Official Transcript of Proceedings

NUCLEAR REGULATORY COMMISSION

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

Docket Number: (n/a)

Location: Rockville, Maryland

Date: Tuesday, June 4, 2013

Work Order No.: NRC-4277 Pages 1-130

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

+ + + + +

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

(ACRS)

+ + + + +

DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS

SUBCOMMITTEE

+ + + + +

OPEN SESSION

+ + + + +

TUESDAY

JUNE 4, 2013

+ + + + +

ROCKVILLE, MARYLAND

+ + + + +

The Subcommittee met at the Nuclear Regulatory Commission, Two White Flint North, Room T2B1, 11545 Rockville Pike, at 1:00 p.m., ***CHARLES H. BROWN, JR.***, Chairman, presiding.

COMMITTEE MEMBERS:

CHARLES H. BROWN, JR. Chairman

J. SAM ARMIJO, Member

DENNIS C. BLEY, Member

WILLIAM J. SHACK, Member

ACRS CONSULTANT:

MYRON HECHT (via telephone)

DESIGNATED FEDERAL OFFICIAL:

CHRISTINA ANTONESCU

TABLE OF CONTENTS

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

1:00 p.m.

CHAIRMAN BROWN: The meeting will now come to order.

This is a meeting of the Digital Instrumentation and Control System Subcommittee. I am Charles Brown, Chairman of the Subcommittee.

ACRS Members in attendance are Dennis Bley. Coming, will be Sam Armijo, Bill Shack, myself and Myron Hecht, our consultant, is participating by phone as a consultant for the Subcommittee meeting.

Christina Antonescu of the ACRS staff is the Designated Federal Official for this meeting.

During this meeting, the staff and the Office of Nuclear Security and Incident Response NSIR will brief the DI&C Subcommittee on staff's activities associated with cyber-security.

The Subcommittee will gather

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

The rules for participation in today's meeting have been announced as part of the notice of this meeting, previously published in the Federal Register on May 30, 2013.

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

Also, today's agenda highlights areas for which the meeting may need to be closed, in order to protect unclassified safeguards information.

In particular, the open session for the public will be from 1:00 p.m. to 2:45 p.m. and the closed session will be from 3:00 p.m. to 5:00 p.m., right after the break.

Also during the open session, we have the following people from the public on the bridge line, listening to the discussions.

Skip Butler, Peter Yandow, Patricia Campbell, Matthew Bohne, excuse me if I pronounced that wrong, Brian Buckley, Sara Rudy, Lee

Doughtery, all from GE Power & Water, and Bob Hirmanpour, Southern Nuclear Company.

If there is anyone else on the line, would they please identify themselves at this time?

MR. RUSSO: Scott Russo from GE.

CHAIRMAN BROWN: Okay, Bob Russo?

MR. RUSSO: Scott Russo.

CHAIRMAN BROWN: Okay, Scott Russo, okay, thank you. Have you got that?

To conclude, anyone else? Excuse me?

Okay, to -- we would appreciate to preclude interruption of the meeting, the bridge line will be placed on listen-in mode during the discussions and presentations and Committee discussions.

A transcript of the meeting is being kept and will be made available, as stated in the Federal Register Notice.

Therefore, we request that participants in this meeting use the microphones located throughout the meeting room, when addressing the Subcommittee.

The participants should first identify themselves, and speak with sufficient clarity and

volume, so that they may be readily heard.

We will now proceed with the meeting. I call upon Christiana Lui, correct?

MS. LUI: Correct.

CHAIRMAN BROWN: Thank you, Director of Division of Security Policy in the Office of Nuclear Security and Incident Response, to provide some introductory remarks, followed by Tom Bergman, Director of Division of Engineering of the Office of New Reactors, who will also provide some introductory remarks for NRO, before we proceed.

Christiana, would you like to go ahead?

MS. LUI: Yes, thank you. Good afternoon.

As Mr. Brown has mentioned, I am Christiana Lui, currently the Director of Division of Security Policy in the Office of Nuclear Security and Incident Response.

Sitting with me at the table to my right are Tom Bergman, Director, Division of Engineering in the Office of New Reactors, Ron Albert, Chief of the Branch -- Chief of the Reactor Security Oversight Branch in the Office of Nuclear Security and Incident Response, and Craig Erlanger, Chief

-- the Cyber-Security and Integrated Response Program Branch Chief in the Office of Nuclear Security and Incident Response.

Sitting at the table is Barry Westreich. He is currently the Deputy Division Director in the Division of Security Operations in the Office of Nuclear Security and Incident Response.

In the audience, we also have staff and management coming from the Office of Nuclear Reactor Regulations, the Office of Nuclear Material Safety and Safeguards, the Office of Regulatory -- sorry, the Office of Nuclear Regulatory Research, and I think I've seen some staff coming from FSME, but I don't see them right now.

All right, so, many of our past interactions on cyber-security were in the context of regulatory guide reviews and digital instrumentation and control, and cyber-security licensing actions in the past.

We're glad to have the opportunity to support these dedicated Subcommittee meetings on cyber-security regulatory programs today.

We worked very closely with the ACRS

staff, in developing today's agenda.

In the next few hours, we plan to first introduce the cyber-security staff, and followed by the Cyber-Security Regulatory Program elements.

Specifically, we want to provide you an overview on how we have developed and implemented the existing regulatory program, the various technical and regulatory products produced and to be produced, any notable domestic and international engagements, and how we are working the interface on those regulatory issues that have both safety and security considerations.

Our goal is that by the end of today's meeting, you will all have a clearer picture on the agency's cyber-security and regulatory program.

With that, I would like now to turn to Tom, for him to offer a few thoughts.

MR. BERGMAN: Yes, again, my name is Tom Bergman. I am the Director of Engineering in the Office of New Reactors.

Actually, the purpose of mine is to update all of you on the EMPOWER DSRS initiative. We committed to periodically update you, as we

make progress on that, and this is a very good opportunity.

So, this is a current status briefing. It's subject to change. Much of what I'm going to talk about is influx. I hope that is enough caveats for what I'm going to go forward with.

Previously, the ACRS raised issues on communications independence and the cyber-security framework in new reactors, in numerous letters, and most recently, in the interpretation of a clause in IEEE 603, dealing with control of access, and that is the one where we committed to get back to you.

We've had a series of meetings in the staff. We tasked the Branch Chiefs involved from NSIR, NRO, NRR and Research, to come up with a set of options, which they presented to Division Management.

We refined it a bit, and late last week, we met with the Office Directors for NSIR, NRR and NRO, and they modified our proposals and added one.

We have engaged key stakeholders, but we need to re-engage, in particular OGC, on a couple of the options, as well as others, as we go forward.

What was approved by the Office Directors was to move forward, to continue to explore three concepts in parallel, four new reactors.

The first one is actually kind of already underway, and that is engaged licensees early during construction, regarding implementation of the cyber-security program and the I&C design.

We've already had meetings with the licensee. We'll continue to do so.

We're looking for an effort more like what NRR did with Diablo Canyon, and you're going to get briefed on that in more detail later, and then you'll also get briefed more specifically on the activities between NSIR and NRO on new reactors.

The second item is to incorporate a requirement regarding cyber-vulnerabilities with respect to certain designs into the current 10 CFR 50.55(a)(h) rule-making to endorse IEEE 603-2009, and this is still a concept. We haven't turned it over to the staff, to figure out how you would implement it, and if you can implement it.

But the concept is that for those

designs that need an alternative or an exemption to the requirements in 50.55(a)(h), they would need to describe the cyber-vulnerabilities of their design that they've introduced through their design.

In other words, if they don't meet the requirements as written, and they come in under either 50.12 or 50.55(a)(a)(3), then they would need to address the cyber-vulnerabilities.

So, the assumption is that 50.55(a)(h) provides a decent system, all right.

The purpose of this requirement is to ensure that the cyber-vulnerabilities and the design are understood and there is a clear hand-off from the design certification vendor in the COL applicant and licensee, as to what aspects of the design do need to be addressed through the cyber-security program.

So, it doesn't really change the current framework of the cyber-security program in a safety base design. It augments or enhances the implementation of the program, by being clear up front, where there may be some vulnerabilities in the design with respect to cyber.

This approach is generic. It would not be specific to EMPOWER, as we currently envision it. It would -- if we can do it through this current rule-making, it would be done in a time frame that would support the EMPOWER review, as well as other new reactor reviews.

We believe it may address your concerns, as expressed previously, regarding the most recent letter. At this time, we do not expect to modify the staff's interpretation of what control of access is meant. We think this other requirement is more effective.

The third concept in parallel would be to develop a new regulation to consider the impact of design on cyber-security, and in the model that was discussed, was 2014-06, which is minimization of contamination.

Are you familiar with that regulation? It's very short, that's why I brought the book. It's actually really, only about a sentence.

It says -- it only applies to new reactors, and it says that, "They shall describe how the facility design and procedures for operation will minimize, to the extent practical,

contamination of the facility and the environment, facilitate eventual decommissioning and minimize, to the extent practical, the generation of radioactive waste."

So, we think that sort of concept up front is workable. It's a good analogous rule in a different part.

That would be a long-term effort, because that is a whole new rule-making. So, it would go through prioritization and budgeting process, and with that, unless you have any specific questions for me.

CHAIRMAN BROWN: I guess I do have a question, in terms of -- I'm trying to connect the dots between radioactive contamination of the site during decommissioning, with --

MR. BERGMAN: Oh, no.

CHAIRMAN BROWN: -- control of access, or whatever you said.

MR. BERGMAN: You could replace contamination with cyber.

In other words, it would be that same framework of -- in new reactors, they have to look at their design and say, "Have we done things that

would mitigate the release of radioactivity, due to whatever?"

So, a lot of the plants are basically lined in stainless steel, right, to a -- certainly, anything that is handling radioactive waste is lined in stainless steel.

That's saying, consider the long-term consequences of operation early in the design.

The analogy is, you would say, "Consider the ramifications on -- of cyber-security on -- or of your design on cyber-security program later."

This is the longest term one that requires the most work. It's the most conceptual, but that is -- it's just a model. It's not going to be in Part 20. It would be, likely in Part 50, as a design requirement or potentially, in Part 73 as a cyber-requirement.

But again, that is to augment the existing framework, but that would be a new rule-making.

So, when I say that is a long-term, I mean, typical rule-making from concept to the finalization that isn't of a crisis mode, you know,

it's five-ish years.

CHAIRMAN BROWN: Right, I'll be dead by then, potentially.

MR. BERGMAN: Well, we do a lot of rule-making for the agency. So, it has to enter that whole process. That is why the second one is more the near-term fix.

CHAIRMAN BROWN: But yes, the second one, I'm trying to get a little -- that was the second question was, you talked about if a licensee or a designer, whichever, I've forgotten the terminology you used, when you went through the phrases, requires an exemption from 50.55(a)(h)(2), I think you said, which (a)(h) implements 603.1991, if I remember correctly.

MR. BERGMAN: Yes.

CHAIRMAN BROWN: And the issue we brought up is, we've separated the cyber thought process from the existing regulations that require the plant design to provide control of access, and that the engineer -- the design of the plant has to do that.

So, are you saying that they would be exempted? They would apply for an exemption and

say, "No, we don't have to provide for control of access," is that the --

MR. BERGMAN: So, we're trying to --

CHAIRMAN BROWN: I'm trying to connect the dots on that.

MR. BERGMAN: Whether they need an exemption or an alternative, without getting too deep into 50.55(a), depends where the requirement exists in 50.55(a).

Some parts of it require an alternative. Some parts of it would require an exemption.

CHAIRMAN BROWN: Yes, but 603-1991 is very specific.

MR. BERGMAN: Right.

CHAIRMAN BROWN: And that's implemented -- you know, that is actually a part of the rule, that says you have to design your plants in accordance with that, which talks about control of access, very clearly.

And it says, not only do you have to have procedures to do that, you have to have a plant design that allows you to execute it. That's got to -- you know, the plant has to accommodate to

be able to do that.

Therefore, that means -- and the point we've tried to make is, we've got to consider those types of things during the DCD or the licensing process, not post, not wait. That was the point of our last -- that was the -- you know, one of the three points that we made in our last letter in EMPOWER.

So, I'm having a little bit of difficulty of connecting those dots, in terms of an exemption or where they -- that the --

MR. BERGMAN: You know, if you need it -- if you meet it, and it would be 2009 we're talking about, right. This is the new -- this is the rule-making to endorse the more recent edition of the standard.

CHAIRMAN BROWN: Yes, I haven't read the 2009 for control of access, but I've -- isn't it the same?

MR. BERGMAN: I don't know on that specific clause, but in the -- in a rule-making like this, much is -- I mean, if you look at 50.55(a), most of it is staff exceptions to the codes and standards.

So, you have the standard, plus you have the staff exceptions to the standard. That combination of requirements, if met, we would say, they need to do nothing. We would rely solely on the -- on the existing framework.

If they do not meet all those conditions, then they would need to come in under -- with either an alternative -- let's just use alternatives, to keep it simple, an alternative.

In that case, where they need an alternative to meeting the rule, as written, then they need to address the cyber-vulnerabilities in the design, that they've introduced, by not meeting the --

CHAIRMAN BROWN: Okay, let me put this -- let me craft this into something I can understand.

I understand your general point, at least two of the new designs, I'm pulling on my memory, over the last three years now, that we've looked at maybe three, and referencing this to the concern we raised with EMPOWER.

In other words, you've got the safeguard systems and the reactor trip systems all

feeding a giant network, which goes up to the main control room, and the technical support facility center.

That network has a computer on it, which then connects to the outside world, either the business network or the corporate network, or call it whatever you want. It goes -- it leaves the plant.

MR. BERGMAN: Leaves the page.

CHAIRMAN BROWN: That is right, and that computer, in the earlier versions that we had talked about, has a firewall in it, but it is a software based firewall. It could have been a software -- in fact, as one said, it would be, but they hadn't really -- you know, it was part of the design, and they hadn't done it yet, and so, we had that interchange in the earlier -- in the meetings.

Now, the rule is -- doesn't get real specific, in terms of how you do that. We've tried to make the point that it needs to be an incontrovertible hardware one-way firewall, not something subject to a hacker, playing games with bits and bytes, to allow himself access, and I use

-- you know.

