pictorical background of how each agency interacts and along with each of the MOUs that we have in place. As you can see on the top, we have FERC and the NRC with three different agreements that we have in place as well as NERC. Then FERC provides the oversight over NERC. And then NERC implements the reliability standards over the utilities.

And this is what we were just talking about, the NRC and FERC jurisdictions. So this -- was revised last year to encompass all that information. So that's pretty much the line between the first breaker and the switch yard all the way to the grid. That's under FERC jurisdiction. And then from the first -- from that point to the plant is under both agency jurisdiction, however because of mutual agreement the -- both agencies have agreed that NRC will provide the oversight of those areas.

CHAIR HALNON: Back on the dam safety, that's less cyber and more physical dams, is that correct?

MR. CINTRON-RIVERA: I believe that's

correct.

CHAIR HALNON: And any cyber controls would be picked up by the NERC process downstream of -- because I mean, there certainly is a cyber element to operating a dam as well, especially a hydro, but --

MR. CINTRON-RIVERA: Yes, when we talk about that -- and, Kenneth, feel free to jump in -- when we talk about dams most of these dams that we are -- under our jurisdiction are because they are the ultimate heat sink of the plant. So therefore this is -- maybe it doesn't have to be hydro or -- but it -- because is of the ultimate heat sink, that's why we -- they're our jurisdiction. And then FERC is the one that provides assistance in performing those inspections.

CHAIR HALNON: Okay. How about Keowee and Oconee's emergency power system? I mean, that's very unique and special. Do you have any -- you know anything about how that coordination is taken care of?

MR. CINTRON-RIVERA: Kenneth, you're in the line?quality

MR. SEE: Yes, that -- Oconee is not one of the plants that we have in our Dam Safety Program. I think the list I have -- I can just rattle it off real quick, if you're interested.

So it's North Anna, Harris, McGuire, Catawba, V.C. Summer, Farley, and Comanche Peak, though you should understand Oconee has got a great deal of interest.

CHAIR HALNON: Those are the ultimate heat sink dams basically?

MR. SEE: Yes, if I had time I'd give a little presentation. To fall within the Dam Safety Program they have to basically be I'm just going to say an ultimate heat sink and they have to be of certain size or volume. Certainly there are a number of ultimate heat sink at nuclear power plants that are smaller than the criteria to be defined as a dam. So they are handled outside the Dam Safety Program, but they are inspected by the agency. So it's a little different.

CHAIR HALNON: Okay. And I would assume that the plant technical specifications would pick up where maintaining requirements and safety of the plant from the standpoint of levels of lakes and whatnot, just like at -- for instance V.C. Summer has a separate pond for their emergency cooling system ultimate heat sink.

MR. SEE: Yes, sir.

CHAIR HALNON: And that has a temperature and level requirement in the tech specs.

MR. SEE: Yes, there are tech specs that they have to meet. But you ask a very good question. I wrote this down earlier listening to the -- are there any cyber vulnerabilities to operating the gates, because they do allow water in and out of these ponds. Could there be a vulnerability there? That's a question that I will be asking this summer when we go out and conduct some inspections.

CHAIR HALNON: Okay. Yes, and it would -- certainly the physical -- that's -- you hit exactly where my question was leading was into the --

MEMBER KIRCHNER: Yes, Greg, that's an example that I was trying to raise earlier of an important to safety.

MR. SEE: Yes.

CHAIR HALNON: Yes, I think there's linkage that need to make sure were covered in the programs. Thanks, Ken.

MR. SEE: No problem.

MR. CINTRON-RIVERA: So NRC coordination with FERC and NERC. The NRC and FERC, the nuclear regulatory policy coordinations. NRC consults with FERC and NERC staff for transmission system status when nuclear power plant requests informant's discretion, for example. And we also exchange information of interest during accidents affecting the grid such as severe weather, dam safety inspection coordinations, and EMPs.

So some of these -- one example that we have that we recently engage in a lot of coordination between the NRC and FERC was the 2001 Texas weather -- cold weather event from -- it was unprecedent cold weather. Both of the sites remained safe during the degraded grid conditions. And for Comanche Peak the power plant shut down and proactively started on-site emergency diesel generators to ensure that there is no issues. And for South Texas Project 1 and 2 one of the safety shut downs due to a frozen instrumentation line.

MEMBER MARCH-LEUBA: So number one, this was not a cyber issue. This was a weather issue, right?

MR. CINTRON-RIVERA: It was a weather-related issue. I think was a winter storm that hit the area of Texas and pretty much --

MEMBER MARCH-LEUBA: Yes, we're all familiar with it.

MR. CINTRON-RIVERA: Okay.

MEMBER MARCH-LEUBA: I'm just making sure we're talking cyber here.

MR. CINTRON-RIVERA: Yes, most of my presentation is a broader -- not just specifically for --

MEMBER MARCH-LEUBA: So this event is a good driver and if it was a cyber issue. So did you guys got with FERC into the control -- the emergency operating center and monitoring the plant or were you on the phone continuously or did you talk a couple of weeks after the fact? How did it happen?

MR. CINTRON-RIVERA: From my perspective it was after the event --

MEMBER MARCH-LEUBA: Yes.

MR. CINTRON-RIVERA: -- when all the responses were issued. And then we pretty much assessed what happened and how we handle the event. And based on that we start communications with FERC to ensure us what will be the next actions in terms of the grid. The regional staff also contact us to asking some questions as well.

MEMBER MARCH-LEUBA: The plant themselves were mostly in contact with the region?

MR. CINTRON-RIVERA: Yes.

MEMBER MARCH-LEUBA: And FERC was an afterthought?

MR. CINTRON-RIVERA: So the regions contact us, let us know what was happening, their concerns of the event. And we start communications, me as a point of contact, which our -- my counterpart can pretty much establish communications such as the event and further actions that later on during the year, during the time period.

MEMBER MARCH-LEUBA: Yes, because I'm not a resident of Texas, but it could have one worse than the way it did. So are there any lesson learned on how we could have made it better or --

MR. CINTRON-RIVERA: So the FERC issued a report, recommendations, which are still -- we are soon going to be coordinating as well another meeting to ensure what's the status of the implementation of those coordinations. And, but yes, that -- as soon as the event happen FERC performs studies and issue a report. And it was communicated to us as well to -- two presentations in a workshop and later on for Region IV.

MEMBER MARCH-LEUBA: Yes.

MR. CINTRON-RIVERA: Some of the -- most of the recommendations are for the revision of these NERC standards to address cold weather events, pretty much will the critical infrastructure be able to support those. And there is also some recommendations that will be implemented later on that pretty much relates to the challenges that the grid presented that day, that -- during that winter event.

MEMBER MARCH-LEUBA: Okay.

MR. MATHARU: Yes, Jorge, this is Singh. If I may interject a little bit here.

MR. CINTRON-RIVERA: Sure.

MR. MATHARU: Couple of things: Number one, the region was in constant contact with the South Texas and Commanche Peak during the cold weather event from early because everybody was aware of the challenging grid conditions.

And I think the other question was the interaction between FERC and us and the plants. Texas is kind of unique because it's not controlled by FERC as such. It's not under their jurisdiction to a large extent. The grid is controlled by an entity called ERCOT. And they are an independent authority so they have their own guidelines and regulations.

There is a clause within FERC requirements that the ERCOT will try and maintain the voltage and frequency requirements as put in by the standards, but in essence ERCOT is an independent authority.

So we were negotiating between ERCOT, FERC, region, and the plant operators.

So to answer your question, yes, we were on site, but we were not really -- FERC was not really engaged as such during the event.

MEMBER MARCH-LEUBA: So I'm listening here. I'm just offering this for comment. Is there a hole in Texas and do we need an MOU with ERCOT?

MR. CINTRON-RIVERA: We are taking in considerations that because the uniqueness of the state on ERCOT. ERCOT is still subject to NERC reliability standards, so some regulations from FERC are not applicable because there not interstate connections, but they still need to meet the reliability requirements on following the FERC standards.

MEMBER MARCH-LEUBA: Yes.

MR. CINTRON-RIVERA: But it's something that we plan to started this questions with FERC. Because of the uniqueness of ERCOT it might be -- I know that it might be challenging in terms of coordination of inspections since it's not FERC or NERC. It's ERCOT that is performing those inspections. We want to make sure that we have more communications between the regions, regional staff and ERCOT as well for these type of inspections.

MEMBER KIRCHNER: I have a question. This is Walt Kirchner. So three of the four units remained online during this event. The ERCOT grid, if I remember correctly, the capacity of wind alone is like 35 percent. Did you have trouble -- did the plants have trouble -- I'm looking at your sub-bullet here, they proactively started the emergency diesel generators. So there probably were serious concerns about loss of off-site power.

MR. CINTRON-RIVERA: Correct.

MEMBER KIRCHNER: Yes.

MR. CINTRON-RIVERA: For certain points of the event the ERCOT presented issues with grid reliability. There were some voltage frequency drops in which the plants start communications with the grid. And therefore what pretty much happen in that ERCOT started load shedding so they can maintain the grid stability, therefore not losing the power plants as a base load.

MEMBER KIRCHNER: Right. Yes. As they load shed, I'm just guessing in terms of -- we were talking about reactor power. I'm not an electrical engineer, but I've got the -- and my intuition is telling me that these three units were keeping the stability, the ERCOT grid likely.

MR. MATHARU: That is correct.

MEMBER KIRCHNER: Yes. Okay. Thank you.

MR. MATHARU: So just to answer Walt's question a little bit more, the issue with the Texas grid was mainly related to gas power plants because they did not protect the instrumentation and control systems from the cold weather. The gas units started shutting down or tripping off line. And even the transmission network, grass transmission -- sorry, gas transmission network was ineffective in getting the gas to the right locations. So --

(Simultaneous speaking.)

MEMBER KIRCHNER: Well, right, and it's dependent on electric, which is different than coal.

MR. MATHARU: Correct.

MEMBER KIRCHNER: I mean coal you have a pile of coal, like a week's supply at the plant, whereas you're relying on the gas line compressors also that are electrically-driven.

MR. MATHARU: Absolutely. So it was a cascading effect. And as a result of that the voltage and the frequency was decaying and the transmission system operator was trying his level best to maintain reasonable parameters before the grid collapsed. And there was a report that was published that stated that they were like close to total blackout in Texas. I think it was a question of minutes. And the nuclear power plants did maintain some stability in the grid. Yes, absolutely.

MEMBER KIRCHNER: Thank you.

CHAIR HALNON: Okay. I wanted to steer this back towards cybersecurity again. Very interesting event, but it really was meant to show the coordination between the NRC and FERC. And that FERC report, is that a -- that's a public report, I assume --

MR. MATHARU: Correct.

CHAIR HALNON: -- that you mentioned?

Christina, can we get a copy of that?

MS. ANTONESCU: Yes.

CHAIR HALNON: That would be interesting to see. That's good. Thank you.

Go ahead and finish up, Jorge.

MR. CINTRON-RIVERA: So this pretty much is a summary of what -- the coordination that we did. We had multiple meetings to identify the role of each agency in Texas. As was -- we mentioned, ERCOT is a ISO. It's an independent transmission system operator. So we pretty much thought those were one of the main questions that we have. What are its -- I mean, for us this is clear, but what are -- was FERC responsibility within ERCOT. As we mention, there is a event report that was issued providing recommendations. And we also hosted a workshop of the event in which we had presentations related to the bright line. We have NRC and FERC jurisdiction. And so some other topics as well.

Next slide, please? In summary, the agreement facilitates and continues cooperative relations between the agencies. The agreement provides an avenue for us to exchange experience, information of data related to the gird. And the agreements optimize stabilization of agency resources and prevent overlap while allowing agencies to carry out their respective responsibilities. That concludes my presentation.

CHAIR HALNON: Thank you, Jorge. We're going to be visiting Region IV in July and we'll pick up the fragmented questions relative to the cold weather event with the region and see how they coordinated it.

So I didn't see Chris Brown on the line, but, Larry, if you wouldn't make sure that goes onto the ask list for our Region IV presentations during our Subcommittee meeting there, I'd appreciate it.

Any other questions for Jorge?

Okay. Thank you.

Ryan, I think you're going to close out for lunch. How does it feel being the last person before lunch?

MR. BECHTEL: No pressure, right?

CHAIR HALNON: No pressure. Go ahead.

MR. BECHTEL: I'm Ryan Bechtel from the Department of Homeland Security, Cybersecurity and Infrastructure Safety Agency, or CISA for short. I'm representing today the Nuclear Reactors Materials and Waste Sector sector management team within CISA.

CHAIR HALNON: Just real quick, Ryan does not have any slides, so there's not going to be any screen sharing for those of you online.

MR. BECHTEL: So I'm actually covering for my colleague Dan McKenna, who's on leave this week. So I will do my best to answer any questions that you might have, but I might have to take some questions for the record and get back to you if you need certain specific pieces of information.

Today I'm largely going to be talking about the partnership model between CISA and all the other agencies, as well as the stakeholders within the nuclear sector.

So to start off under the National Infrastructure Protection Plan there is a partnership model which is -- establishes how federal, state, local, territorial, and tribal agencies can coordinate with each other and within critical infrastructure stakeholder operators and owners in order to furtherance the goal of improving security and resiliency within all those respective sectors.

Again, I represent the nuclear sector. And we have two parts within our partnership model. One is the Government Coordinating Council, which includes federal agencies as well as some state-level groups. And then also the Sector Coordinating Council, which represents the private sector side of the nuclear sector. And then the SEC covers a wide variety nuclear power plant operators as well as radioisotope nuclear material providers and users, and also research reactors.

So within the GCC it's made up of many federal agencies including Department of Homeland Security and all its sub-components including CISA, Coast Guard, Customs and Border Protection, amongst many others. There's also the Department of Transportation, the Department of Justice, including the FBI, Department of Energy, and of course the

Nuclear Regulatory Commission, which is a very active member within the GCC. Probably have I would almost say hourly if not daily -- I'm sorry, daily if not hourly contacts with somebody within the NRC just going over the various odds and ends of daily operations within the nuclear sector.

So my office -- I should say CISA acts as the sector management resource agency within -- discharges those duties for the Department of Homeland Security. And we are the ones that facilitate coordination and collaboration between the private sector and the public sector within the nuclear sector.

So just to go over some examples of things that we work on for collaboration between the nuclear sector, specifically CISA, and the NRC, we work very closely together within the Nuclear Government Coordinating Council in order to improve communication and coordination amongst -- between the two agencies. NRC is a very active member. They're involved in almost all of our sub-councils and working groups. Amongst the sub-councils the biggest one for here would be the Cyber Sub-Council. Dan McKenna, who again could not be here today, he is the co-chair of that Cyber Sub-Council. We also have one for research and test reactors and one for radioisotopes.

For working groups there is the Private Sector Transportation of Spent Nuclear Fuel Working Group, which is a pretty active one, which NRC is the vice-chair for that working group. And then there's also a few other working groups which -- specific just to the nuclear sector which are under development.

There's also some larger working groups that are outside of not just the nuclear sector, but also all the other 16 critical infrastructure sectors. And the biggest one that I can think of would be the Countering UAS -- UAS is, depending on your definition, either unmanned aerial system or uninhabited aerial systems -- Working Group, and that deals with the -- and that working group specifically is talking about how to deal with the threats and the environments that UASs operate within.

So one of the ways that we facilitate coordination within the nuclear sector is we hold quarterly meetings between the Nuclear Government Coordinating Council and the Nuclear Sector Coordinating Council. Every quarter -- the next one I think is in three or four weeks. It's in early June. And at these meetings we have discussions that are usually topical going over ways to improve security or best practices, but also on the outskirts of those meetings there are classified threat briefings.

Typically DHS will host -- DHS always hosts those, but we'll bring in speakers from within different parts of DHS or other agencies to talk about topical or necessary matters related to security that we think would be necessary to share amongst all the industry stakeholders, industry and government stakeholders. NRC is also involved with those and has occasionally provided some speakers for those meetings, but they're always involved in those threat briefings.

I specifically talked about the classified threat briefings. We do also have monthly threat briefings, unclassified threat briefings, but those are not specific to the nuclear sector. They do cover threats to all critical infrastructure. They're not handled by my office, but they're handled within my division.

Let's see. Just making sure I'm covering --

MEMBER BROWN: Can I ask you a question?

MR. BECHTEL: Yes.

MEMBER BROWN: You talk about threat --

I've forgotten the other word that went along with threat. You're talking about all the threats that could come in, cyber threats could come in?

MR. BECHTEL: Cyber and physical threats.

MEMBER BROWN: Okay. We're talking about cyber today. How do you connect -- I'm trying to figure out how you connect and let NRC know that there's something -- or the rest of the electrical grid operation system that could impact nuclear power plants. How is that done. I mean, do you all have this intelligence gathering set and then every day you have a download or this is important, this is not, or --

MR. BECHTEL: There's different tiers of it. So there are -- so as threats do emerge, it is posted -- sorry, the acronym escapes me right now -- on the CISA website as announcing here's threats that have come in and what you need to be aware of. And that's continuous. There are some things; and I'm speaking right now at the unclassified level, where we'll send out emails or notices for widest distribution letting our stakeholders know, hey, this is out there. You should be aware of it. And we probably send out something like that every other day, but --

MEMBER BROWN: But emails -- I mean, if you --

MR. BECHTEL: It's by email. But that's the more --

(Simultaneous speaking.)

MEMBER BROWN: Doesn't anybody ever use the phone to say, hey look, there's something going on right now?

MR. BECHTEL: Oh, yes.

MEMBER BROWN: Get off your chair and go do this or is there a protocol for how you -- the level at which the communication is taken? I mean, I get emails all the time --

MR. BECHTEL: Right.

MEMBER BROWN: -- or I get a text or whatever it is, but if I'm not looking at them or I'm doing something else, then you can miss it. And if there's something important, a real vital threat that comes up, seems to me the right place to voice --

MR. YIP: Ryan, I could take that.

MR. BECHTEL: Yes.

MR. YIP: This Brian Yip. So I can use some real-life examples over the past couple years for some of the more significant vulnerabilities and threats that we've seen. One of them I want to say was almost two years ago at this point related to the BlackBerry QNX real-time operating system. The government became aware of a vulnerability related to that system. And we had interagency engagement for at least a month or two leading up to the disclosure of that vulnerability to the cybersecurity community.

There was again interagency engagement to ensure that we distributed that information to all o four concerned entities. With the NRC we coordinated directly with CISA to ensure that we drafted and released a security advisory, which is one of our generic communications, coordinated to be released on the same day that CISA disclosed the vulnerability along with the vendor.

We took a similar approach with the start of the war in Ukraine going back a little over a year ago when CISA stood up its Shields Up Campaign to start getting people more aware of potential Russian cyber threats. And we issued a security advisory related to that.

There was also -- we didn't potentially see much impacts with the nuclear power plants, but going back maybe three years at this point there was a significant vulnerability with Microsoft Exchange server. We issued a security advisory in coordination with CISA on that, too.

MEMBER BROWN: Was that email? Text?

MR. YIP: So it's on the NRC website and then it gets distributed to each licensee either by email or to the control room. I'm not exactly sure of the distribution mechanism.

MEMBER BROWN: How does a hair-on-fire communication get done? That's where I'm -- that's what I'm on the substance of the immediate threat that's coming in and, my God, we got to tell everybody now and how do you get their attention? Is there a little alarm bell in a control station somewhere that says --

MR. YIP: There is.

MEMBER BROWN: -- hey look, go look at this because there's a hair-on-fire -- I don't have any hair, but some people do.

MR. YIP: If we need to make an immediate notification, we have the ability to contact the control rooms using the Emergency Notification System telephones. We can do that.

MEMBER BROWN: Okay. Just there --

MR. YIP: Yes, there is a way.

MEMBER BROWN: Okay. Thank you.

MR. BECHTEL: So I think that actually

covers most of it. So yes, when we -- most of it does go out through email. I think there's been a few cases where we have called people for something that's particularly urgent just to make sure that certain principals are in attendance for pop-up meetings that might occur. Brian already mentioned a few examples of that. There's a few others that have come up. And again, this isn't specific to the nuclear sector, but to all the critical infrastructure sectors. That some major world event happens. We need to get everyone on a call. And we're talking 2,000 or 3,000 people for a briefing at the end of the day. And that's when we'll either email or call them specifically to make sure the principals are involved in that.

During the early days of CISA there were meetings amongst all the critical infrastructure sectors weekly to see -- to take a pulse, figure out what was going on and see what needed to be worked immediately. Does that help answer?

MEMBER BROWN: Yes.

MR. BECHTEL: Okay. Yes, so just going through my notes, I believe I've covered everything. Sorry. One other thing is there was a law passed last year which dealt with cyber incident reporting and CIRCIA. That process is still ongoing within CISA right now on what that will look like, but NRC and other nuclear sector members have provided feedback explaining what they would like to see that goes into that process.

Right now, as Dan alluded to earlier, it's -- NRC is usually one of the first people that gets notified. And then NRC or FBI would then notify CISA on certain types of incidents. But the CIRCIA is applying to all -- across all the critical infrastructure sectors.

CHAIR HALNON: I have a couple questions. And these can be short yes/no-type things.

Does CISA have connections to the private industries as well?

MR. BECHTEL: Yes.

CHAIR HALNON: Okay. So you go direct to the private industries if you have information needed to --

(Simultaneous speaking.)

MR. BECHTEL: Yes.

