

Official Transcript of Proceedings

NUCLEAR REGULATORY COMMISSION

Title: Advisory Committee on Reactor Safeguards
 Digital Instrumentation and Controls System
 Subcommittee

Docket Number: N/A

Location: Rockville, Maryland

Date: November 2, 2016

Work Order No.: NRC-2707

Pages 1-435

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

DISCLAIMER

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

UNITED STATES OF AMERICA
 NUCLEAR REGULATORY COMMISSION

+ + + + +

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS (ACRS)

+ + + + +

DIGITAL INSTRUMENTATION AND CONTROL

SYSTEMS SUBCOMMITTEE

+ + + + +

WEDNESDAY

NOVEMBER 2, 2016

+ + + + +

ROCKVILLE, MARYLAND

+ + + + +

The Subcommittee met at the Nuclear
 Regulatory Commission, Two White Flint North, Room
 T2B1, 11545 Rockville Pike, at 8:34 a.m., Charles H.
 Brown, Jr., Chairman, presiding.

COMMITTEE MEMBERS:

CHARLES H. BROWN, JR., Chairman

MARGARET CHU, Member

JOSE A. MARCH-LEUBA, Member

DANA A. POWERS, Member

JOHN W. STETKAR, Chairman

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
 1323 RHODE ISLAND AVE., N.W.
 WASHINGTON, D.C. 20005-3701

MATTHEW W. SUNSERI, Member

ACRS CONSULTANT:

MYRON HECHT*

DESIGNATED FEDERAL OFFICIAL:

CHRISTINA ANTONESCU

ALSO PRESENT:

SUZANNE ANI, NMSS

NIMA ASHKEBOUSSI, NEI

MATT BARTLETT, NMSS

BRAD BERGEMANN, NSIR

MICHAEL BURKSDALE, Public Participant*

JOE DEUCHER, NMSS

JAMES DOWNS, NMSS

CRAIG ERLANGER, Division Director, FCSE

AARON KENT, Public Participant*

JIM MALTESE, OGC

CARDELIA MAUPIN, NMSS,

CHARITY PANTALO, NSIR

CASEY PRIESTER, NSIR Contractor

MICHAEL SHINN, NSIR Contractor

BRIAN SMITH, Deputy Division Director, FCSE

NORM ST. AMOUR, OGC

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

ANDREA D. VEIL, Executive Director, ACRS

*Present via telephone

T-A-B-L-E O-F C-O-N-T-E-N-T-S

Page

Introduction and welcome.....5

By Chairman Brown

Opening Remarks.....7

By Craig Erlanger - Division Director
of the Division of Fuel Cycle Safety
Safeguards and Environmental Review in
the Office of Nuclear Material Safety
and Safeguards

Presentation of Cyber Security for Fuel.....8

Cycle Facilities

By James Downs - Program Manager for
Cyber Security for the Fuel Cycle
Facilities

Types of Fuel Cycle Licensees and Regulations.....9

By Brian Smith - Deputy Director in the
Division of Fuel Cycle Safety Safeguards
and Environmental Review

History of Fuel Cycle Cyber Security

Current Requirements

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

Brad Bergemann, NSIR.....	88
Development of SECY-14-0147	
James Downs, NMSS.....	103
SRM to SECY-14-0147	
James Downs, NMSS.....	105
Regulatory Basis	
James Downs, NMSS.....	110
Overview of Draft Proposed Rule Language	
Consequences of Concern	
James Downs, NMSS.....	129

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

(8:34 a.m.)

CHAIRMAN BROWN: Good morning. Meeting will now come to order. This is a meeting of the Digital Instrumentation and Control Subcommittee. I'm Charles Brown, Chairman of the Subcommittee. ACRS Members in attendance are Dana Powers, John Stetkar, Mike Corradini possibly, Jose March-Leuba, Margaret Chu, Matt Sunseri, and possibly our consultant Myron Hecht. Have you heard from Myron?

MS. ANTONESCU: I haven't.

CHAIRMAN BROWN: Okay. He was flying in, so, from California. So it could be happening. Christina Antonescu of the ACRS Staff is our designated Federal Official for this meeting.

The purpose of the meeting is for the Staff to brief the ACRS on the technical basis for the fuel cycle cyber security rulemaking including the draft proposed rule language 10 CFR 73.53 and the draft regulatory guidance DG 5062 and other related

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

(202) 234-4433

(202) 234-4433

documents for the fuel cycle security rulemaking.

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.

The meeting will be open to public attendance with the exceptions of portions that may be closed to protect information that is proprietary. We have received written comments and request for time to make oral statements from members of the public, the Nuclear Energy Institute regarding today's meeting. That will, those oral statements will come at the end of the meeting.

To preclude interruption of the meeting, the phone line will be placed on listen in mode during the presentations and Committee discussions. Also the bridge line will be opened at the end of the meeting for anyone listening on the bridge line who would like to make any comments.

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

Participants should first identify themselves and speak with sufficient clarity and volume so that they may be readily heard. And then also please silence all cell phones, pagers, iPhones, iPads, and all other appropriate electronic appliances, devices that you may have on your persons, including me. Thank you.

We will now proceed with the meeting. I call upon --

(Off microphone comments)

CHAIRMAN BROWN: Okay, okay. I thought I was going to have somebody over there. So Craig Erlanger, the Division Director of the Division of Fuel Cycle Safety Safeguards and Environmental Review in the Office of Nuclear Material Safety and Safeguards to make some opening remarks followed by James Downs to start the presentation. Have at it.

MR. ERLANGER: Good morning. Thank you for the opportunity to present today. As Mr. Brown mentioned, my name is Craig Erlanger, I'm the Director of the Division of Fuel Cycle Safety Safeguards and

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

Environmental Review.

As discussed, we will be briefing you today on the Fuel Cycle Cyber Security rulemaking effort. The Staff's goal is to get a proposed rule package to the Commission in March of 2017.

We have a full agenda today. At this point I'm going to turn it over to James Downs who is the Senior Project Manager for this effort and he's going to talk you through the agenda and a few other items, and then we'll be followed by an overview of the fuel cycle facilities themselves. James?

MR. DOWNS: Thanks, Craig. As Craig said, I'm James Downs. I'm the Program Manager for Cyber Security on the Fuel Cycle side of the house. This effort has been about five years in the making. So you know, when we started out it was just an initiative to kind of gather the lay of the land at the fuel cycle facilities as far as cyber security is concerned.

Over those five years, we've had various directions and approaches that we've taken, and hopefully the presentation today will kind of provide some detail on where we've been and hopefully where we're going.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

And obviously, as we go through the presentation, if you've got questions, please let us know. So the agenda today, on slide two here, going to give you a quick overview of fuel cycle facilities. By that we mean just kind of a discussion of some of the, you know, to try to get a physical description of what a fuel cycle facility looks like, the different types of facility types that are out there.

A lot of people at the NRC are familiar with the power reactors and don't have a lot of experience with fuel cycle facilities. So we like to give this kind of introduction to fuel cycle, just kind of get everybody thinking outside of the reactor box and into the fuel cycle world.

After that, we're going to give a history of fuel cycle cyber security, give a quick overview of the draft proposed rule language, and then go into the draft regulatory guide which is the guidance document associated with the proposed rule language.

So with that, oh there's a slide three, just some acronyms that we're using in the presentation. We intentionally tried to limit the use of acronyms which is very difficult for NRC Staff to do because we love our acronyms, but we've just got a

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

few here that we're going to have over the course of the presentation.

MEMBER POWERS: Charlie is from the Navy. You're rank amateurs.

MR. DOWNS: Is that right? Then okay, so slide four, I'm going to turn it over to Brian Smith who is going to walk us through this overview of fuel cycle --

MR. SMITH: Good morning. Okay. Good morning. My name is Brian Smith, I'm the Deputy Director in the Division of Fuel Cycle Safety Safeguards and Environmental Review. And as James mentioned, we want to go over the various types of fuel cycle licensees that we have and some of the related regulations associated with those.

Our division doesn't get to come in front of the ACRS all that often, and so some of you may not be that familiar with our types of facilities, and so we want to give you that kind of overview.

So we'll touch on the facility types. We'll go through some of the process fundamentals associated with the various types of facilities that we have, and then we'll touch on the regulatory framework as well as we get through that. So next

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

slide.

Here's a version of the fuel cycle. You've probably all seen various versions of it along the way. The types of facilities in this chart here that we're going to be focusing on are the conversion, enrichment, low enriched fuel fabrication, high enriched fuel fabrication.

And there's a type of facility that's not located on here that's in the step between enrichment and final disposition, and that's depleted uranium de-conversion facility. So we'll go through what those are as well.

CHAIRMAN BROWN: That's not shown on there, right?

MR. SMITH: shown, that's correct.

CHAIRMAN BROWN: All right.

MR. SMITH: Okay, so here's a listing of some of the facility types that we have. We'll give you a couple of slides associated with this. And it kind of flows through the cycle, the one that we just saw. And it starts off with uranium conversion.

We have one facility located in Metropolis, Illinois here in the United States called Honeywell. The primary material present there is

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

source material which is licensed under Part 40.

CHAIRMAN BROWN: Can you answer, I need a little bit of an education.

MR. SMITH: Okay.

CHAIRMAN BROWN: What are Categories I, II, III, and IV?

MR. SMITH: Types of facilities.

CHAIRMAN BROWN: Yes, that's right.

MR. SMITH: I would say Category III.

CHAIRMAN BROWN: I know. But what, I just, I don't even know which ones.

MR. SMITH: Okay.

CHAIRMAN BROWN: I was searching for that and couldn't -- not real hard but --

MR. SMITH: Okay. There are three types. When it comes to categories of facilities there's three types, I, II, and III. Category III has to do with low enriched uranium. Category II has to do with special nuclear material moderate significance. And Category I is strategic special nuclear material, or high enriched uranium.

CHAIRMAN BROWN: Say that again on Category I.

MR. SMITH: It's a special nuclear

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

material of moderate significance.

CHAIRMAN BROWN: What does that mean?

MR. SMITH: It means it's enrichments between, it's up to 20 percent. Low enriched is up to, I forget the, they're described in Part 70 and Part 73.

CHAIRMAN BROWN: You can't say what low enriched is?

MR. SMITH: I don't remember the threshold.

CHAIRMAN BROWN: It's lower than 20 percent?

MR. SMITH: Yes, yes.

CHAIRMAN BROWN: You said 20 percent for the --

MR. SMITH: Between 20 and 100 is high enriched.

CHAIRMAN BROWN: That's Category III?

MR. SMITH: Category I.

CHAIRMAN BROWN: Okay, I'm sorry, Category I. You're working down the list. I'm writing so hold up a second.

(Off microphone comments)

CHAIRMAN BROWN: And moderate is between,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

you just said 20 percent for the Category II?

(Off microphone comments)

CHAIRMAN BROWN: Don't make it too complicated, I'm old.

MR. SMITH: So that just in general, the categories of the facilities are based off the material attractiveness associated with the level of enrichment present.

CHAIRMAN BROWN: I understand the high enrichment stuff is --

MR. SMITH: And that would be the Category I.

CHAIRMAN BROWN: That's very important stuff?

MR. SMITH: That's right, that's right. So if we strictly just stick to enrichments, because the definition is more complicated, it's between ten and twenty percent for moderate.

CHAIRMAN BROWN: That's Category II?

MR. SMITH: Category II.

CHAIRMAN BROWN: And low is less than then then?

MR. SMITH: Yes, sir.

CHAIRMAN BROWN: All right.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

MEMBER MARCH-LEUBA: And the mass, because lots of places has a gram quantities of U-235.

MR. SMITH: Yes, that's how it makes the definition more complicated.

MEMBER MARCH-LEUBA: Okay, so the mass --

MR. SMITH: It's in the definition section of Part 70, but also in the definitions of Part 73.