There has been examples where plants in existence today, with some systems connected off to a business network somewhere through a firewall, somebody left the firewall in a two-way communication mode, while they were updating their software, and ended up getting some error code back in the rest of the plant, not a fun circumstance to have to clean up.

So, I'm trying to envision how this works, if they come in, in this design and they say, "Well, ghee, we're going to ignore the obvious, and say we're so smart, we can manage having people pound us to death with hackers for the next 40 or 60 years," and constantly changing software all the time.

Therefore, "We're going to tell you why it's going to be okay," from a cyber -- that is -- that is what I get out of the comment that you're making.

They have to justify not doing it the right way.

MR. BERGMAN: And that is -- and there is interplay between this -- this potential new

requirement and what is already in 50.55(a)(h), right.

So, without -- that is -- that regulation is currently being worked on by the staff, and there is a healthy and diverse range of views of how restrictive, going from, you know, nothing to hardware based only, to allowing software controls under certain conditions.

Where we'll end up, we don't know, right. So, but where we end up does influence the effect of this new requirement.

So, that will be worked out, through that rule-making, and you'll have an opportunity to weigh in on that rule-making. I think we're coming to you in the October time frame.

So, yes, it does --

CHAIRMAN BROWN: Well, in 603 --

MR. BERGMAN: You picked up on the point --

CHAIRMAN BROWN: -- 2009?

MR. BERGMAN: Yes.

CHAIRMAN BROWN: And 55(a)(h)?

MR. BERGMAN: Yes.

CHAIRMAN BROWN: Whatever.

MR. BERGMAN: Yes, so, you're correct.

How that rule is written affects how those types of designs would be viewed and what -- whether or not they would need an alternative to that regulation, addressing their vulnerabilities.

But understand, this concept that has been agreed to explore wouldn't preclude a design having those vulnerabilities by itself, right.

It says you need to explicitly acknowledge what the vulnerability is, so that the COL applicant understands the vulnerability they will need to address, that is created by the design, through their program.

So, it leaves intact the safety based review we do today, coupled to a cyber-security program, but highlights very early, before the COL has, in theory, even been applied for, but certainly, before it's been issued, that this design has these features that create known cyber-vulnerabilities.

CHAIRMAN BROWN: Okay, I'm going to make a personal comment that doesn't reflect the

views of the Committee, if you don't mind. Okay, Sam? Thank you, since I said that --

MEMBER ARMIJO: I didn't say it, because I want to make a comment too.

CHAIRMAN BROWN: I guess, I just want to make an observation, relative to the networks and this interplay between how you get data in and out, or if you do.

Obviously, zero going -- no connection is a great way to do it. You would never get any argument from me, okay, and I've made the point -- or through the Committee, which we've agreed with, that hardware one-way incontrovertible can't be modified -- can't be changed by any way, other than ripping it out and putting in some new hardware.

We would accept that, okay, as a satisfactory means of getting stuff outside the plant.

The third way obviously, we're not -- I personally wouldn't be particularly happy with, although that would be one of the options, but one of the things that has been my major -- one of my major concerns, this is not -- plant is not an

information technology system.

You can't just be constantly changing cyber-security protection software down in the plant, while the plant is operating. I mean, you just can't go put patches in, every other day.

It's not like sitting at home, "Oh, ding, your software has been updated. Restart to fix it again," or to make it viable in operation. It just doesn't work that way.

I mean, you've got a two-year refueling cycle, when you have an opportunity to go in and make changes, and patches, and the way these smart people that are hacking stuff are operating, they're changing stuff on a daily basis.

I mean, every day I come in, my software has been updated, every day, and so, it -- this thought process, you are the regulator in charge of protecting these plants, and making sure they're satisfactory.

So, I am just giving you a thought process here that there is an opportunity to make sure this comes out right.

MR. BERGMAN: We certainly understand that perspective and like I say, it's one of --

we got the full spectrum of perspectives, a healthy and diverse range of views within the --

CHAIRMAN BROWN: I didn't say they were all healthy.

MEMBER ARMIJO: Yes, I don't agree with the healthy part.

If you just designed a new instrumentation and control system for a nuclear power plant, and you recognize that it already has existing vulnerabilities to cyber-attack, hackers, why wouldn't you just fix it? Why do you just -- you know, why would you even design a system like that?

MR. BERGMAN: I think --

MEMBER ARMIJO: Sure, you can design a system that everybody agreed was great, and then in time, a new vulnerability was discovered, you know, that is fair.

CHAIRMAN BROWN: Probably take it to --

MEMBER ARMIJO: But you know, if it's just software based, it is maybe seconds later, I don't know.

So, just the problem is, are these

systems really fundamentally being -- these problems being addressed at the right point in the architecture, as Charlie has pointed out many times, of the design, and there is very --

MR. BERGMAN: And that will be the process we go through to develop --

MEMBER ARMIJO: This is very, very troubling, that --

MR. BERGMAN: Right, that is the rule-making process. We'll go through that, as we finalize -- I shouldn't say finalize. It hasn't gone out for proposed yet. Before it goes out for proposed rule-making.

CHAIRMAN BROWN: Well, the --

MR. BERGMAN: That is part of the debate that is ongoing.

CHAIRMAN BROWN: Well, 603-2009 change is a primary opportunity short-term --

MR. BERGMAN: Yes.

CHAIRMAN BROWN: -- to get it right and make it right and keep it right, and it really -- and then it obviates something.

You can do whatever you want to with the five-year rule, but this certainly takes the

issue kind of off the table, for the most part, if you get it right, and it's very easy.

If 2009 version has the same words as 1991, you can just say, "We accept this, however," bang, put that in the rule, and that makes it easy. It's done.

MR. BERGMAN: It's never easy.

CHAIRMAN BROWN: And it is --

MR. BERGMAN: Rule-making is never easy.

CHAIRMAN BROWN: Well, that is the --

MR. BERGMAN: It's a fickle beast.

CHAIRMAN BROWN: Anyway, all right, Sam, do you have any other comments?

MEMBER ARMIJO: No, I think we're just feeling disagreement, that's all.

MEMBER BLEY: No, I'd just note that the things we've been urging are a little bit akin to the evolution of designs towards something that hopes to be inherently safe, and we're looking for something that is inherently resistant, and it's hard to see that happening in software.

CHAIRMAN BROWN: I want to amplify that a little bit, since I don't know when to stop

talking.

When going from analog systems to the digital computer based systems, we've gone from individual electrically driven, you got four temperature instruments, you got four temperature instruments. You got four pressure detectors, you've got four pressure detectors.

You got four neutron high range. You've got so many source range. You've got so many whatever, flow, individual pieces all lumping and making their own particular two out of this, two out of that, two out of whatever, and you can't -- nobody can touch those. The only access is to go down to the cabinet and start tweaking potentiometers.

But with the digital computer approach, they've -- that -- those 20 instruments have now been integrated into four trains.

You've got all kinds of instruments -- sensors feeding one train, and another diverse set -- not diverse. Another similar set, equal set, feeding the next, and on down the line.

So, we've increased the integration. We've made it -- if we've increased the

connectivity vastly with the networks and everything else that are going on, still the problem of maintaining independence and making these designs inherently safe has been compounded exponentially, by going that direction.

And if anything is proved that you need to pay attention to this now, it's just watching what is going on, I mean, even with the latest pilfering of our defense infrastructure and half the secrets of our defense contractors being pumped over to China.

MR. BERGMAN: And I think you've seen that in our reviews of the more complex designs we've had.

They're very difficult to -- for the applicants to show they meet the regulations and are acceptable, and for our staff to find them, right. Those are very lengthy reviews, largely driven by that connectivity and inter-dependence.

CHAIRMAN BROWN: Okay, well, we should probably get on with the rest of this.

MR. BERGMAN: Rest of this. We're going to make it up right now.

CHAIRMAN BROWN: That's all right,

this was a useful discussion. I do appreciate -- Tom, I appreciate you coming down and taking the time to go through the status and the update, with what you're all doing and where you're going, because it gave us an opportunity for this interchange.

By the way, Bill, I didn't ask you if you had any comments.

MEMBER SHACK: You guys covered it pretty well.

CHAIRMAN BROWN: Anything else?

MEMBER BLEY: Yes, if you're leaving, I would like to say the idea that across NRC's divisions, you're looking at this as a whole group, is very good, and we're pleased to see that.

CHAIRMAN BROWN: No, I agree with that, also. Thank you very much.

MR. BERGMAN: Thank you.

CHAIRMAN BROWN: I didn't know that you intended to stay or not, and enjoy this.

MR. BERGMAN: Until this Panel exits, you know.

CHAIRMAN BROWN: Okay, all right, you all can proceed on your process.

MR. BERGMAN: Yes, thank you, Charlie.

MR. ERLANGER: Good afternoon, everyone. My name is Craig Erlanger. I'm the Chief of the Cyber-Security and Integrated Response Branch.

As Christiana mentioned, I'm joined by Ron Albert, who is the Branch Chief, responsible for the Oversight Branch, and that's the Reactor Security Oversight Branch. Next slide, please.

What we would like to do for the next couple of minutes is orient you to our organization.

I think historically, we've done a hot start with these meetings, assuming that you understand how NSIR is organized and who is who in the organization.

We recognize that we don't interact with you as frequently as the other offices, so, we thought it would be helpful, just to spend a few minutes on the front end.

We are very sensitive to our use of acronyms today. So, we will do our best not to use them, but what we try to do is highlight a few in here that you'll probably hear throughout the

day, in the hopes of just heading that dialogue off.

A little bit about the agenda today. What I will mention is the order has been slightly modified, due to the open and closed sessions today.

I'll be followed by Mr. Perry Pederson and Mr. Tim Mossman, who will give an overview of the cyber-security program.

Again, part of our thought process on that is, there is some new faces out here who weren't here the last time we met, and we thought it would be helpful to spend a little bit of time, to explain the existing requirements and what Part 73 is all about, specifically, Part 73.54 of the cyber-regulation.

The topics you see up there, we are definitively going to give you some insights into the oversight program, talk a little bit to extend -- to expand upon the previous comment about our inter-office coordination and how we've been taking some of the ACRS feedback and translated it to action and improvements we've made in that area. Next slide, please.

We came up with three desired outcomes, and hopefully, they're in line with what your expectations are for the day.

We, first and foremost, want to give you an overview of the program and explain how it's being implemented today.

Since we started interacting with ACRS on this topic, and it was for the endorsement of Regulatory Guide 5.71, we are actually out there today, inspecting interim milestones.

So, we can share with you, some insights on how that is going and where the program is today and where it's headed.

We obviously want to improve our communication and coordination with ACRS, and we think this meeting is a good step to do that, and we'll continue the dialogue.

Throughout the day, I'm sure we're going to identify some areas of interest for future interaction, and we should take note of that, and when we wrap up the day, just agree and understand what you want to hear a bit more about. Next slide, please.

A little bit about NSIR. NSIR,

probably similar to the many organizations in the Federal Government, was formed post-9/11 to react to some of the threats out there, and just the environment that the United States was in at the time.

You know, our mission is to prevent nuclear security incidents and prepare for and respond to safety and security events.

The regulations you'll find in Part 73 are all predicated on preventing a malicious actor from doing bad things, where in historically, you've dealt more with Part 50 and Part 52, which were based on safety and reliability.

Those two intersect at various points throughout the regulatory framework, and we'll hope to amplify and explain that a bit more, as we go through today.

We have three technical divisions, and this is where you'll start hearing some acronyms throughout the day.

Division of Security Policy, in a general sense, we handle everything from rule-making to licensing, in that division.

The Division of Security Operations,

that is your oversight, inspection, your contemporary issues, as well as our intelligence function, as it relates to cyber.

The Division of Preparedness and Response, they deal with not only EP issues, but they also deal with the manning of the Operation Center.

As many of you are aware, the NRC has a 24 by 7 Operations Center. There is some connectivity and relationship due -- related to cyber-security and reporting, which will grow over the coming years, and they have a piece of that, as well.

We have, similar to most organizations with the NRC, a PMDA type function, but these are the three technical divisions that we have in our organization today.

Very quickly, this is the -- the current organization as it stands today, within the Division of Security Policy, there is two branches, the branch that I represent, the Cyber-Security and Integrated Response Branch. The painful acronym you'll hear is CSIRB, throughout the day.

We focus on rule-making, guidance,

licensing. A topic called the cyber-security roadmap, which you'll hear about in a later presentation, this is a -- tracked on something called SECY-12-0088.

It recognizes the existing regulatory framework for operating reactors and new reactors, but also discusses the path forward for fuel cycle facilities, non-power reactors ISFSI's and byproduct material licensees.

So, we'll give you some insights on larger agency programs, as they relate to cyber-security and where we think the agency is headed.

You'll see this statement, inter-governmental and international coordination throughout these next couple of slides.

Both divisions, Division of Security Policy, Security Operations and I'll even say Division of Preparedness Response, have inter-governmental and international ties, due to what their focus areas are.

So, we all interact in the inter-government. There is no one clear -- or there is no one point of contact to work with one

agency.

The best example would be Department of Homeland Security, and my folks focus on policy issues, where the Oversight Branch would focus on getting advisories from organizations like US and ICS-CERT, those type of things.

So, we have a -- basically, we're a matrix organization, is the thought I would leave you with.

Fuel Cycle and Transportation Security Branch, we will go into greater detail on this topic later today, and what they support, and this is the cyber-security roadmap and activities related to cyber-security and fuel cycle facilities.

They are supported to a great extent, by NMSS, so, we matrix with another organization, as well as two branches within the Division of Security Policy.

We'll be able to give you an update of where those activities are in a general sense. We've gone out there. We've looked and we're preparing some recommendations on a path forward, and am going to present that to Commission in the short-term, but we'll get into some details about

that in a bit today. Next slide, please, Chris.

For the Division of Security Operations, as the title alludes to, they're dealing with operational real -- things that are happening today.

So, they're dealing with -- dealing with the threat picture, as well as overseeing the inspection programs.

They also deal with something called the Cyber-Assessment Team. We'll speak in detail about this later today, and how the NRC deals with real threats, when we're made aware of a piece of malware out there, how do we get that information out to our licensees? How do we share information across the board?