CHAIR HALNON: Are you guys mainly a coordination clearinghouse-type organization rather than like a response resource perspective? Or maybe the better question is what other resources do you have other than the coordination and information clearinghouse?

MR. BECHTEL: So my office is specifically the coordination and information clearinghouse. There are other parts of CISA that take more active roles like threat hunting and that sort of thing.

CHAIR HALNON: Okay. I know it's a pretty young organization so finding that --

MR. BECHTEL: Yes, the agency is a little over three years old, but we historically were part of DHS Proper.

CHAIR HALNON: Okay. So it just brought those under an umbrella and named it?

MR. BECHTEL: I call it a nameplate doxology sort of things just -- there was an act that just split out one MPPD, or IP -- Office of Infrastructure Protection -- and then through some doxology made it into CISA.

CHAIR HALNON: Do you have a, for lack of a better term, five-year plan to expand to your role or is it pretty much set where you're at right now?

MR. BECHTEL: Within my office or within CISA as a whole?

CHAIR HALNON: Well, your office and CISA. I would say just --

(Simultaneous speaking.)

MR. BECHTEL: CISA certainly yes. Within my office we're a pretty mature agency.

CHAIR HALNON: All right.

Anyone else have any questions?

Charlie?

MEMBER BROWN: If you have a cyber threat come in, an immediate -- somebody's attacking our infrastructure, where is the defensive action taken? How do you get people to come in and stop it as opposed to just informing everybody that they're about to go down? I didn't mean that negatively, but I'm -- that's kind of the thought process. I'm thinking here we've got somebody -- all of a sudden we've got a foreign threat or an internal threat that's -- they're getting -- bang, bang, bang, they're trying to get in and they have gotten in and all of a sudden you need people to say get on this and close it out. How do you stop an attack, or do you --

MR. BECHTEL: I'm not really the right person to answer that question.

Brian, you're --

MR. YIP: Yes, Brian Yip. That would be the Threat Hunting Group that Ryan mentioned, and also Dan mentioned in his presentation. They have the capability. And we have engagement with them. They have the capability to actually go on site and assist a licensee or some other critical infrastructure --

MEMBER BROWN: That's too late then. I mean, when you say go on site, you mean they hop on a plane and fly to the site? By then they're compromised.

MR. YIP: I mean, I don't know what their standard operating procedures look like, but --

CHAIR HALNON: Charlie, I would say that each utility -- I mean, the program we've heard this morning is preparation and protection, but the utilities have a response team as well. And I think it gets down to you take care of the nuclear reactor first --

MEMBER BROWN: I got that.

CHAIR HALNON: Yes, and in the parallel with that, while you're responding to that you're communicating to get -- be proactive outside of that. But I'm going from my experience that you have a CRT, a cyber response team on site that is like an emergency response team that takes care of that. And part of that is communication what they're dealing with. And part of this is 73 boarding part that you used to mention, but it's also just 50.72 as well.

DR. BLEY: Hey, Greg?

CHAIR HALNON: Yes, go ahead, Dennis.

DR. BLEY: The questions are getting awfully close to things that probably don't belong in a public meeting. You're probably watching that carefully. Just wanted to mention it.

CHAIR HALNON: Yes. Thanks, Dennis. This is all part of the cyber plans that are not -- I mean, I understand where you're going.

But nevertheless, there's parallel actions going on in addition to the cyber response.

MR. YIP: Yes, that's exactly right. CISA's capability is -- at least for the nuclear sector is a supplement to what we already require through the Cyber Security Plans.

MEMBER BROWN: My thought was just you've got a plant, you've got operators, all of sudden they see some systems are all of a sudden not operating under their control. What do you do?

MR. YIP: Well, that's --

MEMBER BROWN: I mean, is there a --

(Simultaneous speaking.)

MR. YIP: I think they're on site, yes.

MEMBER BROWN: Oh, you've got on-site teams that would say hold it, we respond to this, and then go take action? So that's part of this overall set-up? And I hadn't heard that before and that's what I was looking at. Who takes immediate action as you start losing control.

CHAIR HALNON: Yes, I think the industry is pretty deep in that area. Take it very seriously and they're really -- from my experience did a really good job of making sure that they're at the line ready to go if they need to be.

MEMBER BROWN: Okay. All right. Thank you.

CHAIR HALNON: Other questions on this?

DR. BLEY: Well, Greg, I'm not sure who I'd address this to. A lot of the kind of things Charlie was just talking about are things that could happen because of mechanical failures like problems with instrument error or instrument AC, as well as cyberattack. And how one discriminates seems pretty tricky to me.

CHAIR HALNON: It is. And I would just say that when I was in the control room, Dennis, we dealt with the issue at hand and then -- and we talked about post-mortem in the past, that if it was caused -- we asked the question could this be a cyberattack? And when we asked that, if that question was answered either I don't know or yes, we engaged with the NRC and it went -- blossomed from there. So that question was always asked. When you're actually in it I think you deal with the issue at hand. I don't know if you're -- you're not trying to necessarily stop a cyberattack because you don't know if it is or not.

DR. BLEY: Yes, that's what --

CHAIR HALNON: That's my experience anyway.

DR. BLEY: Yes. The last time I was in a plant these issues of cybersecurity weren't even coming up.

CHAIR HALNON: Right.

DR. BLEY: So it's -- didn't know how they were actually handling that.

CHAIR HALNON: Go ahead, Vicki.

MEMBER BIER: One other comment, just clarification or background for people is that I think most computer systems would also have electronic intrusion detection that would be automatic or near instantaneous if something suspicious is observed, that certain actions are taken automatically. And of course as Jose will tell you, that will only work for the threats that you can anticipate well enough to code in. But a significant fraction of things are probably caught that way.

CHAIR HALNON: Other comments/questions?

Okay. We're right exactly on schedule, so we're going to recess for lunch. We will reconvene at 1:00 Eastern Time. Thank you.

(Whereupon, the above-entitled matter went off the record at 12:00 p.m. and resumed at 1:00 p.m.)

CHAIR HALNON: Welcome back, everybody. I want to continue with the Subcommittee on Cybersecurity and give that back to the staff, so you guys are up.

MR. GARCIA: Do a sound check, can you hear me okay?

CHAIR HALNON: Yes. Point it right at your mouth.

MR. GARCIA: Hi, my name is Ismael Garcia. I'm from the Office of Nuclear Security and Incident Response at the NRC. I want to thank the ACRS subcommittee the opportunity to present this afternoon to give you a high-level overview of the efforts being taken by the staff to develop a cybersecurity and regulatory framework for advanced reactors.

For intent of this briefing, just to give you a high-level overview of the work, that is, we are doing, but the key takeaway, the key message is it's a lot of work out of us we have developed, staff has developed a framework in the form of regulations and the draft regulatory guidance, which was included in the Part 53 rulemaking package that's being reviewed by the Commission.

So we're still waiting for the commentary process by the Commission to be able to address those and subsequently if the package is approved, then comments will be received in the public review process. But again, it's a lot of work still ahead of us.

Next slide, please.

The current proposed advanced reactors involve diverse technologies, and these have a unique set of functions and systems that support both nuclear safety and security. To address the challenges in there, cybersecurity, as I mentioned, the NRC staff is developing a risk-informed, performance base that includes the regulation and associated regulatory guidance.

For the first part of the presentation, I'll be discussing at a high level the development of the cybersecurity requirements for advanced reactors. And then for the second part, I'll discuss the companion regulatory guidance development efforts. But please know that all information I'll be discussing in this presentation is predecisional, because as I said, the Commission is still reviewing the Part 53 rulemaking package which includes the cybersecurity requirements and necessary guidance.

Next slide, please.

To kind of recap what Dan Warner covered this morning, the cybersecurity requirements for the legacy power reactors are found in 10 CFR 73.54, which is titled Protection of Digital Computer and Communication Systems and Networks. And these requirements are based on the function assets perform. Specifically, licensing must protect assets necessary with safety, security, and emergency preparedness functions and support system, which is compromised to adversely impact safety, security, and emergency preparedness functions.

The licensees must ensure the systems are protected from cyberattacks up to and including a design basis threat or DBT, which is defined in 10 CFR 73.1.

CHAIR HALNON: Go ahead.

MR. GARCIA: So March 1st, 2022, the staff provided the proposed Part 53 rulemaking package for the Commission for approval of the SECY 23-0021, which is publicly available. The Part 53 rulemaking package provides an option for the reactor licensee to either implement the cybersecurity requirements in 73.54 or the cybersecurity requirements documented in Part 73.110, which is titled Technologically Inclusive Requirements for Protection of Digital Computer Communication Systems and Networks.

The new cybersecurity requirements will implement a greater approach based on the consequences determining the level of cybersecurity protection required for digital computer and communication systems and network technologies.

The greater potential consequences intended to facilitate risk-informed approaches results in insights for a wide range of reactor technologies to be assessed by the NRC staff. The proposed rule recognizes that the most significant role that may be played by digital computer and communications systems for future reactor designs and the proposed rule also leverage the operating experience and lessons learned from the power reactors' implementation or the current cybersecurity requirements.

Next slide, please.

So this slide provides a high-level overview of the cybersecurity regulations or regulatory framework defined in 10 CFR 73.110 that require a licensee to protect systems associated with functions such as those dealing with safety, security, and emergency preparedness. Using a greater approach for implementing the cybersecurity program in a manner that is commensurate with the potential consequence from a cyberattack.

The proposed rule will allow scaling the design implementation of the cybersecurity program at a given advanced reactor design while ensuring adequate cybersecurity posture. The first consequence shown in this slide deals with radiological sabotage, with scenarios where a cyberattack adversely impacts the functions performed by these assets, which may lead to off-site radiation doses that will endanger health and safety of the public by exceeding the established criteria defined in Part 53.

The second consequence shown in this slide deals with physical intrusion or scenarios where a cyberattack adversely impacts the functions performed by these assets used to maintain physical security of radioactive material that could be at the facility.

So let me put out an example to better explain the concept behind the proposed cybersecurity regulatory framework. So let's assume that the outcome and cyber assessment performed by a licensee for a given advanced reactor design reveals that a potential cyberattack will result in the consequence listed in the rule and the implementation of a cybersecurity program will need to address the cybersecurity controls required for protecting against such a cyberattack.

On the other hand, if the outcome of the cyber assessment performed by a licensee for a given advanced reactor design reveals that a potential cyberattack would not result in the consequence listed in the rule, then the implementation of the cybersecurity program requirements will be minimized. So such an outcome from a cyber assessment will be indicative that the reactor design can demonstrate an adequate cybersecurity posture without the need to implement additional cybersecurity controls.

So while the licensee will still be required to implement a cybersecurity program, it will only need to address requirements such as those dealing with analyzing modification to any assets before implementation to see the design will still demonstrate adequate protection against cyberattacks.

CHAIR HALNON: So Ismael --

MR. GARCIA: Yes.

CHAIR HALNON: A quick question. The risk-informed piece is aimed mainly at the consequence of those two items, radiologic release and the security of special nuclear material essentially, correct?

MR. GARCIA: That's correct.

CHAIR HALNON: Given our discussion this morning with the bulk electric system, does that enter into that equation anywhere relative to the integrity of the grid as well? Or is it only looking at what we just talked about?

MR. GARCIA: At this point, based on -- thank you for that question, at this point, based on this version of the rule, these are the only two consequences listed, but we recognize there will be other consequences that will be listed in the rule. That's one of the areas we're going to be seeking feedback if the Commission approves the rulemaking package to see what any additional consequences should be factored into the framework.

CHAIR HALNON: So the disconnect in my mind that's occurring is that -- and I don't know if it's a problem, I'm just saying it feels like a disconnect, if you have a -- inside the nuclear plant, you have some pretty important components, but they won't lead to the off-site dose. May lead to a problem with the core, but not to an off-site dose issue.

The cybersecurity controls on that component or those series of components may be less than you might put on something in the switchyard, which could only cause maybe a grid issue. So unless we put that same cyber controls across the board, you may have an unbalanced cyber program. In other words, a very deep cyber program for things beyond the breaker, but maybe not so necessary because of the inherent safety features of some of these advanced reactors.

Am I making sense on that question, the imbalance that I can see occurring? Because if you're going to go into the CYP rules that require -- what we presently see as cyber controls on bulk electric systems, yet we're risk informing inside the nuclear plant, you could have actually a small, less intense cyber program inside the nuclear plant and you might have your bulk electric system -- I'm not sure if I'm making sense, but that's the disconnect I'm seeing in this.

So I guess the question is is the same constant going to be pushed over into the impact of this bulk electric system?

MR. GARCIA: Thank you for that question. One thing we need to do going forward is, you know, with FERC and other agencies as we continue to develop this framework, based on the presentation this morning --

CHAIR HALNON: On the punch list to do --

MR. GARCIA: Yeah, so you could add this in a to do list as we move forward.

CHAIR HALNON: That makes sense. I mean we're still early on, and you're working with a lot of hypotheticals at this point.

MR. GARCIA: At this point, basically, yes. That's one of the things we need to do going forward.

CHAIR HALNON: Thank you.

MR. GARCIA: So as part of the proposed regulatory framework, as I mentioned, licensees will need to perform analysis, assess the potential consequences resulting from cyberattacks, identify those assets that need to be protected, and also establish, implement, and maintain a cybersecurity program as defined in the cybersecurity plan to protect the assets identified by a planned defense-in-depth approaches like the ones that Dan discussed this morning to ensure the ability to detect, delay, respond, and recover from cyberattacks capable of causing the consequences defined in the rule.

In addition, a licensee will need to implement cybersecurity controls commensurate with the safety and security significance of those digital assets.

Next slide, please.

Now we will discuss the efforts the staff is planning to support the development and the companion guidance to allow Part 53 licensee implement the cybersecurity requirements that I just went through.

Next slide, please.

So the NRC staff, with the support of the cybersecurity experts from the Sandia National Lab, have been taking efforts to develop a regulatory guide to provide a commercial nuclear power reactor on their Part 53 license with an acceptable approach to implement the requirement, the cybersecurity requirements in 10 CFR 73.110.

This guidance, documented in DG-5075, which eventually will be known as Reg Guide 5.96, entitled Establishing Cybersecurity Programs for Commercial Nuclear Power Plants Licensed under 10 CFR

Part 53.

This Draft Reg Guide was included as a reference, along with the ADAMS accession number in SECY 23-0021. The Draft Reg Guide will provide an example method that applies risk-informed, performance-based, and technology-inclusive approach to account for the different commercial nuclear power plant technologies licensed under Part 53 to demonstrate protection against a potential cyberattack.

CHAIR HALNON: But does it have to be solely under Part 53, or could it just be an advanced reactor? Because some of these, like the Army's, we just did under Part 50. So I mean, is there something special about Part 53 that causes you to limit this Reg Guide to only Part 53?

MR. GARCIA: Thank you for that question. Right now, we're developing to support the Part 53 framework, but some of the questions that we have even during the development of the cybersecurity requirements is like, hey, perhaps a light water reactor commercial nuclear power plant can apply those requirements. Nothing will prevent them from doing that. So right now our focus is to support the Part 53 effort, but one can make a case at the end that either Part 53 maybe to use that guidance as well.

CHAIR HALNON: We made the same comment for Reg Guide on the alternative evaluation of risk process. It looks like it could be expanded beyond Part 53, if it's really good to use, the new technology may not necessarily all be licensed under Part 53.

Same comment, could look at maybe making it broader?

MR. GARCIA: Yes. Thank you for that comment, so yes, some of the concepts I'll be discussing in the guidance could be applicable relative to a commercial nuclear power plant light water reactor versus non-light water reactor.

So this Reg Guide, Draft Reg Guide will describe, among other things, elements required in a cybersecurity plan, including a template of how to develop a cybersecurity plan, the different cybersecurity controls that need to be applied by a licensee, and it leveraged information from Reg Guide 5.71 that the ACRS got a chance to have some meetings on this topic on this Reg Guide titled Cybersecurity Program for Nuclear Facilities, which again was developed for the commercial nuclear power reactors.

The Reg Guide also leveraged information from IAEA and IEC documents on cybersecurity. And again, pretty soon that the guidance documents will be made publicly available if the Commission approves the proposed rulemaking package.

Next slide, please.

Some other technical areas the Draft Reg Guide will document and approach to determine the level of cybersecurity protection required against potential cyberattack, which will be based on a three-tier approach to analysis of the facility and at the function and at a system level. So basically, a top-down kind of approach.

At the facility level, the intent of the analysis will be to rely on existing security and safety assessments to determine whether a plant's design basis and existing physical protection system are sufficient to effectively prevent the potential consequences from a cyberattack.

At the functional level, the intent of the analysis is to develop adversary functional scenarios to understand the adversary's access to attack pathways that could allow the compromise of regular plant functions resulting in unacceptable consequences defined in the rule.

The primary intent of this portion of the analysis will be to eliminate or mitigate potential attacks to pass the cybersecurity plan and defend the cybersecurity architecture elements such as the use of the data value that was discussed earlier today.

And then on the system level, the intent of the analysis, to identify critical plant systems along with adversary technical sequences that involve detailed attack steps, to determine the active cybersecurity plan and defensive cybersecurity architecture protective measures including the cybersecurity controls just like the one that Dan mentioned, discussed this morning, to prevent or mitigate the impact of such systems.

Yes?

MEMBER BROWN: You're finished with this slide? Did you have something else to say? I interrupted you, I apologize.

MR. GARCIA: That's perfectly fine.

MEMBER BROWN: Use active cybersecurity plan and defensive computer security architecture ID intrusive detection systems to protect against cyberattacks. In other words, I'll take a reactor protection system's software and I'll crank all kinds of cybersecurity software in it so I can make sure that it's not operating when it's asked to because it's also evaluating and scanning the system.

MR. GARCIA: Thank you for that question. The intent is not to --

MEMBER BROWN: That's not the intent, but that's what it says. I'm going to incorporate -- I'm going to put McAfee or whoever the other magic virus protection systems are, and I'm going to install it inside of my protection systems and safeguard systems.

MR. GARCIA: Yes, the intent is not to affect or adversely affect the performance of the safety system. I'm trying to clarify. The intent here is to apply the same kind of controls we apply to the other Reg Guide, 5.71.

MEMBER BROWN: That's not what that says in your architecture.

MR. GARCIA: The intent is not to adversely affect the performance --

MEMBER BROWN: Oh, I know -- I agree with you. I understand the intent is not to do that, but as soon as you open the door, that effectively -- you're going to be arguing about it every time an application comes in. They're going to say ah, we're going to throw all this other stuff in there and don't worry about it. We don't need data diodes. We don't need this, because we've got all this great intrusion software that's going to figure everything out, and now it's going to be a big fight in order to get the darn system through NRC.

And if I'm on the committee, it will be a big fight to -- I couldn't resist that.

MR. GARCIA: That's perfectly fine.

MEMBER BROWN: To get a committee to agree to do that. And I'm not arguing that there's not some things you would, what I would call the non-active internal things you can put in to verify that data is being transmitted accurately throughout the entire process. There's start-up things you check to see, hey, look, everything looks the same every time I boot it up as it did the last time. But that's not the same as what I call the active intrusive cybersecurity stuff, like when you're sitting into your personal computer at home, and all of a sudden something doesn't happen for 34 seconds, and all of a sudden the thing pops up because it was, oh, I completed a scan, and now you're okay. That's -- I didn't get that out of the Part 53 reviews.

Has this been included in any of the detailed Part 53 reviews? I don't remember that. Am I behind the part, Dave? Am I right?

MEMBER PETTI: Yes, I don't think it's at that level of detail.

MR. GARCIA: Yes, because this portion is getting into the guidance level.

MEMBER BROWN: I understand that. I just didn't remember that we had addressed it on the Part 53 section by section details.

MEMBER PETTI: I think it's important though that these concerns get reflected in guidance, that in no way does this mean one should go against the guidance on data diodes and somehow reflect what the subset of options are, right?

MR. GARCIA: And at this point, yes -- thank you for those comments. Yes --

MEMBER BROWN: I was just going to say, now we've got 5.71, but then you're going to say we're going to have another Reg Guide now, 5.96 or some other alphabets or numerical soup, to work to do cybersecurity when -- why do I have to have a whole new set of guidance on how to do cybersecurity for operating plants -- for the new plants that I didn't need to address on the existing plants? I'm having a hard time walking my way through that shark-baited -- I'll have no feet by the time I get finished with this walk.

MR. GARCIA: Thank you for the comments,

so let me say for the purpose of the system, when we get to the system level, the draft, it's still a draft document, but the draft guidance has basically leveraged information of Reg Guide 5.71.

MEMBER BROWN: They have what?

MR. GARCIA: Leveraged information of Reg Guide 5.71, used the information of Reg Guide 5.71, in terms of pointing to that document for the cybersecurity controls that should be applied to your control systems.

MEMBER BROWN: That means you've got to have one document, and then you've got to have the other document in order to complete your determination --

CHAIR HALNON: Yes, but 5.96 would be risk-informed, so --

MEMBER BROWN: Yeah, I understand, I just love risk-informed cybersecurity.

CHAIR HALNON: Is this how your staff meetings went?

MEMBER BROWN: Pardon? He worked for me at one point.

CHAIR HALNON: No, I was wondering if this --

MR. GARCIA: Kind of deja vu. So those

questions about taking all that information for Reg Guide, the cybersecurity controls, and put them into the enclosure, into this new Draft Reg Guide, but again, this is still draft form, so that may an option that could be explored down the road.

