Official Transcript of Proceedings

NUCLEAR REGULATORY COMMISSION

Title: Advisory Committee on Reactor Safeguards

Docket Number: (n/a)

Location: Rockville, Maryland

Date: Friday, September 6, 2013

Work Order No.: NRC-208 Pages 1-80

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

UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

+ + + + +

607TH MEETING

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

(ACRS)

+ + + + +

OPEN SESSION

+ + + + +

FRIDAY

SEPTEMBER 6, 2013

+ + + + +

ROCKVILLE, MARYLAND

+ + + + +

The Advisory Committee met at the Nuclear Regulatory Commission, Two White Flint North, Room T2B1, 11545 Rockville Pike, at 8:30 a.m., J. Sam Armijo, Chairman, presiding.

COMMITTEE MEMBERS:

J. SAM ARMIJO, Chairman

JOHN W. STETKAR, Vice Chairman

HAROLD B. RAY, Member-at-Large

RONALD BALLINGER, Member

SANJOY BANERJEE, Member

COMMITTEE MEMBERS: (cont'd)

DENNIS C. BLEY, Member

CHARLES H. BROWN, JR., Member

MICHAEL L. CORRADINI, Member

DANA A. POWERS, Member

JOY REMPE, Member

PETER RICCARDELLA, Member

MICHAEL T. RYAN, Member

STEPHEN P. SCHULTZ, Member

GORDON R. SKILLMAN, Member

NRC STAFF PRESENT:

CHRISTINA ANTONESCU, Designated Federal Official

MONIKA COFLIN, NSIR/CSD

RALPH COSTELLO, NSIR/CSD

CRAIG ERLANGER, NSIR/DSP/CSIRB

RUSSELL FELTS, NSIR/CSD

ERIC LEE, NSIR/CSD

TOM MOSSMAN, NRO/DE/ICE2

MOHAMMAD SHUAIBI, NRO/DE

STACY SMITH, NRO/DCIP/EVIB

BARRY WESTREICH, NSIR/CSD

TABLE OF CONTENTS

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

(8:28 a.m.)

CHAIRMAN ARMIJO: Good morning. The meeting will now come to order.

This is the second day of the 607th meeting of the Advisory Committee on Reactor Safeguards. During today's meeting the Committee will consider the following: 1) cyber security activities; 2) future ACRS activities/report of the Planning and Procedures Subcommittee; 3) reconciliation of ACRS comments and recommendations; 4) assessment of the quality of selected NRC research projects; and 5) preparation of ACRS reports.

A portion of the session on cyber security activities may be closed pursuant to 5 USC 552b(c)(3) to protect unclassified Safeguards information applicable to this matter.

This meeting is being conducted in accordance with the provisions of the Federal Advisory Committee Act. Ms. Christina Antonescu is the Designated Federal Official for the initial portion of the meeting.

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

There will be a phone bridge line. To

preclude interruption of the meeting, the phone will be placed in a listen-in mode during the presentations and Committee discussion.

A transcript of portions of the meeting is being kept, and it is requested that the speakers use one of the microphones, identify themselves, and speak with sufficient clarity and volume, so that they can be readily heard.

We have one item of interest that I'd like to announce is that our long-time Court Reporter, Ms. Kayla Gamin, will be leaving us after, I don't know, I think at least four years of tremendous service. And she is leaving to go to law school in Chicago, which is -- I can't understand it, but --

(Laughter.)

-- I think she deserves a great deal of thanks from the members of the Committee.

(Applause.)

With that, I'd like to turn it over to Mr. Charles Brown, who has got the lead. Charlie?

MEMBER BROWN: Okay. This first agenda item is obviously an update on cyber security. We know I guess that Rule 73.54, and I guess the entire Rule 73.1 which says you've got to work on cyber, is now at the point of being implemented. And the team that is doing

that is going to be here to try to give us an explanation or an update on how they are organizing themselves and how they are setting themselves up, so you can manage, monitor, and ensure that the sites are in a good cyber position.

They will also be reporting a little bit on I guess the pilot project, Diablo Canyon, where the initial pilot project on their I guess inspection and audit, whatever they did in terms of evaluating that particular plant. There will be both a closed and an open -- and open and closed session, in that order. I guess they will inform us when we're ready to go into the closed session.

As a prelude to this, I guess we are going to have a small lead-in here on an issue we have raised in prior meetings on control of access and what their general thinking is. And I feel -- I think they have not gotten all of the agreements and concurrences from all of the various directorates, but we will at least get an idea of what some of the options are.

Now, Tim is here. Did you want to say anything? Do you want me to go -- head over to Mo? Okay. I will -- anybody else -- Barry or Monika? I don't know. Who is going to lead this thing off.

MR. WESTREICH: I'm Barry Westreich. I'm the

Director of the Cyber Security Directorate in NSIR, and that's a new organization, so I think we -- Mo is going to talk about a subject with the new reactor group, and then we are going to talk about cyber security in general, the programs and processes we have in place. So I think we'll start with Mo and let you --

MR. SHUAIBI: Okay. Good morning. My name is Mohammad Shuaibi. I'm the Acting Director for the Division of Engineering in the Office of New Reactors. And the purpose of my remarks -- and I'm going to try to keep them brief today -- the purpose of my remarks is to provide you an update on the staff's activities to address the ACRS's March 19th letter on Chapter 7 of the mPower design-specific review standard.

By way of background, the Committee has previously raised issues on the area of communications independence and cyber security framework for new reactors. Examples of where you raised issues include ACRS letters of December 18, 2012, and March 19, 2013. And we have responded to those two letters in corresponding letters of February 6, 2013, and April 29, 2013.

In the Committee's March 19th letter, the Committee comments focused on interpretation of Clause 5.9 of IEEE 603, which addresses control of access.

In that letter, the Committee referred to an earlier letter that -- where you had taken a position, and you wrote, "We recommend that the control of access review section of the DSRS be expanded to require the reviewer to assess the architecture and firewall to ensure that it is hardware-based, one-way firewall."

The Committee's letter continued with, and I quote, "No software should be involved in either its operation or setup." So that's kind of where we are -- where I am going to focus my remarks.

In our April 29, 2013, response, we indicated that we are considering the Committee's recommendation, and that we will update the Committee on our progress as we meet with you. So this is one of these updates.

So then we move into ongoing activities and next steps. First, specific to the mPower design-specific review standard, we have engaged B&W regarding Chapter 7 of the DSRS to address your recommendation. We are currently in dialogue with B&W on how to address the recommendation, and we are planning meetings with them as a way to get a better understanding of their design, discuss the issues, and reflect what we need to do in our DSRS to address the recommendation that you provided.

We owe you a letter to inform you of our

decision on this issue, and we plan to provide you that letter before we finalize the DSRS. So you will see something from us that shows you how we address that for the DSRS. So that portion is specific to the mPower design.

But more generically, as a result of your March 19th letter, we held a series of meetings in the staff to consider options on how to address your recommendation more broadly. The meetings culminated in an Office Director level meeting between the office of NSIR, NRR, and NRO, on May 30th of this year. And the last time when the Subcommittee met Tom Berglund was here to brief you on that. And so I'm going to summarize what Tom Berglund provided to you.

Office management was provided with the staff's recommendations, and office management approved moving forward to explore three concepts in parallel for new reactors. I want to focus on one of these concepts. It is one of the more immediate concepts, and I think the one that you would probably be most interested in at this time. But there are two others which I could address. I think Tom covered them quite a bit at the last meeting, but I think the one I'm going to cover now is probably more relevant to what you want to discuss for this status meeting.

So using this concept, we would incorporate specific requirements for independence for new reactors in our 10 CFR 50.55(a)(8). That's the rule that addresses IEEE 603 or incorporates IEEE 603 into the NRC regulations.

And we would also include a rule that would require that if a design cert applicant were to take an alternative to our new independence requirements, that they would have to identify any resulting communication pathways that they have introduced as a result of that alternative. They would have to identify those communication pathways because they may introduce vulnerabilities.

The purpose of these requirements is to ensure that the pathways created by the design and the alternatives that they would take to our new requirements are identified, and that there is a clear handoff between the design certification applicant and the COL applicant, so that the COL applicant would know what they need to do and what communication pathways exist that they would need to address in their future activities.

This rulemaking approach is generic. Like I said, the first item I addressed was specific to mPower. The rulemaking activity would be generic. It would

be for design certification applications, not just mPower. So it goes beyond the mPower design.

We are also -- I also want to note that we are currently deliberating on this option as part of the ongoing rulemaking activity for 50.55(a)(8). So this goes back to Charlie's comment that we are not done yet. I'm giving you a status that we are still discussing this. And we are making good progress, I believe, so we look forward to coming back and briefing you again on this topic. As we indicated in our letter to you, we will be briefing you and giving you status as we make progress.

But I do want to note, final decisions have not been made. So at this time, we don't expect to change the interpretation of Clause 509 of 603, of IEEE 603, but we do believe that our approach and the way that we are proceeding is sound and has merit, and we look forward to bringing that to you and having a dialogue with you at the right time.

MEMBER BROWN: I'm certain we will have a dialogue --

MR. SHUAIBI: I'm sure we will.

MEMBER BROWN: -- because there is obviously some strong opinions on the use of -- and I presume you're alluding to the fact that you are trying to update the

rule to be 603-2009. Is it within that realm, or is it going to be -- are you all trying to do this in one or two pieces?

MR. SHUAIBI: No, you're right. It's the IEEE 603-2009. I'm sorry, that was --

MEMBER BROWN: When you're ready to go do that and make that part of the rule.

MR. SHUAIBI: We are doing this as part of that activity, yes. The generic option that I talked about here is part of the IEEE 609 -- the IEEE 603-2009 rulemaking activity.

MEMBER BROWN: Okay.

MR. SHUAIBI: And I believe the lead PM for that rulemaking activity -- and Christian and Christina have already been in dialogue about when we could come to the Committee and give you an update on that activity. And they are working out --

MEMBER BROWN: Ongoing activity to try to get that -- once you are all ready to go, to get that scheduled for a Subcommittee meeting and then a representation at the full Committee.

MR. SHUAIBI: That's right.

MEMBER BROWN: You commented, if I'm not mistaken, that there was kind of two pieces relative to our letter, which we specified some thought processes

and then you threw in this alternative, if design agents or designers or vendors or whoever, you come up with an alternative path, so you still want to leave these open doors for folks to tell you why they don't want to do it the right way.

MR. SHUAIBI: It's not --

MEMBER BROWN: I'm being a little bit pejorative in that because --

MR. SHUAIBI: I read the transcripts before coming to this meeting.

(Laughter.)

I remember the questions that were asked then.

I understand what you're saying, but within 50.55(a), if you read the regulations, there are -- with the required standards that we have on the applicants, and then there is a clause in 50.55(a)(8)(3) that says that a licensee could propose an alternative to what we have in there, but they would have to justify it.