So, they'll give you some insights on how we do that in a real sense today.

As I previously mentioned, they also deal with inter-government and international coordination. They also serve as our liaison to the Regions, and work with them on a daily basis.

The Intelligence Liaison Threat Assessment Branch, ILTAB, just as it says, they focus on cyber-security threat analysis and

inter-governmental and international coordination. They are our liaison to the intelligence community.

We actually -- and you'll hear from Perry Pederson shortly. He has just accepted a position in that branch, where he is a cyber-security intelligence analyst over there.

This is the first time we've had that position at the agency. So, we're growing the program in that area, as well. Next slide, please.

A little bit about staff experience, and this is a, I guess --

CHAIRMAN BROWN: Wait a minute.

MR. ERLANGER: Sure, Charlie.

CHAIRMAN BROWN: Let me ask you one thing. Can you back up, just a second?

MR. ERLANGER: Absolutely.

CHAIRMAN BROWN: On the -- when you're talking about the Security Oversight Branch, and you talked about -- your set up, to be able to at least monitor what the threat picture is in general, in the country, or around -- or from whom, or is this via commercial threats, as opposed to those that are identified in other areas, and then you

pass those on?

Is there something that the licensee -- I mean, this is his stuff, once he's got the plants up and running.

MEMBER BLEY: By the way, if we ask anything that ought to be put off to the close session, let us --

CHAIRMAN BROWN: Yes, thank you.

MEMBER BLEY: You have to remind us.

MR. ERLANGER: Absolutely.

CHAIRMAN BROWN: Yes, I don't think I'm going to get into that, but my point being is that -- not specifics, but where is the division? Where does this licensee responsibility begin?

I mean, it would seem to me, once they've taken over and they're operating, then are they expected to have a staff that is constantly -- separate the plant --

MR. ERLANGER: Sure.

CHAIRMAN BROWN: -- that interface that I talked about, you know, that thing that talks out to the business network. They've got to take care of the rest of their site.

They obviously don't want all their IT

systems going belly-up, while they're, you know, trying to run this plant, for a lot of different reasons.

So, that is one set of threats. Then there is another set of threats that you wouldn't expect, if you design the thing correctly, to ever get into the plant type systems.

So, do you expect them to have an organization that is primarily responsible for making sure their systems are safe and secure, or it's not totally your responsibility?

MR. ERLANGER: I think I can answer that in this setting, but I will tell you, the level of detail we can provide in the closed setting will give you --

CHAIRMAN BROWN: Okay.

MR. ERLANGER: -- a bit more. Licensees do have organizations that monitor the threat environment. They have access to information provided by the Department of Homeland Security.

There is the industrial control systems cyber-emergency response team and the U.S. computer emergency response team, passed the advisories.

There is a hard-token method that they can get that information from.

Part of the requirements we've built into the cyber-plan is, the licensee needs to be able to be aware and monitor the threat environment.

That being said, we do have a responsibility, that once we learn this information, we have to get it out there in a timely manner.

A part of the -- I guess, what I'll call the landscape today is, there is a proposed rule-making related to reportability, Appendix G to Part 73. It's out there, and that will have a cyber component that will help codify the reporting requirements.

It's already been out for public comment. It's not, as I think Tom alluded to, something that we're starting fresh, that we have to go through a whole rule-making process.

What we did in the interim is, we put a security advisory. It's marked OUO Security Related Information, related to reportability and the type of information we would want to hear from licensees, if they find out something is going on

in their facilities.

But to answer your question, it's a joint shared responsibility, and when we learn something, we want to get it out as soon as possible, but there is also a responsibility of the licensees, to monitor the threat-scape and understand what is going on out there.

DHS plays a pivotal role in that function of sharing information.

MR. WESTREICH: Craig?

MR. ERLANGER: And we will talk about it in -- actually, the mechanics of it, in the closed session this afternoon.

CHAIRMAN BROWN: Okay.

MR. WESTREICH: Craig, just to respond.

There is some information -- there is plenty of information that licensees aren't able to get, classified Government information that we --

So, this Intelligence Liaison Threat Assessment Branch is the liaison to provide -- get that information from the Government intelligence community, then we package it in a way that we can

provide to the licensee community, so they can take action.

But in some cases, we're the only connection they are going to have to that information.

CHAIRMAN BROWN: Okay, I can understand it at some levels.

MR. ERLANGER: Does that satisfy for the --

CHAIRMAN BROWN: Yes, I mean, one of the driving reasons for my question was, when you get into the switch yard, and I'm not talking about balance of plant, but out in the switch yard, all of the switch yard breakers and everything else are not totally under control of the local operators, in terms of how they connect to the grid.

Those are, in many circumstances, maybe all now, I don't know, are reportedly subject to this state of type supervisory control and what is it, data acquisition, where the remote grid operator can control those breakers and open -- so, if somebody hacked in, you're subject to a complete -- a loop -- a loss of offsite power, if they trip everything off, and now, you're into a

comp.

So, that is -- you don't have to say anything more. That is the reason I asked the question about, I presume the licensee doesn't have any control over that part of it, but yet, their plant has to be inherently safe, with respect to it.

Now, we have requirements for that, but it is -- it just seems to me, it's -- you're much more set up to end up in a circumstance where somebody can do some damage -- damage, that is the wrong word. Some -- create a problem in the plant, that you have to deal with, without -- totally outside your control.

MR. ERLANGER: Yes.

CHAIRMAN BROWN: And that was one of the reasons I was asking a little bit about their organizational capabilities.

MR. ERLANGER: In another presentation, that I think will add a little bit to this conversation is, our -- when Tim Harris gets up here and speaks about our inter-governmental relationships, our relationship with the Federal Energy Regulatory

Commission and the North American Electric Reliability Corporation for Grid Issues, we can kind of step through what -- where that relationship is, and I think that will answer some of --

CHAIRMAN BROWN: All right.

MR. ERLANGER: Some of your questions.

CHAIRMAN BROWN: Thank you.

MEMBER BLEY: Yes, and we'll be looking forward to hearing how that is formalized, how that works.

MR. ERLANGER: Absolutely. A little bit -- this is very briefly on staff experience.

Cyber-security touches so many aspects of plant life, as you're well aware, from the safety side to the maintenance side, to the operations side.

What we've recognized over the last couple of years is, it takes a village type mentality to get this done.

We have so many disciplines that support this program. You look at it, you look at a little bit about backgrounds.

The staff has -- they have worked in every office, virtually every major office in the

agency. They come from private sector companies. Strong backgrounds in digital I&C and industrial control systems, electrical information -- electrical engineering and information technology.

There is no one cyber-security specialist who can do it all.

So, I think one thought we're trying to convey today is, and you'll hear more about it in our inter-office framework, we fully recognize and appreciate it. It takes a -- it takes a group of people to get this done, and this program really touches virtually every aspect of the plant life.

MEMBER BLEY: You didn't mention operations. Do you have former operators?

MR. ERLANGER: I'm sorry, I thought -- yes, we have people who have operational experience, whether they're exactly SRO's, I can't speak to that. I know organic to my branch, I do not have a former SRO in my branch, working on this today.

But you have Senior Resident Inspectors, you have people who are employed by utilities, out there working in digital I&C shops, but whether they're actual operators, I can't

answer that right now, sir.

MEMBER BLEY: Okay.

MR. ERLANGER: Okay, next slide, please. That concludes my portion.

Up next is -- and thank you for allowing me to get through that pretty quickly.

Perry Pederson is going to come up with Tim Mossman, and we're going to begin our technical presentation, if that is -- if there is no further questions.

MR. HECHT: This is Myron Hecht, calling from Los Angeles. I am just wondering if I could ask a question, with regard to ICS-CERT?

MR. ERLANGER: Absolutely.

MR. HECHT: The ICS-CERT has a number of advisories. Among them, the ones I find the most interesting are the ICS vendors or others reporting on the vulnerabilities that they find in their control systems, and in some cases, these vulnerabilities can't be solved by a simple patch.

Leading to this in the previous presentation on -- or discussion on the three conceptual approaches, how is it that major vulnerability in the ICS, not necessary an alert

due to a virus or something like that, but a major vulnerability in a I&C application that is installed at a plant, would be handled?

MR. ERLANGER: Myron, can I ask just a clarifying question, and I'm going to need some help from some of my oversight folks, who deal with this on a day-to-day basis.

Is your question -- to restate your question, if we learn from ICS-CERT that there is a vulnerability related to CERT and industrial control system, is your question, what do we do with that information? I'm not sure I'm following.

MR. HECHT: What is the expectation of, how shall I say it, solving that problem from the plant and from your office and the entire process, I guess?

How does the problem get fixed, from the time that the vulnerability is noted, and I'm pausing that as a major system vulnerability, and that might require re-installation of a -- you know, a major server, or a number of servers.

MR. ERLANGER: Well, I think the first step -- I can speak to it from the policy side.

We want to get that information out

there, right away. We don't maintain a catalogue of what industrial control systems are at every site.

Ralph, are you walking up this way? Mr. Ralph Costello, from the Division of Security Operations, who works with the Cyber-Assessment Team, is going to add some remarks.

But we would get the information out there, and I'll just let Ralph.

MR. COSTELLO: Yes, sir, I think that is a very good question.

Obviously, each industrial control system is different. Each potential vulnerability is different.

To give you a blanket answer, would probably not be answering appropriately, but let me give you an example.

If say, there is an industrial control system design, I won't mention any names, that has an apparent vulnerability and the licensee hears about it through ICS-CERT, obviously, they have multiple ways to secure an incident.

In many cases, in ICS systems, the vendors haven't done a lot of security

implementations, but some are doing it.

With that being said, there is ways in which they can prevent the spread, and this is a simple answer, first, the elimination of the pathway, and then screening for, obviously, the virus definitions, if they exist.

Also, there is an anomalous detection, which should be going on in your ICS system, up front. Does that answer your question?

MR. HECHT: In part. That is basically saying now, you've gotten an alert. The immediate response is basically, do what you can to mitigate the problem.

But I guess my question is, you have to do a re-install or a major upgrade. What happens next?

MR. COSTELLO: Well, without going into a specific scenario, it would be hard to know what they would do.

It may be a simple fix. Then again, it may be a more complicated fix, like you just mentioned.

I can tell you, the Department of Homeland Security is working closely, not only with

our industry, but with vendors also, and in this open setting, I can't go into more detail, but I'd like to in the closed setting, if I am permitted.

MR. ERLANGER: Myron, maybe -- you know, any digital asset that is brought into the environment has to go through a whole -- a very robust process.

This would be no different from the sense that if there is a problem with a particular system, if it's within scope of the cyber-security rule, i.e., it performs a safety/security emergency preparedness function, there would be a deliberate process to re-introduce it into the environment.

How to do that is spelled out in detail in the Regulatory Guide, but that would be, the licensee would follow a process, to make sure it's okay, before it's up and running again.

We can talk -- I mean, as Ralph said, probably if -- I don't know if we answered your question.

CHAIRMAN BROWN: Yes, Myron, we're going to go on, on this.

I don't want to get -- I understand -- I think I kind of understand your question, from

the standpoint of, if a vendor makes a PL -- a programmable logic control, for instance, and there is -- it's installed in some industrial control systems, and they identify a vulnerability with it, and we've got it installed in say, all the circuit breakers, control circuits at one of the plants, we obviously have some vulnerability, under those circumstances. The plant has a vulnerability.

So, how is that dealt with? Is that an example of what you're talking about?

MR. HECHT: Yes.

CHAIRMAN BROWN: Okay, so, I guess the question was, well, how do you deal with that, and I'm not sure you can be as specific, other than to say, somebody has to figure out what to do, once they know what the vulnerability is.

MR. HECHT: Well, I guess the point is that we should be considering not only the -- solving the problem of the vulnerability, but also, the additional impact on safety, and how do we do that?

CHAIRMAN BROWN: I think you have to think about that at the time, once you know what

it is.

MR. HECHT: Right.

CHAIRMAN BROWN: All right, we've got that on the record. Let's go ahead and proceed on, okay, Myron?

MR. HECHT: Okay, thanks.

CHAIRMAN BROWN: Thank you.

MR. ERLANGER: We're going to do a quick transition, sir.

CHAIRMAN BROWN: Okay, that's fine. Thank you.

MR. PEDERSON: Good afternoon. As Craig said, my name is Perry Pederson, and although I have a background in IT and general technology research and development, for many years, I've been focusing in the last 10 years on industrial control system security.

I first got started in this, working for DoD. I was a PM for Infrastructure Protection at the Combating Terrorism Technology Support Office.

I transitioned from that to the Director of Control System Security at Department of Homeland Security.

Just over four years ago, I joined the NRC and was fortunate enough to be part of the team developing the Regulatory Guide 5.71, and I also led the team that did the review and approval of all the cyber-security plans for the operating plants and the new reactor applicants that we had at that time.

I'm currently the Senior Cyber-Threat Analyst within NSIR, and today, I am going to do my best to represent the collective effort of a lot of folks in this room, but I welcome them to stand up and point out any mis-statements or mis-characterizations I might make. Next slide.

I'd like to provide you with a high-level view of NRC's current approach to cyber-security, by covering these topics.

I'm going to touch on some terms that are used repeatedly. I'm going to talk about the cyber-threat landscape, give you a view of the historical time line, touch on coordination efforts, look at the regulatory framework itself. That is the regulation, the guidance, licensing and oversight, and then look at it in terms of a cyber-security life cycle, followed up with some

Q&A at the end. Next slide.

I'm sharing some of these terms with you because I think it's important, because these terms are used in the cyber-security plans by each of the licensees, and then when they are reviewed and approved by the NRC, they then become part of the licensing basis, and then that drives the oversight and inspection process.

So, it's important to understand that we all have a common understanding of what this means, so when a licensee commits to do something, and then they go do that, and we show up to inspect it, there is a common understanding of what we're looking for. Next slide.

I would like to spend a little time on the cyber-threat landscape. I think anyone who reads the newspaper and watches television these days, understands that it's changing and it's getting a lot more serious.

I would have to say that what you see on television and read in the paper is fairly accurate. It may not be the complete picture, with all of the details, but it does give you a real sense of the dynamic nature of this threat that

we're facing.