MEMBER BROWN: I just don't understand why the guidance, the techniques, the guidance, the defensive levels, all that stuff, in my own mind, is technology-inclusive, it's risk-informed, and it's performance-based. And I can apply it to any design they come up with for an advanced reactor or non-advanced reactor. It makes no difference.

The 5.71, I reviewed it three times now, maybe just two, a number of revisions, let's put it that way, and it is very generalized such that it doesn't restrict. It doesn't say applicants can't do this or do that, so it's this own risk-informed -- whether I like risk-informed or not is irrelevant. It has options for applicants to take various actions and propose those for acceptability to the staff. It's not dictatorial. Most of the stuff in there says we can accept this type of thing. We can accept this. This method is acceptable, so is this.

I just don't see the benefit of developing a whole brand new Reg Guide, where it references back to the other one, now I got to have two Reg Guides to sit in front of me to determine whether I'm going to be satisfactory when I go and make my presentation to develop my process.

CHAIR HALNON: So I would just take that comment --

MEMBER BROWN: I was on a roll.

CHAIR HALNON: Yes, I'm going to give you square tires.

(Laughter.)

Dennis, on line, you're up.

MR. BLEY: Yes, Dennis Bley. Hi, Ismael. I'm listening to Charlie, but I'm not quite with him. I'm looking at your slide, which is only a slide. It's a cartoon of what's going to be in the guidance, but the first level up there, eliminate potential adversary scenarios through facility design, is I think the first time the staff's been really responsive to an old SRM that says integrate safety and security efforts through the design. I think that's a big step.

The other things, you were down at the system level, but at the functional level, it's got the things I think Charlie's most focused on that are still there. And finally, if this proceeds like several of the other places we've seen guidance developed for a new function, I think some of what you're putting in here is new, and I suspect what must be in the future is that being adapted back into what we have for light water reactors in general. I don't know if you want to comment on that or not, but that's at least my reading of where you're headed.

MR. GARCIA: Yes, thank you, Dennis, for those comments. I agree with you. Let me step back to respond to some other remarks, Member Brown, that like I said in the rulemaking package, we give the option to the reactor licensees to either apply existing framework or the new one.

MEMBER BROWN: Framework A and B.

MR. GARCIA: No. 73.54 requirements or 73.110. And the reason being that while we developed 73.110 is because, in the case of 73.54, as we discussed earlier this morning and I briefly summarized it at the beginning, that you pretty much have the -- you need to protect safety and security measures for various functions and all support functions.

But looking at advanced reactors, there might be cases that hey, they may not have the assets for safety-related functions and they may rely on panel devices for example, let's assume for a second. So in those cases, they may have to then start requesting exceptions in some portions of those requirements in the system rule, and then that's not perhaps an efficient way to be able to apply the regulatory framework.

So that's why we developed this 73.110 set of requirements to develop a framework that kind of mimics what we have today in terms of cybersecurity or other framework in the sense that when you look at the entire spectrum of NRC licensees, you have -- you go from research and test reactors, they don't have -- that case cybersecurity requirements apply to them. We have guidance. We don't have requirements applied to that. All the way up to nuclear power plants that have, as we discussed, a fairly robust cybersecurity framework.

So we're trying to develop this regulation that kind of mimics the same approach that we have today for cybersecurity requirements or cybersecurity framework that we apply to NRC licensees.

So based on that framework that we're trying to develop a guidance that captures some of the concepts like the secure by design to try to promote that kind of concept that then cybersecurity could be applied early in the process versus late, but then at the end when you get down to different levels of analysis, it pretty much will be at the same kind of level as we did today for power reactors and the guidance in Reg Guide 5.71.

Yes, it will require, like Charlie mentioned, having two documents available. That's the kind of discussion we need to have going forward. Does that really make sense if you're going to go down that path of developing this new framework?

MEMBER BROWN: Just to counter, I might disagree with Dennis, there's always room for something new floating through, but when you look at the -- eliminate potential adversary scenarios to facility design, 5.71 lays out an architecture of level 1, level 2, level 3, level 4 -- you design your plant within those levels. You're doing the same thing with 5.71, you don't need another document.

The mitigation of CDAs, you've got a whole bunch of different paragraphs that discuss how to do that, and what some data diodes are an acceptable way of doing it. There may be other ways you can do that.

Your comment relative to well, the new plant may decide to use analog circuits. Well, that's no longer a CDA, so it doesn't matter whether or not they pay attention to the other document or not.

All I'm trying to do is lay on the table that you ought to give some thought to not proliferate documents that people have to deal with as we go forward with Part 53. That's the thought process.

The more paperwork, I mean right now, I've looked at some old Reg Guides that we looked at, and there were five different IEEE standards that you may have to go through to pull out enough detail in addition to the positions you have in the Reg Guide. I mean it's a nightmare trying to figure out what do you need and what do you don't need in your design.

Proliferation of documents you have to review is just difficult. So I'll quit.

CHAIR HALNON: The question is as you're drafting this document, are you seeing a delta, a huge delta between 5.71 and your draft 5.96?

I mean if you get done with 5.96 and you say well, that looks pretty much just like 5.71, then you have to ask the question was Charlie -- is the wisdom he's putting out there, really was it worth the work, I guess, is a way of putting it.

MR. GARCIA: And we're looking into that, because again, the document, the new Reg Guide leverages that information but includes some of the concepts that -- I know that Charlie mentioned you have the level 1, 2, 3, and 4 architecture. Well, this one is getting in at a higher level, but at some point can you look into the way that you define -- design your protection system, physical protection system, because there might be some credit you can take there to mitigate the potential consequences from a cyberattack. It takes it to a higher level.

This is the kind of discussion, I agree, it's the kind of discussion we need to continue having going forward.

MEMBER BROWN: I cannot see anybody going backwards from computer-based reactor protection systems to analog protection systems.

MR. GARCIA: You would be surprised some of the conversations we have at pre-application meetings.

MEMBER BROWN: Has anybody come in who wants to use an integrated circuit, operational amplifier circuits?

MR. GARCIA: Not yet.

CHAIR HALNON: Okay, you guys are going way back in the vault for this one. Let's move on.

MEMBER BROWN: I did the first transistorized mag amp combination average. It was for a cruiser.

CHAIR HALNON: And it's probably still floating --

(Simultaneous speaking.)

MEMBER BROWN: No, they got turned into razor blades years ago, 25 years ago.

CHAIR HALNON: You're almost --

MEMBER BROWN: Go ahead.

MR. GARCIA: Yeah, I was going to say -- yeah, thank you for those comments. So in terms of the approach, is that you want to do an analysis up to a level that you can show the adequate protection against cyberattacks. So it could be analysis the first year, the facility level to demonstrate adequate protection against cyberattacks.

The analysis could involve two tiers, meaning at the facility and the function level or to build all three tiers. But again, the guidance is based on doing the analysis up to a point. And you can demonstrate adequate protection against cyberattacks. Next slide, please.

So wrap it up, there's future work. Like I said, it's a lot of work ahead of us, there are some other, time for some other concerns, comments you provided during this briefing. At this time, we continue to support Part 53 rulemaking efforts, including the cybersecurity portion not only in the comments we get from the commission. But if the rulemaking package is approved, then we'll address any comments when the product review -- and also address some of the technical issues that my colleagues in research are going to be discussing during the next presentation.

CHAIR HALNON: Do you have a target when you're going to have that draft guidance document at least to a point where it can be read internally?

MR. GARCIA: It is available in ADAMS. So when you go to SECY 23-0021 in the cover letter --

MEMBER BROWN: You don't even have to do that. Just go look at the slides. You can look at it. I've already looked at --

(Audio interference.)

MR. GARCIA: And then it has the reference number to the draft reg guide. So it's available. It's just not publicly available but it's available. Yes?

MEMBER MARCH-LEUBA: Does this work combined with autonomous or a remote operation?

MR. GARCIA: Right now -- thank you for the question. At this time, the reg guide is silent in that area mainly because we got direction from management that for the purpose of this version of the rulemaking language, I was just focused -- we put that issue aside. Nonetheless, we're doing work with the college research to understand what is out there in terms of the technology, operation and remote operations, so we can think about, okay, what kind of cybersecurity controls would be needed for perhaps the licensee that decides to use that kind of technology.

MEMBER MARCH-LEUBA: Remote operation is diametrically opposed to what we say this morning about the philosophy of cybersecurity, an autonomous (audio interference). So if you are going to create something new, you should at least invest it, right?

MR. GARCIA: Yeah, and then so we're doing the research to see what kind of -- like, I guess, in terms of operation, do we need to impose any additional controls? We'll be back to delta, a question about the delta between this reg guide and the previous one will address that in the document.

CHAIR HALNON: Any other questions? Okay. Let's move on. Anya, are you up?

MS. KIM: Actually -- excuse me. Actually, Brian is going to do his introduction first.

MR. YIP: I can get started while the

slides are getting up. So our engagement with the Office of Research is really important to our ability to execute the cybersecurity mission. And we're engaging with research, all levels on cybersecurity, at the staff level.

Frequently, my counterpart, Chris Cook, and I talk at least on a weekly basis. We're briefing our management on cybersecurity research on a monthly basis. And so what you're going to see in this next briefing is the activities the Office of Research is doing to support the cybersecurity mission.

And as we're looking towards advanced reactor reviews and also novel technology applications. And when I say novel technology, I'm referring both to new technologies as well as applications of existing technologies in new and different ways even with the operating fleet. So with that, I'll turn it over to Anya and Doug. Thanks.

MS. KIM: Thank you. My name is Anya Kim. Can you hear me? And can we move to the -- Tammy, can we move -- actually, all of this should be Brian. You should be presenting or I can present.

MR. YIP: Anya, why don't you go ahead and present if you have the notes.

MS. KIM: Okay. So just to give you a

brief description of what we plan to talk about, we'll give you a brief introduction and let you know what our research goals and drivers are for doing this various research. And we have a research approach that we generally take for our research topics. And we will give you a brief overview of four representative research topics on our novel technologies project umbrella and then a quick wrap-up.

So I think Brian mentioned this already. But I will just briefly summarize. The research department -- research branch cyber security research supports the current and future NSIR activities and the novel technologies that we look at. And I think Dan mentioned this earlier.

They're not necessarily novel to everybody but novel to nuclear. But novel technologies are applicable to both operating and advanced reactors. So anything we learn from examining them for operating reactors, we could apply to advanced reactors and small modular reactors.

So we are looking at these technologies to be ready for the future and to help staff to support them in any way we can. And next slide. So the goals of our research as I briefly mentioned is to perform anticipatory research to anticipate the needs and prepare NRC staff to meet the potential challenges that they would face within the nuclear domain. And so the main goals would be to educate NRC staff and identify potential cybersecurity implications of using these technologies and develop awareness of and collaboration with any government or nuclear industry partners that could exist.

Okay. So there are drivers for doing this research is that licensees are considering using these new technologies or novel technology implements in current or future applications. In that case, there's likely to be a change in the attack vectors. And we want to be able to understand what the associated cybersecurity issues would be and how to address that. Excuse me.

And from there stems a need to develop a technical basis for licensing guidance and oversight of these new technologies. And even for inspection tools to help NRC staff in their work as they review these new technology applications. The four technologies we will be looking at today are field programmable gate arrays, autonomous control systems, artificial intelligence and machine learning, and wireless technologies.

So for field programmable gate arrays, I will be presenting this in the autonomous control systems. And Dr. Eskins, my colleague, will be presenting the AI artificial intelligence and wireless security. For each topic, in general, we will present a brief background of the technology and the reason we're doing the research, the motivation behind it and any insights we've gained from the research.

First, let's talk about FPGAs. I spelled out the acronym there because it helps understand what FPGAs are. They are devices in which the application logic is implemented in hardware circuits. So there is no software and they can be configured to perform a user defined custom function.

And as their name suggests, they can be programmed and reprogrammed in the field. However, that's not as easy as you think. It's not like the software updates that get pushed to our computers and our phones. It requires access to the FPGA device as well as a constant power supply. So FPGAs in the operating nuclear fleets have been --

MEMBER BROWN: Can I ask you a question on that?

MS. KIM: Yes, sure.

MEMBER BROWN: There's two types of FPGAs.

There are volatile and non-volatile.

MS. KIM: Yes.

MEMBER BROWN: The non-volatile are the ones you just talked about in one way, shape, or form. The volatile ones lose their programming. So you have to have rem somewhere when power comes back, you reprogram it on the spot. That's internal to the system.

Now the way I view those is that the rem that you got, the memory that you got that's going to reprogram it has to be done over and over again every time you lose power. That would be possibly to access by some cyber operation because that more than likely is e-squared or something that's electrically erasable and then you can redo it or whatever the latest version of those suckers are. So you really got to address those into formats. The FPGAs themselves when they're sitting there, you're right. You have to take -- either take the chip out or you have to be able to isolate and then go reprogram it which is a fairly complex operation to reprogram.

MS. KIM: Right. And that's why I did say they can be reprogrammed. And I do want to step back and say actually so when we talk about FPGAs, we have to think about them in terms of are they volatile? Or are they re-programmable? And the non-volatility is basically -- so what they've called the configuration logic is -- or bit stream is if it's volatile, when it's powered off, it gets erased.

So that's why you have to constantly reload. But that's different than reprogramming. It's the same thing that you're taking from an EPROM onto the FPGA. And yes, there is a cybersecurity concern there because when you're loading it from the EPROM to the FPGA, there's a connection where you can obviously steal it or try to manipulate it.

MEMBER BROWN: We'll you could've already had manipulated the --

(Simultaneous speaking.)

MS. KIM: And that's --

MEMBER BROWN: -- EPROM.

MS. KIM: Yes, and I'll get into that right now. I was just going to give you a background. But yes --

MEMBER BROWN: Sorry to interrupt.

MS. KIM: No, no, I prefer that. Yes, so in that case, some countermeasures are that nowadays the volatile FPGAs do offer encryption. You can encrypt the bit stream.

So even if you intercept it, you can't

read it. And then the re-programmable part is the one where if you want to change the design or the configuration, that's where you can reprogram it as many times as you want. And some FPGAs, you can reprogram it multiple times. And then one type of FPGA, it's only one time.

MEMBER BROWN: That's not unlike some of the early EPROMs that you had a limited number of times you could reprogram it until they --

(Simultaneous speaking.)

MS. KIM: Exactly.

MEMBER MARCH-LEUBA: Yeah, you've got to be a little careful. You're thinking what's similar to what it had to do with what's called secured good. Before you load up the present system --

MS. KIM: Secured, yes.

MEMBER MARCH-LEUBA: -- you're loading the proper one. We do that every single time we turn power on, on a computer.

MS. KIM: Right.

MEMBER MARCH-LEUBA: It's pretty good. But our guys are finding ways to mess with it.

MS. KIM: Exactly.

MEMBER MARCH-LEUBA: I mean, there is a patch for the WiFi (audio interference). They inject the virus before secure boot. So you cannot discard it.

MS. KIM: No, you cannot.

MEMBER MARCH-LEUBA: You have to keep an open mind when you're doing this attack vectors.

MS. KIM: And this is a great conversation we're having because this is all the stuff that as -- when it's our job to review these FPGA-related -- sorry, FPGA-based systems, we need to know all this stuff because some chips offer it, some don't. And then some have ways you can intersect it. Some are more vulnerable to this secure boot attack than others.

So having that knowledge helps us determine what the security posture is. And that's what research is doing. We're trying to compile --

(Simultaneous speaking.)

MEMBER MARCH-LEUBA: And that is your job to understand it so you can tell these guys --

MS. KIM: Yes.

MEMBER MARCH-LEUBA: -- what they have to worry about.

(Simultaneous speaking.)

MEMBER MARCH-LEUBA: The other thing I wanted to point out maybe in the next slide but I can do it now since I have the microphone is the easiest attack -- cyberattack you can have is a denial of Service. And we talk about that certainly for autonomous and remote operation. It's so easy that you can fire up your browser and go buy one.

I mean, you can buy a couple hundred bucks. It gives you denial of Service for five minutes. And then you pay by the hour. It's kind of interesting.

So denial of Service means is there anything I can do to make my FPGA not work? Can I have a some notice? Can I have some change in temperature?

So how can I deny the FPGA from performing its work? That would be my vector for attacking you. And you're the researcher, guys. You need to think about this, not me.

MS. KIM: The threat. And if we can move to the next slide, we can talk about it on this slide. So the purpose of this research is to identify those potential security concerns with FPGAs for future nuclear applications.

And basically, we're investigating whether FPGAs are inherently cyber secure since there is no executable software on it or whether or not they are vulnerable to these internet cyberattacks. And our research right now is ongoing, but our preliminary findings show us that it's not that the attack surface has disappeared. It's more than it's shifted.

So while there is no software on the FPGA device, there are many software-based design tools involved in the entre process of manufacturing development and design of this FPGA device. And in that process, there are sever attack points in which malware could enter. Basically, it's a supply chain concern.

I think earlier in the morning, how does acceptance testing test against malware? That was asked. And that's one of the concerns, one of the big things about FPGA is what they call hardware trojans which is basically malware in the FPGA. How do you test for that?

And that's the kind of things we're researching right now. So what are the main concerns on how to protect against them? And if they do occur, how do you defend them?

And so while most of these attacks do require physical proximity or access to the FPGA, some of them can be done remotely or through the supply chain which is one of the bigger concerns. So the findings and insights that we're developing, we want to capture in a way that provides NRC staff with the knowledge they need when they're reviewing these FPGA-related materials that are submitted by the licensees and applicants. And what we learn here will be applicable to future architectures or future nuclear power plant applications.

Okay. So moving on to autonomous controls and remote monitoring. So while remote monitoring and operations was actually a separate topic under our novel technologies research umbrella, as you'll see later, it's very closely related to autonomous control technologies. So I sort of piggybacked it here on the title.

So with autonomous control systems, they can replace the human operators to the degree that there's a human out of the loop. And it can range from basically totally manual operations where the human has to be involved and makes all the decisions all the way to a fully autonomous system where the autonomous control system acts and thinks intelligently and independently with a human not in the loop. Yes?

MEMBER BROWN: Pardon the interruption. Take after Jose here. In a way or if you want to look at that, the reactor protection systems you build are already autonomous. They don't require human action at all.

You've got sensors. They process. They determine whether you exceed a particular range of operation that's acceptable. And they scram or don't scram. They are autonomous already. This is not new.

MS. KIM: Mm-hmm.

MEMBER BROWN: That's all I'm saying. But there are no operator actions other than the backups you may have in case the system fails for whatever reason. I just wanted to make sure we understood that our existing systems, the critical safety systems we have in existing reactors today are basically -- not even just basically, fully autonomous.

They require no operator to do anything. He'll be reading meters, and he'll see the plan shuts down. So that's the first thing he sees that is the end result of the whole thing.

You don't need sophisticated equipment to do that. We did it with mag amps and vacuum tubes. You probably might not know what a vacuum tube is, but that's okay.

MS. KIM: I'm not that young.

MEMBER BROWN: You look way to young.

Anyway, I'm just saying we've got to be a little bit careful we don't really -- the world of autonomous has been with us for quite a while, forever almost. So --

MEMBER MARCH-LEUBA: But that's for the simple functions.

MEMBER BROWN: I'm not arguing about that.

(Simultaneous speaking.)

MEMBER MARCH-LEUBA: What autonomous they mean, they have complete control of the emergency operating procedure. They shut down on recovery and everything else the operator does after the control rods.

MEMBER BROWN: That's a second layer of autonomous operation.

MEMBER MARCH-LEUBA: That's what they --

MEMBER BROWN: We already have simplified autonomous operation.

MS. KIM: Well, I would slightly disagree. I was sort of getting there, but we have a full range of autonomous operations. And what you were talking about I would say would be more, like, automated systems. So yes, they don't need --

(Simultaneous speaking.)

MEMBER BROWN: But those are autonomous.

MS. KIM: Autonomous in my view and in the general research seems to have to have intelligence. So I sort of underlined the important keywords in the definition I used in the slide. So it has to be able to think independently which it does.

MEMBER BROWN: That's what it does.

MS. KIM: Under uncertainties.

MEMBER BROWN: Does that also.

MS. KIM: And has to learn -- well, I didn't write it down. But it has to compensate and learn from failures all without human intervention in a very dynamic environment. So it has to have some concept of intelligence and independents in there to be a fully autonomous system.

(Simultaneous speaking.)

MEMBER KIRCHNER: This is Walt Kirchner. I had to deal with this, a whole issue 40 years ago. We were designing a reactor to be remotely operated, the north warning system.

And so Charlie, what I would say is yes, what we were designing was essentially on and off, much like a reactor protection system. You've got either you lose power or you lose your signal or you reached your safety limit set points and you trip. And then it shuts down.

And if it's an advanced -- well designed, advanced reactor, it passively remains shut down and cools itself and all those other nice features that you would like to see. But you really didn't have control. So I think Anya is making that kind of distinction that it actually can perform.

It's not on-off. It's the ability to actually operate and meet the mission requirements whereas what we thought was, well, we lose that comm link, then we're just going to shut down the reactor and the redundancy was the next radar site filling the gap in the defensive line. But it was on-off essentially.

It wasn't rally performing its functions as designed to meet the mission requirement. It was just safety. So that's a distinction I would make. And yes, the protective system does function as you indicated.

CHAIR HALNON: But I don't that we're talking something that's smarter than bistable controlled --

MEMBER BROWN: Well, they are.

CHAIR HALNON: -- instrumentation.

MEMBER BROWN: No question.

CHAIR HALNON: Oh, no. It's only because you got a whole bunch of them. And it votes bistables. It's just all bistables basically, measure bistable.