We are proposing -- or we are working on a proposal for requirements for independence. We would allow an applicant to come in and say, "We would like to use an alternative to what we are proposing," but this is where we would -- we are considering the requirement that would say, if you want to do that, and

if you want to introduce complexities and communications pathways, you would have to identify those communication pathways, so that a COL applicant would know what they have to address in terms of vulnerabilities that are introduced by such pathways.

MEMBER BROWN: As part of the DCD or the design -- the license approval --

MR. SHUAIBI: That's the thinking right now. That's right. That's the thinking right now. So --

MEMBER BROWN: So we just capture it as part of the licensing process, as opposed to having it kind of deferred out to the future sometime.

MR. SHUAIBI: That's right.

MEMBER BROWN: Okay.

MR. SHUAIBI: This is not inconsistent with the rest of our regulations. We have our regulations, and within 50.55(a) we use the word "alternative," because that's the word in the rule. But even our other regulations, there is an exemption requirement, 50.12, that says, "If an applicant comes across a situation where they choose to take an exemption, they could propose to do that, but they would have to provide a justification." And we have criteria for what we would look at in order for us to be able to provide or be willing to approve an exemption.

So the regulatory process -- and I know "process" is not usually a good word in this setting, but the regulatory process allows for them to try -- don't take those paths. But there are criteria that we would follow, and we would have to do a review to decide whether an alternative that they may propose would be acceptable or not, if it would be acceptable or not.

MEMBER BROWN: All right.

MEMBER CORRADINI: Can I ask a question?

MEMBER BROWN: Yes.

MEMBER CORRADINI: Since I -- Charlie is the expert here, so -- so if we go to Summer and Vogtle, how does what you just said affect those plants that are in construction?

MR. SHUAIBI: That's part of the rulemaking activity, and that becomes the scoping requirement that would be included within the rules. So that would be a good discussion topic for when we talk about the specific rule and how it comes out. So I don't want to talk specifically about Summer and Vogtle in the context of a rule that we haven't fully developed yet, because that is under deliberation right now within the staff.

MEMBER CORRADINI: Okay.

MR. SHUAIBI: But let me generically, just

-- if I may just add one statement. In the case of a plant like Summer or Vogtle where they are -- where they have referenced a certified design and they have received a license already, we would be under the backfit requirement. If we wanted to go off and do something on our own initiative, that says, "We want you to do something different than what we have licensed you to do."

MEMBER CORRADINI: But I guess since we're talking process and not technical, I'm still not clear. Do they satisfy, under their current design and what they're building, the rule? Or would they need to take -- I mean, there must be some feeling from the staff where they sit relative to this. So where do they sit? Or there is no feeling from --

MEMBER BROWN: No, it was mushy. When we approved the license --

MEMBER CORRADINI: But you agree with Mr. Brown that it's fuzzy?

MEMBER BROWN: It's very mushy on that plant design. We discussed that during the DCD and our approval letters, and we got a lot of pushback. So it's --

MEMBER CORRADINI: With all due respect, I hear you. I'm curious what the staff thinks.

MR. SHUAIBI: As part of the activity that we have undertaken, we will be looking at what it looks like for previous designs and what it looks like for ongoing designs and what it would look like for future designers.

MEMBER CORRADINI: So I take that to mean it's unclear.

MR. SHUAIBI: I think what I would rather say is maybe that would be a good topic to discuss in detail, probably at the time when we come back to you with --

MEMBER CORRADINI: I've heard that before. I'll stop. Okay. Fine.

MR. SHUAIBI: Let me just say, in our minds we have done a lot of work already, so we've got some answers to those questions.

MEMBER CORRADINI: Okay. Fine.

MR. SHUAIBI: But I do think it's a longer discussion. I really do think it's a longer detailed discussion --

MEMBER CORRADINI: That's fine.

MR. SHUAIBI: -- of you wanted to go down that --

MEMBER CORRADINI: I just want to understand what's out there now and how it relates to what you explained. That's all. Thank you.

MEMBER BROWN: And now there's one more piece that -- you know, you talk about new reactors, but we really haven't addressed yet how we may want to cover existing plans when they do a backfit or an extensive digital I&C upgrade where they now bring in the networks, where they bring in the whole new vulnerabilities relative to control of access to these systems, and that has not been covered yet. That is still part of the general way it is right now, and it's -- so if we get this new -- my view, and I'm not sure this is right, because if we get the 50.55(a)(8) modified with 2009 with whatever we and everybody else agrees to, and then a plant -- a licensee comes in with an upgrade, do they have to make it to the new guidance? And does that then require them -- and how does that hand off? And how is that going to match? I just don't understand.

So that's another subject of discussion I think we --

MEMBER BANERJEE: Are there licensees coming up or --

MEMBER BROWN: Some are already in place. Okay? Now, I don't know what other folks have in mind because we haven't -- I know Oconee has had a full backfit, and I guess there's -- is there another --

MR. MOSSMAN: Diablo.

MEMBER BROWN: Diablo, that's right. I'm sorry. Diablo Canyon, right. So, but I don't know what else is in the queue, if anything.

MR. SHUAIBI: And this has been part of the long discussion within the staff about, how do we do this? How do we do this for new reactors? How do we do this for operating reactors? Do we do things differently between the new and the operating reactors? Are there differences in designs? Are there differences in the level of integration, the level of communication between a whole new design that is all integrated and, you know, possibly an old design that gets updates or upgrades in different areas versus the whole system? So that --

MEMBER BANERJEE: How urgent is the situation?

MR. SHUAIBI: I'm sorry?

MEMBER BANERJEE: How urgent is it?

MR. SHUAIBI: I don't want to say it's urgent. I don't think it's urgent that we need to be in front of the Committee today or tomorrow. I think it's on a good -- I think it's on a good path, and we'll deal with it in a good --

MEMBER BANERJEE: Does that increase vulnerability right now?

MEMBER BROWN: Yes. No, I'm not going to let him answer that. I knew what Mo was going to say. No, I'm just teasing.

The plants are out there. Oconee and Diablo Canyon have been done, and they did not address this issue up front during the architecture development for those systems. So what -- you know, when I first looked at the -- had one look at the Oconee one and -- after I had been here for about three months or something like that, they -- the vulnerability was there. They were connecting to the outside world via little block boxes with software in them and into the plant.

So what's the level of detail? I don't know. Because it was just a box; that was it.

MR. SHUAIBI: And that's part of the big dialogue within the staff is level of detail available at different stages of time, and for different --

MEMBER BROWN: Well, I just wanted to give you a heads up that we're going to -- you know, this subject is not dead once we finish that, go to the next part that's in the queue to try to get, you know, a good framework established as to how we -- how the staff, how the Commission and everybody else handles this on the long haul.

MR. SHUAIBI: I came in here optimistic that

I could talk you out of that, but I understand. Actually, I knew that. I knew that we would continue this dialogue. I was just being facetious.

MR. WESTREICH: With regard to your comments about the current -- we are going to talk about the inspection program and implementation of the cyber security. So that does address some of these vulnerabilities on the back end. I know your issue was on the front end, but we have done quite a bit already to kind of address some of these issues. So we'll talk about that.

MEMBER BROWN: No. That's why we wanted to have this briefing, so the full Committee would have an idea of what's going on from that regard, because I have a few more questions that I didn't ask in the Subcommittee meeting that -- because it just didn't dawn on me. Now they have dawned on me.

MR. WESTREICH: Okay.

MEMBER BROWN: Based on your all's marvelous presentation.

MEMBER SKILLMAN: I'd like to ask a question. If in the course of the next 12 months there were to be a cyber attack that allowed an outside party to get control of Diablo or Oconee, what action would the agency take?

MR. WESTREICH: Well, that's difficult to answer if we don't know the specifics. You know, at this point --

MEMBER SKILLMAN: Wait, wait, wait, wait.

MR. WESTREICH: -- we've taken a number of actions already to isolate --

MEMBER SKILLMAN: And any of the plants, if something goes wrong, you've got an AIT, you've got a shutdown, you've got bells, lights, and whistles, you've got admin, you've got all kinds of stuff coming out of the sky.

So for a non-cyber attack, a lot of us around this table have lived that life, when something really goes wrong. I would say this is something that went wrong. What would the agency do?

MR. WESTREICH: Well, we would use our same process as we use now. We'd have -- we activate our response mode. We do onsite activities. We have teams that would go out to try to understand the issue. We'd be communicating with the licensee. So we'd be in incident response mode, just like we would for any other event.

So, and we're hopeful. I think what we've done in the operational programs to mitigate a lot of these issues is to really address the vectors that could

cause that to occur. So I think we've done the major things already to mitigate something like that from occurring. And we're continuing to implement that program, and we'll be doing that over the next several years.

MEMBER SKILLMAN: Doesn't that kind of move into the sense of urgency that Dr. Banerjee asked about?

MR. WESTREICH: Well, I mean, that's why we're moving out pretty quickly. We had -- the rule went into place, and we've had them implement these first seven milestones that we'll talk about to address the major vectors. That's already in place. So we've done that already. I think that gives us some confidence that we have a little time to address some of these other issues.

MEMBER SKILLMAN: Okay. Thank you.

MEMBER BROWN: Yeah. I think it would be useful to let them go through and then take -- see how they address your question because I've got a couple of amplifying thoughts that we didn't address as how they do that. And they've done a bunch of stuff, but you've got to know what that is to see what -- to kind of address your thought process.

MEMBER SKILLMAN: Thank you.

MR. WESTREICH: Yeah I think once we go

through what we've done, you can --

MEMBER SKILLMAN: Okay. Thanks.

MR. WESTREICH: -- give us more.

MR. SHUAIBI: Are there any other questions for me?

MEMBER BROWN: I'm finished. I appreciate your update, and looking forward to trying to get this general concurrence within the management and of the staff, so that we can get on with the rulemaking revision and then fight it out, letter, you know, dueling swords or whatever we want to call it, but our letters and then the EDO responses to see how that plays.

MR. SHUAIBI: I'm looking forward to the dialogue. I think it will be a good dialogue.

MEMBER BROWN: Oh, yeah.

MR. SHUAIBI: I agree. So if there are no other questions, then I'll leave and --

MEMBER BROWN: Thank you, Mo. Appreciate it.

MR. SHUAIBI: Thank you.

MR. WESTREICH: So, as I said, I'm Barry Westreich. I'm Director of the Cyber Security Directorate, which is part of our Office of Nuclear Security and Incident Response. That's a new organization. I'll talk about that change in a minute.

But here is our agenda. It's a pretty full

agenda. We appreciate the opportunity to come speak before the Committee and discuss cyber security issues. It's a current issue. There's a lot of changes taking place. So this is a fairly dynamic area. We have in the audience staff from a number of the other offices, if questions come up related to their activities.

Next?