However, some things have not changed.

For example, the first computer virus I ever saw was on a 5 1/4 inch floppy disk, and 30 years ago, it would have been easy to simply ban the use of all floppy disks.

Now, we can see the fallacy of that kind of an approach, that kind of prescriptive approach to dealing with the issue.

Therefore, the NRC staff has concluded that this performance based regulatory framework that I'm sharing with you today, is superior to a highly prescriptive approach. Next slide.

One take-away from this slide is that cyber-security is really not new for the NRC.

We started to pay attention to this back in the 1900's. None the less, security, including cyber-security, moved up several notches in everybody's mind, after 9/11.

I won't go through every milestone on this chart, but if you'd like information on any one of them, certainly, we can provide additional details.

But in summary, key points are the cyber-rule was introduced or issued in 2009. The Regulatory Guide 5.71 was published in 2010, and subsequent to that, all operating plant cyber-security plans were reviewed and approved in 2011, and inspections began this year. Next slide.

The main point of this slide is that regardless of the perspective, be it intra-agency, inter-agency, international or industry, coordination on cyber-security has taken place on multiple levels and continues today, as you would expect.

Multiple NRC offices work together on various aspects of this framework, and Tim Mossman to my left, will provide some additional information on the inter-agency coordination and the latest on the inter-office instruction.

Furthermore, Tim Harris will provide you with some details on NRC's efforts in the inter-agency realm. This would include DHS, and as mentioned previously, FERC and NERC, as well as international fronts.

As for the last bullet on this slide,

I think you're well aware of the transparent and open process that the NRC is known for and has -- and the public has provided valuable input to this process.

For example, based on some recent research that I was doing on this topic, I learned that it was public input, was not the driving factor, but it was a factor for including cyber in the design basis threat.

So, I think it's important to note that all the brains, when it comes to cyber-security, don't sit at the NRC, and we recognize that and we accept input from many stakeholders. Next slide.

So, just as a way to depict the regulatory framework, you know, it seems obvious that every element in this framework is necessary, and each one informs the other three.

Although the NRC process is tried and true, and the staff leveraged the experience from other major program implementations, cyber is different.

The NRC is breaking some new ground here, and there is no doubt that lessons will be

learned and the next iteration of this cyber-security framework will be an improvement. Next slide.

Ten CFR 73.54, you already know about the rule, but just to hit a couple of highlights.

Licensees are required to provide high assurance against a cyber-attack.

On numerous occasions, I've been asked to define, well, just what does that mean? High assurance? My answer is always the same, Regulatory Guide 5.71.

In other words, if you follow the guidance in 5.71, by definition, that will provide high assurance. Next slide.

I'd like to explain a little bit about how this came about and the pedigree behind it, and there was a tremendous amount of work, as I'm sure you're aware of, done by NIST in this arena.

So, there wasn't a need for us to reinvent the wheel, and as outlined in the NIST guidance, they recommend that you take their set of security controls, their security program and you tailor it for you industry and for your specific application, and that is exactly what we did in

this case.

Therefore, with Special Publication 853, as the base set of security controls, with input from many contributors, the staff created the guidance for implementing a cyber-security program for nuclear power plants. Next slide.

Now, I'd like to get into a little bit of the details of Reg Guide 5.71, and just step you through this process.

I'm not going to touch every detail, but one of the first things you need to do is recognize, as Craig had mentioned earlier, is that this really takes a multi-disciplinary cross-functional team, to really do this right.

You need the IC engineers. You need the nuclear engineers. You need the IT folks at the table. You need a lot of folks involved in this process.

So, after you form a team, then you go through identifying what is a critical digital asset.

Once a CDA has been identified, regardless of whether its function is safety, important to safety, security, emergency

preparedness or a system that supports those functions, there is the same three-step process that is required.

But just imagine a large funnel. Everything in the plant really is considered, and only those systems that are tagged as a critical digital asset come out the bottom of this funnel, and those are the ones -- those are the systems that we apply security controls to.

The defensive architecture is one thing, and we've already touched on this issue early on this afternoon. The defensive architecture is an important aspect of a defense in-depth concept.

In this slide, for example, you'll see five levels, and you might consider that levels of trust, Level 0 being the internet. In other words, zero trust.

Level 4 being typically where you would find safety systems, and that is my highest level of trust.

But a critical digital asset could sit in Level 0. It could sit in any of these levels, and it would have to be protected in the same way.

In other words, we don't employ a graded

approach and say, "Well, security systems are not as important as safety or EP systems are not as important to safety, so you don't have to do as much."

We can see a lot of these systems may reside on the same network. There may be pathways, whether it's wired, wireless or sneaker-net, that connect a lot of these systems. So, you have to protect them all equally.

If it is a critical digital asset, then you have to apply the security controls.

MEMBER ARMIJO: Could you give an example of a critical digital asset that would be at Level 0 in a nuclear plant?

MR. PEDERSON: Probably some emergency notification systems. EP is one of those cases, where an EP system could be compromised, and it may not directly lead to radiological sabotage, but none the less --

MEMBER ARMIJO: It could confuse --

MR. PEDERSON: -- it wasn't important enough -- pardon?

MEMBER ARMIJO: It could confuse people, mis-inform people --

MR. PEDERSON: Right.

MEMBER ARMIJO: -- things like that.

MR. PEDERSON: Correct.

MEMBER ARMIJO: Okay, but not actually in the control of a pump or --

MR. PEDERSON: Correct.

MEMBER ARMIJO: -- some other system?

MR. PEDERSON: Right. So, that was considered during the rule-making process, that emergency preparedness systems and notifying the NRC and the public of any potential event was as important to protect from a cyber-attack, as a safety system.

MEMBER BLEY: You're probably going to get into it in a minute, but if not, I guess I'd have a little trouble seeing how you can protect something up at Level 0, as well as you can protect something down at Level 4.

MR. PEDERSON: Well, the protection comes as a result of a couple of things.

Certainly, if you have a safety system sitting at Level 4, there is that extra measure of protection by the additional boundaries and the boundary in the flow control devices between those

boundaries.

So, you could say that a safety system has those additional measures of protection, right.

Like for example, in the diagram between Level 4 and 3, we'd certainly like to see some kind of a deterministic device there. You could call it a data diode. Certainly, I'd be happy with an air gap, but something to enforce the data flow at that point.

You get out to between Level 1 and Level 0, you need bidirectional flow, and so, you may need some additional controls, in order to address that protection of that device.

So, that would be the difference. So, it --

MEMBER BLEY: Yes, but me at least, that's a pretty substantial difference.

MR. PEDERSON: Well, it is a substantial difference, but in our Regulatory Guide, there is -- I forget the number exactly, 147 or 148 controls.

If you identify a CDA and it's in Level 0, you have to address all 148 of those controls. Doesn't matter where it resides in this

architecture.

MEMBER BLEY: Okay.

MR. PEDERSON: Next slide. Similar to the physical security plan, the cyber-security plan contains essentially, a commitment to implement a program as outlined therein.

However, the plan is reviewed. After the plan is reviewed and approved by the NRC, it becomes part of the licensing basis, and as I mentioned, drives the inspection and oversight process.

One thing I'd like to add to this first sub-bullet under the essential elements, is that while everyone would expect the inspectors to look at a list of CDA's that licensees maintain onsite, we're likewise interested in those things they considered were not CDA's.

We really need to understand their thought process, and we want to make sure that they didn't accidentally, or through a misunderstanding or mis-interpretation, identify a system to not be a CDA, when in fact, it is a CDA.

This is something, as you can imagine, would have a serious consequence. Next slide.

CHAIRMAN BROWN: Before you leave that one.

MR. PEDERSON: Sure.

CHAIRMAN BROWN: Question. Have you -- a CDA -- I'm looking at the essential elements, after the basic plan part.

Have you all been involved in evaluating a specific plant yet, relative to its defensive model? A plant? Not a -- I'm asking this in the context of your earlier slide, where you talked about the threat vectors.

I mean, if I look, and I look at, say the reactor trip system, I'm picking one in the plant, not in emergency -- not up in the Level 0 world, but down in the Level 4 world.

There are still things you have to do, if you -- because there is a communication path, and if -- I don't want to get back into how that path is executed.

But if it's not executed in a manner that is totally secure, then you have to start looking at the access -- I hate to use that word, but the control of access to the things that are accessible through that path, whatever they may

be, whether they're controls, whether they're data that is going to inhibit a trip or actuation of a safeguard system, or whatever.

MR. PEDERSON: Well, I would think Ralph Costello --

CHAIRMAN BROWN: So, my question -- let me finish.

So, my question is, if -- I was thinking about this, when I was going through your slides the other -- you know, couple of nights ago, and trying to think of circumstances, based on my own experience, when we were first in the Naval Nuclear Program, when I was first doing this kind of stuff. We put it in proto-type plants, not ships, which were kind of disconnected from everybody.

One of the things we looked at was, we made sure you couldn't -- you didn't just connect up a laptop to something. You didn't do business that way, or you did not have a US -- a thumb-drive port, or there were certain -- you just didn't build those in. There was no way.

The only way you could change the software would be to pull out the card, take off a programmable read-only memory, put a brand new

one in. That is really hard to have.

Doesn't mean it can't be compromised at a vendor's place, as Stuxnet has illustrated, when you build stuff into a design somewhere that gets in, although that one got in via thumb-drive, I guess, or something like that. That is the hypothesis.

But you could postulate somebody doing that maliciously from some other source when it was brought in. But that is hard.

So, I was looking for again, a strategy -- well, I keyed on your words 'protected strategy'. I mean, you have to look at the assets, and you start having to look at, well, what are the touch points? What are the controls of access?

I remember one of the designs we were looking at, where there is a maintenance computer.

So, whenever they update software or anything else, it is done through that, I think -- this is my memory again, old memory, so, it might not be working right all the time, but it goes through the maintenance computer set up, to go into each of the individual trains.

So, that is why I was asking you if

you've actually done this, for a particular installation, and then walked through the strategy of how you were going to -- how you were going to do that?

Maybe that is a 'yes' or 'no' answer. I don't know.

MR. PEDERSON: I think the answer is, we have an answer.

CHAIRMAN BROWN: I'm sure.

MR. PEDERSON: And well, Ralph Costello, and perhaps in more detail later during the closed session --

CHAIRMAN BROWN: Okay, in closed session, fine.

MR. PEDERSON: -- we could get into some of those details.

CHAIRMAN BROWN: That's fine.

MR. PEDERSON: But he may be able to speak to it now, to some degree.

CHAIRMAN BROWN: We'll wait, we'll do it at the other time. There's no sense in doing this twice.

MR. WESTREICH: Well, I'm Barry Westreich, Deputy Director in DSP.

We are, in fact, doing that for types of systems that we're inspecting against.

So, licensees have identified their critical digital assets, and then in this current version, in these interim steps for what we call target set equipment, the most sensitive equipment, they have implemented controls for each one of those target sets to use, and we look at the controls and we look at all the vectors associated with those CDA's, to determine, have they considered all the vectors that are associated with that system? Is it vulnerable to, you know, portable media?

Are there -- is it in the right level in the architecture? You know, we talked about the Level 4. Are they in Level 4 as they're supposed to be? Have they placed the data diode in place?

So, we do look at that specifically, related to the systems on a sampling basis, that we address during these inspection activities.

But we're in this interim implementation phase. So, it's not the breadth of the plant now, it's associated with what we're calling target sets.

CHAIRMAN BROWN: These are existing -- these are operating plants, right?

MR. WESTREICH: These are operating plants.

CHAIRMAN BROWN: Not the -- one of the points of my -- one of the -- the thrust of my comment is that on a go-forward basis in new plant designs in -- you can certainly simplify the vulnerability problem by -- I love to use, not allowing certain assets to have access via certain means.

In other words, you make sure that you don't have those vulnerabilities built in, in the beginning, even though you can't theoretically dictate it, you can certainly encourage it during the design and licensing stage via the architecture, because we do have fairly complete block diagram, functional diagrams of what these look like.

It's irrelevant, what the technology is. Blocks are blocks.

MR. WESTREICH: Right.

CHAIRMAN BROWN: So, anyway, that is just a thought process. We'll wait until the closed session, to hear the --

MR. PEDERSON: Yes, and it's a perfect segue to the next slide.

CHAIRMAN BROWN: Okay, thank you. You're doing a good job of catching up, after our half-hour digression, by the way.

MR. PEDERSON: No problem. So, recognizing that full implementation is down the road for some sites, we prioritize some of those activities and developed these interim milestones.

These interim milestones focused on, as you were just mentioning, some of these key threat vectors, with an emphasis, as Barry was also just mentioning, target set equipment, where these were identified and licensees committed to complete all of these interim milestones by December 31, 2012, and that is also what Ralph and his team are inspecting, and have begun to inspect this year.

So, for example, Milestone 3 is installing a deterministic one-way device between Levels 3 and 4, or between 4 and 3.

Another example -- and that would essentially isolate those most critical systems in Level 4.

Milestone 4, another example,

implementation of security controls related to portable and mobile devices, recognizing one of the threats that we all learned recently, otherwise known as Stuxnet, is a really good example and very illustrative of just what an air gap buys you.

It's not your sole savor. It has to be part of an entire programmatic approach.

In that, you know, just to point out, I think it's worthwhile pointing out, I've had this discussion, that it really doesn't matter how much malware is loaded on a USB stick, if you don't let it in the door. That is a critical point.

Then there is Milestone 6, for example, application of security controls to target sets.

So, for those particular CDA's that are part of a target set, then all 148 controls have to be addressed.

So, we're trying to make sure that right up front, the most cyber-sensitive systems are identified, isolated and protected, and that is, in a nutshell, the essence of these interim Milestones 1 through 7.

CHAIRMAN BROWN: One of the -- just a comment on your thought, relative to, if you don't

ever let the USB in the door.

That is a different -- that is a different -- that is an administrative control type thing.

MR. PEDERSON: Right.

CHAIRMAN BROWN: Okay, and it's considerably simpler to apply that administrative control and checks to prevent that, than it is to protect yourself from somebody who has -- can hack through your network, through a communications network, where it feeds both the control room and the plant.