If you look at the second bullet there, capabilities that diagnosis, prognosis, planning, decision making, those are pre-programmed into the bistables. We're talking about uncertainty, uncertain condition and figure it out and then take an action. It may not be pre-planned.

MEMBER MARCH-LEUBA: Yeah, being able to look at the senor signal and say, hmm, it doesn't look right.

MS. KIM: Yes.

MEMBER BROWN: Why you build in a redundancy and independence. I mean, there's a number of different ways to slay this dragon.

MEMBER MARCH-LEUBA: That's why we, like, operate. That's what operate does because I don't have to --

(Simultaneous speaking.)

MEMBER BROWN: I was going to echo your words exactly. I like operators as well.

CHAIR HALNON: That set you up, Doug, really well, doesn't it?

MR. BLEY: Anya, this is --

(Simultaneous speaking.)

MEMBER BROWN: Yeah, let me finish here just a minute, Dennis, if you don't mind. What you've got to factor into this if you're going to convince us or me if I'm still around is every time you go autonomous, you have to do exactly what Jose said. You have to have built-in sensing, testing systems that are saying, hey, this is drifting outside of the range of what I think it is. Therefore, that needs to be compensated.

There are multiple ways of doing that and this might be the best which means more senors to say is that available. There's a whole plethora of complexity that falls into this that really has to be addressed analytically to see if that's useful or not or if introduce complexities which we can't even analyze where we have to do a PRA to figure out of the 2,000 sensors we have are going to give us the data and we have the algorithms that are going to do is because it's all for even throwing in the machine learning the AI thought process. You need data to do that. A human being, eyeballs, ears really processes huge amounts of data in just milliseconds when you're doing things. We just need to be thoughtful.

MEMBER MARCH-LEUBA: Let me give you an example. Before talking in the microphone, I have to look and see that this green light is green. So it's not green, and computer gets lost.

It's not green, I cannot talk. An operator looks at it and says, oh, the lightbulb is fused. It's in an analyzed condition. It's different to do. It's not trivial.

MS. KIM: Right. And I'm going to jump ahead a little bit and --

CHAIR HALNON: Dennis --

MS. KIM: Oh, yes.

CHAIR HALNON: -- Dennis Bley had a question. Go ahead, Dennis.

MR. BLEY: Anya, thanks. I was waiting for the AI presentation. But this conversation got kind of deeply into it. If NRC is going to approve artificial intelligence based systems with the machine learning, there's all different sorts.

But one characteristic of them all because they do learn is that there's no way to do what we do with computer programs now and that's verify them because they're changing themselves all the time. The only thing I can think of if you're going to do that, you have to somehow test the systems, quote, knowledge and reasoning capability, sort of the way we test humans. Have you guys thought about how in the world you're going to address that issue?

CHAIR HALNON: Let's first bring us back to this is a cybersecurity discussion, not an autonomous control/AI development.

MR. BLEY: I missed that in the last few minutes.

MEMBER BROWN: The next couple of slides.

CHAIR HALNON: Yeah. Well, we got to remember these fine folks in front of us are talking about how we maintain cybersecurity protection over these systems, not necessary how they got the systems. They're being handed -- good questions. I think it's just outside of the scope of this subcommittee. Go ahead, Anya.

MS. KIM: So yes, I agree with what both of you said. And capabilities were already mentioned. And I just wanted to say I'm probably jumping ahead.

But since you talked about autonomous country with the different aspects. So there's two aspects you have to consider with autonomous control systems. There's the level of autonomy which is sort of what were you getting at earlier.

And also what is being automated, so the process? If anybody here has a military background, you might be familiar with the OODA loop, observe, orient, decide, and act. It's a way to figure out what the situation around you is and figure out what to do, decision making process. It was developed by, like, a Colonel John Boyd or somebody like that.

And while autonomous control systems call it something else. Basically what you have are those four phases. You have the observe where you gather the data.

Okay. The light of this microphone is off. And then orient, okay, what should I do about it? I'm talking. And decide, okay, I better turn it on. And then act and actually press the button to turn it on, right?

So of those four different distinct segments, autonomous controls could be applied in all four of those and to different levels. They could be fully autonomous. It could be something with user feedback. It could be minimal autonomy.

So that whole aspect has to be considered when we're talking about the autonomous control systems. So even though Member Brown sort of said that we already have autonomous systems, I want to say that autonomous systems with varying levels of autonomy have been employed in other industries like robotics, avionics, space craft, transportation, but not in operating nuclear power plants. However, recently the nuclear industry has been looking at it as a way to lower their operational and maintenance costs, particularly for advanced reactors and small modular reactors.

So we are performing this research to better understand what if any cybersecurity concerns there would be with using autonomous control systems in nuclear power plants. And in order to do that, there are a lot of enabling technologies that are needed to provide the capabilities that we saw in the previous slide. And these enabling technologies can shift during large attack surface, thereby creating these new security challenges.

And these are -- oh, I picked a few of them -- remote monitoring and operations, digital twins, artificial intelligence and machine learning. So with remote monitoring, you would probably use that to monitor the safety and security functions and send commands maybe if you're talking about remote operating as well. Remote operations would also send commands to the autonomous control system.

And then if you have remote monitoring, what would be the connection pathway between the remote monitoring site and the site where the nuclear power plant is. Wireless is probably something they want. So there's another security concern we have.

And you probably are already aware, but remote monitoring really isn't as big a concern as remote operations, being able to do operations remotely is a cybersecurity challenge that the nuclear community has to consider. And then digital twins, digital twin technologies are -- it's a virtual representation of the physical system where the data and information being shared between the two systems and to maintain state concurrence. These technologies could be used to monitor the performance, predict plant performance, evaluate potential scenarios before they make -- before the autonomous control system makes a decision.

So there are some security considerations in there like securing that communication link between the virtual representation and the physical system. And also the -- because of the bidirectional nature of the digital twin technologies, if you are able to insert malicious code on side, it can propagate to the other side. And how do you protect the data that goes back and forth?

Because the data protection strategy is an important part of maintaining stay concurrent.

Another technology that needs to be looked at for enabling autonomous control systems or artificial intelligence and machine learning which would be used in that whole OODA loop I was talking about, the predicting, perception planning, the decision making and actually applying of controls. And in this case, my colleague, Dr. Eskins, will get into it.

So I will not go too deeply into it. But you've got explainability. Why did this AI box make this decision? Some AI algorithms are so complicated, it's very hard to understand why with this input, that output came out. And then also there are a bunch of subversion attacks that we need to be able to consider.

So any new technologies used to remotely monitor or autonomously control these facilities have to be thoroughly understood. And this also is a work in progress. So we're working to support NRC staff by developing this necessary knowledge and how to go about securing it and developing a technical basis for it as well as identifying potential research gaps in these areas. And then just let me hand this off.

MEMBER MARCH-LEUBA: And we wait. Okay. So I've been telling you for the last 20 minutes denial of Service because it's the easiest way to attack one of these things.

MS. KIM: Right.

MEMBER MARCH-LEUBA: But there others which I don't know. So the only word I'm going to leave you with is completeness, one of my favorite words. Have you analyzed your system?

You're completely sure that you attach everything that can happen to is before you leave it and make it charge of your facility? And you're only working with cybersecurity. Other people have to work with the completeness of other functions.

But you look at it for the point of view of breaking the VPN or somebody to get this other key. But how do you know you got everything? Completeness, it's an impossible problem.

MS. KIM: It's -- I was going to say you can do the best you can.

MEMBER MARCH-LEUBA: And then I rather you put that best you can reactor in front of your heart, not next to mine. So you have to convince the public that the risk they're running is infinitesimally compared to the benefit.

MEMBER BROWN: May be better after he finishes his AI stuff. I'll wait.

CHAIR HALNON: Okay. One last thing for

me. It goes along with what Jose is saying about denial of Service. You mentioned remote monitoring is not as big a concern.

However, if -- I can understand how you could not -- if decisions are being made off site, you know it's not autonomous operation where it's a remote operation. But if decisions are being made offsite, whether it be short term or long term monitoring relative to trending and whatnot. Or you cut the ability to remote monitor is concerning.

So I mean, it wouldn't just be -- it's not really that important. It's very important, especially if decisions are made offsite. Remote operations is obvious.

Adulterate the operations communication line somehow, that's important. I wouldn't discount remote monitoring as being less important. It could be just as important.

MS. KIM: Yeah, I did not mean to discount it. I was just trying to compare it a little bit.

CHAIR HALNON: Yeah, I understand there's a --

MS. KIM: Yes, but there is a --

CHAIR HALNON: -- degree of urgency. I understand. Any other questions? Charlie, are you kidding me?

MEMBER BROWN: No, this is for her, though. One of the things to think about, I've got this plant remote autonomous. You've got to have remote monitoring. You have to know what's going on somewhere.

And the controls are being done locally because it's smart enough to do things. But it's your cyber security dilution. I want to echo his monitoring is critical because the hacker could hack -- make the plant look like it's just running smooth as silk, and it now has injected also control signals to make it not run smooth as silk.

So it's now going to turn into liquid uranium and he'll never know it because there's nobody on the site. There's nobody in the plant. There's nobody in the operations room. It's a dual problem that you have to deal with.

Once somebody gets in, they can go one way. They can go the other way. And you'll never know it. You will never know it until you got a pile of mush sitting out there in the desert or next door to some small community.

MS. KIM: I agree. And that's why I said in the --

(Simultaneous speaking.)

MEMBER BROWN: I had one other point. My point being with all that, I think it's incumbent upon you all, okay, it can't be us, to say no. There's going to be a big push to go do all this.

MEMBER MARCH-LEUBA: Maybe not incumbent, but it is possible. Don't consider just because a licensee or an applicant sends it to you. You have to say yes which is something that here in this building is almost true.

MS. KIM: I'm in research. They would never send it to me. So I would never have to say no.

MEMBER BROWN: But you are one of the authoritative voices because you all have done the underlying reviews and thought processes about what are the underlying problems that may not be communicated.

CHAIR HALNON: I'm fairly sure that no answer would be a community discussion. The federal office is not just --

(Simultaneous speaking.)

MEMBER BROWN: Somebody has got to raise their hand.

CHAIR HALNON: And identify all the vulnerabilities and potential consequences. It's too expensive. I mean, anything can be protected probably if spend enough money on it. But that's going to be a decision down the road.

(Simultaneous speaking.)

MEMBER REMPE: Sometimes in our meetings, we start off with comments, our meetings by individual members should be considered comments by individual members. And I think I don't recall hearing that at the beginning of the meeting today. And I think it's incumbent upon me to mention that. So go ahead, Jose.

MEMBER MARCH-LEUBA: I wanted to place on the record a comment by an individual member. You can beyond a shadow of a doubt that an autonomous control system operates safer, better than an operate. I mean, you can run it and you can guarantee that it's 100 times better than operate.

Unfortunately, I think that it's hard to prove is that autonomous system when they fail, the fail catastrophically. Those operators always fail nicely. I was reading this week I think of this Tesla in automatic driving mode that saw a pedestrian trying to cross the street and instead of stopping, he accelerate because I've learned that when you accelerate, the pedestrians, they jump out.

I was reading this. So when they fail,

they fail badly. So that goes back to the completeness issue. Don't accelerate against the pedestrians. That's what you need.

CHAIR HALNON: I think Tesla was just observing human behavior. Dr. Eskins, why don't you go on with your presentation.

MR. ESKINS: Thank you very much. Thank you, Anya. I am Doug Eskins. I am Dr. Kim's colleague over in the cybersecurity research team. And I'm going to briefly be discussing our projects in artificial intelligence and wireless technologies.

So beginning with artificial intelligence or AI, as we've kind of mentioned previously today, AI spans a broad variety of technologies from what's called limited AI which is very task specific and reactive all the way to what's called general AI which is much more independent and even theoretically one day could be self aware. A good general definition I use for AI, though, is just technology that can emulate human-like thinking, sometimes even super human-like thinking. Now as far as what we focus on in our research, we're looking at a subset of artificial intelligence known as machine learning or ML.

And this is a type of limited AI. It is

characterized by the ability to learn without explicit programming or even domain knowledge. And as you see in the news, there are constantly seemingly everyday new applications of machine learning. It is a very attractive technology.

Certainly industry, in the nuclear industry are starting to see the attractiveness to this. And there are several reasons. One has to do with its advantages for building models or representations. It can build models that can be built faster and cheaper.

These same models can be computationally more powerful and efficient than the kind of, say, physics-based models we have today. They can also represent new domains and more broad and integrated domains than our current types of models. Another very attractive feature is that machine learning models can be built without explicit domain knowledge.

So just collecting data, not necessarily knowing anything about the underlying system you're building, you can still build a machine learning model. So based on these attractive features, we think the industry and the nuclear industry will in the future expand its use of machine learning models in various capacities. Oh, not quite. Could you go back? Thanks, Tammy.

Now of course of the flip side of this, there are disadvantages to machine learning models. And one of them is that these models can be black box. That is the users and even the builders may not have detailed knowledge of internal structures and relationships which as we mentioned before makes them sometimes difficult to explain and also difficult to validate, verify, and quantify associated uncertainties.

Another issue with machine learning models is that because they are so highly dependent on the data used to build them and the training process with that data that the results can be non-deterministic. And if the data used to train the model is not complete, the model that is created may not fully represent all possible system states. They won't be complete.

MR. BLEY: Doug?

MR. ESKINS: Yes.

MR. BLEY: Dennis Bley. Two related things. Up there in the black box, you kind of hit on what I was talking about earlier. But given that, and maybe you're going to talk about this and that would be great.

One is how in the world can you even identify that such a system has been attacked. And that's the main thing. Since you don't know what's going on inside, you just see what it's doing on the outside. How do you have any idea if it's been the victim of a cyberattack? And if it has been, what can you do about it?

MR. ESKINS: Right. That's definitely an issue with this technology. You cannot look inside and validate the state of the model in many cases. So if there are changes that have been made to it due to a cyberattack, it would be difficult to detect that.

I think that's a subject of ongoing research for the people who intend to use these type of models certainly for applications where those type of state changes would be detrimental to some sort of safety-related process or so on. It's definitely -- I agree. That's a problem. And that's a subject of ongoing research.

(Simultaneous speaking.)

MR. BLEY: You're looking at that. And do you have -- has your research taken you to the point that you have some ideas of how people could attack such a system?

MR. ESKINS: I would say that our research at the NRC is still in its infancy. From looking at the literature, there are some discussions about how these type of models can be attacked. For example, if you can corrupt the training data, then you can corrupt the resulting model.

I think there are several examples. For example, with image recognition where small changes in the image can result in classification errors like -- so you mis-classify an animal or maybe a stop sign as a speed limit sign and so on because you really -- it's maybe not impossible. Certainly with what we know now, it is often difficult to understand how the model is coming to the conclusion --

(Simultaneous speaking.)

MR. BLEY: Okay. It'll be interesting to see how this goes in the future. I guess the only thing I was thinking, I guess you could feed it a bogus set that would teach it to develop wrong conclusions. But I don't know if anybody has been able to do that.

MR. ESKINS: Yes, I think that has been done. And there is also work, I believe, on using a different machine learning model to kind of detect corruption of the first model. But yeah, it's ongoing. And if you have any comments.

MEMBER MARCH-LEUBA: Let me be completely out of character here. As much as you can tell, I was not against but cynical of Anya's topic. I like your topic, Doug.

I think AI has future. And you just have to be limited to what it can do. You have to understand what it can do. If it's really, really good, I'm telling you, hey, this battery is not what I learned.

Your reactor typically behaves this way, and this is parting from it. I don't know what was doing it, but it's not what it's been doing before which is what we do when we're in the car and suddenly start hearing, nick, nick, nick, nick, nick. You say, well something is wrong. It's probably a belt.

But I don't know if it's a belt or not. But certainly it's not my car. So that is very good, and it has possibilities.

MR. ESKINS: I agree. And when we talk about the actual project, we'll briefly cover that kind of potential for classification.

MEMBER MARCH-LEUBA: But it doesn't need to classify as long as it detects departure from normal.

MR. ESKINS: Which I guess if you look at it, that's a kind of classification. But it's very broad. This is normal and this is abnormal.

MEMBER MARCH-LEUBA: The word of the year is going to be hallucination because that's what happens when you try to do too much with AI. You start hallucinating. But as long as you keep is simple, it has possibilities. That's enough.

CHAIR HALNON: I'd take that and run with it.

MR. ESKINS: And then definitely the goal of our research is to try to understand the technology and figure out those applications for which AI is good and maybe those applications for which it's inappropriate.

MEMBER MARCH-LEUBA: But to detect, it has to be in programs, I guess. So to detect that some part of my system has been tapered with and behaving abnormally, AI is perfect. Of course, you probably detect when your reactor starts smoking, right? Maybe before it starts smoking, you can see it. So it's not a bad application.

CHAIR HALNON: Well, I was more concerned and one of the reasons I asked to have it on here is try to understand you mentioned the no so good use of it. I'm thinking of the cyber hackers using it against itself to learn its vulnerabilities and keep on poking. To me, that's one of the worst things about AI is the bad actors taking hold of it and being able to use it more effectively than what we could use it.

MEMBER MARCH-LEUBA: The beauty of AI models is that not even themselves know how they work. So it's very difficult too. And what you heard that somebody just developed an AI model for the dark web.

So instead of you going into touring the dark web, you can ask questions to this. I mean, it's the same thing. So you can train them into bad things.

And you can train them to write software. You can train them to write malware. But that's what you're hearing on the news. This application is different.

MR. ESKINS: And that is a good comment. I agree. That's one of the two main areas in which we have concerns, how attackers would use AI and exploit AI applications, vulnerabilities introduced by it. So next slide.

Our research motivation for this is kind of along the lines of what we discussed here is that we've seen the increasing application of AI to cybersecurity generally across multiple industries. And also within the nuclear industry, we've seen more and more discussions about applying AI to the nuclear domain. So that intersection of those two areas, the application of AI to nuclear cybersecurity, we feel that there is a potential for future regulatory concerns.

And we need to do the research or we want to do the research now to be able to address those concerns in the future. And as I just mentioned, the two categories of those concerns. One is to ensure the cybersecurity of licensees use of AI, and the other, of course, is to look at what vulnerabilities may be introduced and especially by the attackers of, say, nuclear power plants who are using AI for their attack.

So we're kind of interested in both those areas. I think we'll go on to the next slide. So we have one project. It's a future focus research project that is directly related to this area of nuclear cybersecurity and AI.

And this project is exploring whether machine learning can be used to characterize nuclear cybersecurity states. I will say this is future research. So it's more blue sky and speculative than our normal research projects.

So the funding for this comes out of a different pot than our normal program office funded activities. But the overall concept of this project is can plant data be used to train a machine learning model? And can that model then be used to differentiate between cyber events and other events, which could be normal behaviors or equipment malfunctions.

We're also investigating if we can distinguish or differentiate between different types of cyber events. Now this is just basic research, so we're just trying to understand the technology. But if you're looking for an application in the near future, it may be that the licensee would use this as a sort of operator aid, not for direct control system.

Our goals are pretty straightforward with this project. We wish to understand how we would assess and validate these type of models. What vulnerabilities are introduced by this technology, and just basically to develop NRC staff competencies and knowledge in AI and the application to nuclear cybersecurity. I'll move on to the last topic which is --

MEMBER BIER: Excuse me. Before you move

on, I want to make sure I understand what's intended there. It sounds like you're anticipating that machine learning could be used in kind of a worry capacity, correct?

Like, we see something strange going on. This could be a cyber issue. Some human should go look into it. Is that accurate?

MR. ESKINS: I think that's a possible use case. Because of the complexity of plants and the cyber systems and so on, it'd be very difficult for a single individual to gather and understand all that information. So this may in the future be a useful aid to help operators understand the state of the plant and make decisions on what actions to take.

MEMBER BIER: Okay. Thank you.

MEMBER MARCH-LEUBA: This may not be applicable to cybersecurity nuclear plants, but cybersecurity detection. They have guys looking at screens to identify patterns. This computer is sending too many packets to the server in Finland.

And that I never seen before. And that's something an AI can do very well. I don't know how you would apply that to a system before your reactor smokes. But certainly it's applicable. I like you.

MR. ESKINS: One of the things we're doing with this project and we've partnered with Purdue University. They have the only all digital I&C research reactor. So it's very nice because we have access to a lot of those underlying data because it's digital already.

And we're looking at IT and TO data. And we're still in the exploratory phase trying to figure out what data sets are important to collect. What kind of insights can we obtain, and what type of machine learning models might be useful.

So we should complete this project in about a year. And then we'll have a public report that we publish detailing what we've learned. The final area I'll --

MEMBER BROWN: When you say digital, you mean software-based, not analog. You can build analog digital circuits, I mean, without software. I've done that before to control things.

It makes decision processes. You put data in. It decides whether you're going to do this or that or what have you. But it goes through logic based on the inputs you've done. So I presume you're meaning software-based distance. Okay.

MR. ESKINS: Yes, sir.

MEMBER BROWN: I just want to make sure I knew what you were talking about. Digital is not -- it can be other than software.

MR. ESKINS: And I cannot say if they don't have somewhere in the plant an analog meter or so on. But my understanding is that data is being converted over to digital form.

MEMBER BROWN: Absolutely, yeah, absolutely. I wasn't saying that. That wasn't the point. The point is that the overall process is software-based going through a sample time and coming up with the result at the end, not as opposed to a digital logic where data is coming in and boom, boom, steps through like a FPGA type thing.