MEMBER MARCH-LEUBA: So if I have a fusion chamber that has one gram of UT-35 at 99 percent, I'm not a Cat I?

MR. SMITH: Correct.

MR. DOWNS: That's right. I think the definition says formula quantity. So that's a --

CHAIRMAN BROWN: Forcumaic? That means bomb quality?

MEMBER MARCH-LEUBA: No, it's a mass.

CHAIRMAN BROWN: It's a critical mass?

MR. DOWNS: Right.

CHAIRMAN BROWN: Bomb quality. I just wanted to make sure I understood.

MEMBER MARCH-LEUBA: We used to call it the unclassified weapon mass. You really cannot make it critical with that mass.

CHAIRMAN BROWN: Okay.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

MEMBER MARCH-LEUBA: The unclassified bomb.

MR. SMITH: So we have a number of Category III facilities. We have two Category I facilities that are operating and one Category I facility that's under construction. We currently have no Category II facilities.

CHAIRMAN BROWN: Okay, tell me, you've got how many Cat III? Roughly. Is that the list right there?

MR. SMITH: It's some of the list.

CHAIRMAN BROWN: Okay.

MR. SMITH: So we'll go through the list and you'll see. Some of these facilities here, as I'll discuss in a minute, have a license but have not constructed. So back over the last ten years we've issued, well we've reviewed a number of new license applications for enrichment facilities as well as de-conversion facilities. But because of market conditions, some of those were not built. So I'll go through and specify which.

CHAIRMAN BROWN: Which ones are of greatest interest to the --

MR. SMITH: The ones that we're going to

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

be discussing here today.

CHAIRMAN BROWN: But I mean, it's Category III?

MR. SMITH: It's all of these. Honeywell --

CHAIRMAN BROWN: Category I, we have Category I?

MR. SMITH: We have several Category I's and Category III's.

CHAIRMAN BROWN: They were reactors themselves? Or they are --

MR. SMITH: I'm sorry?

CHAIRMAN BROWN: In the reactor, I mean, it's part of the fuel and some of our power reactors, Category I?

MR. SMITH: Yes, they would have what you would consider a Category I quantity of material.

CHAIRMAN BROWN: Okay, and that's where the --

MR. SMITH: There are separate requirements.

CHAIRMAN BROWN: -- mass then comes in? Or am I losing the bubble here?

MR. SMITH: Yes, to be a Category I

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

licensee you have to have a certain quantity of the material.

CHAIRMAN BROWN: No, I understand that. I'm talking about look at a plant today. Power plants have category I as part of their fuel configuration inside the reactor vessel. Is that --

MR. SMITH: No, no.

MEMBER MARCH-LEUBA: No, not --

MEMBER STETKAR: Not for nuclear reactors. It's for the facility that's processing the stuff that may get to the power reactor or not a power reactor. Right? Navy reactor.

CHAIRMAN BROWN: Well just a minute. I understand where Navy reactors are. I lived with that for 35 years. Yes, I'm very well aware that they're in the upper --

MR. SMITH: Brad is our security guy.

CHAIRMAN BROWN: So I'm trying to be quiet and not say too much.

MR. BERGEMANN: Brad Bergemann, NSIR CSD. The operating power reactors that we license are not Category I type facilities.

CHAIRMAN BROWN: Okay. I just wondered where this stuff was going. That's all I was

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

interested in. I'm trying to make sure I understood since I haven't been through this drill before.

MR. BERGEMANN: Yes, it's separate requirements.

CHAIRMAN BROWN: Okay.

MEMBER STETKAR: But a Category I facility could be processing material that eventually gets to a power reactor, is that true?

MR. SMITH: Most of the fuel that's generated at the Category I facilities goes to the Navy or to go to a research reactor, research and test reactor.

CHAIRMAN BROWN: You said most. Is it most or is it all?

MR. DOWNS: It would be most because there is a facility that the mixed oxide fuel fabrication facility and yes, they would down blend the plutonium and --

MEMBER STETKAR: So in principle, you could have a Category I facility that processes material that eventually makes its way to a power reactor --

MR. DOWNS: That's correct.

MEMBER STETKAR: -- but at a much lower --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

MR. DOWNS: Right. Most of the volume of the fuel going into a power reactor comes from the Category III fuel fabrication facilities.

MEMBER MARCH-LEUBA: Are those Cat I facilities regulated by NRC?

MR. DOWNS: Yes.

CHAIRMAN BROWN: Thank you. That was my other question. Why in the world are you all interested in Cat I?

MR. SMITH: They are contractors to the Government, to the Department of Energy.

CHAIRMAN BROWN: Why doesn't, I thought DOE handled all that stuff for that.

MR. SMITH: They handle primarily all of their activities that are located on DOE sites. These facilities are not located on DOE sites.

CHAIRMAN BROWN: So all the enrichment facilities and fuel facilities are under the NRC's regulatory umbrella?

MR. SMITH: The DOE may fabricate some fuel for testing purposes, but that's done on the DOE sites. All of these facilities here are not located on the DOE site.

CHAIRMAN BROWN: I got that.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

MR. SMITH: Even though they may be doing work for the Department of Energy.

CHAIRMAN BROWN: Okay.

MEMBER STETKAR: And in some cases isn't it true that the DOE basically is reaching an agreement with the NRC that the NRC will handle the licensing issues?

MR. SMITH: Yes.

MEMBER STETKAR: Despite the fact that it's, it could be a "DOE" facility?

MR. SMITH: Yes. There is one always, there was always an exception to every rule. And the MOX facility that's under construction is located on the Savannah River site. And there was special legislation that was put through that designated NRC as the regulator for that facility.

MEMBER STETKAR: I'm only trying to get, this is important because we're taking a snapshot today of facilities that are either operating or perhaps plan to operate. But this is a rule going forward, so it has to, you know, essentially cover --

MR. SMITH: Yes, all --

MEMBER STETKAR: -- all eventualities that we can think of.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

MR. SMITH: Yes, so I'll try and clarify some of the stuff as we go through.

CHAIRMAN BROWN: Yes, the reason I'm asking the question is because when you run through the rule in the reg guide there's, you know, a lot of discussion from a cyber standpoint. What degree of issue do you have to deal with or not deal with.

So I've just, that's why I was trying to get an understanding of what these various categories were and what the ranges were and what would be the significance of compromise and/or whatever all the other stuff you talk about, radiological sabotage, theft, disappearance, loss of a counting or what have you.

So I'm just trying to put it in context of what the level of the various enrichments were relative to this and how the rule and how the reg guide tells people what to do.

MR. SMITH: Okay.

CHAIRMAN BROWN: So that's the purpose of mouse milking this one to death here.

MR. SMITH: Okay, well I will try to be more specific when I go through the facilities.

CHAIRMAN BROWN: Thank you.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

MR. SMITH: Okay. So Honeywell, it's a facility that's been in operation since the late 1950s located in Metropolis, Illinois. And its primary purpose at this time is to convert U-308 to UF6 to be fed into an enrichment plant somewhere in the world. It's licensed under Part 40 because it possesses source material, which is natural uranium.

Uranium enrichment gas interfuge, we have three licensees in this category. The one that is built and operating is the URENCO USA Facility also known as Louisiana Energy Services.

It's licensed up to five and a half percent enrichment. Therefore it's a Category III facility. The enrichment technology itself, aspects of it are classified. And so therefore, they possess classified information and matter on the site. They also have classified networks there to process information to run the plant.

CHAIRMAN BROWN: But they're only up to five percent you said?

MR. SMITH: They produce up to. The actual product is, like, up to 4.95. They're licensed to possess up to --

CHAIRMAN BROWN: Enrichment?

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

MR. SMITH: -- 5.5 percent enriched uranium. Yes, sir. They do also possess fairly large quantities of source material. The feed material is -

CHAIRMAN BROWN: Source material?

MR. SMITH: Source material --

CHAIRMAN BROWN: Okay, I don't understand. You said Honeywell does source material Part 40.

MR. SMITH: Yes.

CHAIRMAN BROWN: Now URENCO has source material also?

MR. SMITH: It does. And --

CHAIRMAN BROWN: But they don't do the same thing that Honeywell does.

MR. SMITH: They do not. Honeywell produces the feed material for enrichment plants.

CHAIRMAN BROWN: Yes, that's the UF6.

MR. SMITH: Yes. And so they take the UF6 at the enrichment plant and --

CHAIRMAN BROWN: And URENCO is one of those?

MR. SMITH: URENCO is the only one in the United States operating at this time.

CHAIRMAN BROWN: Enrichment? Okay.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

MEMBER MARCH-LEUBA: So basically the source material is a stockpile for feeding into the centrifuges, right?

MR. SMITH: Yes.

MEMBER MARCH-LEUBA: Yes, they have a yard full of 48 y's.

MR. SMITH: Yes. Source material is natural uranium. And so the purpose of an enrichment plant is to increase the percentage of uranium-235 such that it could be used in today's power reactors which typically range --

CHAIRMAN BROWN: What source material, what's the level of enrichment of source material?

MR. SMITH: 0.711 percent.

CHAIRMAN BROWN: Okay.

MR. SMITH: And so what they want to do is they want to increase it to between three and five percent for use in the current power reactors. 0.711, That's what you mine out of the ground.

(Simultaneous speaking.)

MEMBER POWERS: And there are certainly sources of U-308 that deviate from that.

MR. SMITH: So, like I said, their product is special nuclear material, enriched uranium. The

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

feed material is source material, that's natural uranium.

Their waste material is also considered source material and that's depleted uranium. So it's the natural uranium with less concentration of uranium-235. So it drops down from 0.7 percent down to as far as 0.2 percent.

CHAIRMAN BROWN: At the completion of the enrichment process?

MR. SMITH: Yes.

CHAIRMAN BROWN: Okay.

MR. SMITH: All right, so there's two other facilities that have a license that have not yet constructed. One of those is the Eagle Rock Enrichment Facility that's going to be located in Idaho Falls or outside of Idaho Falls, between there and the Idaho National Lab.

And the other one is the American Centrifuge Plant. That would be located on the same side as the Portsmouth Gaseous Fusion Plant in Piketon, Ohio.

The URANKO facility and the Eagle Rock facility will utilize the same technology, same enrichment technology which is a foreign design, and

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

the American Centrifuge Plant uses a centrifuge based on a DOE design.

CHAIRMAN BROWN: So neither of those two plants have been constructed yet? They've got licenses but no construction?

MR. SMITH: The Eagle Rock facility was a potato farm. And as far as I know it's still a potato farm.

CHAIRMAN BROWN: Still a potato farm.

MR. SMITH: The American Centrifuge Plant, they were going to utilize a prior DOE facility that was a gas centrifuge plant. It was part of a DOE program called the gas centrifuge remission program and there were already two cascade hall buildings built. They had an assembly building as well and some other associated buildings, a feed building. So all those buildings were already constructed. They would have to make some modifications to it and obviously manufacture all of the centrifuge pieces.

CHAIRMAN BROWN: That's all on hold right now?

MR. SMITH: That's correct. They have a test facility, what they call the Lee Cascade that had been operating for the last six or eight years. And

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

that's in the process of being shut down right now.

So any other questions about enrichment, centrifuge? Okay. We do, we have issued one license for a laser enrichment plant. This is for global, GE-Hitachi Global Laser Enrichment for a facility to be built and operated in Wilmington, North Carolina on the same side of GE's global nuclear fuel's America's fuel fab plant which I'll talk about shortly.

It's similar to the centrifuge plants except it would use lasers as part of its separation process. Same material --

MEMBER MARCH-LEUBA: One issue with the laser separation, number one is nobody will ever tell you if they're actually doing it. I mean, you got there to Wilmington and they say it's classified, can't talk about it.