I am beating this horse. It's not a dead horse. It's a very live horse, in case you hadn't noticed, because that is an interactive set of threats that is constantly bearing.

The other one is one that you can look at and take care of, and control with a different level of controls.

I mean, the purpose of the discussion is to see that -- or at least to provide thought process, that keep that thought in mind, when we are doing these -- the thought process, well, like you say, your diode, your data diode from 4 to 3

and from 3 to 2. Those are the two levels that we have, supposedly one-way communications, and we don't want to be able to be compromised.

But it -- because it goes to the point I made earlier, that you just can't be in the mode of constantly trying to patch, and you don't want cyber-software on any of your applications, safety safeguards. You just don't want it in there. It's just -- it's a threat to actually having it perform its function.

And so, you want to have all that stuff off somewhere else, and you don't want to have to fool with it.

So, anyway, I've just --

MR. PEDERSON: Yes.

CHAIRMAN BROWN: It was -- I liked -- I appreciated your thoughts, your comments on what these milestones were and what they did. That provided some illumination of what your thoughts were and --

MR. PEDERSON: Yes, it's a very good point, that vulnerabilities are everywhere. There is no system without them.

CHAIRMAN BROWN: And you need --

MR. PEDERSON: If anyone claims such, then I'd be immediately suspect.

CHAIRMAN BROWN: Absolutely. Air gaps are nice, but they're not the sole thing.

MR. PEDERSON: And so, the vulnerability is a necessary condition. The threat might be considered the root cause.

And so, if you have a vulnerability, you have to be able to separate it from that root cause, so, that you can continue to operate with that known vulnerability, and there are different ways to address that.

CHAIRMAN BROWN: Yes.

MR. PEDERSON: Rule sets, air gaps, additional administrative controls.

So, there are things you can do to mitigate vulnerability, known vulnerabilities, and there is a lot of things that you do, just in your architecture, to try to mitigate the things that you don't know about, that may emerge.

CHAIRMAN BROWN: See, I like the way you said 'architecture', because if you don't do that during the design stage, and you try to do it a year before fuel load, it's --

MR. PEDERSON: Kind of late.

CHAIRMAN BROWN: -- kind of late in the game, to do anything.

MR. PEDERSON: Yes.

CHAIRMAN BROWN: That is where the NRC is, and I think it's very, very important, up front, to make sure you have that control of it and you don't have those vulnerabilities, and limit them to those that you can deal more easily.

So, anyway, you can keep rolling here.

MR. PEDERSON: So, then Milestone 8 is simply the full implementation of the entire program. Next slide, please.

This diagram provides you just a snapshot of how that milestone will be phased in for different sites, over the next few years.

Note that the 'y' axis for the sites, and sometimes there are multiple reactors on a site. Next slide.

The one thing to kind of wrap this up, and this is my last slide, you know, I wanted to leave you with the notion that although you may not look into the Reg Guide and see a section that is titled 'Cyber-Security Life Cycle', if you read

the details and you read through the security controls, you'll see this life cycle emerge from there, that we really address every phase in a nominal life cycle of these digital systems, these critical digital assets.

New reactor licensees, of course, are required to have the full program up and implemented and verified prior to fuel arriving onsite.

The operating reactors are allowed to phase the program in over time, as I was just discussing. So, they'll touch each one of these phases, as they go through implementing their full program.

But eventually, when they get the full program implemented and let's say, a site that has primarily analog safety systems, and they want to do an upgrade, they're going to be working their way through this entire process.

There is a lot of analysis that has to be done, even touch points on the supply chain.

So, there are controls in the Reg Guide that address supply chain. I'm not suggesting we have the perfect solution for the supply chain, but it is there. We recognize it, and licensees

are committed to doing their best to fill those requirements.

MEMBER BLEY: Perry, before you close, couple more general questions.

Few years ago, we had ISG in this area. Now, we have Reg Guide 5.71. We have inspection guidelines that look like they've picked up what was in the IG's.

Do we have something similar in SRP space yet? Is there guidance for reviewers? I don't know if you're the right guy to ask about this.

MR. ERLANGER: Perry, I can --

MEMBER BLEY: Yes, yes.

MR. PEDERSON: Yes, go ahead.

MR. ERLANGER: Yes, sir, there is an SRP Chapter. It is --

MEMBER BLEY: And it's brought up to date now?

MR. ERLANGER: Up to date, and it reflects Reg Guide 5.71.

MEMBER BLEY: Okay.

MR. ERLANGER: Similar to the framework.

All these lessons learned we have -- when we update the Regulatory Guide and the framework, we'll update the SRP at that time. But we do have one related to 5.71 today.

MEMBER BLEY: Okay, and then I had another question, because I've seen something similar in the fire risk assessment area lately.

You have, in the inspection guide, and I don't know if we talk about this here or somewhere else, some things you call FAQ's, and the fire folks have FAQ's.

Theirs are to further define the methodology they've been working on.

Yours, I'm curious about, you know, where they came from, why they're there, and you know, is -- are they going to stay the way they are or do they get integrated into other guidance some time in the future?

MR. ERLANGER: I think I'm the right one to answer that as well, Perry.

Yes, we have a security frequently asked question program. It's the -- the instructions can be found in a document called NEI-0510, that kind of governs the whole process.

As a point of reference, I would say the physical protection program has roughly 80 security frequently asked questions today. Cyber is up to about seven or eight at this point.

MEMBER BLEY: Right.

MR. ERLANGER: We would use those to inform and improve our guidance down the road. The purpose of the program is to provide regulatory clarity, not to provide additional guidance or requirements.

So, it's just a bit more detailed, when there is a different understanding of what the requirement means. This is used to provide clarity.

MEMBER BLEY: So, these are coming along as sort of interim agreement, because they are issued jointly by --

MR. ERLANGER: Yes, sir, there is a Panel process, where the industry signs it out, as well as an NRC representative.

I think it's probably typical of any new requirement, that questions are going to come up and there is going to be a different understanding of --

MEMBER BLEY: No, it seems reasonable. I just wanted to --

MR. ERLANGER: And this is the method through which we would work through it and find resolution.

MEMBER BLEY: At least in cyber-security, there are -- I think they are attached to the inspection guide now, so, the inspectors get to see --

MR. ERLANGER: They exist in a form. There is a database that --

MEMBER BLEY: Maybe that isn't where I saw them. I thought I saw them there.

MR. ERLANGER: But the industry gets access to them, once they're published.

MEMBER BLEY: Okay.

MR. ERLANGER: And the various --

MR. WESTREICH: Yes, they're not attached to the inspection procedures, but they are issued jointly --

MEMBER BLEY: Okay.

MR. WESTREICH: -- between us, and you know, we endorse the NEI guidance document --

MEMBER BLEY: Right.

MR. WESTREICH: -- so, they distribute those, and then the inspectors use those as part of their inspection process. They could use that clarity for what the expectation was.

MEMBER BLEY: Okay.

MR. WESTREICH: So, we have a -- currently, they're just used for each of the milestones. So, there is seven FAQ's.

MEMBER BLEY: Yes.

MR. WESTREICH: One for each milestone, because when we were doing pilot inspections, we identified a number of generic issues that we were trying to clarify before inspection activities started.

MEMBER BLEY: Okay, good, thanks.

MR. PEDERSON: Next slide. Unless there is any other questions?

CHAIRMAN BROWN: Okay, we're -- you did a great job. We picked up about 15 minutes, in addition to getting some good answers.

Tim, I'd like to try to get you and the follow-on one done, so we can just have a completed closed session.

So, I see you're all scheduled for about

15 minutes apiece, if we could go walk through both of those.

MR. MOSSMAN: All right.

CHAIRMAN BROWN: You're next, I think.

MR. MOSSMAN: Absolutely. Thank you.

CHAIRMAN BROWN: Tim, you might want to move that off the microphone, move that microphone a little bit. Yes, thank you very much.

MR. MOSSMAN: All right. Good afternoon. My name is Tim Mossman. I'm a security specialist in the Cyber-Security and Integrated Response Branch. That is Craig's branch in the Office of Nuclear Security and Incident Response.

I've been with the NRC for a total of five years, since I've -- I've been with NSIR since January.

Prior to joining NSIR, I was with actually John Thorp's branch, working instrumentation and control in the Office of Nuclear Reactor Regulation, and if I can segue for a minute.

One of the amusing things about this topic was one of the last assignments, I worked

with John was the inter-office instruction, and shortly before I left, NSIR volunteered to pick that up, and I was more than happy to send it over to NSIR, and a few months later, I got an opportunity to join NSIR, and the first assignment I got was an inter-office instruction.

CHAIRMAN BROWN: Well, the Panel was back in place.

MR. MOSSMAN: Pretty much, yes. So, prior to joining NRC, I supported development of command and control systems for missile defense applications, which don't sound a lot like instrumentation and control systems for nuclear reactors, but although they're on very vastly different scales, they have a lot of the same challenges.

We had a lot of communications. We had a lot of software dependability issues. It was, actually, it was fun, actually to work there.

My educational background. I have degrees in nuclear and reliability engineering, and so, I'm not sure exactly how I got into cyber-security, but that's where I am today.

So, today, I'll be talking about an

ongoing effort to formalize the inter-office staff activities, with respect to cyber-security.

In the very recent past, one of the things that ACRS has expressed to staff is that with the separation of cyber out of the Part 50 and Part 52 licensing process, that some aspects of the safety/cyber-security interface may not be adequately addressed.

That is something that staff is very sensitive to, and previously did commit to ACRS, to provide a more formal vehicle to define this inter-office working relationship.

Up until now, a lot of the things we had been doing had been some formal, some very informal, but we didn't have any kind of governing document or management guidance that said, "This is the way we expect to work together." Next slide.

As has been noted previously, regulation of cyber-security is still a relatively new item.

However, we have already seen the impact that cyber-security may be felt at many different points in the regulatory process.

Staff has an interest in making certain

that appropriate cyber provisions are taken throughout a digital system's life cycle, within the context of our regulatory structure.

One of the primary benefits of enhanced staff interaction on topics related to cyber-security is reduced regulatory uncertainty for licensees, basically ensuring that cyber-security issues are identified early, not letting them slide in the regulatory process, until it's expensive to fix.

Selfishly, enhanced staff interaction regarding cyber-security should also benefit staff, as it should result in a more efficient use of our resources.

Basically, we never want to get in a situation where we're ping-ponging licensees between cyber staff, licensing staff and back and forth. We do not have enough staff to do that.

Evolution of the cyber framework. As I mentioned earlier, this is something that ACRS has previously recommended to staff. Staff did commit to follow up on this recommendation.

Since that time, we've had a number of opportunities to learn from inter-office

activities, where we've collaborated on topics that relate to cyber-security.

Most notably, NSIR has been working with NRR on a pilot study, regarding the Diablo Canyon digital safety system replacement. It's an opportunity for us to view first-hand, how our cyber-security supply chain controls are being handled in the context of the procurement of the digital safety system.

NRO has also participated in that effort, as it has ramifications for new reactor procurement.

Eric Lee, who is in the audience, from our group, will provide details on the pilot study during the closed portion of the briefing.

Also, another area we've had a lot of interaction on, and Tom Bergman probably stole most of my thunder at the beginning of the meeting, and hopefully, he took most of the arrows at the beginning of the meeting too.

We've had a lot of interactions with new reactors on the safety/cyber-security interface for new reactors.

Monika Coflin, who is also with our

staff, will be providing a briefing on the current status of new reactor cyber-security.

Since the beginning of the calendar year, NSIR and the Regional Offices have been actively involved in NRC's first inspections, as we just discussed, of the interim implementation milestones, and Perry provided an overview of those.

Again, in the closed session of the briefing, Ralph Costello will talk about the oversight program and our experiences in the last four or five months on that.

So, although there is still much to learn, staff has had the benefit of learning from various inter-office interactions on cyber-security.

Okay, in developing the cyber-security framework, we've had participation from not only our office, Nuclear Security and Incident Response, but also the Office of New Reactors, the Office of Nuclear Reactor Regulation, and the Office of Research, as well as having gotten some feedback from our Regional Offices.

The framework that we developed

contains expectations for the various headquarters office and the region, regarding regulatory activities that may have implications for cyber-security.

If you go to the next slide, I'll give you some examples of some of the things we tried to address.

Although it's challenging to figure out all the possible regulatory situations where coordination should occur between the offices, and we actually did try to come up with a set of use-cases of situations where we should be interacting, things that we at NSIR may find, things that NRR may come across, things that NRO or the Regions may come across.

I cannot guarantee we got everything, but here were some of the big ones we did identify, and tried to lay out expectations.

For things like a digital safety system amendment, something that NRR may receive, that is something that NSIR should be notified of. If it's something as simple as a set point change to a digital instrument, that may be something that NSIR has very little interest in.

However, if it's a more grandiose whole replacement of a digital safety system, that is an opportunity for us and NSIR to review our guidance, to make sure it applies to the kind of change that is being made, evaluate whether or not a pilot study, like what we're doing with Diablo is appropriate, or at the very least, notify our NSIR and/or Regional Inspectors that, "Hey, there is a big change coming down, and this ought to be in your cue for the next cyber-security inspection at that site."

In addition, one of the other interactions that we already have with NRR, the cyber-security assessment team, which is led by NSIR, John Rycyna in the back, currently handles a lot of these duties.

We receive a lot of input from NRR's operating experience program, specifically any events involving instrumentation and control systems that may have a cyber implication do get sent to the CAT team, and the IOI formalizes that agreement.

Having some experience with some of the things we see, they do tend to err on the side of

conservatism, because we've gotten a handful of events that wind up being for analog systems, when we finally run on the ground.

Then also in the -- with respect to new reactors, although the vendors are not subject to the 73.54 rule, it does apply to licensees.

It is also important for NSIR staff to know that new reactor designs either have been received or will be received.

Very recently, we did have a vendor that NSIR staff participated in telecon with. They had a lot of questions regarding cyber-security guidance. They actually demonstrated a pretty reasonable understanding of our guidance, and they wanted to clarify a few points.

Again, just from their perspective, they are looking to hand over a cyber-ready design to a licensee, and that was an area where we at NSIR could have some value, in talking to them.