So the purpose is to provide you an overview of our cyber security program and how it is being implemented. We have a number of activities across the licensee types that we want to update you on. We talked to a subcommittee about that on a few occasions.

And so we want to continue to improve communication and coordination on cyber security and also identify areas of future interest, so we understand what your topics that you want to discuss in the future are.

MEMBER BROWN: I presume what you mean by communication is to ensure that we have suitable meetings to let us know you've hit different stages of your --

MR. WESTREICH: That's great.

MEMBER BROWN: -- development of your program to make sure we're on board or understand --

MR. WESTREICH: Understand.

MEMBER BROWN: -- what you're doing to see

if we then want to make any suggestions.

MR. WESTREICH: That's correct. Yes.

MEMBER BROWN: Okay. Thank you.

MR. WESTREICH: So our new Cyber Security Directorate -- so that's kind of hard to see, but that's the organization chair for our Office of Nuclear Security Incident Response. And prior to our reorganization -- I'll just -- we had three divisions -- Division of Security Operations, Policy, and Incident Response. And the organizations had -- two of the organizations -- the Division of Security Policy and Operations both had cyber security activities, both on the policy side and the oversight side.

And in order to gain some control of the area, have a focused effort, and more of an effective governance structure, we decided to merge the two division staff that were working on cyber security activities.

So we created this new Cyber Security Directorate, and if you look it's kind of in the upper left. Hard to see. Cyber Security Directorate now reports directly to the front office. I'm the Director of the Directorate, and Russ Felts, to my right, is the Deputy Director. And all the staff that were involved in cyber security activities previously are now combined

into this one directorate.

So we've been in place since June, a little bit of coordination and understanding how to merge those two activities to move forward. So the focus areas continue to be the areas that we were working on before. Yes?

MEMBER BROWN: We have a question. Somehow -- I don't know.

MR. WESTREICH: That's the closed session.

MEMBER BROWN: Do I have an open session? Maybe I'll go -- oh, no, I guess -- sorry, didn't realize I had --

MEMBER STETKAR: The answer to your question is, Charlie, it's Friday.

MEMBER BROWN: I'm awake.

MEMBER BLEY: It's good you're finally looking at the slides.

(Laughter.)

MEMBER BROWN: A positive step here. I didn't get my donut in yet. That's a big problem. Thank you very much for putting up with me.

Barry?

MR. WESTREICH: Can we go back one real quick?

MEMBER BANERJEE: Wow, that's hard to read.

CHAIRMAN ARMIJO: That's busy.

MR. WESTREICH: So the new organization, our primary mission is to be the point of contact for all cyber security activities involving our licensees. So we don't do internal NRC cyber security, but all the activities related to our licensees. And we're the single point of contact for all those communications, both internally and externally, industry and other federal agencies, the White House, and all the various stakeholders involved in cyber security.

MEMBER BROWN: Question on this. Which is the -- from the standpoint of looking and doing all of your inspections and audits, is that the left-hand column over there? I see it's New Reactor Licensing Branch, inspection and regulatory. Is that where --

MR. WESTREICH: Well, the Cyber Security Directorate --

MEMBER BROWN: Is that the top one?

MR. WESTREICH: It's the dangling box, yes.

MEMBER BROWN: Dangling box.

MR. WESTREICH: We have all cyber security-related activities, which includes inspection oversight for cyber security.

MEMBER BROWN: But you don't have anybody working for you, so that's just --

MR. WESTREICH: No, we do. We have all of

this -- we have the staff that has been working on it before, so the staff that was working on it from our Division of Security Operations, where I was the former deputy --

MEMBER BROWN: Okay.

MR. WESTREICH: -- those staff have moved over to this directorate. The people doing the inspections --

MEMBER BROWN: Okay. That was the question that we had as to what is their handoff from the old to the new, and that should be -- the answer is the folks we used to deal with or would see, we are going to keep seeing them.

MR. WESTREICH: Right. You're just going to keep seeing, because we're all in one organization. So we had some management -- a little bit of management organization changes to facilitate this move, but at this point we're up and running and we're continuing on with the same activities that we were doing before.

MEMBER BROWN: Okay. Thank you.

MR. WESTREICH: It is considered a temporary organization, because once we get to a stable program across the licensee types, we will consider merging it back into the line organization in NSIR. So we're talking like a 2019 date that we will -- if we're there

and we're stable at that point, we'll merge back into the organization -- previous organizational structure.

MEMBER BROWN: your box would drop down into the same line with all of the other three, as opposed to --

MR. WESTREICH: It would disappear and get merged back into those other activities.

MEMBER BROWN: So the initial effort here was to have a more focused group to get everything started and stabilized and running smoothly, and then move it into a line --

MR. WESTREICH: That's correct.

MEMBER BROWN: -- organization.

MR. WESTREICH: That's correct.

MEMBER POWERS: Are you saying that you think that by 2019 all of those plants that are going to switch to digital systems will switch. Is that what you're saying?

MR. WESTREICH: No. What we're saying is that the programs will be developed and stable. So currently in power reactors we have an ongoing effort to implement their plans that we have approved. So they have implemented Milestones 1 through 7.

MEMBER POWERS: But when you say "stable," the technology for threatening the security of digital

systems won't be static.

MR. WESTREICH: No, that's true. It's not so much --

MEMBER POWERS: I'm trying to understand what "stability" means.

MR. WESTREICH: Stability from a program, from an NRC regulatory program standpoint. So we will have all of the plants -- power reactor plants will have their cyber security plans fully implemented at that point. So they will be operating under an approved plan that we have inspected and we know how they do upgrades, how they do maintenance activities, all of the stuff that we would be concerned about, if they are going to, you know, make a change.

Same with fuel cycle facilities. At that point, we should have -- whatever path we take to get cyber security rules in place and implemented should be well on their way by that time. And so we'll have to reassess in 2019 to see if we're there.

MEMBER POWERS: I mean, it's --

MR. WESTREICH: Okay? So our activities include rulemaking. One of the things we're working on is the cyber reporting rule. Guidance development, we're still looking at some additional guidance, regulatory guidance, and other inspector guidance. We

have licensing activities for new reactors and updates and changes to the cyber security plans that are already approved and in place.

Continuation of policy issues, which is our road map activities, we are now looking at fuel cycle facilities and we will look at RTRs, ISFSIs, and materials licensees, so that's the policy work that we are still doing. And as we've talked about, we're continuing to provide oversight for implementation of the current rule and implementation activities for power reactors. And we'll talk about all of those things in the presentations in this session.

MEMBER BLEY: Barry, I know our role and it's not to really tell you how to manage, but I just want to make an observation. On the reactor side, in terms of considering the impact of events that occur in the plants, real-world events, we let that kind of percolate through lots of places in the organization. And we built this thing called AEOD some years ago to really start focusing on operating experience, and then said, "Well, we got that working," put it back generally, and now we've got a new program to focus on.

It just strikes me cyber security is always going to be a bit like that because the threats are changing, the technology is changing, and some central

place to be on top of that may be something you are always going to need.

MR. WESTREICH: Well, we will always need that. I mean, we have a cyber assessment team. They are integrated with our ILTAB threat folks, looking at the threat.

MEMBER BLEY: Okay.

MR. WESTREICH: And we're also taking that CAT activities, cyber assessment team activities, and looking from an op e perspective. How is that getting transmitted to the licensee community? What does that mean? What are we seeing? Kind of in a broad perspective.

So you're right, we are looking at that. That's part of -- I think, Ralph, are you going to talk about --

MEMBER BLEY: And that is linked with the op e stuff.

MR. WESTREICH: So we'll talk about that in a little more detail about the cyber assessment team. But that's something we'll probably have in place whether this directorate is in place or not.

MEMBER BLEY: Thanks.

MR. WESTREICH: So any other --

MEMBER BROWN: Yeah. Just one,

springboarding off Dennis'. I mean, the real point is, you know, this is an area where obviously the technology and the capability and what is going to be used. Things are going to be constantly changing. I mean, you can't breathe, go to bed one night, and all of a sudden, you know, the iPhone you bought last night is no longer any good and you have to have the latest whatever --

MEMBER POWERS: Come on, Charlie.

MEMBER BROWN: -- and it not only will communicate with the internet, but it will also communicate with satellites and the NSA, you know, database and everything else, and it's just fancy, fancy, fancy.

So, and that's -- if you want to know why I've been so hard over on the control of access points issue is that there is a way to avoid difficulties if you get ahead of the game, where you minimize the manpower, resources, and dollars, not only from the licensee standpoint but from your all's standpoint of ensuring that threats are not a real threat to the operation and safety performance of the plant.

And that's why you find me kind of pushing back all the time on these alternative proposals by vendors that want to implement the guidelines that you've put out and the way you may end up putting them out.

So I just want to have you keep that in mind, that the cyber security role from a plant safety standpoint -- I'm putting the business, you know, corporate headquarters building off on this side where they can do their IT thing and upgrade every software thing, and they can -- if they lose their files, that's their problem. I'm concerned about the plant, control of the plant, the operators, and people's access to go in and fudge around with what is coming in and out.

So that's why I kind of really get wrapped around the axle on this stuff. They just -- they give you a little heads up in terms of the thought process, and why I continue to hammer on it, that's to simplify the thing, particularly with technology changing the ability to do things.

I mean, I can just see one of these design agents or vendors or licensees proposing some wireless communication thing, which is -- it's not prohibited. There is not a specific statement there. So then you have to have a guy justify it, and you fight your way, you know, for months and months and months going back and forth, and finally you give in and say, "Well, we really can't tell him what to do. It's up to him to make sure his stuff is safe."

Well, that's -- at some point, the regulator

has to kind of be the adult in the room and make sure that they don't put themselves at risk. So I'm not trying to tell you, again, how to do it. Yes, I am.

(Laughter.)

MEMBER CORRADINI: Yes, you are.

MEMBER BROWN: Just to have the thought process to know where -- you know, why I consider the control of access. And it's not just internet to the network, but it's also control of access all the way down the food chain and how you identify it.

So, anyway, you can go --

MR. WESTREICH: Of course, we agree that those are important considerations. I mean, I think we all agree with the wireless example. You know, the cyber security plant controls are going to have to deal with that. If they were to put something wireless, then we'd have to have some pretty significant controls thought about.

MEMBER BROWN: That's an understatement.

MR. WESTREICH: So, I mean, I don't disagree --

MEMBER BROWN: Okay.

MR. WESTREICH: -- that this is an important area.

MEMBER BROWN: All right.

MR. WESTREICH: Maybe how we get there is where we have some discussion.

MEMBER BROWN: Yes. Thank you.

MR. WESTREICH: Okay. Russ, do you want to go ahead?

MR. FELTS: Certainly. Okay. So I'm Russ Felts, Barry's deputy. I just want to take a couple of minutes to sort of set the stage for further presentations by talking a little bit about the regulatory framework. In order for me to get into sort of a historical perspective on the NRC's involvement in cyber security regulation and specifically what we've done to this point, I want to talk briefly about the threat.