The real problem with that is in principle you can enrich to two, three, a hundred percent on the same machine.

MR. SMITH: You can do that with gas centrifuge as well?

MEMBER MARCH-LEUBA: Not necessarily.

MR. SMITH: Depends on how you set up the cascade?

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

MEMBER MARCH-LEUBA: You have to --

(Simultaneous speaking)

CHAIRMAN BROWN: Let's not argue about that. That's not really part of our -- I understand what you're talking about.

MEMBER MARCH-LEUBA: I'm talking about Cat III, whether it really is a Cat III or a Cat, or a potential Cat Class I.

MR. SMITH: They would be licensed to produce only up to, I think, I forget what the percentage was, maybe eight percent. That's what they would be limited to doing.

MEMBER MARCH-LEUBA: Okay.

CHAIRMAN BROWN: But it's not operational or constructed?

MR. SMITH: They have a test facility, a very small test facility located at the Global Nuclear Fuels fuel fab plant.

CHAIRMAN BROWN: So the only real plants of interest for the most part are --

MR. SMITH: On this slide.

CHAIRMAN BROWN: On this slide. Yes, I know what's on the next slide. I went there already. Are Honeywell and URENCO?

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

MR. SMITH: Yes, sir.

CHAIRMAN BROWN: Okay. Thank you.

MR. SMITH: Okay. Any other questions before I move on? Okay. Okay, fuel fabrication. The first three here are the three plants in the United States that produce fuel for the current facilities that produce fuel for the commercial reactors.

They're all licensed to possess only up to five percent enriched uranium. So therefore they are a Category III facility. AREVA has a facility located in Richland, Washington not far from the Hanford site.

Global Nuclear Fuels, as I mentioned they have a facility in Wilmington, North Carolina. And Westinghouse has a facility in Columbia, South Carolina.

These facilities have been around since probably the 1960s. They've made changes over the years. They've modified their process lines for added efficiencies, changes their process a little bit.

MEMBER POWERS: What motivates limiting the Cat III licensees to five percent enrichment?

MR. SMITH: Why do they limit themselves to that?

MEMBER POWERS: Yes.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

MR. SMITH: That's the commercial market at this point in time.

MEMBER POWERS: Yes. What motivates me to ask the question is we have been considering what the difficulty is or challenges would be in going to somewhat modestly more enrichment in the commercial reactor fuel to accommodate longer fuel lifetimes.

And clearly this is one of the barriers that we need to think about if you have a license that stipulates it at five percent and you want to have seven and a half.

You have to do something, okay. And so the question is why would one, what motivates us to put a five percent enrichment limit here? Is this one that I can send you a note and say I want to go up to seven and a half percent interest, enrichment and you say boy, that's interesting. Change your efforts how you are and that's good. Or is it one where we have a more involved procedure?

MR. SMITH: It would be a bit of more involved procedure. It would require a license amendment.

MEMBER POWERS: Yes, but license, there are license amendments and there are license

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

amendments.

MR. SMITH: Yes, this would be one that we would consider probably a complex license amendment.

MEMBER POWERS: Why?

MR. SMITH: We would have to look at it from a criticality safety standpoint. That's probably the biggest hurdle to it.

MEMBER POWERS: Okay, fair enough. Fair enough.

MR. SMITH: The MCNA requirements would probably still be the same because it's still a Category III facility at seven and a half percent. There are certain transportation aspects that might have to be considered outside from the amendment requests for the facility requirements.

But the primary would be criticality safety. The plant's been designed for five percent. So then they have to make some physical changes to the plant or modify their controls that they have to prevent criticality.

MEMBER POWERS: So crit is really your concern here which is one where you would presume somebody could handle?

MR. SMITH: Yes, sir.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

MEMBER POWERS: Okay.

MR. SMITH: Yes, we don't, we didn't tell them that they have to be at five percent.

MEMBER POWERS: They --

(Simultaneous speaking)

MR. SMITH: -- application and asked for a certain enrichment. And so we review and approve that.

MEMBER POWERS: Yes, and it's, there are of course a variety of neutronic challenges in going to higher enrichment. But if clad designers had their way, eventually people are going to be asking for higher enrichment, not to violate the category limits but rather to modest increases to accommodate longer fuel lifetimes. And the challenges inherent in that need to be anticipated.

MR. SMITH: Right. They would need to have an enrichment plant that would be able to produce up to that amount.

MEMBER POWERS: Doesn't seem to be a problem according to UNESCO.

MR. SMITH: Or URENCO? Yes, they're not currently licensed to do that. Probably not here or in Europe where they have three other facilities. But

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

they --

MEMBER POWERS: They think there's bigger regulatory challenges in Europe.

MR. SMITH: Okay. We did issue, they did request an increase in their enrichment level a few years ago to go from five to five and a half percent. So we did approve that as well.

MEMBER POWERS: Yes, but it's not, it doesn't involve changes and technology of the operation?

MR. SMITH: Of the enrichment plant?

MEMBER POWERS: Yes.

MR. SMITH: No. Not significantly, I wouldn't think so.

CHAIRMAN BROWN: Okay, now I need to calibrate myself now that we're down through Westinghouse. The plant that's, the facilities of interest are then Honeywell, URENCO, Honeywell source material converted to UF6. UF6 is given to URENCO. They produce up to five or five and a half percent --

(Simultaneous speaking)

MR. SMITH: The product is UF6.

CHAIRMAN BROWN: Product --

MR. SMITH: Is UF6.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

CHAIRMAN BROWN: Yes okay, product.

MR. SMITH: In smaller cylinders.

CHAIRMAN BROWN: All right. And then AREVA Global Nuclear and Westinghouse say give us X amount and they go build fuel pellets or whatever the configuration needed to put into our fire plants?

MR. SMITH: Yes, sir.

CHAIRMAN BROWN: Okay.

MR. SMITH: So moving down to fuel fabrication high enriched, we have two of those facilities at this time, BWXT in Lynchburg, Virginia and Nuclear Fuel Services in Erwin, Tennessee.

These are licensed to possess HEU quantities greater than 90 percent, therefore they are a Category I facility. They do also possess classified information and matter that's all associated with the Navy Fuel and technologies associated with that.

The difference here is that for the classified information of matter, the Department of Energy Naval Reactors is the cognizant security agency for that. We do play a role in it, although we defer to the Naval Reactors for the actual protection of the classified information of matter.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

For the enrichment plant, that possessed classified information. We are the cognizant security agency, so they have to follow our rules and we do the direct oversight of those.

CHAIRMAN BROWN: Okay. That is a committee note in the discussions. And I didn't say this earlier. If any of us open our mouth and start to say something that you know shouldn't be said, do not hesitate to stuff a rag in it. Just tell us right out. Don't wait, just tell us hey, you're encroaching on some stuff and I just soon not get involved in that. Okay? Don't be shy is what I'm telling you, or asking you.

MR. SMITH: Okay, all right. I mentioned the CSA role, Cognizant Security Agency role and the DOE's involvement there because that plays a factor into the regulation, the rule that --

CHAIRMAN BROWN: CSA role?

MR. SMITH: The Cognizant Security Agency.

CHAIRMAN BROWN: Okay.

MR. SMITH: The agency with primary responsibility for oversight. So because that plays a role the rulemaking which they'll explain a little bit later on.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

CHAIRMAN BROWN: So is DOE, that's the one for the Nuclear Navy --

MR. SMITH: The two Cat I's.

CHAIRMAN BROWN: Yes, okay. That's what my memory was. It's been a while.

MR. SMITH: And will be for the MOX facility as well.

CHAIRMAN BROWN: Okay.

MR. SMITH: That one's still to be determined. That final decision is end of May on that. There's still some time there.

CHAIRMAN BROWN: Okay, thank you.

MR. SMITH: Okay. So fuel fabrication mixed oxide. This is the facility that we have under construction now down at the Savannah River site in South Carolina.

It's been under construction for a few years now and will be a few more years as well before it actually gets to operating. This is a plutonium facility where they'll be bringing in plutonium from weapons to be converted into mocked fuel and used in commercial power reactors.

We do have one facility that's been licensed to do depleted uranium de-conversion. And so

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

what this facility does, it takes the waste, or it's called tails, from the enrichment plants, depleted uranium, and converts it to a form such that it can be disposed of.

The tails at an enrichment plant, the uranium is UF₆. That cannot be readily disposed of in the waste sites that we have right now. It has to be a more stable oxide to be buried. And so that's the primary purpose of this facility. I will go into more detail on that in a couple of slides. And that facility will be located in the same county in New Mexico as the URENCO USA Enrichment Plant.

CHAIRMAN BROWN: Thank you.

MR. SMITH: All right, next slide. So to add to your list of facilities that were of significant interest, we have to add the two Cat I's to it, DWXT and NFS.

CHAIRMAN BROWN: But they're not subject to this rule that they would be --

MR. SMITH: All of these facilities that I've just discussed would be.

CHAIRMAN BROWN: Has Naval Reactors been involved in this rulemaking?

MR. SMITH: We've been keeping them

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

informed of what we've been doing.

CHAIRMAN BROWN: I didn't ask that. Are they involved in the configuration of this rulemaking?

MR. DOWNS: Yes, so again, so Naval Reactors' involvement is as the cognizant security agency for the classified information at those sites. The NRC has jurisdiction as the cognizant security agency for the material at those sites.

So the potential safety consequences would fall under NRC. Some of the physical security aspects fall under NRC. So what you have is we have an exception in the rule language that would actually exclude classified, digital assets that are on classified systems under the accreditation of other federal agencies.

So that's where the digital assets on Naval Reactors classified networks would be excluded from the rulemaking. So that's how we've kept, as Brian's said, we've kept them informed.

CHAIRMAN BROWN: Have they followed their normal pattern and said we're not going to deal with you?

MR. DOWNS: Right.

CHAIRMAN BROWN: Include us.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

MR. DOWNS: Yes, we you know --

CHAIRMAN BROWN: We'll take care of ourselves. Am I phrasing that properly?

MR. SMITH: Well, they didn't phrase it quite that way.

MR. DOWNS: They never do. I'm just --

MR. SMITH: That's a good way to, that accurately captures the premise of what we're trying, we're trying to avoid dual regulation. Dual regulation is something that, you know, you've got two federal agencies fighting over the same thing with potentially different requirements, different guidance, different ways of looking at things.

But it would cause a lot of headache for our licensees. So we're sensitive to that and it's something that we're trying to avoid.

CHAIRMAN BROWN: So fundamentally the Naval nuclear program would be responsible for ensuring that they were protected from cyber attacks in whatever, I mean, in the manner in which they deemed necessary.

MR. SMITH: For the classified networks.

CHAIRMAN BROWN: For their, yes, for all the digital assets which deal with their product.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

MR. SMITH: Yes. We currently have an exclusion, as James said, in the Rule 4 classified networks.

CHAIRMAN BROWN: Yes I'm just, yes I understand the exclusion. But I mean --

MR. SMITH: They also have, Naval Reactors also has requirements for their contractors to protect, like, OUO type, Official Use Only networks as well. And so that's an area that we're still discussing with them, with them and NSA for the MOX facility as well.

So there's changes that DOE's considering and Naval Reactors are considering for the protection of those networks, and we want to see how that ends up before we add that exclusion into this rulemaking.

MR. DOWNS: And to clarify, Brian called those OUO networks. They're commonly referred to as unclassified networks. Those same entities have a third tier as well that are business networks.

MEMBER STETKAR: So called, just to make sure I understand it, so we've got classified and that's the Navy's business. We've got something in the middle, and we're still negotiating over that. And there's something at the right end, because I'm

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

going left to right, that are, you called it business. That would come under the purview of NRC, is that correct?

MR. DOWNS: It would. But that's true --

MEMBER STETKAR: If they could affect, you know --

MR. DOWNS: Safety or security.