Then also, NSIR has an interest with NRO's vendor quality staff, regarding control and protection of the supply chain.

The vendor quality staff approaches it probably more from a quality assurance standpoint.

Our vent is a little more a malicious activity, but there is a significant amount of overlap in that area.

CHAIRMAN BROWN: Have you provided them with the supply chain guys? I mean, they're buying piece parts, some of those EP piece parts are active piece parts.

They have installed software on them, that are designed by vendors for -- I use -- you can use -- for radiologic control or those things that are -- or one set of things, or other sets, as well.

Have you all tried to put together a -- this is way down the food chain.

So, I mean, you're starting to look at experience levels of people that are buying these pieces, to build a bigger system, and there may be something buried in those things, or vulnerabilities that people ought to be asking about up front.

Have you all started a list of any kind, or do you all look at different types of piece parts, before you -- I don't know how you would do this.

MR. MOSSMAN: Yes.

CHAIRMAN BROWN: I thought about it, but I am not --

MEMBER BLEY: I think one of the concerns, I think especially in the electrical business, is the issue of counterfeit parts.

A vendor makes something, and it's got a part in it that has got the logo and everything of the right manufacturer, and yet, it's not, when you open it up, something different.

MR. MOSSMAN: Yes, in fact, there is really three different flavors of the CFSI problem and I apologize, I might start to get a little bit on thin ice, because I'm not technical expert in this area.

But there have been a log of public information reports out there. There are parts that are much like counterfeit bolts from 20 or 30 years ago, where people will manufacture a part, that is just hard to get, for purposes of making a profit.

It may function like the part you're looking for, but it may not be qualified like the part you're looking for.

There are also recycled parts, it's an

issue, people salvaging e-waste, you know, which in theory will be the same part, might actually be the real part, but it may have tens of thousands of hours of operating time on it, plus it may or may not have been soldered three or four times, by the time you receive it.

Then the last category is one that probably is of most interest, or is of more specific interest to cyber, which would be like if malware is implanted.

So, there are different flavors of things out there. There are different tools. Dan Pasquale has been leading a lot of the efforts on CFSI, and --

CHAIRMAN BROWN: Say that. What does that mean again?

MR. MOSSMAN: Counterfeit and fraudulent --

CHAIRMAN BROWN: Okay, got it, yes.

MR. MOSSMAN: I apologize, and we, at NSIR, have been working with him, just to -- on some of his efforts, and interfacing with industry on that.

I don't know that I can give you a whole

lot more detail off the top of my head, on that.

CHAIRMAN BROWN: Yes, I wasn't expecting you guys to go work with the part suppliers, themselves. But I mean, obviously the person building the systems are the point at where those parts come in, and they're the first touch point.

MR. MOSSMAN: Yes, I am aware that there are databases out there, and I want to say, Stacy might be able to help me in the back.

CHAIRMAN BROWN: I think I've done enough.

MR. MOSSMAN: Yes.

CHAIRMAN BROWN: Unless you've got another comment, Dennis. I thought we'd move on, on this one, okay.

MR. MOSSMAN: Okay, so, very good, the next slide. Okay, we're already there.

All right, in summary, very recently, the Branch Chiefs, affected Branch Chiefs in NSIR, NRR, NRO and Research signed out an internal memorandum that detailed the inter-office working arrangement for regulatory activities and cyber implications.

Basically, it's the working arrangement that everybody agreed to, and I apologize if you did not get a copy yet. I know it was something that did not get signed out in time for the main distribution package. So, it got to Christina very late.

CHAIRMAN BROWN: It's the closed part, you mean?

MR. MOSSMAN: No, it was an internal memorandum.

CHAIRMAN BROWN: Okay, yes, no, that is what you sent out?

MR. MOSSMAN: Okay, yes.

CHAIRMAN BROWN: Yes, I got it, yes, okay.

MR. MOSSMAN: And so, anyway, that is -- constitutes an internal agreement that everybody has signed off on, and referencing back to the ACRS recommendation to formalize that, our next step is to actually get that under an inter-office instruction header, so, it's in a formal tracked document, and when we get that published as a formal IOI, we can provide that to the ACRS.

MEMBER BLEY: That's great. I am

really glad to see you've moved on now.

CHAIRMAN BROWN: Thank you.

MR. MOSSMAN: Yes.

CHAIRMAN BROWN: Tim Harris.

MR. MOSSMAN: Okay, thank you very much.

MR. HARRIS: I never know whether it's good to talk before a break, after a break, before lunch, after lunch.

CHAIRMAN BROWN: You could help us out.

MR. HARRIS: I'll try to help you out.

Good afternoon. My name is Tim Harris. I am the senior program manager in the Division of Security Policy.

After joining the NRC in 1994, I've held a number of technical and managerial positions related to byproduct, source, special nuclear safety and security.

Over the last eight years, I've worked on a variety of policy issues, ranging from materials and reactor security, to cyber-security a nuclear installations.

I've also had extensive experience with

the International Atomic Energy Agency in the development of its nuclear security series fundamentals and recommendations level documents.

So, this afternoon, I'll discuss some of NRC's recent inter-governmental and international cyber-security activities. Next slide, please.

So, this is kind of and overview of my talk.

I'll begin my presentation with some history on the interactions with the Federal Energy Regulatory Commission or FERC, and the North Atlantic Electric Reliability Cooperation, NERC. I'll also discuss some of our other key inter-governmental interactions.

Then I'll discuss some of NRC's involvements with the recent Presidential Executive Order and Presidential Policy Directive to improve critical infrastructure of cyber-security, which includes the development of a voluntary framework for the -- for reducing cyber risk through critical infrastructure.

Last, I'll talk about some bilateral and multi-lateral international efforts that we've

been involved in.

This slide provides some history and recent interactions with both FERC and NERC.

As you are probably well aware, NRC's authority is derived from the Atomic Energy Act, while FERC's authority for grid reliability are tied to the Energy Policy Act of 2005.

These two authorities relative to cyber-security, intersect at nuclear power plants, and I think you had some questions earlier. So, hopefully I'll be able to clarify some of those.

Back in January 2008, FERC issued Order 706. This order specified critical infrastructure protection or CIP, reliability standards to safeguard cyber-critical assets.

This order also exempted NRC facilities from those requirements. Both NRC and FERC recognize the need to ensure that there was no gap or overlap between their regulatory programs and their regulatory programs.

Subsequent, FERC issued Order 706 Bravo, which clarified that the balance of plants and equipment within the power plant that are not within the scope of NRC's regulatory requirement,

would be within the scope of the NERC order.

As a result --

CHAIRMAN BROWN: Tim, to sum up -- maybe you're going to answer the question.

As a result, go ahead and finish your --

MR. HARRIS: That is actually the next words right here, "As a result."

So, you can ask a question if you like or --

CHAIRMAN BROWN: Finish.

MR. HARRIS: Okay.

CHAIRMAN BROWN: And then I'll ask.

MR. HARRIS: So, as a result, all nuclear power plants were asked by NERC, to determine which structures, systems and components or SSC's would be potentially subject to the CIP standards, and which would be potentially subject to the NRC regulations.

This analysis was known as the Bright Line Process. So, it was basically a process whereby plants tried to define when that bright line, where NRC regulations would apply and where CIP standards would apply.

CHAIRMAN BROWN: Did you get to vote?

MR. HARRIS: Did I get to vote?

CHAIRMAN BROWN: Did NRC get to vote?

MR. HARRIS: I think NRC was intimately involved in the discussions.

CHAIRMAN BROWN: There is a memo of --

MR. HARRIS: Yes, there is a memo --

CHAIRMAN BROWN: I'm just asking, is there a memorandum of understanding --

MR. HARRIS: Yes, sure, sure.

CHAIRMAN BROWN: -- that you know what is yours and they know what is theirs? If there was an agreement or a consensus reached?

MR. HARRIS: Yes.

CHAIRMAN BROWN: Okay, that is what I meant by, did you get a vote? I apologize for being obtuse.

MR. HARRIS: Just staff. They don't typically let me vote.

MR. ERLANGER: We had an opportunity to review the framework and to -- we basically just reflected in a Commission policy decision, which came down in a staff requirements memorandum.

The staff subsequently wrote an

information paper on how we interpret it, the Commission's policy decision.

CHAIRMAN BROWN: Okay.

MR. ERLANGER: So, we were intimately involved in the process.

CHAIRMAN BROWN: Okay, now, you answered my question. I didn't have to ask it.

MR. HARRIS: Okay, so, basically, all power plants indicated that if compromised, balance of plant SSC's would affect re-activity and were important to safety.

Licensees further stated for this reason, all balance of plant SSC's fall within the scope of NRC's regulation, which I think is what you were getting at.

I think Craig mentioned that the -- it wasn't an SR. I think it was a COM.

Basically, the Commission determined as a matter of policy, that the cyber-security regulations NRC 73.54 should be interpreted to include SSC's and the balance of plants 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.

I'll also note that NRC has a memorandum of agreement with FERC that provides a basis for cooperation on subsequent bright line processes to discuss things of mutual interest, and similarly, we have a memorandum of understanding with NERC, which helps also in the bright line process. Next slide, Perry.

So, NRC staff maintains periodic communications with staff from FERC and NERC, to exchange information and to ensure that requirements that are in place are effective and meet both organization's interest.

For example, NRC and FERC staff recently met to discuss FERC establishing its Office of Energy Infrastructure Security, which addresses cyber-security, and we also discussed future coordination.

In addition, Commission level meetings have occurred to discuss issues of mutual interest, such as the scope and boundary between FERC and NRC cyber-security programs.

Most recently, the Office Director of

NSIR Jim Wiggins, met with FERC last month, and it was agreed that a meeting between the Chairman of NRC and FERC would occur later this year.

So, now, I'll turn to some other inter-governmental activities.

MEMBER BLEY: I'm just a little curious, since you have agreements with both FERC and NERC, and I don't know those guys completely, but I know that CIP seems to originate in NERC, but then FERC issues regulations based on it.

I'm not sure how these --

MR. HARRIS: FERC issues orders and approves -- Perry can jump in, if you like.

FERC issues order. NERC is actually the one that issued the CIP's, which were approved by order through FERC.

MEMBER BLEY: So, it's not --

MR. HARRIS: So, it's not the --

MEMBER BLEY: FERC has got regulatory authority and NERC develops things that sometimes FERC uses?

MR. PEDERSON: Yes, NERC is the executor of the regulation. So, they are the ones that develop the standards, do the inspections and

levy the fines.

MEMBER BLEY: Oh, they do the fines, as well?

MR. PEDERSON: Yes.

MR. HARRIS: But it's a little --

MEMBER BLEY: So, because regulation, FERC has the --

MR. HARRIS: -- different situation then the --

MR. PEDERSON: Yes, so, they've been split up, you know. In the NRC, we are all under one roof.

MEMBER BLEY: Yes, okay.

MR. PEDERSON: Where we have all those functions, all within the NRC umbrella, but they've been split up that way.

MR. HARRIS: Go ahead, Craig.

MR. ERLANGER: I just think it's important to note that we did a side-by-side comparison of our requirements and our guidance, as compared to the NERC/CIP standards, and Perry, correct me if I'm wrong, but the verbiage we used at our requirements were equivalent, if not -- equivalent requirements for both type, and they

were asked -- they were satisfied --

MEMBER BLEY: You don't really go further? They're essentially equivalent?

MR. ERLANGER: We leave it at that. They did a side-by-side and they felt comfortable with us, looking out for some of their activities --

MEMBER BLEY: Okay.

MR. ERLANGER: -- out there, and the MOU and LOA leave the door open though, if they have an interest to explore a particular topic further down the road.

But we did a side-by-side of the standards and Reg Guide 5.71.

MEMBER BLEY: Okay, thank you.

MR. HARRIS: Yes, for example, FERC would construct NERC to develop standards. NERC would develop the standards and they'd be approved by FERC. It's a little different done situation.

MEMBER BLEY: Okay, but this gets into something Charlie was getting at earlier, in that the things they have responsibility for in enforcing, can affect our plants, because of the power connections.

CHAIRMAN BROWN: Yes, the switch yard, or the grid side of the switch yard, not necessarily the generator side.

MR. HARRIS: Yes, I mean, that could be an initiator for loss of offsite power.

MEMBER BLEY: Yes, or some unusual configuration, okay.

CHAIRMAN BROWN: Just, let me ask one question on that.

Have you -- I mean, the loss of offsite power thing, which has -- because it seems the SCADA stuff seems to hit periodically, keep popping up, if you read -- you know, from what I read in various, you know, publications and things.

Have you actually looked at their oversight or what things they have tried to oversee or put in place, to maintain -- ensure that the control of those grid connections are protected?

MR. ERLANGER: Can you clarify, by look, do you mean have we physically gone out there and seen the --

CHAIRMAN BROWN: No, I don't mean that. I mean, what processes do they have in place? Do they have something in place with the grid

operators that people look at the systems, or how do they maintain the security of the ability to maintain control of those, without having somebody come in and trip them inadvertently -- not inadvertently, but maliciously?

MR. ERLANGER: Perry, do you have any concession on the CIP standards that are --

MR. PEDERSON: Well, we have looked at their -- as Craig mentioned, we did a cross-walk between the requirements and the NERC/CIP, one thing to note about their process, to distinguish it from the NRC process, is they maintain an ANSI standard process.

In other words, it's by consensus of the regulated, unlike the NRC, where we accept input and then we make a decision.

And so, this is my personal opinion, but as I read some of those standards, there are things that are not perhaps, as rigorous and there are things that would fall out that -- you know, if our process were applied, we might call it a critical digital asset, and maybe in the case of the NERC/CIP, if it's a device that has a -- for example, and non-routable protocol, then they may

not call it a critical digital asset.

They have different terminology and a different framework, but their focus, of course, at the grid is on reliability, where our focus is on safety.

So, you would expect some of those differences.

MR. ERLANGER: And I would offer, their program, similar to ours, it's evolving, and they're learning, and we meet with them, at the staff level, on a much more frequent basis, to share information, and learn what they're doing and approve our requirement and vice-versa.

CHAIRMAN BROWN: Yes, the reason I -- there is a number of -- publically, you read about some of the -- what I would call the independent consultants and others, who rail-on in the various -- like the various electrical publications, whether it be IEEE publications or what have you.