So on this slide you see that we recognize that there are a number of different avenues through which an adversary could attempt and potentially succeed in conducting a cyber attack. And we recognize -- and it's in regulation in 73.1 -- that we have a knowledgeable, dedicated, intelligent adversary, and implied there really is the fact that the adversary is looking for vulnerabilities and is smart enough to attempt to figure out ways to exploit those vulnerabilities. Right?

So our programs are intended to put licensees

in a condition where these vulnerabilities are mitigated. And because of the fact that we recognize that these vectors can't be completely eliminated, we took a performance-based approach in terms of how the regulation was set up.

Next slide, please.

From a historical perspective, NRC has been involved for over a decade now in the cyber security area. I want to call your attention to a couple of things specifically on this slide, the fact that in 2009 is when the cyber security rule at 73.54 became effective. It was issued in 2009.

Licensee's cyber security plans for power reactors were put in place, approved in the 2011 timeframe, and we are currently inspecting the interim implementation. All right? So we've got a number of milestones, which I'll talk more in depth about here in a second.

We are out currently inspecting those programs as we speak.

MEMBER BROWN: You recognize that there was significant disagreement on Rev 3 at 1.152 relative to the statement that says the design folks are not going to look at anything. They are actually almost virtually prohibited from looking at anything other than how the

system implements its safety function, and that's it. In other words, don't bother us; we'll do it later. So we lost that battle, but it's not over.

MR. FELTS: We understand that was a change.

MEMBER BROWN: Yeah. It was a change because it was different in Rev 2.

CHAIRMAN ARMIJO: Could you go back to Slide 8? In your threat vectors, where are the insider threat? Is it just under vendors and vendors to vendors?

MR. FELTS: No. Actually --

CHAIRMAN ARMIJO: It seems to me that is the most challenging problem.

MR. FELTS: I think --

CHAIRMAN ARMIJO: You know, your own employees, for reasons of their own, decide to create problems --

MR. FELTS: Sure.

CHAIRMAN ARMIJO: -- and have routine access, and it seems to me that is one of the most difficult problems to deal with. Do you -- if you could just tell us a little bit about your thinking.

MR. FELTS: Right. I think that, if you look at the list of threat vectors there, the only place where you are really -- we are saying that someone would not need either inside access or figure out a pathway to

exploit inside access, like giving something to someone either knowingly or unknowingly to put that malicious code in the system --

CHAIRMAN ARMIJO: Eventually, you're going to need some sort of a device, right?

MR. FELTS: -- is really the internet, right? Obviously. So an outsider could potentially exploit a vulnerability that existed that had a face on the internet, and the supply chain, as you pointed out. All of the others, clearly there is a potential for an insider to exploit any of these vulnerabilities.

So it certainly is an aspect of the design basis threat, the insider, and we recognize that.

MEMBER BROWN: Sam, just a simple example. Somebody could go down and say they are authorized to take a laptop down. But that laptop has a USB port on it, and they have to have a thumb drive where they alter somehow -- don't ask me how because I'm not an expert. Plug that in, and now when they update the software it introduces some wrinkle in the software how it executes the software, and now all of a sudden you've got a problem.

And if you -- you've got to control that. So thumb drives, any access to that laptop and how that software is input to it, even down to the cabinet level,

how do you modify it? Do you change out proms, or do you do a software upgrade via a laptop or a USB drive or via a network connection into it? All of those are vulnerability and access points.

MR. FELTS: Well, like -- you know, as in the physical security realm, there are programs in place to address the insider threat, which applied both in physical security considerations and in terms of cyber security. So, you know, there is an insider mitigation program the licensee is required to have in place and it's inspected.

CHAIRMAN ARMIJO: I guess that's the best you can do, because it's really people. And you can't get into their minds and --

MR. WESTREICH: This idea is included in our interim actions, actions that have been implemented now. This insider mitigation program is something they need to maintain and enhance actually.

CHAIRMAN ARMIJO: Right.

MR. FELTS: Let's move on to the next slide.

I wanted to talk just a bit about the regulation at 73.54. It currently applies to power reactors, both new and operating. And I mentioned it's performance-based. It's a high level regulation. It's only about a page and a half. But it has -- the basic

requirements there are for the licensee to, you know, establish and implement the cyber security plan, which for all the power reactors that are operating is in place.

They have to protect those critical digital assets, and we'll talk a little bit more about what those are. And the things that are covered, the things that -- the aspects that define what is a critical digital asset are the fact that we require cyber security protections for things that could impact safety, important to safety, security, and emergency preparedness functions, or systems that could impact those functions.

So it doesn't have to be something that directly performs a safety, security, or an emergency preparedness function. It could be something that is required to operate effectively or to function in order to support the system that performs the function.

They have to have a defense-in-depth protective strategy, which includes a defensive architecture. So there's a requirement for the licensee -- in guidance it discusses -- and the licensees that have not committed to this in their plans, to have this defense-in-depth approach through the architecture that essentially isolates the most critical systems from the internet with various layers of protection. And then,

of course it addresses technical, operational, and management controls.

So, again, this is Reg Guide 5.71, and we talked about the fact that there are interim milestones. And these are some of those that you see laid out on the slide here. The formation of a cyber security team to actually go and identify critical digital assets, and then to apply that defensive architecture, which has these five levels that you see there starting at Level 0, which is the internet.

You see that you can have two-way communication between Level 0 and Level 1, Level 1 and Level 2. But beyond Level 2 you are not allowed to have two-way communication. You either have to have those systems air-gapped or you have to have a data diode in place to ensure that you don't have things that potentially originate on the internet finding their way into the most important systems, the highest levels of protection.

And then the licensee needs to address -- is required to address security controls for the CDAs.

MEMBER POWERS: Can I ask you about the first step? Form cyber security team. This is an obligation of the licensee to do this?

MR. FELTS: Correct.

MEMBER POWERS: So who is on that team?

MR. FELTS: It's a multidisciplinary team, so it would include engineers, IT staff. It needs to be multidisciplinary to make sure that all of the appropriate perspectives are considered.

We don't want these teams to just be composed of folks that are knowledgeable about IT systems but don't necessarily understand the impacts of, say, a loss of function of a CDA they are looking at. We need people that have that cross-disciplinary perspective to make sure that the appropriate things are being protected at the appropriate level.

MEMBER POWERS: I'm just thinking of one or two plants that I am reasonably familiar with. And I can certainly find people that can outline for you in some detail what the loss of a function is. There probably are few on that plant staff right now that are familiar with the kinds of threats that the high end of your threat vector -- I mean, what are you saying? I have to have somebody on my team that knows those kinds of things?

MR. FELTS: No. I don't think the team specifically has to include folks that are experts in the threat, but they do need to understand those vectors so that they can essentially plug the gaps and ensure

that vulnerabilities are addressed.

So, for example --

MEMBER POWERS: Does your guidance give them enough to do that?

MR. FELTS: I think from what we've seen, we've seen -- at least so far in our inspection program we've seen fairly -- we've seen implementation that indicates that, obviously, there is a range of capabilities we've seen across the spectrum of plants that we've inspected.

So I don't know if I can specifically address whether or not the guidance is adequate in terms of telling them who needs to be on the team. I think it does fairly clearly lay out who they need to have involved.

MEMBER POWERS: My concern is that the threat vector evolves very fast, and once you get up to the high end of that vector, it's very sophisticated stuff. And I don't see how anybody on the -- I don't see how a licensee can keep up with that, because he's got another line of business that he is pursuing and that's a chore.

And, I mean, if your guidance provides him enough --

MR. WESTREICH: I think the guidance provides the type of people they need to have on their team.

So like Russ said, it's multidisciplinary, includes IT people, it includes a plant --

MEMBER POWERS: Those IT people, you know, I mean, how many IT people are there on a plant site?

MR. WESTREICH: Well, we're talking about typically corporate IT who are dealing with protecting their corporate structure from the threat as well. So most of the guys we see are fairly aware of where we are in the threat landscape.

Ralph, you had something to add?

MR. COSTELLO: Professor Powers?

MEMBER POWERS: Yes.

MR. COSTELLO: I'd like to answer your question, if I may. This team is multidisciplined, and we have it specified in intimate detail who has to be on, how many people, but it had to be multi-faceted, in accordance with subparagraph 3.1.2 of the 0809, which is in fact our license condition cyber security plan.

And what we found with the first 14 inspections is some sites had a very good mix, a very good team. They had to do very little to change it, improve it. But this is not a stagnant team you just make up one day and it stays that way for 50 years. They are going to adapt, change, improve the team makeup, so they get better and can be better.

For instance, we found that at some sites they didn't include physical security as much as they probably should have. And they realized that after we left the last day of the inspection, and so they include some more people that have more physical security experience, et cetera, et cetera, et cetera.

So that's how this team composition seems to be working. The good news is it seems to be improving continuously. That's what we're seeing in real-time inspection space.

MEMBER POWERS: It's slopes that I'm worried about. And, you know, if we demand too much, you know, I cannot -- I worry about asking the sites or even the corporate IT organization to have the same level of knowledge on cyber security that people on your staff have, because I just don't think it's possible. I mean, they just can't -- they have other missions.

MR. WESTREICH: And, frankly, they're not privy to some of the information because it's classified. So it's our job to provide that information to them, which is part of what the cyber assessment team does. And these inspection activities are -- you know, it's the first time through. There's a little bit of a learning that is going on where they understand what the expectation is.

So I think, as Ralph said, as we move forward, the teams are getting more robust. We have an obligation to provide them that threat information if it's -- if we think it's affecting them.

CHAIRMAN ARMIJO: There are cyber security consultants and organizations that provide support or reviews. What is the -- your view of their role in either advising or participating in some way in these cyber security teams?

MR. FELTS: Well, I think we've seen certainly licensees using consultants to assist them, if they may not have the expertise necessary to do an effective job resident in their organization. And we have definitely seen a mix -- at a particular site we've seen a mix -- at each site we've seen a mix of staff that work at that site and corporate support people, and in many cases contract support to bring the right expertise to the cyber security team to put the adequate protections in place.

But I really think that the point is they are not necessarily focused so much on the threat as they are in plugging the vulnerabilities, understanding what is -- what infrastructure is at the plant and how an adversary might exploit that and making sure that those pathways are addressed.

MEMBER RAY: But do you envision at some point having a designated particular point of contact between the agency and the licensees on this topic?

MR. WESTREICH: Well, I think that's -- do you mean in terms of a specific individual or --

MEMBER RAY: Well, or a position, a position to which the licensee would designate people, rather than, you know, just, well, somebody from corporate will respond to this particular communication that we're having. I mean, there are positions in the operation of the plant that traditionally have been established, and people hold those positions. I'm just wondering if in this area there ought to be something similar.