MEMBER STETKAR: Safety or security.

MR. DOWNS: That's right.

MEMBER STETKAR: The consequences of concern we'll eventually get to.

MR. DOWNS: And so Naval Reactors has requirements in place for all three of those flavors of networks. Obviously they're graded requirements. But they're also in a state of flux right now. So we're waiting to see what information comes out as to what we can potentially exclude and again avoid this dual regulation.

MEMBER STETKAR: Thank you.

CHAIRMAN BROWN: Before you go any farther, so I'm trying to, again, just trying to categorize stuff a little bit for how we apply the cyber perspective to these. We've got the source guys that convert, we've got the enrichment guys.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

And those are material control fundamentally converting, you know, source material to some other stated material. So it's just spent nuclear material, not spent. Excuse me, I've got spent fuel pools on my mind. Special nuclear material.

So they build, that's the crunches or chunks of stuff that gets sent to people to fabricate fuel elements or fuel --

MR. SMITH: Enrichment plant since --

CHAIRMAN BROWN: And then they get parts of this material and then they have to control that as they make their fuel pellets and elements, rods, et cetera as they go and control those to ensure they don't get lost?

MR. SMITH: Yes, there are material control and accounting requirements under Part 74 that they have to comply with.

CHAIRMAN BROWN: Okay. One of the questions I might be asking later, and the reason I'm asking the question now or preparing you is the rules seem to deal with accounting, sabotage, radiological whatever.

And material control for the most part did

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

not deal, or didn't mention in my mind manufacturing or fuel pellet rod element manufacturing processes which have, and/or quality control of those materials, how they could be compromised by cyber. It only dealt with, seemed to only deal with material accountability and making sure it didn't disappear somewhere along the food chain.

So you don't have to try to answer that now, but it will come up later. I'm just planting the seed for in terms of how we apply these rule, the rule and the regulation to those particular parts of the overall fuel element generation process.

MR. DOWNS: We can talk to it briefly right now if you like. But basically the license, the NRC licenses are issued under the NRC's mission of protecting public health and safety and common defense and security.

The actual quality of that fuel that's being produced, that's a business concern for those licensees. That's not something that we really want to get involved in.

MR. SMITH: Yes, on the Part 50 side. There are requirements on them for the quality aspects.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

MR. DOWNS: Right, right. So right.

MR. SMITH: And they do perform quality checks of the fuel every rod, every pellet. They verify its location and each rod before it gets put into a bundle.

CHAIRMAN BROWN: Yes, but what if your process control and your monitoring and your quality control check are all lumped into a bunch of digital assets connected to the network and it could be hacked and could tell you well you think you've got this but you don't have this. You've got something else.

MR. DOWNS: Well, that's where the quality control on the Part 50 side, on the reactor side would pick up on that.

CHAIRMAN BROWN: Except --

MEMBER STETKAR: Let me try something --

CHAIRMAN BROWN: Go ahead.

MEMBER STETKAR: -- and maybe it's probably better when we get into the active and passive types of consequences of concern. But when I thought about this, if there could be an intrusion, let's call it that disrupts the normal manufacturing process, and that disruption could then lead to a so-called consequence of concern either because of safety

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

or security or materials accounting or whatever, then that digital asset would fall under the purview of this rule, right?

If it was strictly a business manufacturing, you know, creating this little clip that has to have some tolerance on it but could not affect any of those consequences of concern, that would be outside the scope of this rule, right?

MR. DOWNS: That's correct. You've captured it, yes.

MEMBER STETKAR: And that was part of my concern, okay in that --

MR. DOWNS: I know. But again, the NRC doesn't, aside from the fact that they have to meet the quality control Part 50 requirements for manufacturing this thing, that's not safety or security or --

CHAIRMAN BROWN: Well, I don't know. If you could produce random pellets that were fooled into some concentration and they were put in where they created a hot spot within a fuel rod --

MEMBER STETKAR: That's part of --

CHAIRMAN BROWN: -- one hot spot within the rod --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

MEMBER STETKAR: That's part of their quality control under Part 50 of the manufacturing.

CHAIRMAN BROWN: But where does that get factored into this whole cyber protection from intrusion or hacking?

MEMBER STETKAR: That's their business decision.

MR. SMITH: We'll talk about it --

CHAIRMAN BROWN: We care only about the accountability and we don't care whether somebody can be hacked and produce --

MEMBER STETKAR: I believe we care about safety, we're for safety --

CHAIRMAN BROWN: And that's safety, if we --

MEMBER STETKAR: But with health and safety and security.

CHAIRMAN BROWN: If we overheat and blow out a fuel rod because of it or several of them because they've got hot spots, isn't that a safety issue?

MEMBER STETKAR: Certainly care about that. We certainly care about that, and that's cared about under the manufacturing the same way as

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

manufacturing pipe to certain tolerances is controlled under Part 50, and we don't talk about cyber security of pipe manufacturers, do we?

MR. SMITH: We'll talk about --

CHAIRMAN BROWN: And it seems to me that pipe manufacturers is a little bit different than --

MEMBER STETKAR: Not necessarily.

CHAIRMAN BROWN: Well, I guess we --

MR. DOWNS: But you've captured a good point there. I mean, we had, this rule isn't really -
-

CHAIRMAN BROWN: You're trying to make me feel good.

MR. DOWNS: No. You've captured a point. It's this rule, this proposed rule isn't focused on the supply chain concept for fuel for nuclear power plants. That isn't something that we focused on, and it's --

CHAIRMAN BROWN: That's what I -- you're telling me I understood what the rule says, and that's what blows my mind because I wasn't sure whether I understood it or not.

MR. DOWNS: Yes, you're on it.

CHAIRMAN BROWN: Now it's material

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

accountability. And as John phrases it, there's the manufacturing part, as what you stated also, falls under this business part relative to the actual manufacture of elements and/or processing and/or quality control and assurance, et cetera.

MEMBER STETKAR: I'm trying, at least in my mind I'm trying to look at kind of the extremes. There's a grey area in between. And that grey area can be kind of dicey. That's each, I think, facility needs to look very carefully at their processes to see if an intrusion on their control systems could result in any of, at least under the aspects of this rule, any of these consequences of concern.

Now that intrusion might also result in not so good, you know, control over enrichment or other aspects of the manufacturing.

CHAIRMAN BROWN: Yes, when I read --

MEMBER STETKAR: So there's that, you know, that sort of grey area in between. But something that's strictly related that can't result in -- a manufacturing process that can't result in any of consequences to worker health and safety, public health and safety, security, materials accounting.

CHAIRMAN BROWN: Well, largely fell under

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

the one called active, didn't it? I mean, it's --

MEMBER STETKAR: Well that's, I mean yes, that's where I focused. That's why I said later when we talk about active, perhaps that's --

CHAIRMAN BROWN: That's I think more of the sense because the, I've forgotten what term you used.

MEMBER STETKAR: Consequences?

CHAIRMAN BROWN: The latent, yes latent.

(Simultaneous speaking)

MEMBER STETKAR: The latent stuff is more focused toward, in my mind, protection functions that would be identified as IROFS in these facilities. Given a perturbation from some other source, those things need to function appropriately and be like a reactor protection system, you know, reactor safeguards or something like safeguards actuation in the reactor.

MEMBER MARCH-LEUBA: So before Charlie starts getting paranoid about time, we are scheduled until 5:00 and I hope you haven't made dinner plans for 5:30.

CHAIRMAN BROWN: Yes, they can make dinner plans for 5:30. We're on eight slides of 61 or 62 and

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

we will make it.

MEMBER MARCH-LEUBA: Okay. Changing the topic, I wanted to ask you from the point of view of proliferation, the diversion of SNM material, whose responsibility is it? Is it NRC?

MR. SMITH: It's the NRC's.

MEMBER MARCH-LEUBA: Because in other countries it will be IAEA will be looking over that. But here is NRC?

MR. SMITH: Yes. We have Part 74 which is our material control and accounting programs.

MEMBER STETKAR: Well, but IAEA --

MR. SMITH: IAEA is involved in one of our, well several of our facilities but at different significance levels.

MEMBER STETKAR: So that's in the same case that other countries have -- IAEA isn't the primary controller for other countries, I don't believe. They're --

MEMBER MARCH-LEUBA: Well, there is a European, what they call that, the primary. But the IAEA is in all the regions of Europe, they're there every other week.

MEMBER STETKAR: Yes. They have full IAEA

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

safeguards applied to the three URENCO plants in Europe.

MEMBER MARCH-LEUBA: But here the NRC follows that? I mean, you actually go there and count the 30(b)s that come out of the facility before they leave?

MEMBER STETKAR: We don't count every one before they leave and I don't think IAEA does that as well.

MEMBER MARCH-LEUBA: So you just believe their paperwork?

CHAIRMAN BROWN: You count what? I didn't catch that.

MEMBER MARCH-LEUBA: 30(b) is the name of the container where you put the --

(Simultaneous speaking.)

MEMBER MARCH-LEUBA: 30(b). 30 bravo.

CHAIRMAN BROWN: Oh, okay.

MEMBER MARCH-LEUBA: Three zero bravo.

MR. SMITH: You'll see a small picture of one as we go through the slides. But we do an inspection program on the material control and accounting, and we go out to each of the Category III sites at least once a year to inspect that program.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

There are reporting requirements that go into DOE/NRC database called NMMSS, N-M-M-S-S. They have to report into that monthly. They have to report shipments of material.

So there's a lot of record keeping involved, and we keep a close eye on that. For the Category I facilities it's a much more in depth inspection because the requirements are much more detailed for a Category I facility.

So we pay close attention to those. But IAEA is not really involved in the two Cat I's. They are involved with URENCO, but only at a lower level, not full IAEA safeguards. It's under the reporting protocol I believe is what it's called for right now.

They always have the choice of going to full safeguards in the future, but not at this time.

MEMBER SUNSERI: Can you tell me one more time where the enrichment is done for the Category I fuel fabrication facilities?

MR. SMITH: Currently there is no enrichment being performed to produce HEU in the US.

MEMBER SUNSERI: Okay. So there's just stockpiles I guess.

MR. SMITH: There's just stockpiles.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

MEMBER CHU: Quick question. So NNSA is responsible for the weapons side, right? And you guys are responsible for the commercial facilities?

MR. SMITH: Yes.

MEMBER CHU: Am I correct?

CHAIRMAN BROWN: Say that again, Margaret. What was the first one?

MEMBER CHU: I say NNSA is responsible for the weapon side.

CHAIRMAN BROWN: Okay. NNSA is who?

MEMBER CHU: DOE and NNSA, yes.

CHAIRMAN BROWN: Oh, okay. Thank you.

MEMBER CHU: Yes.

CHAIRMAN BROWN: I didn't know the alphabet soup.

(Off microphone comments)

MR. DOWNS: Where you get into that grey area is where the nuclear fuel for the Nuclear Navy. That's where it's not really weapons but it's high enriched but it's, as Brian stated, these two facilities are not on Department of Energy reservation, so that's why the NRC's got involved in those.

CHAIRMAN BROWN: That was an interesting

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

point that I guess I've forgotten. You said there's no HEU enrichment currently?

MR. SMITH: That's correct.

CHAIRMAN BROWN: And now remember -- how long's that been? It's been a while, hasn't it?

MR. SMITH: Since Portsmouth shut down. Well, they stopped producing HEU before they shut down the GEP. GEP shut down about ten years ago.

CHAIRMAN BROWN: Okay.

MR. SMITH: So it was probably 1990s maybe when it stopped producing HEU.

CHAIRMAN BROWN: I remember having arguments about that.

MR. SMITH: DOE --

CHAIRMAN BROWN: Not me but --

MR. SMITH: DOE did a study about a year ago in looking at the current levels of HEU and the future need for enrichment services like that. And I think they determined that they have enough for at least the next couple of decades, all depending upon the needs of the Navy.