MR. ESKINS: I believe they mentioned to me last time they had a data collection breach of about 20 hertz. So it was just a few minutes of information. There's quite a pile elected from all the different instruments which is a challenge in itself to try to understand that data.

Okay. So wireless -- our last topic is research on nuclear application of wireless technologies. And now because we already discussed wireless a little bit this morning and the technology is ubiquitous, most people understand when I say wireless what I mean. But for our project just to be specific, we looked at recognizable protocols like WiFi and Bluetooth.

But we also considered the more industry protocols like ZigBee and WirelessHART. And also as we discussed, the background here is it's a little redundant. But a current licensee cybersecurity plans which have to be approved by the NRC prohibit the use of wireless in safety applications.

And what this does is in addition to certain design features like deterministic data diodes, it helps to establish isolation for the safety-related systems as well as supporting the required defense-in-depth for their cybersecurity protected strategies. Now we're motivated to perform this research because licensees have become very interested in using or expanding their use of wireless and nuclear power plants. And they desire to do this because they want to reduce radiological exposure to their staff or O&M costs, a couple of reasons.

And as we discussed it this morning, these applications could include the installation of monitoring and control functions on or near safety equipment. Now this obviously could be a concern because it could violate or it could affect the isolation requirements that is the predicate for a lot of our cybersecurity plans and analysis. Because it's possible that licensees may want to engage with the NRC to allow the use of wireless, we are conducting this research.

And we are anticipating engagement to address these issues. Some examples of the challenges that we face or a licensee would face is ensuring that any changes to a wireless system or any implementation of wireless would maintain the same or better levels of cybersecurity. Also that it would maintain the required defense-in-depth requirements.

So one step that we are taking is to try to learn from other applications of wireless and safety critical applications. And we undertook a research project in 2021 where we went out in a two-step approach. We looked at literature regulations and guidance from other places on their use of secure wireless.

And we also surveyed critical infrastructure subject matter experts on how they use wireless in safety critical applications. Now what we found from this report was that there's a large amount of material on the secure use of wireless in a traditional IT network. But both are lit reviews and interviews with subject matter experts indicated that there is no significant use of wireless for safety critical applications.

MEMBER MARCH-LEUBA: This was a consequence of the fact that it was a problem with the technology, the fact that people do not feel comfortable using it, or there was no history, I don't want to be the first one? What do you attribute it to?

MR. ESKINS: The report listed these two reasons that I can recall. One is the lack of appropriate guidance.

MEMBER MARCH-LEUBA: I don't want to be the first one.

MR. ESKINS: Right, right. And there were considerable unknowns in how to implement this securely.

MEMBER MARCH-LEUBA: Anybody concerned about EMI, electromagnetic interference, on other equipment? When you start beaming electromagnetic energy in a room, your cables start getting it.

MR. ESKINS: We did actually. We had a separate project which looked at those kind of issues from a safety perspective. It's outside of cybersecurity. But actually we kept an eye on that report as well. I supposed an adversary could use some sort of an EM pulse weapon to exploit that sort of vulnerability as well. In this case, we just looked purely at the cybersecurity implications.

MEMBER MARCH-LEUBA: Yeah, the Bluetooth especially is a short length. You cannot pack my Bluetooth device on the street. WiFi, you can do 100 feet. It has some advantages, but cybersecurity.

CHAIR HALNON: So with what you know now, do you see an avenue where this wireless could be used safely? I mean, I know you haven't really found any place that it's being used at this point. But do you see potentially an avenue where it could be?

MR. ESKINS: I would say it's too soon to tell. We are just really beginning to explore this area in research space. So I wouldn't venture to comment on that right now. I don't know if anyone.

MR. GARCIA: I was going to say -- Ismael Garcia. I was going to say do we have a following effort, research that's getting to that question. If you were to use safety-related functions, for example. What needs to happen to do it --

CHAIR HALNON: Yeah, I mean, I know that --

MR. GARCIA: -- in a safe and secure manner?

CHAIR HALNON: -- industry is using it in work controls and other things, business applications for lack of a better term. But I know there's a high desire to move into being able to employ the technology to do this because the wiring and the fiber optics and all that stuff is very expensive to do to get into a place where we can do locally WiFi type, then maybe not same frequencies. Maybe some way encrypting it or whatever the case may be.

That would be highly desirable. Now when we get into the advanced reactors, especially potentially movable reactors, you're not going to have the ability to wire up a new control room every time you move the potential transportable reactor. So you have to start thinking about, okay, how do we move the whole infrastructure or this reactor control? And I don't see any other economical way to do it other than somehow wireless. But of course, I know you have to make it safe too. So anyways --

MR. COOK: If I could make a comment.

CHAIR HALNON: Sure.

MR. COOK: Sure. I'm Chris Cook, Chief of Instrumentation Controls, Electrical Engineering Branch and Research. What I just want to add onto that is one of the things that we're doing as Doug was talking about is trying to make sure that we're following the research that is being funded outside particularly by DOE. There's a large effort through LWRS, through other programs that are happening within DOE where they're looking to try to use wireless.

We're trying to monitor their efforts and work collaboratively. We have MOUs with DOE. We also have MOUs with EPRI. And that's part of what we see in the Office of Research is really understand as they're pushing forward with looking at the capabilities of technologies.

What are the vulnerabilities? What changes would need to be made to the security controls? I'm sure Brian can expand upon that and some of the things that industry and other groups like NEI you're already approach the agency about.

But that's really what we see our mission as trying to help them be ready -- the staff be ready for when that comes, if it comes. And looking at the amount of money that these other federal agencies are putting into it, I think it's more of an if -- sorry, a more of a question of when and not if. It'll come.

CHAIR HALNON: That's good to hear because obviously the regulatory process needs to be in parallel, not --

MR. COOK: Yeah.

CHAIR HALNON: -- blocking it.

MR. COOK: And we're trying to be ready for that. But we're also -- Member Brown, other comments by other people, understood, clearly understood that. And that's why we're looking at it trying to see, well, how can we be ready for that? What do we need to be looking at?

What are the controls, the other things that need to be changed to put in place to have that for the operating fleet because it's the O&M costs? And then we're also trying to look ahead into whatever would happen after the rulemaking go forward and the guidance happens. And I realize it's more of the advanced reactor type of meeting than the operating ones. We're trying to be ready for that.

CHAIR HALNON: And it's not just you don't have it. It's obsolescence. By the time you hook up your computer at the house, it's obsolete. So just trying to keep these plants going for 80 years. We need to have new technology.

MR. COOK: And what we're seeing, like, with DOE, they have the advanced monitoring program, the program that's there. They're trying to go in and say, can we, outside of our secure network, just put a camera? Watching an analog gauge and then beam that into control.

Can we remove particular surveillance for fire watches if we just have a monitor that's there that's all the time working? You don't have to worry about them missing. So these are the things that DOE is putting a lot of money into in funding and looking out with different utility groups.

And so this is what we're trying to keep up with. That's the fun part of our job is, like, okay, what's going to happen. When is this coming? How do we get ready for it to sort of see what are our controls? Because they're looking at trying to put these technologies out there. But we're looking at with our different perspective of what are the safety and security impacts on making sure we fully flesh that out.

CHAIR HALNON: Thank you.

MR. COOK: Yeah, thank you.

MR. ESKINS: Thanks for those comments, Chris. Appreciate it. So the results of this report have been published in a technical letter report with the ADAMS session number on this slide. This is just our first step in trying to explore the nuclear wireless cybersecurity problem space. As Ismael just mentioned, we have an ongoing project to do a security impact assessment on a wireless application. And of course, we are monitoring other activities and hoping this will inform future research in this area.

MEMBER BROWN: I thought you were done.

MR. ESKINS: I am.

MEMBER BROWN: Then I'll raise my hand. We're going to do all this wireless and where are we going to store all the batteries for all the remote wireless devices we're laying around. I mean, if --

MEMBER MARCH-LEUBA: That's what the power cable is for.

MEMBER BROWN: Well, we're just seeing as Greg said, you got to run this cable down there to get this data back out. Well, we're going to have to have battery storage, thousands of batteries sitting up there, all different kinds because nobody will use the same type of battery. And they won't use the ones you can buy in the hardware store.

There'll be special ordered that you have to go online to guy because there'll be no store to go to. There's a little bit of a supply -- it's not a supply chain issue. It's a matter of uniformity of what you could do.

If you're going to do wireless, you sure as heck better think about what you're going to do. And you also have to make sure, like, with my high tech smart phone. I walk three feet in my house and I go from two bars to none. So depending on the wireless system you have set up, of course, this is an exception. You've got your towers that you have to deal with and there's loads.

You're going to have the same type of things. So the pattern when you walk around a hunk of big huge wall that's all steel, you might all of a sudden not have information. So there's a lot of other little nuances that need to be thought about with this.

And I haven't heard a single person tell me about the thousand batteries they're going to use once you hook up all these wireless things because they're all unique locations. Every instrument will need a new wireless device to broadcast because otherwise you got to run cables between them with other sensing devices, computational devices, and input devices to get the data where it can be used by the wireless thing you're using. There's a lot of -- people talk about how nifty it is.

I'm a great one for -- one of the arguments these days in the plant world is for backup systems. Could you be allowed to use diverse software type systems or backup systems as opposed to hard wire switches to turn your pump on or off in the existing reactors and stuff like that? I'm not going to use a new set of complex diverse software that I have to validate that doesn't ever get compromised as opposed to a switch that I turn and the motor stops if the rest of the plant has been compromised for some -- or you don't have access to the main control room.

Small thoughts like that just seem to be dismissed. I just think you have to be careful as you're walking down the path. There are some valid uses or critical uses when you talk about high radiation areas.

Then you make -- do I want to run a cable or does the wireless device give me better, more suitable results? And that could be a battle between simplification of the cables or the more complex wireless. I'm not sure I know how I would probably votes. But you'd still need a battery for the wireless device.

CHAIR HALNON: You can tell what keeps Charlie up at night.

MEMBER BROWN: I hate to say it, but I do. I worry about this stuff. I know we got to look at it. You can't ignore it. It's just like you were talking about the AI machine learning a minute ago.

You made the comment about it can build models, the physics models we build using our brains. But hold it. If it's going to build models, it's got to have physics embedded in it and somehow be able to use that physics. And it's the same physics you would be manually building the model with.

So the training is all what you would be using. And now you're going to embed it. And now you get all the nuances that you know are embedded in that training into it. That's another difficult problem in itself.

CHAIR HALNON: Let's go ahead and move on before another --

MEMBER BROWN: Oh, I've got more.

CHAIR HALNON: I know. That's what I'm saying.

(Simultaneous speaking.)

MEMBER MARCH-LEUBA: I need to add something for the record because I don't dislike (audio interference). I know you don't know what a smart TV is.

MEMBER BROWN: What?

MEMBER MARCH-LEUBA: Smart TV. I have

many of those in my house. You just go plug it to the 120 volt and they work. WiFi, they could get the signal. And everything works fantastic. So even though you have a power cable doesn't mean I have an ethernet cable.

MEMBER BROWN: No, I got a smart TV, but I'm not.

CHAIR HALNON: All right. Let's bring it back, guys.

MEMBER MARCH-LEUBA: So there are applications. There are applications where certainly I wouldn't want to have a cable for my smart TV.

CHAIR HALNON: Okay. Take control.

MEMBER BROWN: Mine's got a cable.

MS. ANTONESCU: There's a bunch of research that --

CHAIR HALNON: No, you're on. It's just you got to state your name.

MS. ANTONESCU: Oh, Christine Antonescu. Some of the research that was undertaken with Oak Ridge National Lab. I don't know if you're aware. I think two of them at least assessing the impact of wireless technology and the other one as deploying wireless technologies for safety systems. So I don't know if you're aware of them.

But we've done a lot of work. Research was ahead of the game about ten years ago on wireless. I was part of it.

MEMBER MARCH-LEUBA: I never copied.

MS. ANTONESCU: Yeah.

MEMBER MARCH-LEUBA: The email numbers.

CHAIR HALNON: Okay.

MS. ANTONESCU: I have to find the NUREG numbers. I forgot.

CHAIR HALNON: Doug, go ahead and wrap up your presentation.

MR. YIP: I can wrap up. This is Brian Yip. I'll just wrap up by thanking Dr. Eskins, Dr. Kim for their presentations and as well as to Chris and the rest of his branch. As you saw, these are really complex topics and their work is critical to us being able to review these appropriately once they come down the pipe to us.

Many of these topics are interrelated. Like we saw the discussion about machine learning and how that might apply to autonomy or operations and wireless. We'll just highlight these three bullets here, just highlight some additional research we didn't cover in this presentation today. But we're looking at EPRI has an approach called the technical assessment methodology.

We're looking at that approach and how it looks. Critical digital assets, how you look at their attack surface. And then address different ways that they can be exploited by security controls.

We're looking at that and similar approaches and how licensees might be able to apply them in novel ways, including during digital I&C upgrades. I know Vogtle used that approach for some of its applications too. Just looking to see where that might also be able to be applied.

Also looking at digital I&C upgrades. The current research is looking at all of the security controls in the cybersecurity plans and sort of a final life cycle approach to them. So if a plant wanted to start thinking about cybersecurity in advance during a digital I&C upgrade process, what controls might they consider during the design, during early on in the upgrade if that's their advantage.

And the lastly although there are a lot of -- some are rigid cybersecurity controls in the security plans, there are processes for plans to take an alternate approach if that's appropriate. And so research is also helping us look at how we think about what is a alternate approach and how inspectors might be able to assess those out in the field. With that, I'll just say thank you and turn it back over to you.

CHAIR HALNON: Thank you, Brian. Members or consultants, any other questions?

Okay. This time, we'll go out for comments from the public. Anyone from the public desires to make a comment, please unmute yourself. Identify yourself and state your comment. I'll wait for a couple minutes. So anyone from the public want to make a comment at this time?

Okay. Not hearing any comments, I'll go ahead and close the meeting. I want to thank the staff. You all did a fantastic job bringing this all together and a very comprehensive topic.

Also wanted to thank, if you guys would pass on to Ryan from DHS, for joining us today. It's a very important topic. I'm sure that we'll -- as the technology moves on, we'll probably maybe next year ask for an update.

Probably shorter, but we do appreciate the passing along of information and everything that you were able to bring to us. The information that we heard today and the dialogue that we had look at future reactors. Every time we get to the advanced reactor application, we talk a little bit about autonomous, wireless, all kinds of things.

And knowing that you guys are looking at this and aggressively going after it will help. And certainly if we come up with any show stopping type questions in any of our reviews, we'll call on you to come in and help us understand how we get beyond that. Again, I want to thank you, Brian. Thank you for your staff, Chris, for coming in. Last chance, any members?

MEMBER REMPE: I want to thank not only the staff but also you and Christina and Charlie and Jose because I think all of you worked together to get this together.

CHAIR HALNON: Yeah, I appreciate that because especially what Dan and Christina put together the agenda. And we had a couple scheduled meetings that were very good. So everyone did a fine job getting this put together.

Like I said, it's very broad. As we know, we went around the circle a few times on some of these things. So thank you for reminding me. Anything else?

MEMBER MARCH-LEUBA: Yeah, I wanted to thank you guys. As I say at the end of these presentations, if I talked too much, it's because the topic is interesting. So if you look at the topic, the transcripts, and you see, Jose, shut up, it's because it's boring.

I was not complaining about your devices or your approaches. I did have an agenda. I make a prediction. I won't be here forever. I'm making a prediction that one of these days we're going to have a cyberattack in an operating plant.

And you guys are going to be on CNN all weekend. And they're going to call on you and say why didn't you prevent? So I do have an agenda. I know that this is serious.

As much as I love research, I love research most of my life. We protect operating reactors. And it's not just the nuclear island and the RPS. It's everything that is around it.

We need to protect the aquarium. And every time you guys go to a power plant and do an audit on the cyber protection system, ask them what is their program and is it protected. Because somebody is going to get into one and we have a lot of egg in our faces when we say that we have a program, and we have audited, and this still went past us. Thank you.

CHAIR HALNON: We started with an aquarium of dead fish and we're ending with an aquarium of dead fish. Charlie, you had --

MEMBER BROWN: Another dead fish here. No, I've made a lot of what sounds like very skeptical, negative, critical comments. I am skeptical, but its' incumbent upon us to be skeptical.

And as Jose noted, we're both very, very cautious when we look at this whole world. And even I don't want to take comments or questions as negative because it was really to engender the input that we got from all the presenters, okay, relative to the subject. It's a very important subject and it's getting more and more as the days and months go on.

So I just really appreciated the candid back and forth, the disagreements when you disagreed which was just fine. That's why we do it. I did want to thank everybody, and that's all. You can pass it on to the earlier presenters as well because I thought the meeting came out very, very well.

CHAIR HALNON: Thank you, Charlie. Vesna.

MEMBER DIMITRIJEVIC: Well, I was quiet most of the meeting. But I just really want to thank for the great presentation. I took a million notes.

I just want to make a comment which I actually find most fascinating that you didn't talk about this 53 and technology includes risk informed and performance based. And I think that this is the area where this is totally not applicable first because this is not technology inclusive. Technology is unlimited.

They're merging. They're growing every day. Performance based, there is no way that we can make performance because as Jose pointed in the beginning, the challenges -- numerous challenges coming every day.

And then what is my area when it comes to the risk informed, risk informed is only possible if we don't really define pre-release. And this million new risk challenges come with that. Totally something never considering the PRA or, you know, like, what happened errors of commission or the -- it doesn't have to happen during the plant operation.

If we look what in Chernobyl, in the different test and maintenance. So it's a fascinating area. And my favorite slide is this last slide with the million question marks lined down because that's something which we will be addressing in the future. So thank you.

CHAIR HALNON: Thank you, Vesna. At the risk of someone taking me up on it, I'm going to look around the room one more time. Okay. We thank you again. And with that, meeting is adjourned.

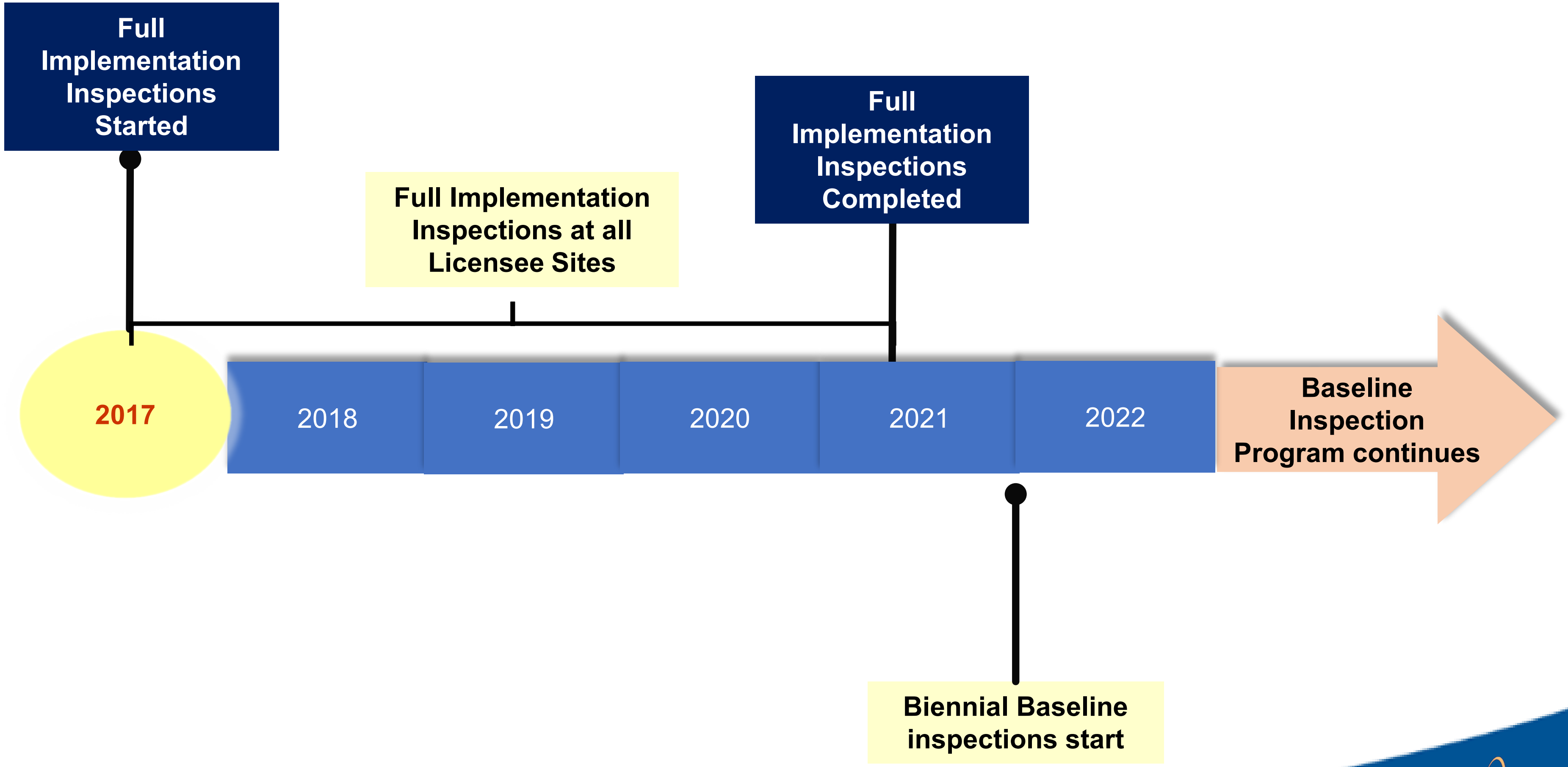
(Whereupon, the above-entitled matter went off the record at 2:58 p.m.)