MR. WESTREICH: Well, I think we've seen that licensees are coming around to the notion that this -- and, clearly, I understand --

MEMBER RAY: I'm asking, do you think as an agency, not that we just observe that they're doing it, but that should become part of the requirement that, okay, we want a designated point of contact for this subject.

MR. WESTREICH: I don't think that's something we've thought about.

MEMBER RAY: Okay. Well, I'll just give it to you to think about.

MR. WESTREICH: Yeah. I think --

MEMBER RAY: I mean, you have lots of other things if that's the case. It seems like, following up on the comment the Chairman was making, that it would be maybe worthwhile if we said, "Okay. It's time that everybody have somebody who is designated." It may not be their only job, but --

MR. WESTREICH: We currently do have designated points, but there are people that are designated as the lead procurement activity. And that's primarily because they're trying to implement this thing, and they're going to go out through 2015, '16, '17, so there is a designated point of contact. We have a lot of communication with them. Downstream I'm not sure if that's something we need to think about.

MR. FELTS: Aside from the cyber security team, there is no prescribed requirement for a particular point of contact. But I think we've seen licensees recognize the importance of cyber security, and those that have multiple facilities certainly have sort of a core group of experts that are implementing --

MEMBER RAY: Yeah. But it's natural, it's an observation that you've made. But, you know, there is always the outlier, somebody who is -- maybe the job has been vacant for a while, and that's not good.

MEMBER SKILLMAN: Let me ask you to go back to 10, please, on the requirements. Is there a requirement to identify that the security system has been pinged, that there has been an attempt to gain access and to mine that information for usefulness?

MR. FELTS: Well, there is a requirement in the cyber security plan, not the regulation but the cyber security plan, for detection and response capability. And, as Barry mentioned earlier, we are working on a reporting requirement right now, a rulemaking for reporting requirements for cyber security that would -- you know, depending on how that works through the rulemaking process would require licensees to report to us that they have experienced a cyber attack.

So I'm not sure which part of that addresses specifically your question. I presume you're asking about detection and response capability or detection and --

MEMBER SKILLMAN: What I'm really thinking about is how the fleets have generally implemented some form a near miss process, where -- whether it was an injury or avoidance of a trip, or a near miss on a cycle or a process failure that could have resulted in some significant event, and it did not occur, the employees are on their honor to say, "Hey, this is what I did.

This is what happened. This was truly a near miss event."

And I'm thinking of a cyber attack being a near miss event when your protection systems have repelled incoming, but the need to disseminate that information for learning, which is why the near miss process is so effective out in the fleets. People say, "Hey, you know, this could have happened. It didn't happen. This is why it didn't happen." Maybe we'd better make a stronger letter, a better gate, more protection on the switchgear, or something such as that.

I'm thinking of a true threat that was repelled. Is there a requirement to report it and to mine the information, so that the next time it happens it is more robustly reported.

MR. FELTS: Right. I think that's really the focus of the rulemaking effort we have ongoing for a cyber reporting requirement.

MEMBER SKILLMAN: Okay. Thank you.

MEMBER BROWN: I want to make one observation relative to Dana's lead-in. If you go back to Slide -- the threat one, the landscape -- 8. One way of looking at this -- and this springs from all of your all's questions -- is if you look at that list -- and whether I'm right or wrong, it's kind of the way I've categorized.

There's active dynamic threats, which are real-time. They are happening bang, bang, bang, but you've got to fight them off.

And then there is what I call the slower moving threat, such as somebody -- a person taking a USB drive or a laptop, test equipment, whatever it happens to be, into the plant and doing something. I mean, so there is active dynamic in the threats, and then there is the more administratively controllable type threats that are not real-time where you are trying to fight off the latest worm, malware, or whatever the fancy new terminology that the world comes up with for these threats.

And that all goes back to literally the defensive architecture from the dynamic. If they have to fight these dynamic threats every day, hour in and hour out, they're going to lose. They will not have the staff at the plant. They will not have the resources at the plants. Even the corporate umbrella will not have the ability to protect those plants from that. The financial community has proved that.

I just got a letter the other day from DOE. All of my data was compromised. My entire -- all of my PII was compromised. It's out there, they gave away Social Security numbers, addresses, phone numbers, work.

Everything I've ever done has been thrown out in the wide world. I don't know what the hell I'm going to do with that, but DOE lost it. So I'm really happy.

So that was a dynamic threat, came in and took the stuff out of their databases. So the key is the architecture that just literally puts a wall that can't be penetrated from the dynamic threat, so that they can concentrate on those that can be handled internally. So internet, intranet, wireless, Bluetooth, all that stuff, dynamic threats.

Look at the rest of those. You can deal with those on an administrative basis. Doesn't mean they're not important or critical or complex, but you can deal with vendors, vendor to vendors, laptops. All those are just -- I mean, you can, you know, go to bed one night, I've got a procedure, I can do that. You can check a guy. You can check the thumb drive. You can do all kinds of things before he goes down there. And you can know what your threats are that you'd have to -- and you're going to probably miss some at some point. But that's a different -- it's not as dynamic as these other ones.

So if you listen to me beat the dead horse, that defensive architecture is extremely critical, and you've got to have it mapped in the plants. You've got

to know where those touch points are that give you the vulnerabilities to dynamic threats.

Sorry, just had to -- based on the discussion, I thought I'd throw in that thought process.

MEMBER SCHULTZ: I think it's important, because everything we've heard since the opening discussion has reinforced your comments and the discussion and the need to create and isolate the environment in which the threat can occur.

MEMBER BROWN: And you can't -- they can't put people on --

MEMBER SCHULTZ: Programmatically, it's going to be difficult to control.

MEMBER BROWN: -- these teams that are going to be able to do all of this. Okay. I'm --

MR. WESTREICH: That's a good segue to the next slide.

MR. FELTS: All right. Let's talk a little about implementation. Okay? All licensees were required to implement the first seven milestones by December 31st of last year, and that's what we're out currently inspecting now.

So those Milestones 1 through 7 address the key threat vectors, including controls for portable media. But they are focused on target set equipment,

so CDAs that are related to target sets are the ones that we were focused on because they are the most significant.

Milestone 8 --

MR. WESTREICH: One of the key threat vectors is this architecture issue. So Milestone 3 is installing data diodes or some other deterministic device that doesn't allow internet access, to address your --

MEMBER BROWN: Yes. But 5.71 doesn't -- that's guidance.

MR. WESTREICH: Well, that's in the cyber security plan, so that's not guidance, that's required.

MEMBER BROWN: Yes. I understand that. But you've -- they do have -- they don't have to have -- they can come to you with a non-one-way data diode that is software controlled.

MR. WESTREICH: They could, but --

MEMBER BROWN: They just have to fight off the hordes of --

MR. FELTS: They have all committed to the architecture in their cyber security plans, which is now a condition of their license. So certainly when they came to us with their plan for approval, had they requested approval of an alternative, we would have had

to consider it.

MEMBER BROWN: That's these 14 plants you have gone off and looked at? They've committed to --

MR. FELTS: I'm talking about all of them. All the plants require the defensive architecture. No, operating plants.

MEMBER BROWN: So they've committed to a hardware-type data diode --

MR. FELTS: Right.

MEMBER BROWN: -- non-software controlled?

MR. FELTS: Correct.

MR. COSTELLO: Ralph Costello, Office of Nuclear Security Incident Response. Thank you, Mr. Brown.

Your question is a good one, Mr. Brown, in terms of, yes, they could by way of the requirements opt to maybe try something like firewalls. But we all know they are ineffective. We all know they're insecure. Someday they may become secure.

And licensees ultimately, going back to the one and a half page rule, which is a gem in and of itself, because it says they have to protect against cyber attacks, so we don't tell them specifically, there's no mention how to do things, but we tell them what the ultimate performance objective is, and there is no way

I know of, unless somebody else in the room does, that a firewall is a good way to do it.

So the end result, as what Russ has mentioned, is they are using data diodes, hardware-related data diodes, not software, because otherwise when we inspect it, the first question --

MEMBER BROWN: I understand.

MR. COSTELLO: -- we're going to ask them is, tell me how you're protecting against this event.

MEMBER BROWN: Okay.

MEMBER BALLINGER: I have a question. Maybe it's in the closed session. But is there the equivalent of -- in the organization of the physical threat teams that go out and try to get access physically to a plant? Are there teams that --

MR. FELTS: I think you're asking --

MEMBER BALLINGER: -- "cyber terrorist teams" -- in quotes -- that try to get access to the plant, that probe the plant, just like these physical threat teams do?

MR. FELTS: I think what you're asking about is force on force.

MEMBER BALLINGER: Yeah. That kind of thing.

MR. FELTS: No. We're not currently -- we don't have a separate FOF team that is going out and

trying to attempt a cyber intrusion.

MEMBER BALLINGER: Because that would be one way to quickly sort out the vulnerabilities that you -- you think you've covered all of your bases, and then all of a sudden one of these teams goes out there and you get a bunch of 25-year old, you know, gamers, and then all of a sudden they're in the plant.

MR. WESTREICH: It is an attribute of the DBT. So we could test it, but we likely wouldn't test actual hacking on an operating facility no matter what we do because that's not how we can get --

MEMBER BALLINGER: Well, but hacking to a point --

MR. WESTREICH: Yeah. We have to simulate it when we -- we just haven't got there yet, to think about how we would do that. That may be something --

MEMBER BALLINGER: Because that's one way to solve Dana's issue of this continuing evolution of methods that people have. You know, I come from a university, and, believe me, you do need a couple of 23-year olds.

MR. WESTREICH: We have some capable people involved in the inspection activity that are looking for things a licensee might have missed.

MEMBER BALLINGER: But inspection is a lot

different than hacking.

MR. WESTREICH: That's true.

MR. FELTS: So for Milestone 8, those are site-specific dates. They range from dates in 2014 out to 2017. And for Milestone 8, they're going to have to have full program implementation, which really requires them to have procedures in place, policies and procedures in place, for training, attack mitigation, incident response, continuity of operations, and so forth.

And rather than just focus -- being focused on target set CDAs, this is the broad scope where they have to go through and evaluate the necessity and application of additional controls, cyber security controls, on all CDAs across the plant, which is a substantial number.

So in terms of life cycle of a plant system, there is nothing in the reg guide that specifically talks about life cycle, but it does touch on all of the various stages from acquisition of technology all the way through its use and retirement, use at the plant and retirement. So there are requirements associated with every one of these stages.

And I wanted to touch on one point just to potentially brush up against the topic that we were

earlier discussing, and that is for operating reactors it's a phased approach, like we just talked about, the fact that there's Milestones 1 through 7 now, Milestone 8, plant-specific dates, but for new reactors the full program implementation all the way through Milestone 8, essentially everything, the whole ball of wax, has to be done before fuel is loaded. So they have to have their full program in place before fuel loading.