CHAIRMAN BROWN: The Navy was conservative in other ones, in their request earlier.

MR. SMITH: I never saw --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

CHAIRMAN BROWN: That's it, we don't need any more on that.

MR. SMITH: Okay, pictures. Some process fundamentals at a high level. I've already talked about some of these. The first step that we license here on the fuel cycle side is uranium conversion which see there's a picture of yellow cake. Not all yellow cake is yellow, this one just happens to be.

MEMBER POWERS: In fact, very little of it nowadays is. That's mostly sodium urinate from when I was a kid. In the processes nowadays they don't take, they don't do a basic extraction on the thing so you don't, what you get out is an ugly commonly referred to baby shit brown.

MR. SMITH: Technical term.

(Simultaneous speaking)

MR. SMITH: Honeywell gets their feed material from all over the world, Canada, the US, Kazakhstan, Australia. There's various sources, and depending upon the producer of it it comes out in various colors, and various qualities as well.

And so Honeywell's process is different from the other processes in the world, and there aren't very many conversion plants. Canada has one,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

Russia has some, France has one, but there's not very many. And it's the only one in the United States.

And their process is able to produce very pure UF₆ whereas other processes are not quite as pure. The facility there in Metropolis, Illinois used to produce other fluoride related chemicals, but they stopped that several years ago and they only produce UF₆ at this time. And the picture you see there in the middle is the main process building for this facility.

Simple process, basic steps. There as you see they take the U-308, add some hydrogen, get uranium oxide, start adding fluorine to it through two steps, and ultimately have the UF₆.

UF₆ comes out of the process as a liquid. UF₆ in its most hazardous state is as a liquid. If it's, if you lose containment of it, it readily goes airborne.

When it does, it interacts with moisture in the air, produces UO₂ F₂ which basically it's heavy, it falls out, basically this particulate, but it produces hydrogen fluoride. And that's very, very caustic, very dangerous to a person's health in low concentrations.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

And so they produce cylinders. These are called 48 either X or Y. It's the one that's used for transport. So they typically weigh about ten tons. And those are what are shipped off to enrichment plants throughout the world, the one in the US and elsewhere.

As you can see, they're trucked. They can also be shipped by barge ship.

CHAIRMAN BROWN: No airplanes?

MR. SMITH: It's a little heavy for airplanes.

(Laughter)

MR. SMITH: So that's Honeywell. Any questions? Like I said, it was begin operation in I think 1956 and it's just across the river from the Paducah Gaseous Diffusion Plant. So a lot of their product went directly across the river, but Paducah has been shut down for a couple of years now and is no longer under NRC regulatory purview. It's all back, given back --

CHAIRMAN BROWN: Oh, Honeywell's not?

MR. SMITH: Honeywell is. Paducah, the NRC used to have regulatory oversight for two of the gaseous diffusion plants under 10 CFR Part 76. But

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

those have been shut down and have been returned back to DOE oversight for decommissioning.

CHAIRMAN BROWN: Okay. You're talking about Paducah, Kentucky, right?

MR. SMITH: Yes, sir.

CHAIRMAN BROWN: Okay.

MR. SMITH: Yes. It's right across the river from Metropolis, Illinois. Okay, next? Okay, enrichment. In this case we're only talking about gas centrifuge enrichment. As we mentioned before, the feed material is source material, natural uranium.

It goes through the enrichment process and there's two components that come out, product, special nuclear material, also UF₆ and the tails as they call it, the waste material, depleted uranium is source material.

As you can see there, they take the 48 extra wide cylinders from a conversion plant, they place it into what used to be autoclaves when they used to liquefy it. At the URENCO plant it's what's called a feed chest. They do not liquefy it.

What they want to do is they want to get gaseous UF₆ into the centrifuge process, into the cascade halls. And when they do is they provide a

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

little bit of heat to it and draw a vacuum on it. And it goes through sublimation, it goes directly to a gas and gets pulled into the cascade hall.

And once it's in there, it will go through one cascade. There are numerous cascades at URENCO. And so basic centrifuge design there.

So the product is placed into 30D cylinders, 30 inch diameter cylinders. And those will weigh about two and a half tons. The tails will go into either a ten ton cylinder, basically the same cylinder that was used as feed material, or it could be a 14 ton cylinder which is only used for storage. And those are 48 inch diameter. That's the 48 extra wide.

With respect to laser enrichment, the one facility that we have licensed to do that, their process is very similar except for the box in the middle. They will also utilize UF6 as feed and product. But the enrichment piece is a lot different.

CHAIRMAN BROWN: So the UF6 enriched that goes off to one of the three fuel elements is liquid or gas?

MR. SMITH: It's a solid.

CHAIRMAN BROWN: Oh, it's a solid. That's

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

what I was thinking but then --

MR. SMITH: Normal temperatures it's a solid.

CHAIRMAN BROWN: Okay. So once it cools, it solidifies.

MR. SMITH: Yes, I mentioned Honeywell produces the -- it comes out of the process as a --

CHAIRMAN BROWN: Comes as a gas --

MR. SMITH: -- liquid --

CHAIRMAN BROWN: Oh, it's a liquid.

MR. SMITH: -- but then it solidifies.

CHAIRMAN BROWN: Thank you. Okay.

MR. SMITH: I should have said that.

CHAIRMAN BROWN: No, you did and I just forgot.

MR. SMITH: No, I didn't say it. Basically it has to sit for at least five days before it can be transported to ensure that it's fully solidified.

CHAIRMAN BROWN: And that's out of URENCO? Who ships liquid?

MR. SMITH: Nobody ships liquid.

CHAIRMAN BROWN: Oh, okay. So it's solid when it comes out of Honeywell?

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

MR. SMITH: When it's shipped, yes.

CHAIRMAN BROWN: Yes, okay.

MR. SMITH: But the process itself is when it comes out of the process into the cylinder, it's a liquid. And it will stay partially liquid for about five days until it fully solidifies.

CHAIRMAN BROWN: Okay, so when it cools, it solidifies then?

MR. SMITH: Yes. Okay, so at the enrichment plants, as I said before, liquid UF6 is when it's in its most hazardous state. As a solid it's not that significant.

So at the URENCO facility and what would be at the other future enrichment plants. The only place where you would have liquid UF6 is in a true autoclave where you have the product cylinder and they want to do what's called homogenation and sampling for the QA purposes.

You want to draw a small amount of product from each product cylinder into what they call these little sample bottles. And that's for the QA process. And those go along with those to the fuel fabrication facilities as well.

So when it gets there they'll verify the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

enrichment level to ensure that that's what they have in the cylinder.

CHAIRMAN BROWN: Okay.

MR. SMITH: But those, when it's liquid it will stay in the cylinder until it's, will stay in the autoclave until it's solid again. So no real movement of liquid cylinders on site except for Honeywell.

CHAIRMAN BROWN: Okay.

MR. SMITH: Okay, next slide. Oh did you have a question? Okay.

MEMBER POWERS: The hazard from your feed is that you release the vapor, it hydrolyzes. And you focused in your almost parenthetical discussion on the HF that gets produced in that hydrolysis.

Do we have a good understanding of the aerosol of its uranium oxifluoride that is the condensed product of the hydrolysis process. Do we have a good understanding of that aerosol?

MR. SMITH: Yes, sir. Yes, we have, the NRC has a program called RASCAL. It's one that we utilize for a power reactor --

(Simultaneous speaking)

MEMBER POWERS: We're extremely familiar with RASCAL which has an absolutely primitive and

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

archaic model of aerosol physics in it. So it certainly can't accept any sophisticated input. The question is do we have the sophisticated input if we had a decent aerosol transport model in the Agency, which we don't.

MR. SMITH: Okay. Well RASCAL does address UF6 releases as well, and that's one of the programs that we do rely upon. Our licensees utilize it.

MEMBER POWERS: And how unfortunate for --
(Simultaneous speaking)

MR. SMITH: There are other programs. CAMEO is one. HGCIS is another one.

MEMBER POWERS: It's not the computer code, it's the question of all those computer codes require as input some description of the aerosol. And my question is do we have that, do we have anything approaching the technically defensible description of that aerosol?

MR. SMITH: I have to get back to you on that.

MEMBER POWERS: Yes, I'm sure --

MR. SMITH: I don't have anything further.

MEMBER POWERS: It's not your primary, I

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

just thought you might know because I mean, it's extremely difficult to work with these hydrolysis products because they produce horrible fractal aerosols and things like that.

And most of the work gets done in the stimulant materials, things like titanium tetrachloride, things like that that hydrolyze approximately the same way but it's not the actual material.

And you always wonder about whether you have an understanding because we understand the hazard of HF. We can't compute it's transport very well, but we understand its hazard. But we pretty well assume that the aerosol doesn't transport very far.

MR. SMITH: Yes, the UO2 would typically fall out.

MEMBER POWERS: And of course there's always a question about how good your assumptions are in these matters. And I just don't have a feeling for it. I mean, I've spent a lot of time working with hydrolysis aerosols and they're rather benign if you can get the hydrolysis process to occur when the gas is rather concentrated. They're not so easy to work with when you have a dilute hydrolysis process taking

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

place.

MR. SMITH: Okay. Well, we hope that our licensees minimize any releases of UF6. That's one of the main goals.

MEMBER POWERS: Well, I mean, it is their biggest workplace hazard for the --

MR. SMITH: Yes.

MEMBER POWERS: I mean, you went through the challenge at sampling. It's the same challenge every time you connect one of the valves to do things with it. I mean, it is their hazard and you have not lived until you have had an HF burn.

MR. SMITH: Yes, those can be significant. I was at Honeywell one time when they had a very small puff release and you could smell it.

MEMBER POWERS: Oh, really?

MR. SMITH: Just walking around outside, a very, very low concentration, you can smell it.

MEMBER POWERS: Can we move on now? You're going to go off into this deadly bill stuff.

MR. SMITH: Yes.

MEMBER POWERS: Instead of the chemistry and aero stuff.

MR. SMITH: Yes, yes.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

MEMBER POWERS: Well then I am --

(Simultaneous speaking)

CHAIRMAN BROWN: Okay, go ahead.

MR. SMITH: So fuel fabrication commercial use. The product that comes out of an intermission plant as we mentioned is UF6 in a 30D cylinder. So that's what they receive primarily.

They have to convert it to an oxide, UO2, so that's the first part of their process, the conversion piece. And then once they have the UO2 powder, they then create the pellets, the pelletizing process.

They'll clean up the pellets, polish them off, ensure they're the right size and shape and quality to be placed into the fuel rods. As part of that process is what they call uranium recovery, the big loop there in the middle.

Any scrap that they have onsite they will try to recover. And then it's, that's part of a chemistry, part of the chemistry in the plant is being able to recover that uranium and put it back into the conversion process and back into the fuel pellets.

And at least two of the three LEU plants have that process. I think a third one ships their

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

waste off site. So, like, the sweepings on the floor, any scrap pellets go into that process. There's chips that come off of the pellets as it moves through the line. That goes into the uranium recovery process as well.

And then they have the off gas and wastewater treatment processes as well. So once the pellets are ready to go, they then stuff the rods and produce the fuel elements and apply their quality assurance measures to the final assemblies and to the rods as well, all part of the process. From there, they're shipped off to the power plants.

MEMBER POWERS: It is a triumph of American technology in your center box there. I mean, it looks so, it's so simply displayed and yet it is so important and has been, it's so much better than 20 years ago even. Breathtaking.

MEMBER STETKAR: Brian, you talked about sweepings on the floor. Well, I mean, he talks about it so I can talk about it.

(Simultaneous speaking)

MEMBER STETKAR: What I wanted to get to is that is covered under the facilities material accounting program, right?