There is a considerable skepticism, relative to the vulnerability of the grid, not just for nuclear power plants, but the grid in general, relative to mischief, because of the communication methodologies to now control it.

It's so -- so convenient, with the ability to not have hard wires going everywhere, and having little computer sitting around in places that -- that it's very hackable, or at least they maintain it's very hackable.

MEMBER SHACK: It's getting smarter all the time.

CHAIRMAN BROWN: Yes, but that means it's probably even more hackable, okay. That's the problem with complexity is, it increases the opportunities for malicious and -- in reality.

MEMBER BLEY: It doesn't garner confidence, but the distribution system and the sub-stations physically are scattered all over the place.

CHAIRMAN BROWN: That is true.

MR. PEDERSON: Well, and that's also --

MEMBER BLEY: For non-liberal, as well.

MR. PEDERSON: Yes.

CHAIRMAN BROWN: Yes.

MR. PEDERSON: The limit of the NERC relations, the NERC CIP doesn't go through the

distribution layer. It's through the generation and transmissions layers of the grid.

CHAIRMAN BROWN: Oh, is that right? So, it's just been applied to the switch yard itself, in terms of its connection to the plants --

MR. PEDERSON: Yes, it touches us at the switch yard, of course --

CHAIRMAN BROWN: Yes, yes.

MR. PEDERSON: -- where generation --

CHAIRMAN BROWN: But outside of that, they don't go.

MR. PEDERSON: Yes, like whatever happens if your house and in your local --

CHAIRMAN BROWN: Yes, I'm not really worried. If my house goes out, nobody is going to worry about it, except my family, or I should say my wife.

MR. PEDERSON: But this is one of the short-comings of the current NERC CIP, and they're on Version 5 now, I think it is, and looking down the road --

MR. HARRIS: I think they're looking at Version 6.

MR. PEDERSON: Yes, so, another version is coming because they keep trying to address these issues, like the distribution layer, which is where you find a lot of the smart grid evolving now, and the smarts is operating at that layer. But the NERC CIP doesn't touch that.

CHAIRMAN BROWN: Okay, I'm glad I asked the question then, because I didn't understand that completely. Thank you. Okay, you can --

MR. HARRIS: And luckily from a safety standpoint, plants know what to do when they don't have offsite power.

CHAIRMAN BROWN: No, I recognize that. I'm not saying that is -- I mean, that's one of the things they have to cover, so --

MR. PEDERSON: Right, and we do -- just as a footnote, we do coordinate a lot with NERC and FERC on sharing the threat, as well.

CHAIRMAN BROWN: Okay.

MR. HARRIS: So, slide five, as you may be aware, DHS is -- or Division of -- Department of Homeland Security is responsible for critical infrastructure protection.

DHS's national infrastructure

protection plan, or NIPP, provides a unified structure for the integration of critical infrastructure and key resource protection.

The NIPP includes 16 sector-specific plans that detail the application of an overall risk management framework for each sector.

As part of the nuclear sector, NRC participates in the Joint Cyber Sub-Council. The Cyber Sub-Council includes members from Department of Homeland Security, FBI, NRC and private sector representatives.

The Joint Sub-Council identifies cyber-security risk, potentially affecting the nuclear sector, serves as a forum for sharing of relevant information within the critical infrastructure framework, and also helps the nuclear sector participate in cross-sector bodies, such as the cross-sector cyber-security working group and the industrial control system working group.

So, now, I'll move on to the next slide, Perry, thanks, to the executive order.

Back in February 12th of this year, President Obama issued an executive order on

improving critical infrastructure for cyber-security.

Also issued was a Presidential Policy Directive PPD-21 Critical Infrastructure Security and Resilience.

The executive order requires Federal agencies to produce unclassified reports of threats to U.S. companies and it requires the reports to be shared in a timely manner.

The executive order establishes a voluntary program to promote the adoption of the cyber-security framework, again, voluntary program.

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 a significant contribution towards meeting the deliverables from the Presidential Policy Directive. Next slide.

CHAIRMAN BROWN: Who audits the voluntary -- voluntary is one thing. I mean, people work on a business model. If they -- they're going to make a profit somewhere.

MR. HARRIS: Well, I think that --

CHAIRMAN BROWN: So, the cost is really going to --

MR. HARRIS: With the framework of an executive order, it's not like a regulation or a law --

CHAIRMAN BROWN: No, I understand that.

MR. HARRIS: -- which requires that --

CHAIRMAN BROWN: I was reading something else, relative to the executive order, and then it was interesting, the ability to see the -- how voluntary -- voluntary, they've got a

lot of choices to make it a cost benefit analysis, which says that doesn't improve my bottom line.

So, I'll take the risk, that this is not going to happen to me, because I think the risk is manageable. You don't have any control over that.

MR. PEDERSON: In recognizing that, one of the working groups established under the executive order, is focused on incentives.

CHAIRMAN BROWN: Does the taxpayer subsidize those incentives or what? I said that facetiously, okay.

MR. ERLANGER: One of the challenges is that you got a -- try to make -- have a 'one size fits all' model for 16 very diverse sectors ---

MR. PEDERSON: Yes, right.

MR. ERLANGER: -- unlike the other -- and by 16 sectors, what I mean is, DHS has basically, just broken up the United States into their functional areas.

So, everything ranging from financial, dams, nuclear, across the board, unlike the nuclear sector, not every sector has a regulator with

requirements.

So, the attempt of this was to capitalize on a lot of these voluntary efforts, in order to improve cyber-security practices across the board.

CHAIRMAN BROWN: Is the nuclear sector a voluntary sector?

MR. ERLANGER: No, we're -- as Tim mentioned, we're -- because we're an independent agency, and the existence of the --

CHAIRMAN BROWN: So, I mean, so the critical -- I'm trying to think of this in terms of critical sectors. Do the critical sectors have some regulatory --

MR. PEDERSON: Not all of them.

MR. ERLANGER: Not all of them.

CHAIRMAN BROWN: Okay.

MR. ERLANGER: Chemical has just started being regulated by DHS. That was one for a while. There is -- dam sectors vary in degrees. Regulators, obviously, and banking is obviously, a diverse one and the --

CHAIRMAN BROWN: So, that is still a work in progress, is what you're saying.

MR. ERLANGER: Yes, but to answer your question, not every sector has a regulator.

CHAIRMAN BROWN: Okay.

MR. HARRIS: But you can see that the establishing this voluntary framework on a -- applicable to a large number of sectors, could later be used to refine to go into a sector specific, or be adapted.

CHAIRMAN BROWN: Yes, I wasn't advocating that one size fits all, don't get me wrong. I was just trying to get a feel for what voluntary meant, and I think you've given me an answer on that.

MR. HARRIS: Good. So, the executive order also calls for the review of existing cyber-security regulations.

Regulatory agencies are encouraged to use a voluntary framework to assess their programs and to determine if the existing requirements are sufficient.

Independent regulatory agencies, such as the NRC, are encouraged to lever -- leverage the voluntary framework and to consider prioritized actions to mitigate cyber-risk for critical

infrastructure, consistent with their authority.

So, I think what that means is, you know, if you have a program, look at the framework, see if you can glean anything that might help improve your program.

NRC, of course, will review our requirements, as directed by the Presidential Policy Directive, and although we're pretty confident that our cyber-security program is strong, we will of course, implement any improvements that are identified from that review.

So, NRC works closely with international counterparts to enhance nuclear safety and security worldwide. This includes exchanging information, expertise, operating experience, research and best practices.

The next two slides provide examples of bilateral and multi-lateral activities relative to cyber-security.

For example, NRC staff has 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. Next slide.

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

NRC staff has also assisted IAEA in developing guidelines for evaluating computer security during the IAEA advisory missions, and then updating training materials for computer security.

Review of documents also includes review of safety standards, such as DS431, entitled 'Design of Information and Control Systems for Nuclear Power Plants'.

We review these documents, the safety documents, to ensure that proper and adequate interfaces with cyber-security are occurring.

IAEA has documents specific to

cyber-security for power plants, so, the technical content for cyber-security are contained in those documents, but the purpose of the review of the safety documents is to make sure that there is linkages in both documents, so that the interfaces are covered.

In general, we are ahead of other countries in establishing a regulatory framework that considers cyber-security. Staff believes that sharing their experience and 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 relations to NRC cyber-security program, and as additional input for future changes in the program -- we'll use those insights as their program evolves. Next slide.

So, that basically concludes my presentation. I'd be happy to entertain questions, if time allows.

MR. HECHT: This is Myron again, from Los Angeles. Can I ask a question?

CHAIRMAN BROWN: Yes.

MR. HECHT: Okay, in the bright line work between NERC/FERC and the NRC, there is some equipment from the switch yard which -- or I should say there is some distribution and power distribution, which goes back into the plant, and there's equipment associated with that, and of course, there are relays associated with that, and in many cases, these relays are directly attached to the internet.

Do those relays fall under the category of CDA, which makes it belong to the NRC or might those relays actually be vulnerable through direct internet attachment?

MR. HARRIS: Yes, I don't have that. I mean, I guess it may be plant-specific. I don't have that granularity on where the actual bright line was drawn. I don't know if others in the room do.

MR. PEDERSON: One way to describe it is that our regulation covers the balance of plant, out to that first inter-tie in the switch yard. But there may be relays and such, that are physically on the other side, that are impacted

by systems on the inside of that point.

And so, it will, as you say, require a site-specific assessment to determine if it is a critical digital asset under our rule.

If it is not, part of our agreement with FERC and NERC is that we will tell them, everything that is discovered, and licensees are required to report those items that are not specifically identified as a CDA under our regulation, they're required to report that, so that they are covered, and this is to ensure that there is no gap.

MR. HECHT: Okay, so, basically you're saying that in the -- in case of doubt, the NRC covers it?

MR. HARRIS: No, I think there is a process that determines what is covered by NRC and what would be covered by the NERC CIP.

So, there is no ambiguity. No gap, as Perry said.

CHAIRMAN BROWN: Let me rephrase it. The way you're saying it is the plant is required to inform NERC and FERC, for those which are not under NRC control.

So, there is a positive action taken,

as opposed to an ambiguous, let somebody else figure it out type action?

MR. HARRIS: Correct.

MR. PEDERSON: Right.

CHAIRMAN BROWN: Okay.

MR. HECHT: Okay, thanks.

CHAIRMAN BROWN: Thanks, Myron. Any other questions? Dennis? Bill? Sam?

MEMBER ARMIJO: No.

CHAIRMAN BROWN: Okay.

MR. PEDERSON: Did you have a question?

MR. GROSS: A comment from the audience. Actually, relative to this particular topic.

MS. ANTONESCU: Can you please state your name?

MR. GROSS: My name is William Gross from the Nuclear Energy Institute.

While it's not one of the NERC critical infrastructure protection reliability standards, there is a NERC standard that has been approved by FERC. It's been around since as long as I've been engaged in cyber-security that's called NUK-001, or Nuclear Utility Interface Requirements.

That was developed on -- at the request of the industry to address specifically, the issue of the relationship between the plant and the transmission system, regarding the reliability of the transmission system to address the concern of the station black-out.

So, there are interface agreements currently between each plant and the transmission provider, to coordinate on a wide range of topics.

I don't -- I haven't looked at that close enough to understand how much that addresses cyber-security. I met with some of the transmission folks that -- from the Nuclear Utilities, just a few weeks ago, to talk about this issue of where that segmentation is.

They assured me that actually in the NUK-interface agreements, there would be likely a diagram or a textual description of exactly at which point the plants ownership of the switch yard ends and the transmission system begins.

What the transmission system picks up, those facilities would be subject to the NERC critical infrastructure protection reliability standards, for protection from cyber-attack.

Everything from the plant side in, would be subject to the NRC's requirements.

CHAIRMAN BROWN: Okay, thank you very much. With that, we will recess for 10 minutes, until -- or 11 minutes, until 3:30 p.m.

(Whereupon, the open session in the above-entitled matter adjourned at 3:18 p.m.)

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Cyber Security Update

Craig Erlanger and Ron Albert
Office of Nuclear Security and Incident Response
June 4, 2013

Agenda

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

- Opening Remarks – NSIR management
- Overview of the NSIR Cyber Security Organization
- History and Current Status of NRC's Cyber Security Program / Regulatory Framework
- Overview of the Cyber Security Oversight Program
- Inter-Office Coordination Activities
- Interagency / International Activities
- Cyber Security Roadmap Activities
- Path Forward

Desired Outcomes

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

- 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.

NSIR Organization

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

- NSIR was established in 2003.
- Mission: To prevent nuclear security incidents and prepare for and respond to safety and security events.
- Three technical divisions:
  - Division of Security Policy (DSP)
  - Division of Security Operations (DSO)
  - Division of Preparedness and Response (DPR)

Division of Security Policy

Cyber Security Roles

- Cyber Security and Integrated Response Branch (CSIRB)
  - Focus Areas: Rulemaking, guidance, licensing, roadmap implementation, and intergovernmental and international coordination.
- Fuel Cycle and Transportation Security Branch
  - Focus Area: Fuel Cycle Facilities Cyber Security related activities. Supported by CSIRB.

Division of Security Operations

Cyber Security Roles

- Reactor Security Oversight Branch:
  - Focus areas: Cyber Security Oversight Program, Cyber Assessment Team (CAT), regional coordination and intergovernmental and international coordination.
- Intelligence Liaison Threat Assessment Branch
  - Focus areas: Cyber Security threat analysis, intergovernmental and international coordination.

Staff Experience

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

- Cyber Security relies on a team approach:
  - Staff supporting the cyber security program has worked in multiple NRC offices and private sector companies.
  - Strong Cyber Security, Industrial Control Systems, Digital Instrumentation and Control, Engineering and Information Technology backgrounds.