MEMBER BROWN: As part of this initial round of whatever you all did, are you going to talk about it, supply chain aspect of this thing, which is -- you know, that's -- now you're down with the licensee and they're out buying stuff and things like that.

Have you all had any interface or interaction on their supply chain? Or is it just a programmatic issue where they're supposed to do that and tell you that they're doing it. And if they tell you they're doing it, and then you say, "Okay, check the box," and that's -- I'm not trying to be critical. I'm just -- is that -- how far down do you dig on the supply chain side?

MR. WESTREICH: Well, they do have requirements for what they need to procure, some procurement requirements, right? So we look at that aspect of it. We really haven't gone out and looked

at the vendor side yet.

MEMBER BROWN: My point being is that, you know, how do the vendor -- how does the vendor control the development of his software? And how is it managed, such that -- when it's accessed to who can get to it, and then who goes and looks to see a compromise of the code or whatever it is in terms of the development of the code.

MR. WESTREICH: Yeah. We really haven't gotten that far yet. I think that's something we've been talking about with the vendor group here, how do we go do activities to look at the vendors and assess how they're implementing those procurement instructions.

MS. SMITH: Hi. My name is Stacy Smith. I work in the Office of New Reactors in the Division of Construction, Inspection, Operational Programs. So in the vendor group there is a couple of things we're doing now.

There was a paper a couple of years ago, Counterfeit, Fraudulent, and Suspect Items. As part of that paper, there's a cyber security supply chain working group. So there was five actions that came out of that that we're implementing currently.

And we updated our inspection procedures for

routine and reactive inspections of vendors, where we included cyber security requirements. And we are going out to the major vendors, the new reactors right now, looking at the planning phases for software.

So it's stuff that we are looking at now, even though the rule is in effect. Our procedures are updated to look at this as they are going through the process.

MEMBER BROWN: When you say "looking at the vendors and software," is that how they manage the software, how they control it, and who has access to it? Is it a dedicated computer on which -- or server, or whatever it is, which is not connected to anything else?

Aside from the dynamic threat, one of the more vulnerable threats is somebody planting something in the base software that doesn't show up for some period of time. I mean, there's a clock in there that clicks, clicks, clicks away, and three years later it says, "Oh, it's time to play games."

MS. SMITH: The only questions we're starting to ask -- we have been interfacing with Eric and going to vendors now, and we are going to Westinghouse next week, and they are the kind of questions that are in the plan to ask them. And we're following the whole software life-cycle process.

So we are now looking at the planning phase for some of the software that is going into the new reactors, so we are just in the planning stage right now, but we're asking those type of questions for what they consider vulnerabilities. I mean, that's to come in a couple of weeks. We haven't done it yet.

MEMBER BROWN: Yeah. Okay. That's the one other area that I -- that if you've exited the plant where, you know, all of your other administrative controls and controlling who can touch what, you've got the dynamic, you've got the in-plant, but that supply chain side and what that computer -- I've forgotten who it was that -- we had one presentation where their software was actually on the corporate computer. And I'm sitting there saying, "Oops, what do you -- oh, well, there's a firewall." I'm sorry. That is not a wall in terms of separation from access.

Now, they explained something else to me, and I think something was resolved, but I'm not quite -- I'm just too old to remember what it was. So that's a critical area that you really need to focus on I think in terms of the isolation of wherever that software resides, who has access, how the versions are controlled, so that as each version is developed and it has been "inspected, tested," or what have you, there is no access

to it by other than one particular guy that owns the whole thing, even though he may not be the primary program. Just a thought.

That's what I did in my programs, in the naval nuclear program. We just -- it was very, very tightly controlled in terms of version control and who had -- who could make a change to the master set and what were the processes they went through before it ever got there. It's cumbersome, but it's the only way to control what you've got. So just a thought to pass on to you when you're doing your staff.

MS. SMITH: Yeah. And version control is part of design control, which we'd be looking at anyway for software, since it is a safety-related component.

MEMBER BROWN: But think about access.

MS. SMITH: Okay.

MEMBER BROWN: Okay?

MR. WESTREICH: Thanks, Stacy.

MEMBER BROWN: Yeah. I appreciate that.

MR. FELTS: That is my last slide. I'll turn it over to Monika to talk about interagency and international.

MEMBER BROWN: Are we ahead or behind here? We've got until 9:50 before we head into the closed session. I think we're -- we're okay.

MS. COFLIN: I'm Monika Coflin. I'm a cyber security specialist in NSIR. I've been with NRC for five years and worked in cyber security at NRC for those five years.

I'm going to discuss the NRC's recent intergovernmental and international cyber security activities.

As you are probably well aware, NRC's authority is derived from the Atomic Energy Act, while FERC's authority for grid reliability is tied to the Energy Policy Act of 2005. These two authorities relative to cyber security intersect at nuclear powerplants.

Back in January 2008, FERC issued Order 706, which specified critical infrastructure protection, or CIP, reliability standards to safeguard cyber critical assets. NRC facilities were exempt from those requirements.

NRC and FERC recognized the need to ensure that there was no gap or overlap between the regulatory programs. FERC subsequently issued Order 706 Bravo, which clarified that the balance of plant and equipment within the powerplants that were not within the scope of NRC's regulatory requirement would be within the scope of the NERC order.

As a result, NERC asked all nuclear powerplants to determine which structures, systems, and components would be potentially subject to the six standards, and which would be potentially subject to NRC regulation. This analysis was known as the bright line process.

All of their plants indicated that, if compromised, balance of plant structures, systems, and components would affect reactivity and were important to safety, and, therefore, would fall within the scope of NRC's regulation. The Commission determined, as a matter of policy, that NRC's cyber security regulation should be interpreted to include structures, systems, and components in the balance of plant that have a nexus to radiological health and safety. Licensees and combined license applicants subsequently updated their cyber security plans to reflect that Commission decision.

NRC staff maintains periodic communications with staff from FERC and NERC to exchange information and to ensure that the requirements that are in place are effective to meet both organizations' interests.

Back on February 12th of this year, President Obama issued an Executive Order on improving critical infrastructure for cyber security and an associated

Presidential Policy Directive. The Executive Order requires federal agencies to produce unclassified reports of threats to U.S. companies, and requires the reports be shared in a timely manner.

It also establishes a voluntary program to promote the adoption of the cyber security framework that is currently being developed by NIST.

Independent regulatory agencies such as the NRC are encouraged to leverage the voluntary framework and to consider prioritized action to mitigate cyber risk for critical infrastructure consistent with their authority. The Executive Order also calls for the review of existing cyber security regulations.

NRC of course will review our requirements, as directed by the Presidential Policy Directive, and although we're confident that our cyber security program is strong, we will implement any improvements that are identified from that review. Because NRC is an independent agency, the NRC is not obligated to take actions as a result of the Executive Order.

However, NRC is voluntarily participating in a number of areas. For example, NRC management and staff have interacted with national security and DHS staff on policy issues. NRC staff is also participating in the integrated task force working groups that have been

formed by DHS to implement the Presidential Policy Directive.

We believe that given the state of our cyber security program compared to those in other critical infrastructure areas that we can make significant contributions towards meeting the deliverables from the Presidential Policy Directive.

Turning to some other intergovernmental activities, NSIR participates in numerous interagency working groups, such as the Joint Cyber Subcouncil. The Joint Subcouncil includes members from the Department of Homeland Security, FBI, NRC, and private sector representatives, and the Subcouncil identifies cyber security risks potentially affecting the nuclear sector, serves as a forum for sharing relevant information within the critical infrastructure framework, and helps the nuclear sector participate in cross-sector bodies such as the cross-sector cyber security working group and industrial control system working group.

This last slide provide examples of bilateral and multilateral activities relative to cyber security; for example, NRC staff who have had specific technical exchanges with Korea and Spain on cyber security. Staff has also shared cyber security best practices with

organizations such as the World Institute for Nuclear Security.

NRC has also participated in a number of IAEA consultants meetings and larger technical meetings. In these multilateral meetings, topics have included developing guidance for computer security at nuclear facilities, including nuclear powerplants, applying cyber security controls to digital instrumentation and control systems, and developing assessment methodologies for cyber risk.

NRC also reviews IAEA's safety standards to ensure that proper and adequate interfaces with cyber security are occurring.

In general, we are ahead of other countries in establishing a regulatory framework that considers cyber security. Staff believes that sharing their experience in developing NRC's cyber security program will contribute to a more robust global cyber security program for nuclear facilities.

We have also been able to consider the efforts and approaches of other international partners in relation to NRC's cyber security program and will use those insights as the program evolves.

That concludes my presentation.

MEMBER BROWN: Has there been any thought

given -- this is a very perverse thought. Okay? It just occurred to me as you were talking. Sharing of the details of the NRC's cyber security program, what you assess, how you assess, et cetera, et cetera. Doesn't -- while I'm all for international communication, doesn't that somewhat tell other folks to assess where your weaknesses are, such that their nasty people, whoever, whichever country they're associated with, now have a better understanding of where they can throw -- I mean, has there been any thought -- I'm not -- I said it was a perverse thought.

CHAIRMAN ARMIJO: I don't think there's anything perverse about it.

MR. WESTREICH: We don't share information with other government organizations, unless we have an agreement that we can share this information. So we have to have standing agreements in place for like the sharing of Safeguards information and how they can control it. So we have to have an established relationship before we'd share any information, and then --

MEMBER BROWN: I'm talking about them taking this, you know, and their bad guys that are out there wanting to snoop now say, "Oh, they've protected against this, that, that, and that, but, hmm, we've got an end-run

over here that may give us some access." I don't know. It's just a -- I told you it was a perverse thought. I hadn't come to this point with it.

MR. ERLANGER: Good morning. Craig Erlanger.

MEMBER BROWN: You're back.

MR. ERLANGER: I'm back. Can't get rid of me, Charlie. I have just transitioned from the cyber program, but I was involved in many of the international activities. To date, the majority of the sharings have been basically conceptual concepts, a programmatic approach versus looking at an individual asset, prescriptive versus performance-based, nothing with an appreciable level of detail, definitely nothing we're seeing in inspections-based for what areas can be improved.

So we're not at that level yet, so I don't -- it's something for us to be mindful of, but we haven't had those interactions yet.

MR. WESTREICH: Although we do have requests for that information, so we're working through that.

MEMBER BROWN: I'm glad you said that. It wasn't necessarily a bad question.

MR. WESTREICH: No. I mean, we have -- Korea is very interested. Speaking of -- other countries are

very interested in what we're doing and how our programs are established. I think as Monika said, you've got to look at the broader picture. Would we rather have people more protected, or are we -- so we've got to balance those two pieces.

MEMBER BROWN: It's a balance. It's just that you have -- somehow you have to make sure our interests are protected in that manner.

Let me ask one other -- I'm going to ask this question again later when you go through the Diablo Canyon pilot program and your discussions of Oconee, since you've done those. But, you know, we issued Reg Guide 5.71, and you've had -- since then that was about four years ago, 2008 or 2009, whatever. You have now had a number of inspections. I think Ralph alluded to 14 plants.