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

MR. SMITH: Yes, sir.

MEMBER STETKAR: Which is subject to this rule?

MR. SMITH: Yes.

MEMBER STETKAR: So I want to get back to that when we talk about materials control and accounting, under this rule for these types of facilities.

MR. SMITH: Okay, thank you.

MEMBER STETKAR: That's just firing a warning shot so you can think about it.

MEMBER POWERS: Giving you a heads up, Brian.

MR. SMITH: Sure, sure.

MEMBER POWERS: You or James or whoever is going to be doing it.

MR. DOWNS: Yes, I'm the one who's going to actually have to field that later. You know, Brian will be gone at that point.

MEMBER POWERS: I understand he's taking notes.

(Laughter)

MEMBER STETKAR: All right, go ahead, Brian.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

MR. SMITH: Okay, so --

MEMBER STETKAR: Yes, James is going to have to catch up here.

MR. DOWNS: That's right. That's right.

MR. SMITH: All right, the next slide, please. Okay, a little bit of difference for the fuel fabrication HEU side. Obviously their enrichments are a lot higher. The criticality controls are a lot more significant, so it doesn't take as much material to have a criticality.

And as we mentioned earlier, there are no currently NRC licensed programs for producing high enriched uranium or within the DOE program as well.

Mix lot side, the MOX plant is also going to be producing fuel. That plant will be much more complex than the Category III facilities that we have. Specific reminder, this is a Category I facility.

As I mentioned, it brings in the surplus weapons grade plutonium and uranium oxide to make the MOX fuel. In a way, it's similar to reprocessing plant, the complexity of the chemical processes involved.

We see some of the steps in the process there. But once you get into the pelletization and

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

the rod piece, that part of the plant will be a lot similar to the current Cat III facilities.

CHAIRMAN BROWN: Go ahead.

MR. DOWNS: And notice, to keep ourselves out of trouble, we didn't include any pictures on this.

CHAIRMAN BROWN: That's good. Okay, go ahead.

MR. SMITH: Okay.

MEMBER POWERS: The Committee has reviewed the MOX facility.

MR. SMITH: Yes, sir.

MEMBER POWERS: And enough said. Yes.

MR. SMITH: Yes, we have not issued the license for that yet, for the regulations. They have to complete construction first and they have to verify that was constructed in accordance. Then we issue a license.

MEMBER POWERS: And heaven only knows when they will complete in --

(Simultaneous speaking)

MR. SMITH: Yes. So depleted uranium de-conversion, this is what I mentioned earlier. There are two plants in the United States that are operated

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

by DOE that do this. They follow a little bit different chemistry process here.

But the primary purpose, there's this company called international isotopes. They wanted to do this process for the purpose of producing really pure fluorine to be sold in the commercial market.

The enrichers in the US used to be, well DOE has all of the tails that were produced at the gaseous diffusion plants. Those need to be de-converted such that it can be disposed of.

They have two plants that are doing that now that will take several decades to get that done. But we do have URENCO USA is producing tails now that will ultimately have to be converted and disposed of.

And so International Isotopes wanted to provide that service to either DOE or to URENCO. And so this is the chemistry process here. So as the disposal piece here would either be depleted uranium oxide or DU308 similar to the form that goes to Honeywell for conversion.

CHAIRMAN BROWN: Is this the stuff we fight over for low level waste? Is that stuff the disposal part? Okay, that's --

MR. SMITH: The Part 61, it was a big

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

issue and --

CHAIRMAN BROWN: Yes, okay.

MR. SMITH: -- the Part 61 rulemaking.

CHAIRMAN BROWN: All right, that's enough. I don't, I just wanted to confirm that I knew what we were talking about.

PARTICIPANT: Margaret's probably --

CHAIRMAN BROWN: I know, Margaret. All right, go ahead, Brian. Thank you.

MR. SMITH: Okay. Okay, now we want to get into some of the regulatory aspects of it. We've already mentioned source material, special nuclear material, security, MC&A and classified information. They're all covered by different parts of the regulations.

Like, the power reactor is where you probably have Part 50 and rad protection Part 20. There's conversion facilities, de-conversion facilities, those that produce or those that possess source material licensed under Part 40, and those that possess special nuclear material such as fuel -- enrichment plants are licensed under Part 70.

CHAIRMAN BROWN: So Part 40 is Honeywell, Part 70 is AREVA et cetera, the three --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

(Simultaneous speaking)

CHAIRMAN BROWN: Yes, okay.

MR. SMITH: But they would also have, say URENCO, they'll have their license under Part --

CHAIRMAN BROWN: Yes, I got that.

MR. SMITH: -- 30, 40, and 70. Thirty is byproduct material, cesium, cobalt, check sources and such. Part 73 is our physical security requirements. Also after 9/11 we instituted some security orders, Brad will touch on those in a few minutes.

Part 74 is where we have our material control and accounting. Within Part 73 and 74, we have requirements based on the categories of the facilities, Categories I, II, and III. And so it's kind of a graded approach to security and a graded approach to MC&A. So the higher enrichments that you have, Categories II and I --

CHAIRMAN BROWN: MC&A is material control and accounting?

MR. SMITH: Yes.

CHAIRMAN BROWN: Thank you.

MR. SMITH: Kind of like an inventory program of your rad material so that the higher the category, the more strict the controls, both from an

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

MC&A and fiscal security standpoint. Part 95 covers the protection of classified information.

Okay, so one final area to touch on before I turn it over to Brad, and this has to do with what we call our integrated safety analysis in Part 70, it's subpart H. This is another topic that we previously briefed ACRS on, back when Commissioner Apostolakis was part of ACRS.

His issue was PRA versus ISA. He was a big PRA opponent. But because of our facilities being so diverse in what they do and how they do it, ultimately the decision was that we would stay with the ISAs, integrated safety analyses.

And so this was a rule that went into the regulations back in the year 2000 and really started to be enforced after we'll call it ISA summaries were reviewed and approved in the mid-2000s to late 2000s.

And what the integrated safety analysis requires is for these facilities, these major facilities that we've been talking about, primarily those licensed under Part 70 to take a look at their facility, to determine what are the different types of accidents that they can have on site. All the different types of accident scenarios, and look at the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

consequences from those, and determine whether or not they exceed certain thresholds.

And we have high, well in the rule we define high consequence events and intermediate consequence events. And we'll talk about what those thresholds are on the next slide.

But if they, in looking at the licensees and looking at the consequences from various accident sequences, exceed say a high consequence event threshold, then they have to make that accident sequence highly unlikely.

Similarly, for an intermediate consequence event threshold, if one of those is exceeded, that sequence then needs to be made unlikely. So what does highly likely and unlikely mean?

Those definitions are proposed to us by the licensees and they can be either qualitative or quantitative. And for the most part they're qualitative even though they have some numbers associated with them. They are, we consider them mostly qualitative.

They are required to have, to limit the risk of nuclear criticality. For new facilities they have to have the double contingency principle in

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

place. We also have baseline design criteria for new facilities or new processes that exist in the facilities that we would have to address.

The Part 40 licensees, Honeywell and International Isotopes, although not required to have an ISA, they both have produced one and are tied down in their license.

CHAIRMAN BROWN: You said Part 40.

MR. SMITH: Yes, sir.

CHAIRMAN BROWN: So that would be Honeywell --

MR. SMITH: And International Isotopes.

CHAIRMAN BROWN: Okay.

MR. SMITH: We're here to talk about digital controls. So with respect to how licensees make these events either highly unlikely or unlikely, they have to put controls in place.

Those controls can be administrative controls, enhanced administrative controls, passive features or active features. And digital instrumentation controls have been utilized as part of some of the IROFS at these sites.

There are quite a few administrative controls at these facilities, but there are some

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

digital controls mixed in as well.

CHAIRMAN BROWN: Are the digital controls software based by computers or are they what's called combinational logic or FPGA non-software based controls.

MR. SMITH: I think there's a mix.

CHAIRMAN BROWN: Is it a mix?

MR. SMITH: It's a mix.

CHAIRMAN BROWN: Do you make any -- one of the questions later under the cyber discussions, the rule and stuff, I didn't see any real differentiation relative to the types of digital from a design technology standpoint so that, well I don't want to do that now. It's when we get off into the regulation and how you all are treating these. If I can remember this one that long.

MR. SMITH: Okay. So one aspect to clarify is they identify these IROFS, or items relied on for safety. For the most part, licensees have identified more than IROF for each accident sequence. So they don't have what are called, well a couple do, what are called sole IROFS where they're only relying on one control to prevent or to mitigate the accident sequence from happening or the consequence from being

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

as severe.

For the most part, licensees have at least two, three, or four IROFS for every accident sequence. So there will be a mix of controls in there, either administrative as I went through the whole list, some being digital.

And each of those have to be able to prevent the sequence from happening. So that's a factor when James starts talking about the rule later on this afternoon.

MEMBER STETKAR: And James, take notes because I want to delve into that a little bit more when we get into part of the guidance and the rule. It's not appropriate to talk about it now. It's better later.

Brian, let me, while we're on this slide here, you did mention that we had discussions back through history regarding ISAs versus PRAs for these types of facilities. And we clearly understand what they're doing today.

And we've heard anecdotally I think that perhaps the things that they're doing that were initially thought to be easier than a PRA are much more complex than what you might actually do for a

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

real risk assessment and that the number of IROFS that they are identifying and tracking and monitoring, maintaining perhaps might be larger than what you might derive from a real risk assessment.

Pertinent to today's meeting, if a licensee came in and proposed a risk informed approach to complying with this rule such that I rank order my digital assets by risk, not consequence but by risk of the scenarios, would the staff entertain that?

MR. SMITH: Sure.

MEMBER STETKAR: So if I did a risk assessment and actually had a frequency of scenarios and said I'm going to use risk now, frequency and consequences to focus on my protection against cyber intrusion, is that in any way, shape, or form prohibited under the regulations or the guidance?

MR. DOWNS: No, it wouldn't be prohibited. There would be a lot of scrutiny though on the frequency discussion there.

MEMBER STETKAR: Well, there's scrutiny on frequency for, you know, earthquakes and floods and LOCAs and steam generator ruptures and all those other things too.

MEMBER POWERS: I bet you would run into

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

having lots of exemptions because ultimately what he's going to do is he's going to go through and rank his IROFS. And he's going to come down with a much smaller set of IROFS that he's going to protect.

And I think you run into problems in that you're going to have to give him exemptions from some things in the regulations. I don't know that for a fact.

MEMBER STETKAR: And I don't know how they're --

MEMBER POWERS: I mean, ultimately the only reason to do this is to rank the IROFS --

MEMBER STETKAR: Exactly.

MEMBER POWERS: -- because there are too damn many of them.

MEMBER STETKAR: Yes, yes. Or to some, yes. I mean, however you want to come to that conclusion.

MEMBER POWERS: But you know, I would bet that you would end up having to give exemptions. I mean, it's not prohibited but you're just going to run into --

MEMBER STETKAR: Well, but I mean, it's --

MEMBER POWERS: -- you're going to run

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

afoul of the clear written language in the regulation.

MEMBER STETKAR: But it's the same notion for a power reactor. I can come in with a license, a risk informed license amendment and --

MEMBER POWERS: It can be done.

MEMBER STETKAR: -- change my tec specs. You know --

MEMBER POWERS: Here they've got a different set of problems.

MEMBER STETKAR: True.

MEMBER POWERS: They went with a technology that's really common in the chemical industry. And it just runs afoul in heavily regulated areas.

MEMBER STETKAR: Yes. And on the other hand if it becomes, it's really up to the licensees. If it's too burdensome on the licensee and the licensee wants to take a different approach, I'm trying to probe the notion of how the staff would react to that. And I've got a little bit of initial reaction.