NPP Cybersecurity Current Status and Contemporary Threats

Dan Warner
Cyber Security Branch (CSB)
Division of Physical and Cyber Security Policy (DPCP)
Office of Nuclear Security and Incident Response (NSIR)

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

US NRC Cybersecurity Program



Key Messages

- Cybersecurity controls in place at nuclear power plants provide defense against attack pathways of concern.
- Programmatic controls ensure that the cyber program is positioned to address the ever-changing threat environment and ensuring defense-in-depth is maintained.
- Inspection program verified licensee implementation of cybersecurity programs and now reviews program maintenance.

Definitions

- Critical System – An analog or digital technology-based system in or outside of the plant that performs or is associated with a safety-related, important-to-safety, security, or emergency preparedness function.
- Critical Digital Asset (CDA) – A digital computer, communication system, or network that is:
  - A component of a critical system; or
  - A support system asset where failure/compromise by cyberattack would result in an adverse impact to SSEP function

Definitions

- Types of CDAs and Required Controls:
  - EP CDAs – CDAs associated with EP functions that do not have an independent and diverse alternate method to perform the EP function.
    - Controls: Baseline controls or full direct CDA controls.
  - BOP CDAs – CDAs added to the cybersecurity rule scope during the resolution of FERC Order 706-B.
    - Controls: Addressed in subsequent slides.
  - Indirect CDAs – CDAs that cannot have adverse impact on safety or security functions prior to detection/compensation of compromise/failure implemented.
    - Controls: Baseline cybersecurity controls.
  - Direct CDAs – CDAs not assessed as Indirect, BOP or EP CDAs.
    - Controls: Determined through cybersecurity controls assessment.

Baseline Cybersecurity Controls

- The following controls are the baseline cybersecurity controls for EP, Indirect, and BOP Scram/Trip CDAs.
  - Located within the PA/VA, or NEI 08-09 Section E.5 controls applied.
  - No active wireless internet communication on CDA or interconnected assets.
  - CDA and interconnected assets are air-gapped or isolated by deterministic device.
  - Portable media use is controlled in accordance with NEI 08-09 D1.19.
  - Changes to CDA are evaluated and documented before implementation.
  - CDA or interconnected equipment affected by compromise of CDA periodically checked to ensure it is can perform its intended function.
  - Ongoing monitoring and assessment is performed to verify the baseline security criteria remain in place.

Attack Pathways

- Licensees are required to ensure all potential attack pathways are protected. These include:
  - Physical access
  - Wired connectivity or communications
  - Wireless connectivity or communications
  - Supply chain
  - Portable media and mobile devices (PMMD).

Attack Pathways: Physical Access

- Physical access controls ensure only the appropriate personnel are able to interface physically with a CDA.
- Sample applicable controls:
  - Access control policy and procedures
  - Account management
  - Access enforcement
  - Physical access controls
  - Least Privilege
  - Logging

Attack Pathways: Wired

- Wired access controls ensure only the appropriate personnel are able to interface with a CDA using a wired network.
- Sample applicable controls:
  - Access control policy and procedures
  - Account management
  - Access enforcement
  - Physical access controls
  - Least privilege
  - Logging
  - Network access control
  - Open or insecure protocol restrictions
  - Insecure and rogue connections
  - Use of external systems

Attack Pathways: Wireless

- In addition to the previous controls, wireless access controls ensure the implementation of adequate protections and procedures to minimize the cyber risk associated with the use of wireless technologies.
- Sample applicable controls:
  - Only allowing wireless access through a boundary security control device.
  - Prohibiting use of wireless for CDAs associated with safety-related and important-to-safety functions.
  - Disabling wireless when not used.
  - Conducting scans or employing a wireless intrusion detection system for unauthorized wireless access points and disabling them if they are discovered.

Attack Pathways: Supply Chain

- Supply chain controls ensure cybersecurity risks throughout the supply chain are identified, assessed, and mitigated.
- Sample applicable controls:
  - System and services acquisition policy and procedures
  - Supply chain protections
  - Trustworthiness
  - Developer security testing and evaluation
  - Licensee/Applicant testing

Attack Pathways: PMMD

- Portable media and mobile device (PMMD) controls ensure the implementation of adequate protections and procedures to minimize the cyber risk associated with the use of unapproved PMMD.
- Sample applicable controls:
  - Usage restrictions and implementation guidance for controlled PMMD.
  - Authorizing, monitoring, and controlling PMMD access to CDAs.
  - PMMD security/integrity are maintained at level consistent with CDAs they support.
  - PMMD only used in one security level and are not moved between security levels.

Programmatic Controls

- Programmatic controls are necessary to maintain security throughout the life cycle of CDAs. One of the primary purposes of these controls are to ensure that as the threat environment evolves, licensee systems remain secure from cyber-attack.
- Sample programmatic controls:
  - Continuous monitoring and assessment
  - Periodic assessment of security controls
  - Effectiveness analysis
  - Vulnerability assessments and scans
  - Configuration management
  - Change control
  - Security impact analysis of changes and environment
  - Cybersecurity program review

Vulnerability Management

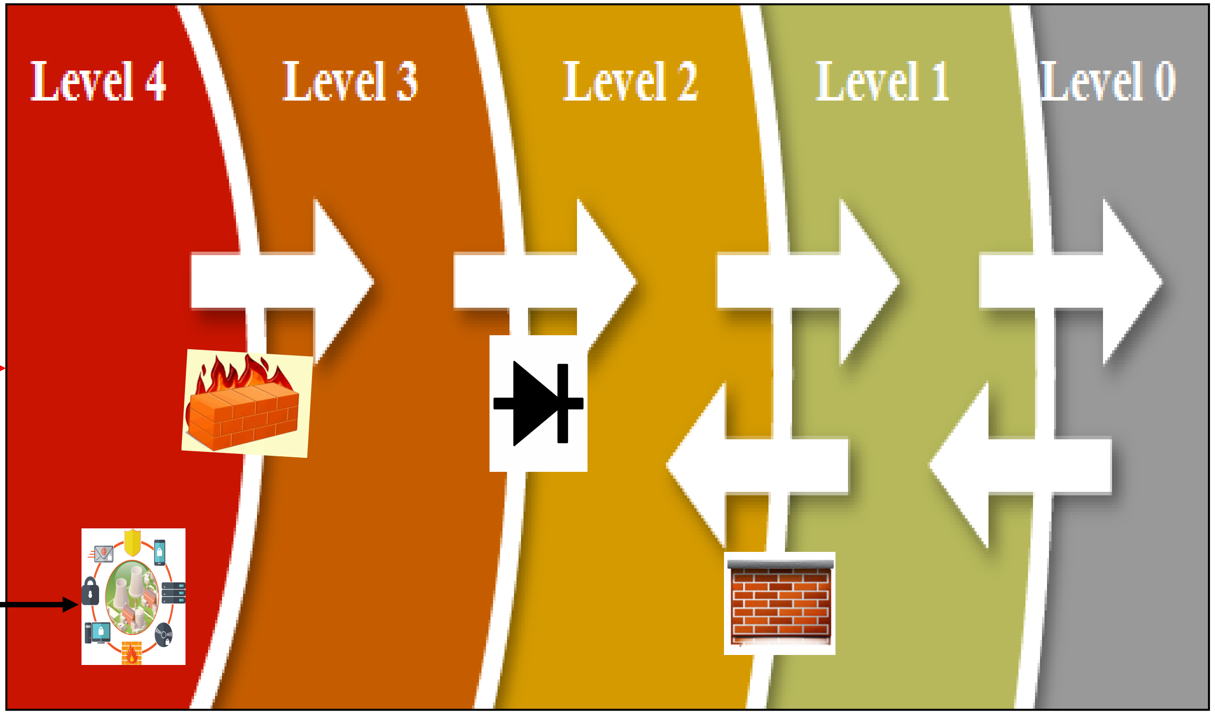
- To protect against the ever changing threat environment, nuclear licensees are required by their CSPs to address ongoing threats and vulnerabilities to CDAs by performing vulnerability assessments or scans and evaluations to identify applicable corrective actions required to mitigate/remediate vulnerabilities to maintain adequate defense-in-depth and prevent CDA compromise or exploitation. The following are some of the controls used to address vulnerability management:
  - Installing operating systems, applications, and third-party software updates
  - Flaw remediation
  - Security alerts and advisories
  - Contacts with security groups and associations
  - Evaluate and manage cyber risk

Defense-in-Depth

- As stated in 10 CFR 73.54(c)(2), the licensee must design its cybersecurity program to apply and maintain integrated defense-in-depth protective strategies to ensure the capability to detect, prevent, respond to, mitigate, and recover from cyberattacks. An acceptable defense-in-depth protective strategy includes:
  - A defensive architecture that describes a physical and logical network design that implements successive security levels separated by boundary control devices with segmentation within each security level.
  - A defensive strategy that employs multiple, diverse, and mutually supporting tools, technologies, and processes to effectively perform timely detection of, protection against, and response to a cyberattack.

Implementation Guidance

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



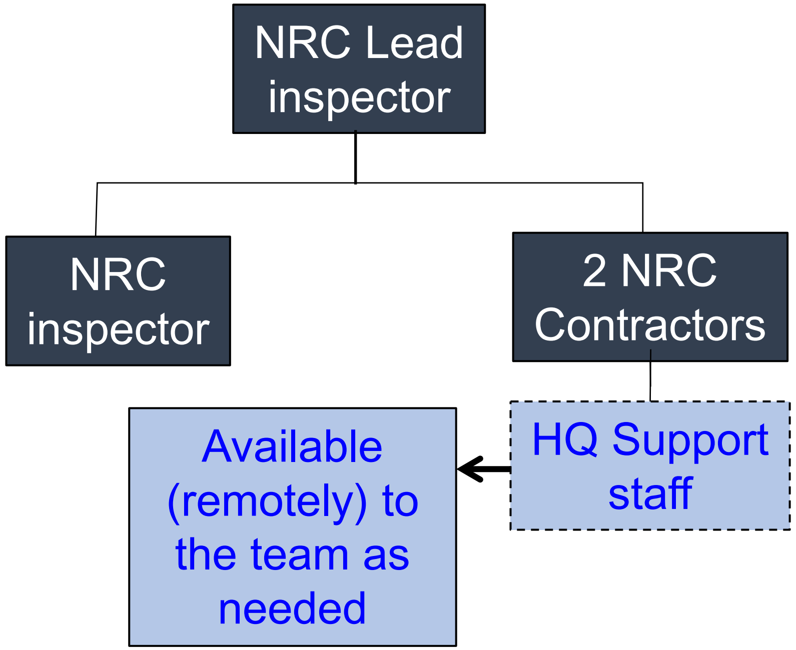
5. Cyber Security Program Must Include These Areas to Support Implementation

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

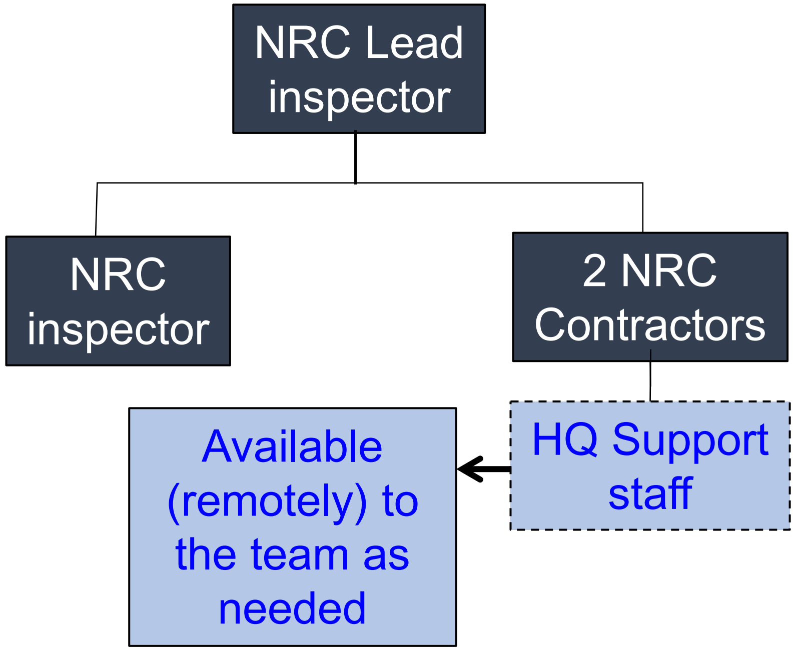
Full Implementation Inspection Resources (2017-2021)

- Inspection Procedure IP 71130.10P
- Team Composition (four-person team)
  - Two regional inspectors
  - Two contractor SMEs
- The initial round of full implementation inspections were completed in 2021 and focused on ensuring licensees were in compliance with the requirements for establishing their cybersecurity program.
- These inspections consisted of a week onsite followed by an offsite week, followed by a 2nd week onsite



Current Inspection Program Resources

- Inspection Procedure IP 71130.10
- Team Composition (four-person team)
  - Two regional inspectors
  - Two contractor SMEs
- Inspections focus on reviewing changes to the program and ensuring licensees are implementing their programs to ensure cybersecurity is implemented throughout the lifecycle for newly installed CDAs.
- Current inspections consist of a prep week offsite then 1 week onsite.



Questions

Government Interaction: Coordination Between NRC/NERC/FERC and the Role of DOE and CISA

Dan Warner

Cyber Security Branch (CSB)

Division of Physical and Cyber Security Policy (DPCP)

Office of Nuclear Security and Incident Response (NSIR)

Key Messages

- NRC has a long history of engagement and cooperation with FERC, DHS/CISA, and other Federal partners on cybersecurity and other issues.
- NRC's engagement with FERC on cybersecurity ensured appropriate protection for balance of plant CDAs.
- The Cyber Assessment Team process is designed both to coordinate internal response to cyber issues as well as support early engagement with interagency partners.

BOP Background

- January 2008 – FERC issued Order No. 706 which specified Critical Infrastructure Protection (CIP) Reliability Standards to safeguard critical cyber assets.
    - Exempts facilities regulated by the NRC.
- March 2009 – NRC issued 10 CFR 73.54, "Protection of Digital Computer, Communications, and Networks" to NRC power reactor licensees.
    - Did not cover all balance-of-plant (BOP) equipment at NRC power reactor facilities, creating potential gap between NRC and FERC cybersecurity requirements.
- March 2009 – FERC issued Order No. 706-B to clarify that NPP BOP systems and equipment not within the scope of 10 CFR 73.54 are subject to CIP standards approved in Order No. 706. Nuclear facilities were allowed to seek exemptions from NERC's CIP standards on a case-by-case basis for those digital assets that they believed were subject to the NRC's cybersecurity requirements.

BOP Background Cont.

- December 2009 – NRC and NERC sign memorandum of understanding (MOU) addressing they would handle respective authorities over NPP cybersecurity issues.
- 2010 – NERC sent "Bright-Line" survey to NPPs requesting that they determine which of their SSCs were potentially subject to NERC CIP standards and which were potentially subject to NRC cyber security regulations.
- In August of 2010, NERC informed the NRC that based on the responses to the Bright-Line Survey, NERC concluded the assignment of regulatory authority for the BOP SSCs from the NERC CIP standards to the NRC cyber security authority was acceptable.
- Memoranda between the NRC and NERC/FERC discussed in more detail in subsequent slides.

BOP Changes

- In November 2012, NERC adopted CIP-002-5 on how to identify and categorize Bulk Electric System (BES) cyber systems and associated cyber assets based on adverse impact of loss, compromise, or misuse could have on the reliable operation of the BES.
- In 2022, NRC approved for use revisions to NEI 10-04 and NEI 13-10, which incorporate the graded approach in the latest versions of the NERC-CIP standards. This approach uses a number of criteria, primarily electrical output of a facility, to determine if they are Low Impact (1500 MWe or less) or Medium Impact (greater than 1500 MWe) to the Bulk Electric System and the required cybersecurity controls.
- NRC staff coordinated with staff in the FERC Office of Electric Reliability to ensure the changes being made were consistent with the latest NERC CIP.

Low Impact Controls

- CIP Reliability Standard 003-7 defines the cyber security controls to be applied to BES Cyber Systems. For Low Impact CDAs (called BOP CDAs), the following cybersecurity controls apply:
  - Cyber Security Awareness
  - Physical Security Controls
  - Electronic Access Controls
  - Cyber Security Incident Response
  - Transient Cyber Assets and Removable Media malicious code risk mitigation
  - Declaring and responding to CIP Exceptional Circumstances

Medium Impact Controls

- CIP Reliability Standard 003-7 defines the cyber security controls to be applied to BES Cyber Systems. For Medium Impact CDAs (called BOP-SCRAM/Trip CDAs), the Low impact cybersecurity controls apply plus the controls listed below. The baseline cybersecurity controls discussed in the previous presentation apply to these CDAs. There are currently no CDAs identified as Medium Impact at NPPs.
  - Personnel and Training
  - Electronic Security Perimeters
  - Physical Security Controls
  - System Security Management
  - Incident Reporting and Response Training
  - Recovery Plans
  - Configuration Change Management and vulnerability assessments
  - Information Protection
  - Declaring and Responding to CIP Exceptional Circumstances

NERC CIP-003-9 Analysis

- CIP-003-9 was recently released and includes an additional control for Low Impact facilities.
- CSB staff reviewed CIP-003-9 to determine what changed from the previous revision and if it impacts BOP CDAs.
- CIP-003-9 adds an additional control specific to Low Impact power generation facilities which requires facilities to implement vendor electronic remote access security controls.
- Staff reviewed the controls required in the revised NEI 13-10 Rev. 7 and determined that the existing controls in Section 3.2 include “electronic access controls; air gapped or isolated by a deterministic device” for any Low Impact BOP CDAs. This existing control already ensures the new vendor remote access control requirements are addressed and therefore no further action is required by NRC power reactor licensees.

Federal Agencies			
Department of Homeland Security Cybersecurity and Infrastructure Security Agency	Department of Energy	Federal Energy Regulatory Commission	Nuclear Regulatory Commission
Cyber Security-Related Responsibilities			
• Lead the National effort to understand and manage cyber and physical risk to the U.S. critical infrastructure • Their responsibilities include communicating threats/vulnerabilities and provide incident response services for the U.S. critical infrastructure • The NRC would interface with the Cybersecurity and Infrastructure Security Agency during a significant cyber incident at an NPP licensee	• Responsible for advancing the energy, environmental, and nuclear security of the U.S. • The Office of Cybersecurity, Energy Security, and Emergency Response leads the Department of Energy's emergency preparedness and coordinated response to disruptions to the energy sector, including cyber-attacks • The NRC would interface with DOE during a significant cyber incident at a nuclear power plant	• Regulates the interstate transmission of electricity, natural gas, and oil • A memorandum of agreement between NRC and FERC facilitates interactions on matters pertaining to nuclear power plant cybersecurity • NRC and FERC coordinate activities regarding nuclear power plant cybersecurity	• Regulatory oversight responsibility of the "Nuclear Reactors" critical infrastructure sector • Perform cybersecurity inspections at nuclear power plants • Coordinates with other federal agencies as needed on matters pertaining nuclear power plant cybersecurity

Cyber Assessment Team (CAT)

- CAT is a team of headquarters and regional cyber experts that activates in response to cyber events at NRC licensees:
  - Includes NSIR cyber security staff, HQ SMEs, and regional cyber security inspector.
  - Evaluates cyber events at NRC licensees (primarily power reactors).
  - Assesses the severity of the event and recommends actions to agency leadership.
- CAT assists in internal coordination between headquarters and regions.

CAT Activation

- CAT is primarily activated by the Operations Center in response to licensee event reports under 10 CFR 73.77.
  - Any reportable cyber event under 73.77(a) triggers notification of the CAT Lead.
  - There have been no 73.77 reports since the rule took effect in 2015. There have been incidents on non-regulated licensee systems such as corporate networks, but the CAT was not activated in part due to privacy concerns.
- Management, the CAT Lead, or regional staff can request activation of the CAT based on information received from/about a licensee or other industry cyber event.
  - CAT has activated to leverage the process to assess non-licensee cyber events.

Example of CAT Interaction with CISA

- CAT lead is notified of an incident involving a licensee's business network, such as a ransomware attack or exfiltration of data.
- CAT lead determines if the incident would have an impact on NRC regulated systems. If not, no further activation of the CAT is needed.
- CAT lead works with CSB Chief to determine if any briefing documents for management need to be prepared and if any courtesy notifications need to be made to DHS/CISA.
- If CISA notification is needed, contact is made with the Nuclear SRMA and Threat Hunting groups to ensure awareness and provide points of contact for any necessary follow-up.

DHS Threat Hunting NRC Training

- NRC staff are working with staff from the DHS Cybersecurity Division's Threat Hunting team, who are responsible for responding to cybersecurity incidents at critical infrastructure facilities, to help familiarize them with nuclear technology.
- The Threat Hunting team visited the NRC's Technical Training Center to attend a session of R-105, "Nuclear Technology for Security Course."
- The team will be visiting the Millstone power plant to become familiar with a licensee facility and will also be participating in a short class on radiation protection later this year.