And you've had these interactions with these other organizations. And if you go back -- and I'm trying to remember, but I think we made some comment that stuff you learned, we ought to see if we need to update or do any revision work to 5.71 to improve what we have -- improve upon that based on what we have found over the last four years.

Is there anything in play to start providing an assessment of that, what we ought to do with that?

I mean, 14 plants to go out and inspect and see, we should have seen a pretty wide variety. I mean, Ralph alluded to some were pretty good and some were bottom-feeders, so --

MR. WESTREICH: Yes. Well, I think there are plans to update Reg Guide 5.71. I'm not sure what the schedule is.

MS. COFLIN: Yeah. I think we have committed to beginning that update in 2014.

MEMBER BROWN: Okay.

MR. WESTREICH: But there is other things we're doing based on the inspection experience.

MEMBER BROWN: Okay. I would appreciate it if you would communicate with Christina to let us know when we might see -- you know, just -- it doesn't have to be something where we have to -- you know, where we have to take massive handlers or anything. We'd just like to know where are the areas in 5.71 that you've got on potentially -- or that you've learned which may help that guidance as we then provide it out to the various vendors.

Yes, hi.

MR. LEE: Eric Lee from NSIR. I don't know whether you remember from last briefing, I think one of the reasons that we may hold up on this revision at

this time is to provide stability during this interim period with the implementing of this cyber security program. And we are collecting all of this information as you have mentioned.

And when we complete -- a licensee completes implementing their full cyber security program, we will be, you know, updating the Regulatory Guide 5.71.

MEMBER BROWN: Okay. Yeah. I wasn't insisting on, you know, every year you have to go change stuff while we're in the process of trying to develop these things, but, you know, it shouldn't be a 2025 type issue either, so --

MR. FELTS: I'd like to add that there are other mechanisms we have to communicate to industry when we believe there may be a lack of common understanding of a requirement, particularly a requirement that is in a plan. And we have exercised the security frequently asked questions process to provide additional information to the licensee community where we found there may have been some misalignment in their understanding of what is required to implement Milestones 1 through 7.

So that's a little more nimble. We can get those out more quickly than a reg guide update. And typically when we go through the reg guide updates we

go back and look at all of the security frequently asked questions and roll in any information we think is appropriate in that update.

MEMBER BROWN: Okay. I guess --

MEMBER SKILLMAN: I'd like to ask a question before we go to the closed session, please. I'm one of the people that was in the industry before there was SALP. I was a director at plants during SALP. I was a director at plants with ROP. And so I've got firsthand experience and bruises from all of those changes.

I'm wondering how the agency is going to integrate, if you find a deficiency in cyber area, with the ROP. Is it going to be an initiating event, cornerstone item? Is it going to be a mitigating system? Is it going to be a barrier to integrity, or is it going to be secure?

MR. WESTREICH: I think it's currently in the security cornerstone. So that's where it exists. Of course, you know, each one of these deficiencies live in some kind of other system, like either it's a safety system, security system, so we're actually fully integrated into the ROP. There are significance determination processes for each one of these findings.

We are part of the ROP process and function, and security now has reintegrated back into that process.

So it's -- there is good communication between our findings and the current programs for ROP in assessing overall licensee performance based on all of the cornerstones.

MEMBER SKILLMAN: Let me go a little bit further. If this agency were to be hacked, would you get a red finding for the agency? And if that same ability to hack --

(Laughter.)

-- is some plant manager going to get fired when that man doesn't have, or that woman doesn't have, clairvoyance? Because that's the way the system works. Out in the plants, if you're the poor guy on watch, or the poor woman on watch, and an event occurs, and it's determined that it might kind of have been avoided, normally somebody gets a change in position.

And so what I'm really wondering here is, to what degree has this been thought through? Because some of the events that lie ahead for the industry affect people, affect their careers, and the same difficulties that would affect the team here at White Flint can affect those individuals who are out in the plants. And often there are threats that those individuals really can't imagine or determine.

MR. WESTREICH: Yeah. Well, you know, we --

I guess we don't control what the licensees do to the people. And I don't -- I agree with you, I don't necessarily agree with the actions that are taken if there's an event or a finding. But if you look at our SDP, I mean, one of the things you might want to look at is our significance determination process.

To get to a significant finding, you really have to have a direct impact on a safety system function. So you really have to get fairly far down the road. You're actually -- there is some vulnerability associated with the safety system function, which is pretty far in.

MEMBER SKILLMAN: Well, clearly, it's the SDP. I understand that. But I'm kind of taken by Charlie's comment that here you have this little black box with a timer, and it has been latent for 36 months and it says, "Now is the time to wake up, and control rods do this." And here is some poor plant manager saying, "What happened?"

MR. WESTREICH: We agree. I mean, if it's beyond the control of the licensee to be able to figure that out, it's not even a finding, right? You know, in the ROP world, they have to have a performance deficiency. So it's got to be something that they would have been able to identify correct. If it's some latent

embedded software from --

MEMBER SKILLMAN: I'd like to make sure that what you just mentioned is well carved on the record.

MR. WESTREICH: Yeah. We can look at --

MEMBER SKILLMAN: Because that's the heart of it.

MR. WESTREICH: I mean, I think it goes to this performance deficiency issue. If it's something beyond their control, we typically don't hold them liable to that because they have no way to control that.

MEMBER SKILLMAN: Good. I'm done. Thanks.

MEMBER BROWN: How did they get into the plant in the first place? If it's intentionally inserted, that's why I made the point the way I did, that this is -- somebody with malicious brainpower, if he had control of the software at the vendor, now there's a routine that is buried that gets triggered. And when you've got a half a million lines of code, they're going to find it.

MR. WESTREICH: Yeah. I mean, the comment was, if it is beyond the licensee's ability to control and identify --

MEMBER BROWN: I'm not saying that is easy to do, okay, because it's really not. But anyway, that's -- the point is valid. Somebody is going to get shot

anyway.

Okay. I guess we've got to go into the closed session.

(Whereupon, at 9:56 a.m., the proceedings went into Closed Session.)

U.S.NRC

UNITED STATES NUCLEAR REGULATORY COMMISSION

Protecting People and the Environment

Cyber Security Update (OPEN SESSION)

Cyber Security Directorate
Office of Nuclear Security and Incident Response
September 6, 2013

Agenda

OPEN SESSION:

- Control of Access Update - NRO
- Overview of the NSIR Cyber Security Directorate – NSIR/CSD
- NRC's Cyber Security Program/ Regulatory Framework – NSIR/CSD
- Interagency / International Activities – NSIR/CSD

CLOSED SESSION:

- Cyber Security Oversight Program – NSIR/CSD
- Inter-Office Coordination Activities – NSIR/CSD
- Cyber Security Roadmap Activities – NSIR/CSD

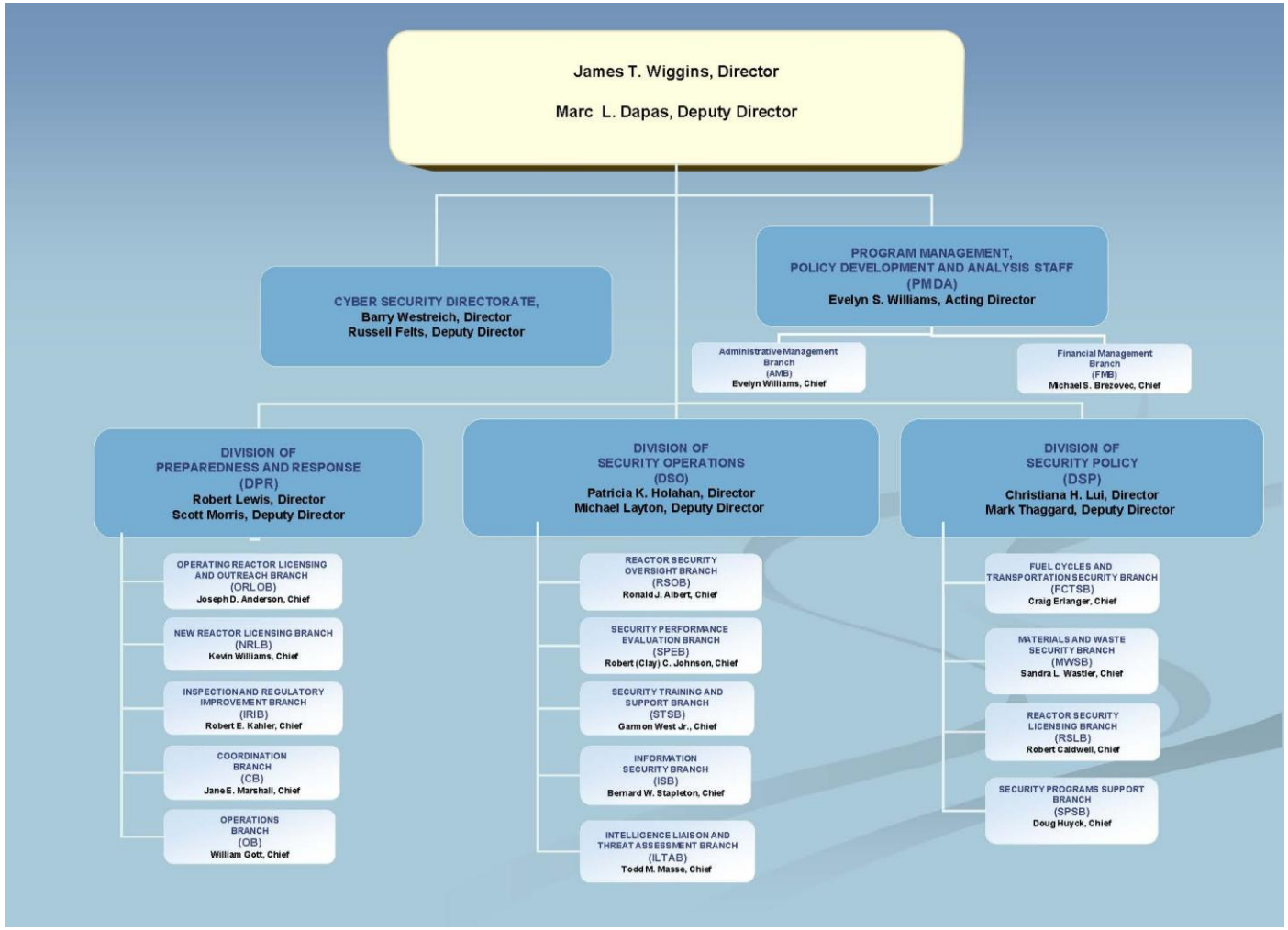
Purpose

- Provide an overview of NRC's cyber security program and explain how it is being implemented.
- Improved communication and coordination with ACRS on cyber security.
- Identify areas of interest for future interactions.