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

Questions

U.S.NRC

UNITED STATES NUCLEAR REGULATORY COMMISSION

Protecting People and the Environment

NRC Approach to Cyber Security

Perry Pederson
Office of Nuclear Security and Incident Response
June 4, 2013

Agenda

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

- Definition of Key Terms
- Cyber Threat Landscape
- Cyber Security Historical Timeline
- Coordination Efforts
- Regulatory Framework
  - Regulation, Guidance, Licensing, & Oversight
- Cyber Security Lifecycle
- Q&A

Definition of Key Terms

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

- Cyber Security
  - Those measures and controls, implemented to comply with 10 CFR 73.54, to protect digital systems against the malicious acts of an intelligent adversary up to and including the design basis threat, as defined by 10 CFR 73.1
- Cyber Threat
  - An individual, entity, or action that by cyber-means has or indicates the potential to harm life, information, operations, the environment and/or property
- Critical Digital Asset (CDA)
  - A subcomponent of a critical system that consists of or contains a digital device, computer or communication system or network
- Adverse Impact
  - A direct and deleterious effect on a CDA.
- Defense-in-depth
  - An approach to security in which multiple levels of security and methods are deployed to guard against failure of one component or levels

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
2006	Published RG 1.152 Rev. 2 – computers in safety systems
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	NPP Cyber Security Plans approved
2013	Inspection of Interim Milestones begin

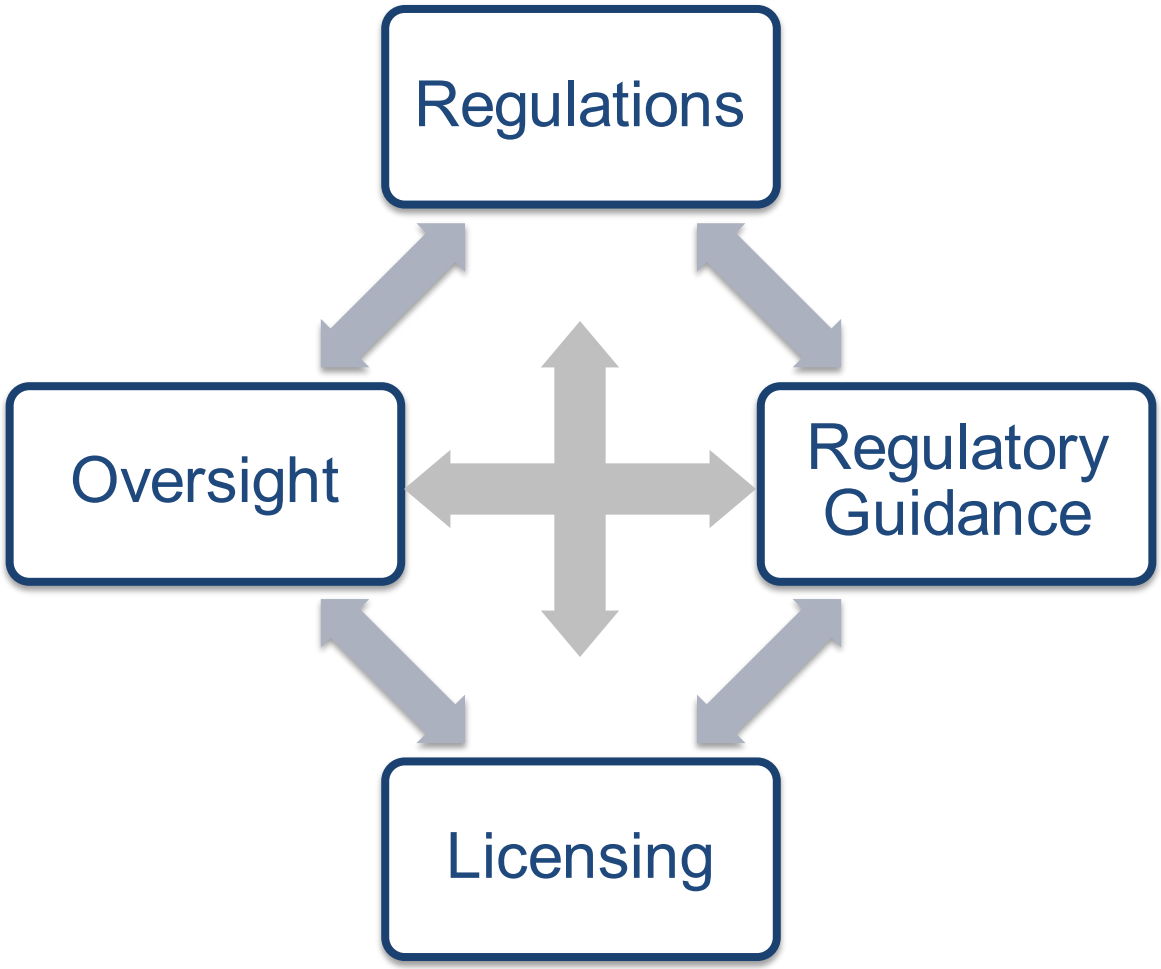
Coordination Efforts

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

- Intragency
  - NSIR, NRR, NRO, RES, and Regions have worked and continue to work together
  - IOI Memorandum
- Interagency
  - DOE, FERC/NERC (Brightline), FBI, DoD, and others
  - DHS under the National Infrastructure Protection Plan (DHS as the Nuclear Sector SSA)
- International
  - International Atomic Energy Agency (IAEA)
  - Bilateral cooperation with South Korea, Spain
- Industry
  - Owners / Operators
  - Nuclear Energy Institute (NEI), EPRI

Regulatory Framework

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



10 CFR 73.54

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

- Title: Protection of digital computer and communication systems and networks
  - Applies to power reactors – operating and new reactors
- Performance-Based, Programmatic (< 2 pages)
  - Provide high assurance against cyber attack
  - Integrated with Physical Security Program (10 CFR 73.55)
- Basic Requirements
  - 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 Guidance Pedigree

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

- 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

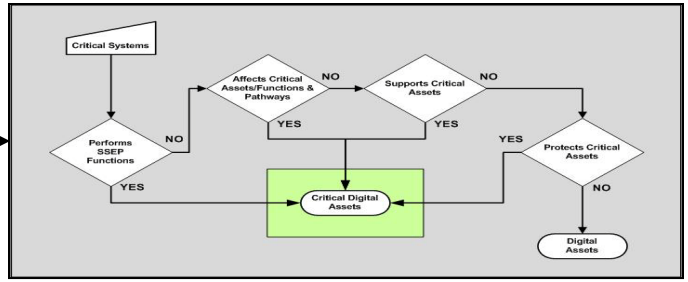
Regulatory Guide 5.71

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

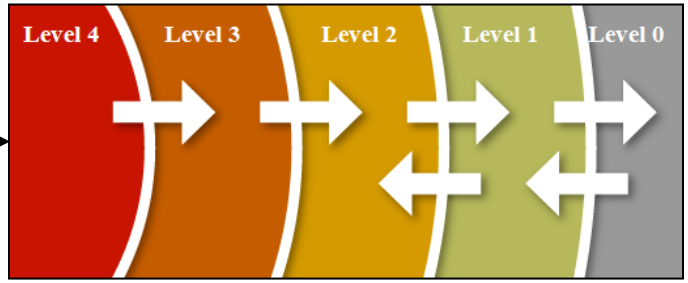
Title: Cyber security programs for nuclear facilities

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

Cyber Security Plan

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

- 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

Implementation

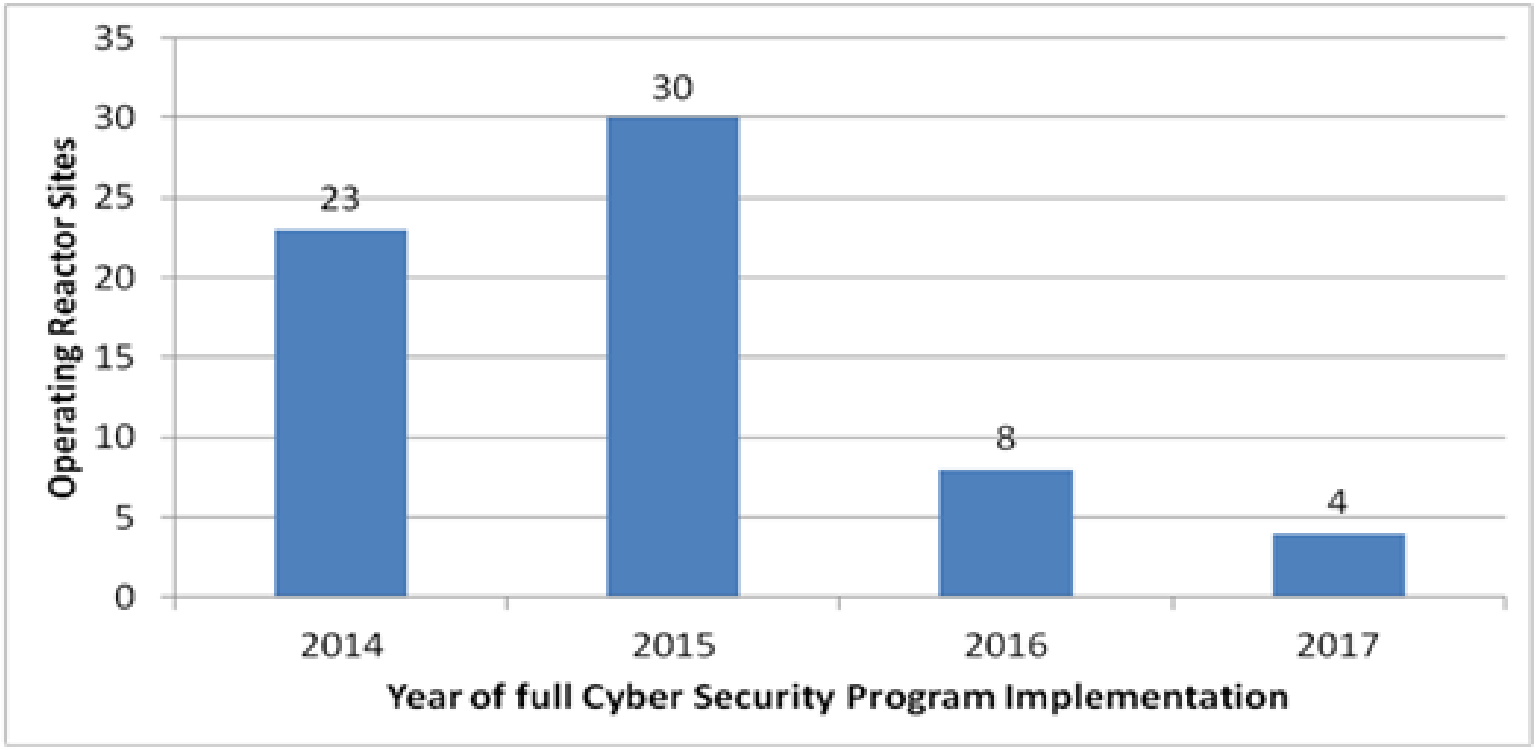
U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

- 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

Milestone 8

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

Full Program Implementation



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

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

Questions

U.S.NRC

UNITED STATES NUCLEAR REGULATORY COMMISSION

Protecting People and the Environment

Cyber Security Inter-Office Collaboration

Tim Mossman
Office of Nuclear Security and Incident Response
June 4, 2013

Inter-Office Coordination

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

- Cyber security concerns may arise at many points in the regulatory process
- Ensuring appropriate cyber protections are taken throughout digital life cycle
- Minimize regulatory risk to licensees
- Efficient use of staff resources

Cyber Framework Evolution

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

- Commitment to ACRS
- Framework has been informed by on-going activities:
  - NSIR / NRR coordination on digital licensing*
  - NSIR / NRO coordination on new reactors*
  - NSIR / Regional cyber inspection activities*

* Closed portion of meeting

Cyber Framework Development

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

- Multi-Office participation
- Addresses expectations for HQ Offices and Regions

Example Regulatory Activities

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

- License amendment involving digital system
- Licensee event report (Operating Experience program)
- Combined License (COL) application / modification
- Design Certification (DC) application / modification
- Vendor inspection that raises supply chain questions
- Standards development activities

Summary

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

- Staff from all NRC Offices work in an integrated fashion on Digital I&C safety and security issues
  - Collaboration has occurred through coordination by the staff on particular cyber-related topics and licensing actions
- Staff recognized the need for more explicit framework to facilitate interactions on cyber security regulatory activities
  - Commitment to ACRS
- Affected Branch Chiefs recently signed out a framework detailing the types of regulatory activities that have cyber considerations and staff interactions that result
  - The framework is intended to be formalized into an Inter-Office Instruction

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

Questions

U.S.NRC

UNITED STATES NUCLEAR REGULATORY COMMISSION

Protecting People and the Environment

Intergovernmental and International Interactions

Tim Harris
Office of Nuclear Security and Incident Response
June 4, 2013

Overview

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

- Federal Energy Regulatory Commission and the North American Electric Reliability Corporation Activities
- Other Intergovernmental Activities
- Executive Order/Presidential Policy Directive Activities
- International Activities

FERC/NERC Activities

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

- Memorandum of Agreement with FERC
- Memorandum of Understanding with NERC
- Gap Analysis
- Bright line survey
- Commission Policy in SECY-10-0153

FERC/NERC Activities (2)

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

- Commission level meetings
  - Joint FERC NRC Meeting – March 16, 2010
  - Joint FERC NRC Meeting – June 15, 2012
- Periodic staff/management meetings
- FERC establishes Office of Energy Infrastructure Security

Other Intergovernmental Activities

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

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

Executive Order

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

IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY

- 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

NRC 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

International Activities

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

- IAEA TM - Computer Security At Nuclear Facilities (May 2011)
- WINS – Workshop on the development and integration of cyber security programs (Feb 2012)
- IAEA CM – Revise Guidelines for computer security advisory/assessment Missions (March 2012)
- Korea Atomic Energy Research Institute (KAERI) -NRC's cyber security and safety-security interface regulations (May 2012)

International Activities (2)

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

- IAEA CM - Application of security controls to instrumentation and control systems (June 2012)
- IAEA CM - Review and update the current training material on computer security at nuclear facilities (Sept 2012)
- IAEA CM - Application of security controls to instrumentation and control systems (Nov 2012)
- IAEA CM - Cyber threat assessment methodologies (Jan 2013)
- IAEA CM – Applying security controls to instrumentation and control systems: Security and Safety Considerations (Feb 2013)

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

Questions