Questions

NRC's Coordination with FERC and NERC

Jorge A Cintron-Rivera
Office of Nuclear Reactor Regulation
Division of Engineering and External Hazards
Long Term Operations and Modernization Branch

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

Outline

- Purpose and Objectives
- Background
- NRC and FERC Requirements and Standards
    - Common interests
- Interagency agreements (IAAs) and interactions
    - Memoranda of understanding (MOUs)/Memorandum of agreement (MOA)
    - Responsibilities for the Nuclear Regulatory Commission (NRC), Federal Energy Regulatory Commission (FERC), and North American Electric Reliability Corporation (NERC)
- NRC-FERC Jurisdiction Boundaries
- Example Scenario of Coordination Between Agencies
    - 2021 Texas cold weather event

Purpose and Objectives

- **Brief the Advisory Committee on Reactor Safeguards (ACRS) on government interactions for protecting the grid and power conversion**

    - Familiarize the ACRS on the agreements between the NRC, FERC, and NERC to facilitate communications between the agencies

    - Discuss the cooperative roles between the NRC, FERC, and NERC

    - Discuss the regulatory jurisdictions for each agency to protect the grid

Background

- The NRC, FERC, and NERC provide the regulatory oversight to protect the grid

- The August 14, 2003, blackout in the Northeastern United States highlighted the need for formal agreements between the NRC and FERC, to ensure communication and coordination

- IAAs/MOUs/MOAs facilitate the coordination between the agencies
  - Roles and responsibilities for each agency
  - Guidelines for cooperative work

- Currently, there are 4 active IAA/MOUs/MOA (related to the grid)

NRC and FERC Common Interests

- Dams – impacts on nuclear power plant safety
- Grid - preferred offsite power source for NPP during normal, abnormal, and shutdown conditions
- Cyber Security - impacts of cyber attacks on nuclear power plant safety
- Physical Security - physical protection of nuclear power plant facilities

- Regulates interstate transmission of electricity, natural gas, and oil, and hydroelectric power projects
- Focuses on reliability, integrity, security, and operation of the Bulk Power System (BPS or electric power grid)
- Oversight of North American Electric Reliability Corporation

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

- Develops and enforces electric Reliability Standards
- Assesses and reports on the reliability and adequacy of the North American BPS
- Cyber and Physical Security – Critical Infrastructure Protection Reliability Standards; impacts on cyber attacks on grid reliability and physical protection of shared critical infrastructure assets

Requirements and Standards Protecting the Grid

- The NRC evaluates the design and operation of nuclear power plant electric power grid systems
  - General design criterion (GDC) 17, Electric Power Systems
  - 10 CFR 50.65, Requirements for Monitoring the Effectiveness of Maintenance at NPPs
  - Technical specifications
  - Generic Letter 2006-02: Grid Reliability and the Impact on Plant Risk and the Operability of Offsite Power

- FERC regulates the interstate transmission of electricity
  - Focuses on reliability, integrity, security, and operation of the Bulk Power System (BPS or electric power grid)
  - Provides oversight of NERC

- NERC's mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid
  - Develops and enforces reliability standards
  - Annually assesses seasonal and long-term reliability
  - Monitors the bulk power system through system awareness
  - Educates, trains, and certifies industry personnel.

Nuclear Safety & Security Enhanced by Interagency Agreements and Interactions

NRC-FERC MOU/MOAs:

--Grid Reliability, Cyber Security and Physical Security (MOA)
--Dam Safety Interagency Agreement (IAA)
--Critical Energy/Electric Infrastructure Information (MOU)

NRC-NERC MOU

--Security (Cyber/Physical)

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

UNITED STATES NUCLEAR REGULATORY COMMISSION

DEPARTMENT OF ENERGY
FEDERAL ENERGY REGULATORY COMMISSION

Grid Reliability, Cyber Security, and Physical Security MOA

- Facilitate interactions between the NRC and FERC on matters of mutual interest related to the reliability of the Nation's electric power grid and nuclear power plant safety and security
  - Cybersecurity
  - Physical Protection
  - Emergency Response
- Provides guidelines for sharing of operational event information between the NRC and FERC
- Agreement to coordinate activities relating to cybersecurity and physical protection of shared critical infrastructure assets, including the sharing of information on threats.
- MOU was revised in 2022
  - Active until 2027

Dam Safety IAA

- Provides guidance to the NRC and FERC for implementing the NRC Dam Safety Program
  - FERC assists the NRC by providing expertise to conduct inspections of dams
- SECY-91-193 establishes the NRC Dam Safety Program Plan
  - Ensure compliance with Federal Guidelines for Dam Safety
- Currently, there are eight (8) dams that come under NRC jurisdiction
  - 7 of the dams are at operating power reactors
  - 1 of the dams is at uranium recovery facility
- Statement of Work provides guidance on performing inspections of the dams
- IAA was issued in 1992

Critical Energy/Electric Infrastructure Information MOU

- Agreement between the NRC and FERC to ensure the safety and security of the electric grid by protecting Critical Energy/Electric Infrastructure Information (CEII)

- The NRC staff is responsible for initially identifying information in its custody that contains CEII
  - Consultation with FERC's CEII Coordinator

- MOU was issued in 2018
  - 5-year extension memo signed in 2022

Cyber and Physical Security MOU

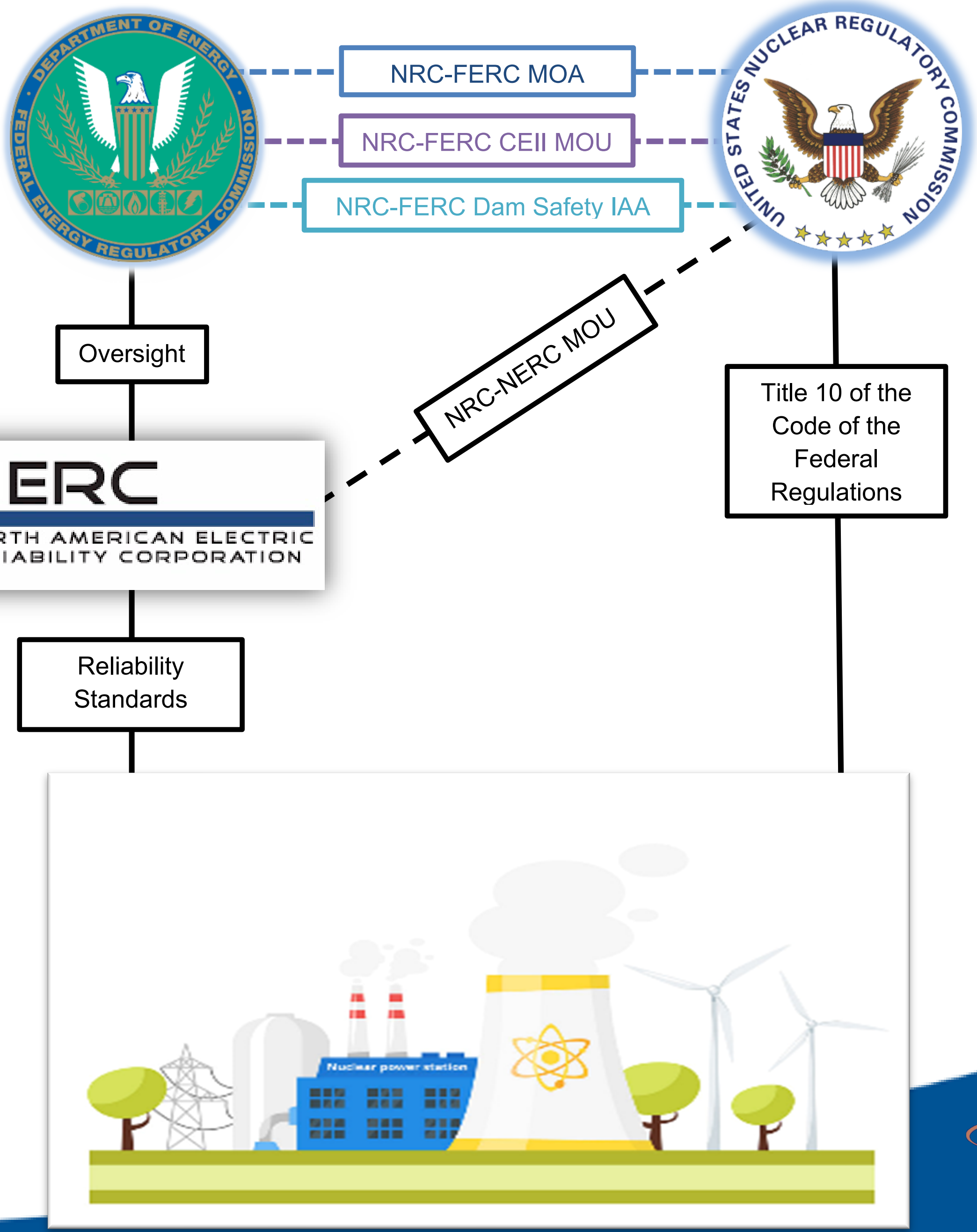
- Establish the roles and responsibilities between the NRC and NERC as they relate to the application of their respective cyber and physical security requirements for the protection of digital assets at U.S. NPPs
  - NRC’s focus is the prevention of radiological sabotage.
  - NERC’s focus is on the reliability of the bulk-power system

- The MOU establishes inspection protocols for each agency
  - Digital assets that can affect safety, security, and emergency preparedness vs. digital assets related to continuity of power

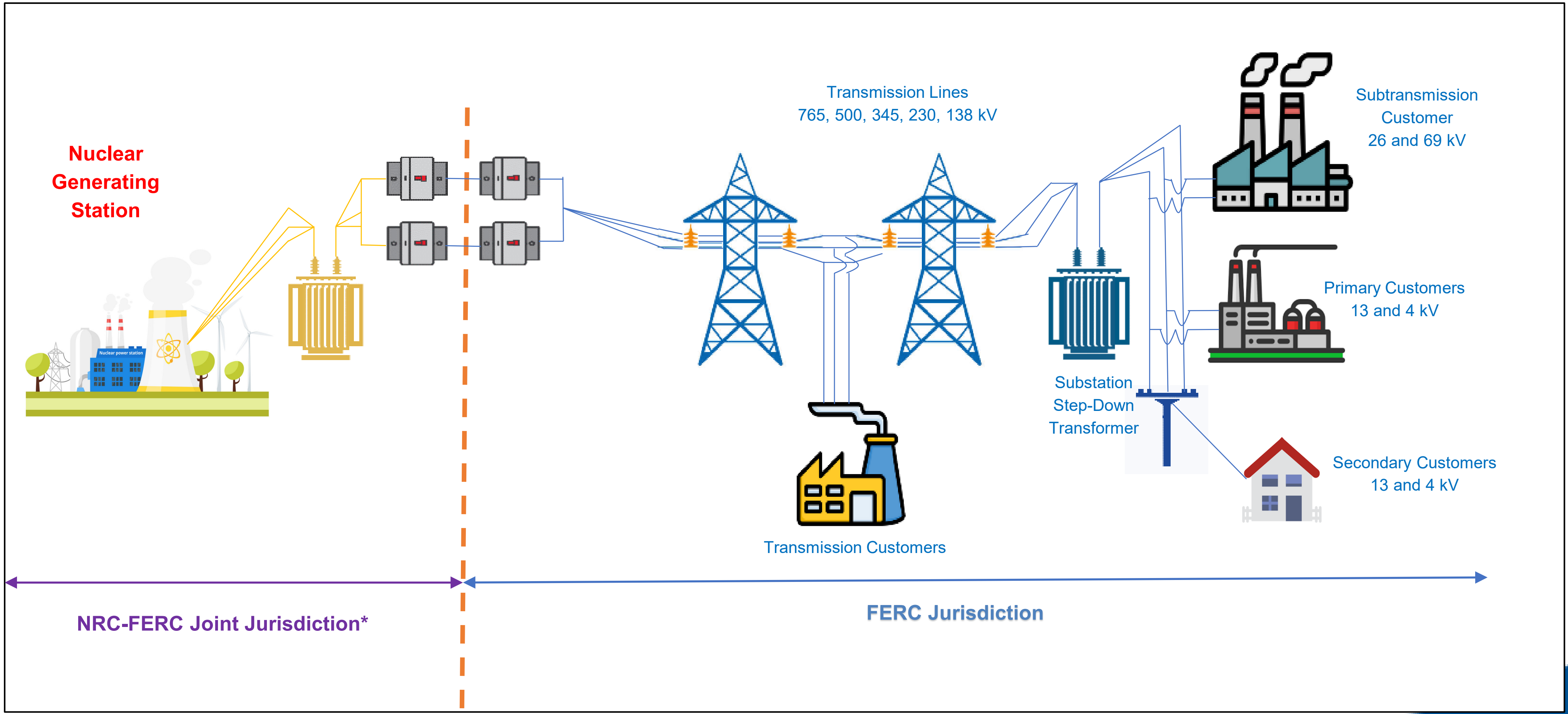
- Provides guidelines for the sharing of all information to carry out the intent of the MOU

- MOU was revised in 2015

Regulatory Oversight Relationships



NRC-FERC Jurisdiction Boundaries



NRC Coordination with FERC & NERC

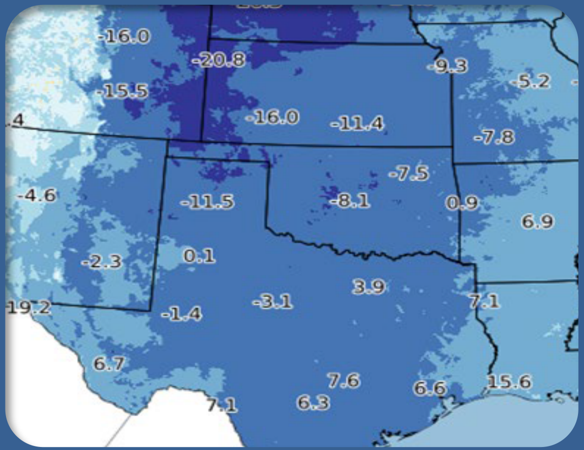
Technical, Regulatory and Policy Coordination

- NRC consults with FERC/NERC staff for transmission system status when NPPs request enforcement discretion

- Exchange information of interest during incidents affecting the grid such as severe weather, dam safety inspection coordination, and EMP.

Overview: 2021 Texas Cold Weather Event

Unprecedented Cold Weather



- Both sites remained safe during degraded grid conditions

Comanche Peak 1 & 2

- Neither units shut down
- Proactively started an onsite emergency diesel generator

South Texas Project 1 & 2

- One unit safely shutdown due to a frozen instrumentation line

Coordination: 2021 Texas Cold Weather Event

- The NRC staff coordinated multiple meetings to identify the role of each agency in Texas
  - Clearer understanding of the responsibilities of FERC, Electric Reliability Council of Texas (ERCOT) and the transmission system operators

- FERC issued a report that investigated the cold weather event
  - Report included recommendations for preparing for cold weather events

- The NRC staff hosted a workshop on the 2021 Texas Weather Event
  - FERC provided status of recommendations

Summary

- The agreements facilitate a continuing and cooperative relationship between agencies to enhance nuclear safety and security

- The agreements provide an avenue to exchange experience, information, and data related to reliability of the grid

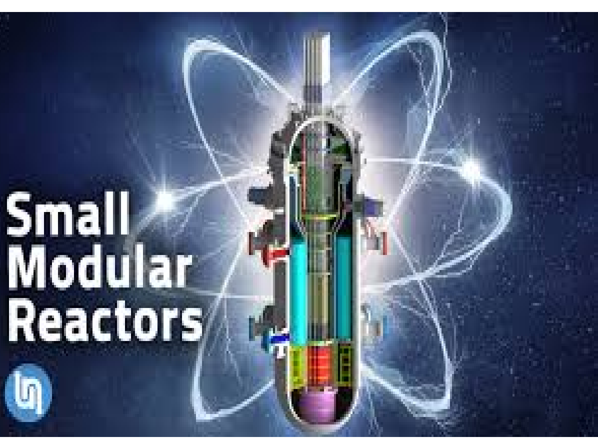
- The agreements optimize utilization of agency resources and prevent overlap while allowing agencies to carry out their respective responsibilities

Questions

ACRS Subcommittee Meeting
May 17, 2023

NRC Staff Efforts for Cybersecurity of Advanced Reactors

Ismael Garcia
Division of Physical and Cyber Security Policy (DPCP)
Office of Nuclear Security and Incident Response (NSIR)



Draft Cyber Security Requirements for Advanced Reactors

Background – Power Reactors Cyber Requirements

- Found in 10 CFR 73.54
- Protect digital assets that perform specified functions
- Protect from cyber attacks up to an including a DBT

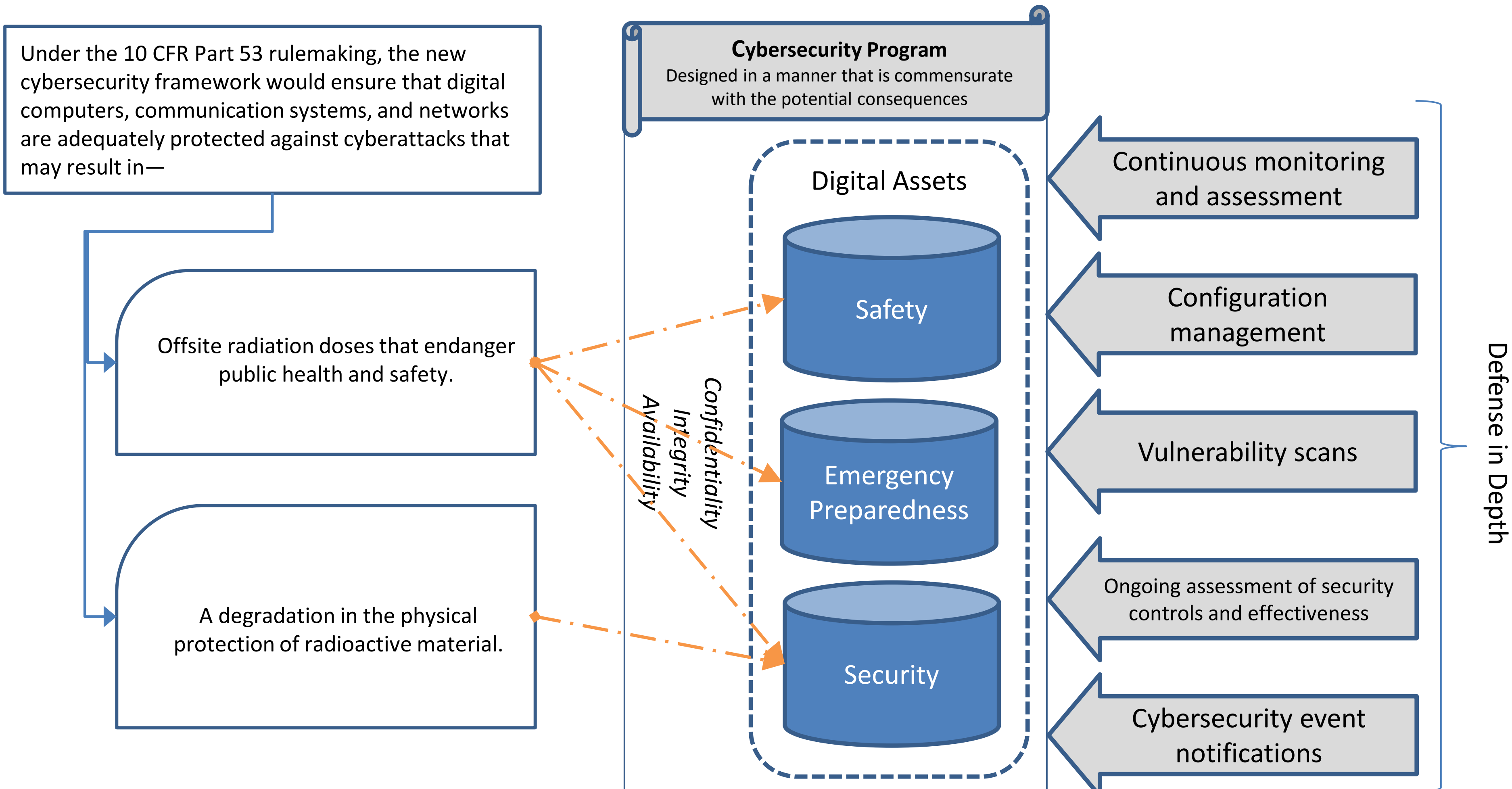
Proposed New Cyber Requirements

10 CFR Part 53 development for Advanced Reactors

Preliminary Proposed Rule Language Publicly Available

New Cyber Requirements in Proposed Rule

Preliminary Proposed Cyber Requirements



Reference: Part 73.110, "Technology-inclusive requirements for protection of digital computer and communication systems and networks," ADAMS Accession Number ML21162A093

Note: This staff-proposed rulemaking has been documented in a SECY and is with the Commission for review. More information on the rulemaking process is available at https://www.nrc.gov/about-nrc/regulatory/rulemaking/rulemaking-process.html.

10 CFR 73.110 – Draft Regulatory Guide Concepts

Draft Regulatory Guide Development

An acceptable approach for meeting the 10 CFR 73.110 requirements

Effective guidance to support a performance-based regulatory framework

Leverage IAEA and IEC security approaches

Note: This staff-proposed rulemaking has been documented in a SECY and is with the Commission for review. More information on the rulemaking process is available at https://www.nrc.gov/about-nrc/regulatory/rulemaking/rulemaking-process.html.