MEMBER POWERS: I think that, I mean, I think I agree. Perfectly feasible it's going to get a lot of scrutiny, fair enough, that happens. You don't

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

have a template.

I mean, one of the motivations that pervades here is all the facilities are very different. So you can't get templating the way we can with the reactors and whatnot.

But clearly the MOX facility would have benefitted greatly by going through that because they just ended up wrapping themselves around the axle with all their IROFS. And you end up, all IROFS in this world are equal, except they're not.

MEMBER STETKAR: Thanks.

CHAIRMAN BROWN: Yes, relative to that question there's no words in the rule that say risk, is devoid of the word risk. I mean, I just went and looked for the word risk in the rule and didn't find it.

If you go into the reg guide it does mention under the cyber security program management it mentions risk informed policies, processes, et cetera. So while the rule neither excludes, it doesn't exclude nor allow or promote, the reg guide, proposed reg guide at least has the words in it somewhere.

I mean, how extensive, I was a little concerned that you were a little bit more ambivalent

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

than I would have anticipated in response to John's question, that's all.

MEMBER STETKAR: Where I was going is, and I don't know the legal, my eyes tend to glaze over when we get into legalities of rulemaking. But where I was headed, and I don't know the appropriate time to discuss it but I wanted to kind of throw it out on the table now because we have this slide up here is should the rule allow licensees to use a risk informed approach, explicitly allow.

CHAIRMAN BROWN: The rule or the --

MEMBER STETKAR: The rule.

CHAIRMAN BROWN: Oh, the rule.

MEMBER STETKAR: I mean, should that be in the rule. I mean, in principle, a licensee can come in with anything that satisfies the rule, as long as the staff doesn't somehow summarily say you can't do that.

CHAIRMAN BROWN: Well, it's interesting you ask that question because on Page 23 of the reg guide it says --

MEMBER STETKAR: But that's a reg guide.

CHAIRMAN BROWN: I know, I'm just saying the rule says nothing but the reg guide actually says

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

that NRC intends for a licensee to focus their cyber security efforts to effectively protect against threats associated with risk significant impacts. In other words, grade it relative to impact.

MEMBER STETKAR: But in the context of everything we're going to be talking about today, that notion of risk is solely focused on a consequence assessment, not on frequency in consequences.

CHAIRMAN BROWN: Yes, I agree.

MEMBER STETKAR: It's a strange use of the term risk.

CHAIRMAN BROWN: I don't disagree. Don't start, David, please.

MEMBER STETKAR: You caught me using the word risk. Or common misuse of the word. Misuse of the word risk, yes.

MEMBER MARCH-LEUBA: Hey, can I change the topic a little bit back to this slide. When you talk about high consequence event, can you give me a visual? For example, in the URENCO plant which I'm more familiar with, what would be a high consequence event?

MR. SMITH: Let me go to the next slide, James.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

MEMBER MARCH-LEUBA: Yes, that would be perfect.

MR. SMITH: Next slide.

MEMBER MARCH-LEUBA: I've been there and the closest hotel is 45 minutes away, and believe me, the drive is not --

(Simultaneous speaking)

MR. SMITH: I've been there many times myself. But there is the town of Eunice only a couple miles away.

CHAIRMAN BROWN: Let me pause for just a minute. When you get at an appropriate point for a break, tell me.

MR. SMITH: This is my last slide.

CHAIRMAN BROWN: Okay. So when we finish this one I'll tell everybody if you have to hold it, hold your horses for a few minutes. Go ahead.

MR. SMITH: So you had a question about what could be a type of accident at URENCO that would exceed these thresholds. Is that essentially what you were --

MEMBER MARCH-LEUBA: Yes.

MR. SMITH: Okay. From a safety perspective, if they were to have a criticality, I

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

mean, it's possible at the plant.

MEMBER MARCH-LEUBA: But the criticality is prevented by geometry.

MEMBER POWERS: No, I think the biggest hazard would be a chemical worker --

MR. SMITH: The biggest hazard is chemical.

MEMBER POWERS: Yes, worker chemical is probably dominant at Eunice.

MR. SMITH: I would say, and you would probably agree, that the URENCO facility is one of our less risk significant facilities, fuel cycle facilities just because of the way the plant's designed, its simplicity.

MEMBER MARCH-LEUBA: We're worried about cyber security here which is a bad actor -- work and spending a lot of effort and time and money trying to produce something bad. And killing a couple of employees is really bad, but it won't make it to CNN.

MEMBER STETKAR: It will make it to CNN, but only for a couple of days.

MR. SMITH: Preventing a criticality is one of the Agency, NRC's strategic goals, that's one of the top measures.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

MEMBER MARCH-LEUBA: That's where all the pipes are less than four inches. Some are six.

MR. SMITH: They do have some solutions, some materials and solutions. They have a waste process, low concentrations there as well. But it's an area that has to be controlled to prevent criticalities.

But safety is only one aspect of it. Security is another. And material accounting is another. So those aspects are important there. But from a URENCO standpoint, I would see this to be a low impact rule.

Just to clarify earlier, we talked about classified networks at Cat I. URENCO has classified networks as well. We are the security overseer for the classified information at URENCO.

We utilize Department of Energy to do the accreditation of the classified networks. So those classified networks would be excluded from the rule as well, any digital assets on those networks.

MEMBER MARCH-LEUBA: So they're excluded from the rules?

MR. SMITH: It would be excluded.

MEMBER MARCH-LEUBA: Because they're

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

already implemented?

MR. SMITH: Very high, stringent controls on those networks.

CHAIRMAN BROWN: By other federal agencies or by NRC?

MR. SMITH: Ultimately the requirements comes out of Part 95. It's the motherhood requirement. But they follow a DOE set of programs and controls for classified networks.

CHAIRMAN BROWN: All right, thank you.

MR. SMITH: So this is the final slide for me, gets to the consequence thresholds that I mentioned. And this is what we have in our rulemaking in subpart H of Part 70.

The radiological thresholds are prescribed in the rule. The chemical ones are not except for the public uranium intake. That's actually a chemical threshold limit, impacts the kidneys.

From a chemical aspect this is something that you may not be that familiar with. We regulate certain chemicals as well, not just the radioactive material and the radiation coming from those.

If it's a chemical that's associated with, there's a definition here, but if it's associated with

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

the rad material in the process and it's co-mingled with it, or the rad material itself is the chemical, we regulate those aspects of it.

And so that's why there's chemical thresholds in here as well.

MEMBER POWERS: The Committee has recently reviewed that material.

MR. SMITH: And so for the chemical side, the licensees will propose thresholds to us that we'll review and approve. They'll be included in their, when I say summaries, their ISA methodology.

So when they do their accident analyses, those are the thresholds that they compare against, those consequences.

CHAIRMAN BROWN: Okay, that's your last slide?

MR. SMITH: Yes, sir.

CHAIRMAN BROWN: We're about, just for a calibration we're about four slides behind based on the schedule here which means we'll end up about a half an hour in time.

We will figure out a way to keep ourselves moving later hopefully. So we'll take a ten minute break right now, recess. Make it 15, I'm sorry, so

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

you can get your coffee.

(Whereupon, the above-entitled matter went off the record at 10:08 a.m. and resumed at 10:31 a.m.)

CHAIRMAN BROWN: Okay, I am going to call the meeting back to order. There we go. She was trying to find Myron, so -- It seems she got a phone call from him.

Why don't we go ahead and proceed. Where do we start now? We are starting with whoever is next.

MR. DOWNS: So we're going to start off with the regulatory framework as it pertains to physical security aspects at our facilities and to discuss that is Brad Bergemann from the Office of Nuclear Security Incident Response, the Cyber Security Director.

CHAIRMAN BROWN: By "physical" do you mean guards and doors?

MR. BERGEMANN: Yes.

MR. DOWNS: Guards, guns, and gates, yes, sir.

CHAIRMAN BROWN: Guards, guns, and gates.

MR. DOWNS: Correct.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

CHAIRMAN BROWN: Okay, I just want to make sure I know what we are talking about. That's not, that's just -- This is just an education part of this because that's not part of the -- so we don't have to have a lot of elucidation of detailed stuff so we can try to catch up a little bit, is that okay, also?

MR. BERGEMANN: Correct.

MR. DOWNS: We will try to keep it rolling, yes, sir.

CHAIRMAN BROWN: Thank you, I appreciate that.

MR. BERGEMANN: All right. So before the break Brian hit on the safety aspects and as James said I was going to hit on the regulatory framework that is currently in place for the licensees for physical security, MC&A, and information security.

So physical security, as discussed earlier we went into detail about the different types of facilities and there is once again a wide range of facilities and so there is a wide range of physical security measures at these types of facilities.

So on one hand you have your Part 40 facilities that do not have any regulations within Part 73 security that apply, and then on the other

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

hand you have Category I facilities that have very, very high security requirements from Part 73, greater than what you would see at a reactor.

So that's the wide range with the facility types and the types of physical security you would have at those facilities.

So after 9/11 the NRC issued orders and the orders went to all the different types of fuel cycle facilities. They were a little different based on the type of facility.

And so part of those ICM orders I guess it may have caused licensees to do an evaluation and to possibly implement security measures beyond what was in their existing regulations.

CHAIRMAN BROWN: ICM is Interim Compensatory Measure?

MR. BERGEMANN: Interim Compensatory Measure orders.

CHAIRMAN BROWN: Okay. Thank you.

MR. BERGEMANN: Sorry. So within those ICM orders there was some physical security requirements and then also some emergency preparedness, some requirements to coordinate with local law enforcement, things of that nature, and

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

there was one requirement in there that talked about cyber and that was applicable to all the different types of fuel cycle facilities regardless of Part 40 or Category I or Category III.

So those orders, some of those requirements were implemented and are still in effect today, okay. And, of course, obviously, this rule focuses on digital assets. Now some of those physical security measures that are digital may be evaluated and may require protection with the proposed rule.

CHAIRMAN BROWN: 73.1 if I recall was -- It was like on Page 2 or something, there was just talk about a programmatic cyber security, is that what we are talking about where you said something got changed after --

MR. BERGEMANN: Yes. I'll --

CHAIRMAN BROWN: You're going to get to that or --

MR. BERGEMANN: I'll get to that, yes.

CHAIRMAN BROWN: Okay, all right. Fine, go on.

MR. BERGEMANN: Okay. So that was the ICM order which, like I said, was issued out to all the fuel cycle facilities and once again had one measure

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

in there for cyber security.

CHAIRMAN BROWN: I thought it was one bullet.

MR. BERGEMANN: One bullet basically, yes.

CHAIRMAN BROWN: Okay.

MR. BERGEMANN: Very generic. And it really didn't -- The thing it didn't do is it didn't go into this is what you must do to protect, do to basically look at and address. It didn't go into any specific requirements.

So for the CAT I's if you look at the second major bullet there, CAT I fuel cycle facilities, which we have the two, they fall under the DBT, design-basis threats under 73.1.

So in both of those DBTs, there is two of them, one for radiological sabotage and one for theft of material, they apply to both of those facilities. So they have to implement measures to protect against the DBT.

And in both of those DBTs there is a cyber attack. Also with the CAT I's they have 73.20 which is the high assurance performance objective and requirements to basically implement a physical protection system that will provide high assurance

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

that they protect against the DBTs.

And then their specific requirements basically fall into 73.45 and 73.46, which is kind of the details of what measures they put in, such as an intrusion detection system for the protected area and the material areas, the vaults to protect the material, access control systems, controlling access within these different areas, the guard force training and qualification requirements, all the different aspects of security for the CAT I's fall in 73.45 and 73.46.

And then for the Category II and III fuel cycle licensees you have 73.67, which goes -- There is different requirements whether you are a CAT II or III, but there is just basically some minimal physical security requirements that go into preventing unauthorized access or activities in certain areas, but they are not nearly the amount of requirements that you would see at a CAT I.