Overview of the NSIR Cyber Security Directorate

NSIR Organization Chart

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



Cyber Security Directorate (CSD)

- Established in June 2013

- Focus Areas:
  - Rulemaking
  - Guidance
  - Licensing
  - Policy Issues
  - Oversight Related to Cyber Security Requirements

NRC's Cyber Security Regulatory Framework

Cyber Threat Landscape

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

Threat vectors

- Hard-wired networks
  - Internet
  - Intranet
- Wireless
  - Wifi
  - Bluetooth
- Mobile media
  - USB thumb drive
  - CD/DVD
- Portable equipment
  - Laptops
  - Test equipment
- Supply chain
  - Vendors
  - Vendors to the vendors

Threat characteristics

- Motivated
- Opportunistic
- Persistent
- Adaptive
- Learning
- Good at info sharing

Cyber Security Historical Timeline

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

1998	Presidential Decision Directive 63 (PDD-63)
2001	Executive Order on Critical Infrastructure Protection (CIP)
2001	Issued advisory to NPP to enhance cyber security
2002	Required NPP to implement Interim Compensatory Measures
2003	Issued Design Basis Threat Order
2004	Published NUREG/CR-6847 – Cyber Risk Assessment
2005	Endorsed NEI 04-04 Rev. 1 – Cyber Security Program
2007	Design Basis Threat Rule 10 CFR 73.1/RG 5.69
2009	Issued Cyber Security Rule 10 CFR 73.54
2010	Published Cyber Security Regulatory Guide (RG 5.71)
2010	NEI publishes NEI 08-09 – used by operating NPPs
2011	Published RG 1.152, Rev. 3 – computers in safety systems
2011	NPP Cyber Security Plans approved
2013	Inspection of Interim Milestones begin

10 CFR 73.54

- Title: Protection of digital computer and communication systems and networks
  - Applies to power reactors – operating and new reactors
- Performance-Based, Programmatic
  - Provide high assurance against cyber attack
  - Integrated with Physical Security Program (10 CFR 73.55)
- Basic Requirements
  - Establish, implement, and maintain a cyber security plan
  - Critical digital assets must be protected
  - Protect safety, important-to-safety, security, and emergency preparedness functions and support systems that can impact those functions
  - Provide defense-in-depth protective strategy
  - Implement a defensive architecture
  - Address technical, operational, and management controls

Regulatory Guide 5.71

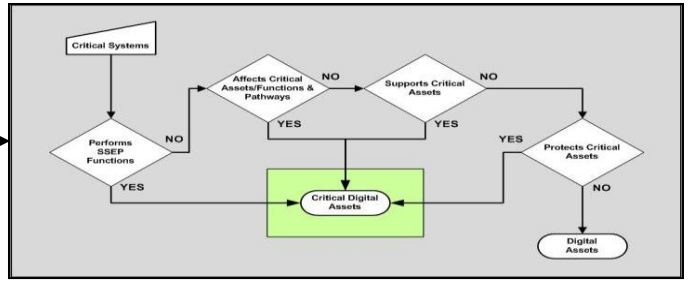
U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Title: Cyber security programs for nuclear facilities

Form Cyber Security Team

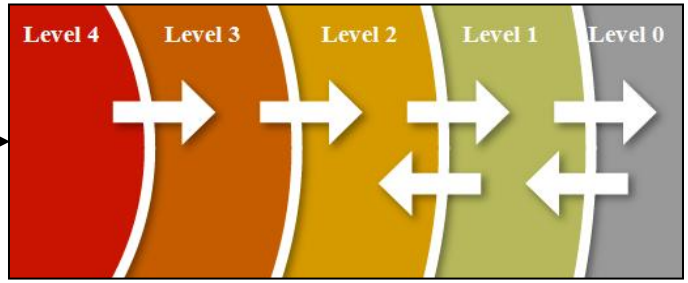
↓

Identify Critical Digital Assets



↓

Apply Defensive Architecture



↓

Address Security Controls

1. Address each control for each CDA, or
2. Apply alternative measures, or
3. Explain why a control is N/A

Implementation

- Interim Milestones 1-7 (December 31, 2012)
  - addresses key threat vectors
  - emphasis on target set equipment
- Milestone 8 (site specific date – 2014-17)
  - full cyber security program implementation
  - policies and procedures: training, attack mitigation, incident response, continuity of operations, etc
  - completion of all design remediation actions including those that require a refuel outage for implementation
  - Address all security controls for all CDAs

Cyber Security Lifecycle

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

- Operating NPPs start in the Operation & Maintenance phase
  - Earlier phases of the lifecycle are implemented as needed based on licensee approved Cyber Security Plan
- New NPPs begin at the Concepts & Requirements phase
  - All regulatory requirements must be met before fuel arrives onsite

Digital system security lifecycle as outlined in RG 5.71				
Concepts & Requirements	Design, Implementation, & Test	Installation, Checkout & Acceptance Testing	Operation & Maintenance	Retirement
• Security planning & requirements analysis	• Supply chain security • Functional security design •System test & evaluation	• Audit of security control effectiveness (operational focus) • Vulnerability scanning	• Continuous monitoring & assessment	• Design control • Media sanitation (digital and non digital) • Disposal testing

Interagency and International Activities

FERC/NERC Activities

- Memorandum of Agreement with FERC
- Memorandum of Understanding with NERC
- Gap Analysis by NRC and FERC
- “Bright-Line” survey
- Commission Policy in SECY-10-0153
- Commission level meetings
- FERC Office of Energy Infrastructure Security established

Cyber Executive Order 13636/PPD-21

Improving Critical Infrastructure Cybersecurity

- Issued February 12, 2013
- New information sharing programs to provide both classified and unclassified threat and attack information to U.S. companies
- Development of a Cyber Security Framework
- Establishes a voluntary program to promote the adoption of the Cyber Security Framework
- Includes strong privacy and civil liberties protections
- Review of existing Cyber Security Regulation

International Activities

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

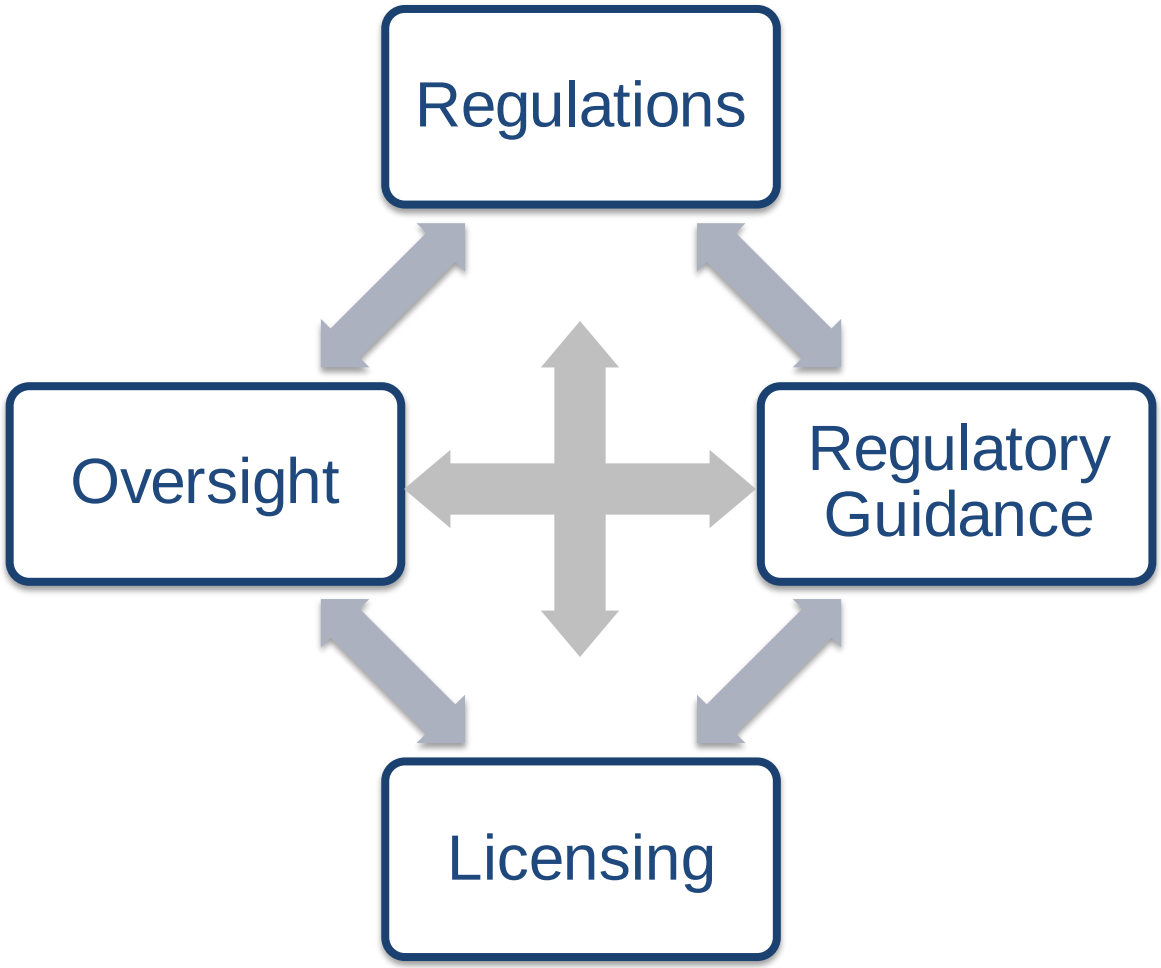
NRC provided support and perspectives to the following:

- IAEA TM - Computer Security At Nuclear Facilities (May 2011)
- WINS – Workshop on the development and integration of cyber security programs (Feb 2012)
- IAEA Consultancy Meetings
- Korea Atomic Energy Research Institute (KAERI) -NRC's cyber security and safety-security interface regulations (May 2012)

Questions

Backup Slides

Regulatory Framework



Regulatory Guidance Pedigree

- Primary Sources
  - National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53
  - NIST SP 800-82
- Contributors
  - NRC staff from NSIR, NRR, NRO, RES
  - National Laboratory
  - Industry / Public Stakeholders
  - Private industry experts

Cyber Security Plan

- Cyber Security Plan
  - Licensing document / required by regulations
  - Describes how cyber security program is established and maintained
- Essential elements:
  - Describe the process for identifying CDAs
  - Describe the defensive model (protective strategy)
  - Reference a comprehensive set of security controls
  - Describe the process for addressing each control
  - Commit to maintaining adequate documentation

Other Intergovernmental Activities

- Joint Cyber Subcouncil
- Cross-sector Cyber Security Working Group
- Industrial Control Systems Joint Working Group

NRC involvement in EO/PPD Activities

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

- Review our requirements, as directed
- Implement any improvements identified by the review
- Participate in executive level meetings and staff level working groups