Draft Regulatory Guide – Three-Tier Analysis Approach

Facility Level—Eliminate potential adversary scenarios through facility design

Function Level—Eliminate or mitigate attack vectors through passive cybersecurity plan and defensive cybersecurity architecture elements (e.g., data diodes)

System Level—Use active cybersecurity plan and defensive computer security architecture elements (e.g., intrusion detection systems) to protect against cyberattacks

Note: This staff-proposed rulemaking has been documented in a SECY and is with the Commission for review. More information on the rulemaking process is available at https://www.nrc.gov/about-nrc/regulatory/rulemaking/rulemaking-process.html.

Future Work

- SECY-23-0021, "Proposed Rule: Risk-Informed, Technology-Inclusive Regulatory Framework for Advanced Reactors" submitted to the Commission on March 1, 2023 for approval
- Continue to support draft Part 53 proposed rulemaking efforts including the cybersecurity requirements and regulatory guidance

ACRS Cybersecurity Research Brief

Overview of staff research in support of advanced reactor cybersecurity engagement

May 17, 2023

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

Presentation Outline

- Introduction
- Cybersecurity Research Goals and Drivers
- Research Approach
- Representative Research in Novel Technologies
- Wrap up

Introduction

- RES cybersecurity research supports current and future NSIR activities
- Novel techs are applicable to both operating and advanced reactors
- RES is proactively looking at these technologies to be ready for the future
- Selected projects are a subset of active research

Goals of RES Cybersecurity Research

RES staff is performing anticipatory research to assist (and prepare) the NRC to meet potential technical and regulatory cybersecurity challenges within the nuclear domain.

RES staff's general goals are:

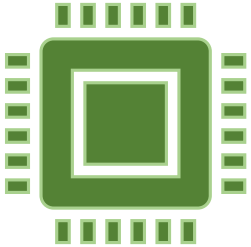
- Educate NRC staff
- Identify potential cybersecurity implications
- Develop awareness of/collaboration with government and nuclear industry (national and international) activities

Novel Technology Research Drivers

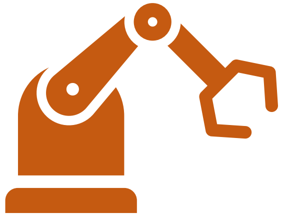
Licensees are considering new technologies or novel technology implementations

- Change in attack surface, new attack vectors
- NSIR staff needs to understand associated cybersecurity issues
- Need to develop technical basis for licensing, guidance, and oversight
- Need for inspection tools

Novel Technologies for Today's Discussion



- FPGAs



- Autonomous Control (w/ Remote Operations and Monitoring)

- AI/ML – Future Focused Research

- Wireless

Field Programmable Gate Array (FPGA)

Dr. Anya Kim
Office of Nuclear Regulatory Research
Division of Engineering
Instrumentation, Controls, and Electrical Engineering Branch

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

Background on FPGAs

- Field Programmable Gate Arrays
- Can be customized for a specific application
- Hardware that can be reprogrammable

Research Purpose & Potential Insights

- Identify potential cybersecurity concerns with FPGAs for future nuclear applications
- Investigate whether FPGAs:
  - Are inherently cyber secure
  - Are not vulnerable to Internet cyber-attacks
- Assist NRC staff

Autonomous Control Technologies and Remote Operations and Monitoring

Dr. Anya Kim

Office of Nuclear Regulatory Research

Division of Engineering

Instrumentation, Controls, and Electrical Engineering Branch

U.S.NRC

United States Nuclear Regulatory Commission

Protecting People and the Environment

Background on Autonomous Control

- What is *Autonomous* control

  “Autonomous systems are able to perform their task and achieve their functions <u>independently</u> (of the human operator), perform well under significant <u>uncertainties</u> for extended periods of time with limited or nonexistent communication, with the ability to compensate for <u>failures</u>, all without external <u>intervention</u> “

  (M. Endsley (2017), “From Here to Autonomy: Lessons Learned From Human–Automation Research,” *Human Factors*, *59*(1))

- Capabilities: diagnosis, prognosis, planning, decision making, self-validation, etc.
- Enabling technologies

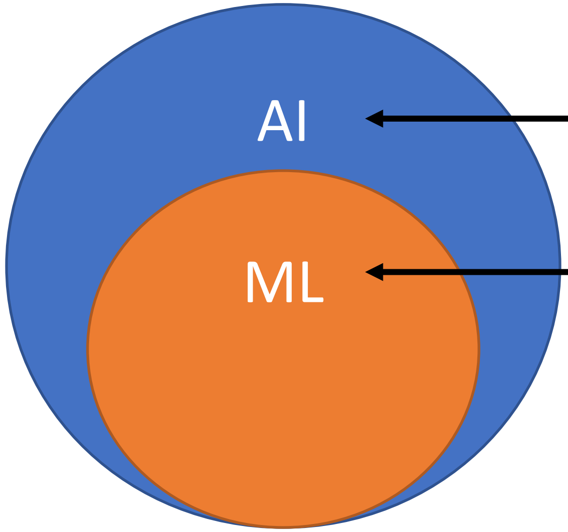
Research Purpose & Potential Insights

- Vendor/applicant interest in autonomous controls for NPPs
- Identify potential cybersecurity concerns with autonomous controls for NPPs
- Understand cyber implications of the enabling technologies:
  - Remote Monitoring and Operations
  - Digital Twins
  - Artificial Intelligence and Machine Learning

Artificial Intelligence and Machine Learning

Dr. Doug Eskins
Office of Nuclear Regulatory Research
Division of Engineering
Instrumentation, Controls, and Electrical Engineering Branch

Background on AI/ML



AI - ability to emulate human-like cognitive activities

ML – subset of AI that uses data to learn without explicit programming

<u>Attractive ML model features</u>:

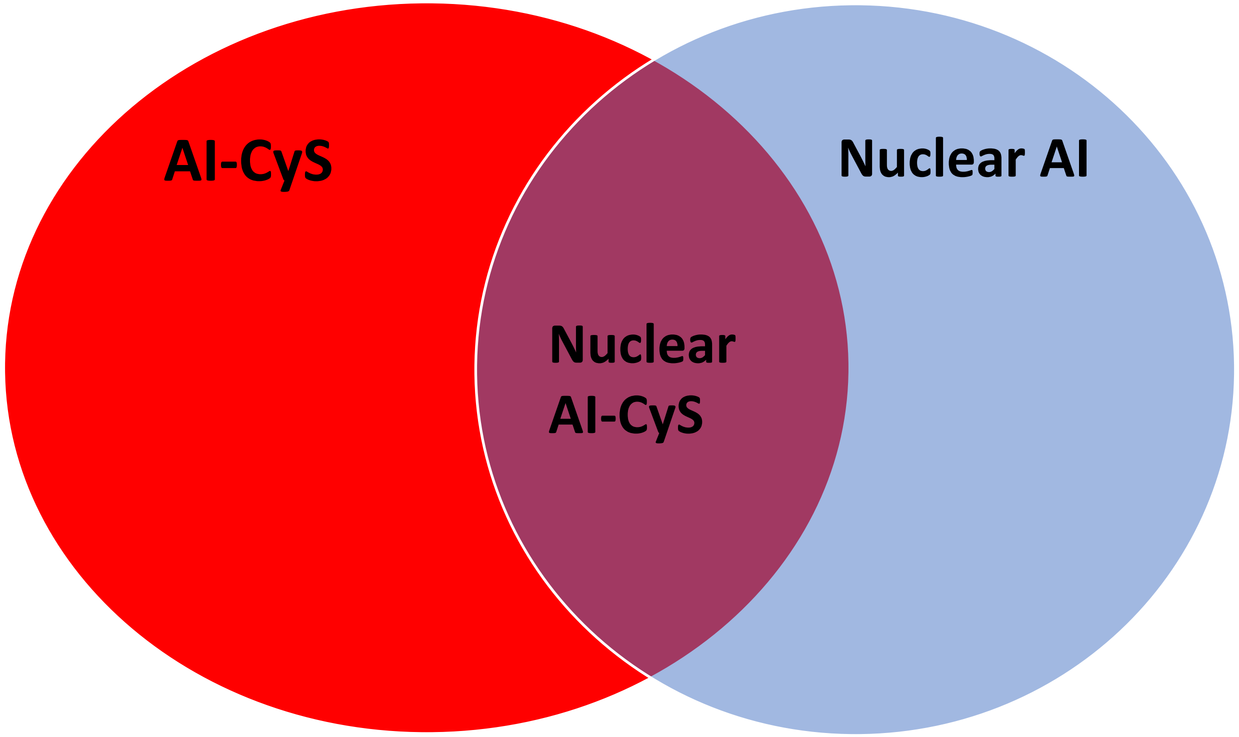
- Faster & less expensive
- More powerful & efficient
- Applicable to new and integrated domains
- Only data-based (explicit domain knowledge not required)

<u>ML model issues</u>:

- Black box
  - Difficult to explain
  - Difficult to validate (VVUQ)
- Highly dependent on data & training
  - Non-deterministic
  - Not fully representative of system states

AI/ML Research Motivation & Purpose

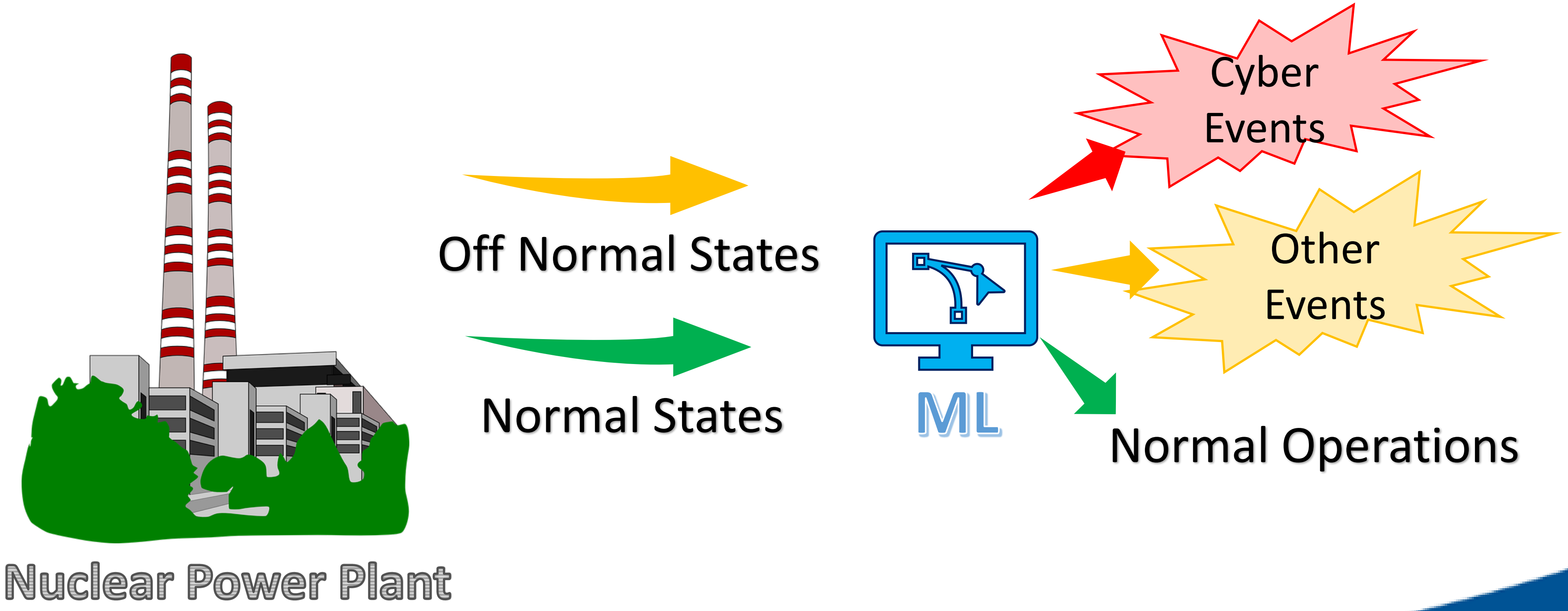
*"Artificial intelligence and machine learning are emerging technologies critical to the current and future national and economic security of the United States"**



* DOE Office of Cybersecurity, Energy Security, and Emergency Response

Characterizing Nuclear Cybersecurity Using AI/ML

Identify Nuclear AI-CyS Use Case → Develop Technical Approach → Gather Experimental Data → Develop & Document Insights



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

Wireless Technologies

Dr. Doug Eskins
Office of Nuclear Regulatory Research
Division of Engineering
Instrumentation, Controls, and Electrical Engineering Branch

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

Background on Wireless

Wireless includes

- Wi-Fi, Bluetooth, Cellular, Zigbee, WirelessHART, GPS, RFID

Safety components are deterministically isolated by

- Data diode & physical separation
- Prohibition of wireless

Wireless Research Motivation & Purpose

Potential expanded use of wireless in nuclear power plants

- Monitoring & Control

Cybersecurity insights from other safety critical applications

Two Step Approach

- Review literature and related regulations/guidance on wireless applications
- Survey industry on the use of wireless in safety critical applications

Wireless Research & Insights Gained

- U.S. critical infrastructure industries **do not use wireless** for safety critical applications

- Technical Letter Report: "*Study of Wireless Technology Implementation in Isolated, High Consequence Networks*"

(ADAMS Accession No. **ML22180A008**, publicly available)

Wrap Up

- RES works closely with NSIR to produce useful research
- These research topics are interrelated
- Potential additional research in the following areas:
  - Assessment of new cybersecurity approaches such as EPRI's TAM
  - Parallel cybersecurity assessment during DI&C Upgrades
  - Alternate approaches for verifying cybersecurity controls

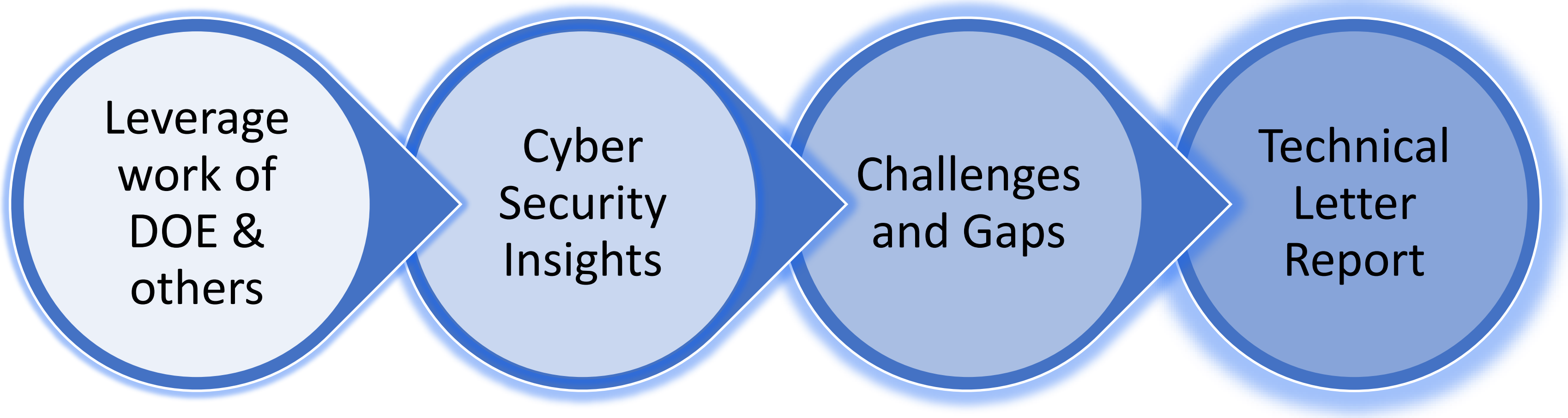
Acronyms

- AI: Artificial Intelligence
- AI-CyS: AI and Cybersecurity
- CSP: Cybersecurity Plan
- DI&C: Digital Instrumentation and Controls
- DOE: Department of Energy
- EPRI: Electric Power Research Institute
- FPGA: Field Programmable Gate Array
- GPS: Global Positioning System
- ML: Machine Learning
- NPP: Nuclear Power Plant
- RFID: Radio Frequency Identification
- TAM: Technology Assessment Methodology
- VVUQ: Verification, Validation, and Uncertainty Quantification
- Wi-Fi: Wireless Fidelity
- WirelessHART: Wireless Highway Addressable Remote Transducer Protocol

Questions?

BACKUP SLIDES

Novel Technology Research Approach



Novel Technologies Background

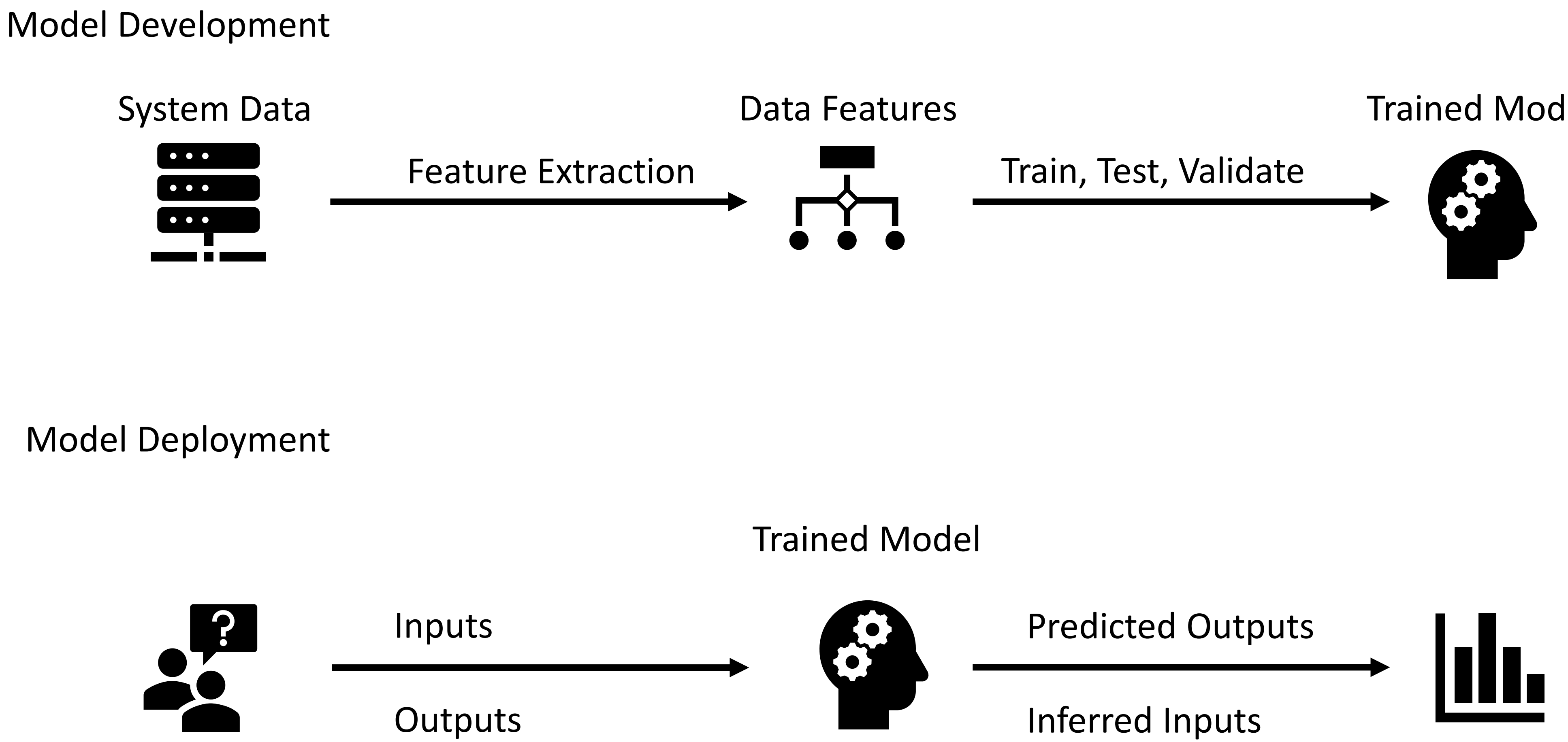
- Licensees are considering the implementation of various technologies such as Field Programmable Gate Array (FPGA)-based systems, remote monitoring and operations, autonomous control system, and other technology-based systems [2]. NRC staff needs to understand the potential safety and security aspects of these technology implementations to evaluate whether they comply with NRC's cyber security regulations.

- Research assistance request (RAR) NSIR-2021-007, "Cyber Security-Focused Overview of Novel Technology Implementations in Nuclear Power Plants" was created to support NSIR staff in understanding the cyber security risks associated with these technology implementations as well as potential graded, and technology inclusive frameworks associated with the application of these technologies.

RES Approach to FPGAs

- Examine current work in this area
  - Lots of research in cybersecurity issues of FPGAs
- Insights
  - Not all are applicable to NPPs, but
    - Some require physical presence, some are not realistic
  - No explicit software, but...
    - Design tools are software, now, even programming language can be SW
    - IP Cores are reused (third party)
    - Supply chain issues
    - Different vendors have different set of security controls for their FPGA families
- Provide technical basis and inspector aids
  - Take these insights and use them

Machine Learning Basics



What are NRC's AI/ML related research objectives?

- FFR project investigating if AI/ML is useful for characterizing NPP cybersecurity states
- Participation of cybersecurity research staff in AI strategy group
- AI/ML Study Group (involves cybersecurity researchers)
- DT use of AI/ML as an enabling technology (future exercise of cybersecurity DT task?)
- Outreach to external entities, e.g., input to DOE-NE cybersecurity research plan (included AI/ML)

Experimental System