CHAIRMAN BROWN: Okay.

MR. BERGEMANN: So that's just the general overview of the physical security requirements and as you see for Part 40 there is no regulation specific in Part 73 for them.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

CHAIRMAN BROWN: Okay.

MR. BERGEMANN: All right, next slide.

MEMBER SUNSERI: So did those physical security include insider threat concerns?

MR. BERGEMANN: So for the CAT I's, yes. Yes, that falls within the DBT protecting against the insider.

CHAIRMAN BROWN: Against the insider person, correct? I mean when you talk about an insider threat I presume you are talking about somebody that's in there that may create a problem and you want to ensure that you're --

MR. BERGEMANN: Right, right.

CHAIRMAN BROWN: Okay. All right, I just wanted to make sure I understood.

MR. BERGEMANN: And I don't want to get into the details of it, but, okay, it does include an insider threat.

CHAIRMAN BROWN: Okay.

MR. BERGEMANN: All right. Next would be material control and accounting and that comes out of Part 74. Of course, there is specific requirements for the CAT I's, II's, and III's, but for the purpose of our rule for cyber security we were only looking at

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

the CAT II's and CAT I type of material.

So within that, for the CAT II's you have 74.41, which is the control and accounting of SNM of moderate strategic significance, and that would be applicable to the CAT II's, and then 74.51 is for the CAT I's, which is the strategic special nuclear material, and that's the two CAT I's.

And basically for both of those types of material the consequences of concern that we would be looking at, which we'll be going into detail later, are location and type of material, knowing that location and type of material, and then identifying losses of that type of material, some of the details involved in that for those two types of material.

MEMBER STETKAR: And let me just, because I'll go back to sweeping the floors, from what you just said that means under the cyber security rule and the implement and guidance Category III facilities do not need to look at cyber attacks that affect material control and accounting, is that correct?

MR. BERGEMANN: With one exception.

MEMBER STETKAR: With one exception?

MR. BERGEMANN: With one exception. From site visits there are sites that are using their -- A

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

Category III site would be using their MC&A system, it is integrated with the safety systems.

MEMBER STETKAR: Okay.

MR. BERGEMANN: So in that case they would have to analyze that to see if it could result in a consequence of concern.

MEMBER STETKAR: But strictly for the safety function of --

MR. BERGEMANN: Right.

MEMBER STETKAR: -- whatever that is?

MR. BERGEMANN: Exactly.

MEMBER STETKAR: Okay.

(Simultaneous speaking)

MR. BERGEMANN: Not for the type of material --

MR. DOWNS: Yes, it would be a safety consequence of concern, right, because we're not concerned about the material control and accounting consequence of concern because a Category III, the amount of Category III material that it would take to cause a significant impact to the common defense and security is such that they would notice it before it was gone.

CHAIRMAN BROWN: Thank you.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

MEMBER STETKAR: Okay.

CHAIRMAN BROWN: Thank you, John, for helping me on this because I guess I didn't dig that out, that particular point out of reading the rule or the guidance.

So if I look at the rule and it talks about the latent consequence of concern design basis threat that only applies to --

MR. BERGEMANN: CAT I's.

CHAIRMAN BROWN: CAT I's, okay.

MR. BERGEMANN: CAT I's, correct.

CHAIRMAN BROWN: And the same with safeguards, is it CAT I's only or is that --

(Simultaneous speaking)

MR. DOWNS: It applies only to Category II.

CHAIRMAN BROWN: That's only Category II?

MR. DOWNS: Correct.

CHAIRMAN BROWN: And safety would possibly be?

MR. DOWNS: Everybody.

MR. BERGEMANN: Everybody.

CHAIRMAN BROWN: CAT I included, right?

MR. DOWNS: Yes.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

MR. BERGEMANN: Yes, I, II, and III.

CHAIRMAN BROWN: And then IV where it's safety and security?

MR. DOWNS: Everybody. Right, the security --

CHAIRMAN BROWN: I think I remember hearing, reading everybody somewhere I just didn't connect the dots well enough.

MR. DOWNS: And the security piece of that would only be for facilities that possess classified information or matter.

CHAIRMAN BROWN: Okay. So a CAT I is your design basis --

MR. DOWNS: Threat.

CHAIRMAN BROWN: -- CAT II -- Yes, I just didn't add the words on.

MR. DOWNS: Yes, all right.

CHAIRMAN BROWN: CAT II is the safeguards and III and IV are everybody?

(Simultaneous speaking)

MEMBER STETKAR: I just wanted to make sure I understood the MC&A part of it because I know there was some -- I had read in some of the background materials some discussion about, you know, the scope

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

of that and how it might apply to Category III facilities.

CHAIRMAN BROWN: Yes.

MR. DOWNS: Yes, and as I go through the -

-

MEMBER STETKAR: So I wanted to make sure I understood.

MR. DOWNS: As I go through the history of how we progressed I'll highlight how some of the functions that we previously considered dropped out.

MEMBER STETKAR: Okay, thanks.

CHAIRMAN BROWN: Okay. Thank you, go ahead.

MR. BERGEMANN: All right. Any other questions on material control and accounting, just the regulatory framework?

(No audible response)

MR. BERGEMANN: All right. And then, finally, the Part 95. So these are the facilities that contain like classified national security information.

CHAIRMAN BROWN: I guess I do have a question on that.

MR. BERGEMANN: Okay.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

CHAIRMAN BROWN: And if I am totally off base just tell me, this rule doesn't necessarily work on the physical safeguarding of it, I mean those rules are in place right now.

This new rule that you are proposing has to do with just the computer-based cyber intrusion-type, whether it's internal, external, what have you, but material accounting rules are already covered under your other, as you noted on your previous slide, am I correct in my understanding?

You are not changing the material accounting rules?

MR. BERGEMANN: Oh, no, no, we're not.

CHAIRMAN BROWN: That's what I --

MR. BERGEMANN: Okay, yes.

(Simultaneous speaking)

CHAIRMAN BROWN: Got a simple statement, thank you.

MR. BERGEMANN: Right.

MEMBER STETKAR: No, but for a Category I or II facility if they take credit for digital assets to perform that material accounting this rule does apply.

MR. DOWNS: Those assets could potentially

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

be --

(Simultaneous speaking)

MEMBER STETKAR: To those assets.

MR. DOWNS: That's correct.

MR. BERGEMANN: That apply to cyber measures.

CHAIRMAN BROWN: Yes, but -- Yes, I understand the application of the cyber, but not the basic material control requirements --

MR. BERGEMANN: No, no, no.

MR. DOWNS: Right.

CHAIRMAN BROWN: -- are not being changed, just the how do you protect them against cyber from being compromised?

MR. DOWNS: That's right. Yes, the goal with this rulemaking is not to change any existing requirements, require no process changes by the licensee. That wasn't, you know, that's not our goal.

What our goal here is is to provide protection from the cyber threat. So all of the existing regulations are going to stay the same, it's just the only thing that would change is the process of how to submit a licensee amendment, you know, associated with a cyber security plan. That's what it

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

was.

CHAIRMAN BROWN: Okay, thank you.

MR. BERGEMANN: Sure. All right, now Part 95 for the fuel cycle facilities that possess classified national security information or restricted data, that falls under our purview. The physical security digital assets would fall within this cyber rule.

So if there is areas that because of the process or the matter that's in that area, it can't be locked in a safe or anything like that, those areas may have access control intrusion detection systems that are protecting that classified matter and those systems would have to be, would basically fall under and be analyzed and if there is a consequence of a concern associated it would fall within the cyber rule.

And that's where 95.29 is those areas, the restricted or closed areas, meaning you can't put it like in a safe or a repository. It's an open type area or room.

CHAIRMAN BROWN: You lost me.

MR. DOWNS: So, for example, at an enrichment facility where they actually would be

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

taking apart some of the centrifuge components, those components internal to centrifuge, some of which are classified.

The size of that can't be done, you would need a fairly large room to do that. So in order to protect that classified matter you would have some physical protection, an intrusion detection, door locks, electronic locks potentially, cameras, that sort of thing.

So that's where you would have this restricted or closed area where that operation was taking place, and that's kind of the premise.

CHAIRMAN BROWN: That's a piece of hardware though?

MR. DOWNS: Correct.

CHAIRMAN BROWN: When I look at security information of restricted data I think paper, okay.

MR. DOWNS: Well paper or --

CHAIRMAN BROWN: I mean data, you know --

(Simultaneous speaking)

MR. DOWNS: It could, yes.

CHAIRMAN BROWN: -- and I don't think it's 17 inches long and 14 inches wide and is filled with, you know, plastic glue or something like that.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

MR. BERGEMANN: But it could be a room full of paper, too, of classified.

CHAIRMAN BROWN: Okay. So this is -- All right, so what you are saying is if I am doing maintenance or have to replace something and I have to take something apart I put it in a room that is isolated, locked, and can't get into with whatever the thing is, that's a physical security --

MR. BERGEMANN: Controlled access, correct, yes.

CHAIRMAN BROWN: -- even though it's not a cyber issue unless your physical protection or modes could be compromised if they are connected into a global network throughout the plant.

MR. BERGEMANN: Exactly. That's correct.

CHAIRMAN BROWN: Okay.

MR. BERGEMANN: All right.

MR. DOWNS: Okay. So that's kind of the overview of the regulations surrounding the facilities that we discussed earlier.

At this point I was going to delve into the history of where the staff has been in regards to fuel cycle cyber security. I'm going to cover some of the orders that Brad discussed, the cyber security

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

roadmap that the Agency produced, an options paper that was sent to the Commission, the Commission's response to that options paper, and then the regulatory basis we recently produced for this rulemaking, and the rulemaking schedule overall.

MEMBER STETKAR: James, just to help me out.

MR. DOWNS: Yes, sir?

MEMBER STETKAR: SECY-14-0147 is still marked as security related, is that true, the SECY paper itself or is it --

MR. DOWNS: So the SECY paper is security related.

MEMBER STETKAR: Okay, that's all we need.

MR. DOWNS: That's correct, yes.

MEMBER STETKAR: That's all I need. Thank you.

CHAIRMAN BROWN: Go on.

MR. DOWNS: Okay.

CHAIRMAN BROWN: I'm just helping you out here.

MR. DOWNS: Okay. So as we kind of discussed there are really no cyber security regulations that are codified in the 10 CFR fuel cycle

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

for facility licensees.

Brad hit on a couple of spots there where the DBT just has a cyber security element but it's not really elaborated on. Some of the orders that were issued had a very vague provision on cyber security but, again, nothing has been codified at this point.

Those ICM orders that relate -- The ICM orders were really geared to emergency response and offsite personnel. As Brad said they are applicable to all fuel cycle licensees, but the language in there, again, I think was kind of vague, it was to evaluate the networks for safety and security vulnerabilities and address as necessary.

Brad hit on the DBT aspects there in Part 73 that that rule was revised in 2007. It didn't establish the specific security requirements for protecting against cyber attacks or establishing a formal cyber security program.

The cyber security programs that exist today at the CAT I facilities are really geared towards protection of the classified networks that they have and those were authorized and accredited by the Department of Energy of Naval Reactors.

It should be noted that fuel cycle

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

facility licensees have implemented some voluntary measures for both business and safety considerations.

They haven't turned a blind eye to this. They have considered within certain limits.

As part of that SRM that the Commission issued on SECY-14-0147 the Commission included a request for the NRC staff to monitor any voluntary initiatives and there were observations, site visits done.

The observations of the staff basically indicated that a defined regulatory structure is needed and it is needed to adequately protect public health and safety and the common defense of security.

So they have implemented some voluntary measures but the NRC staff doesn't feel like they have gone far enough. Questions on that slide?

(No audible answer)

MR. DOWNS: Okay. So in June of 2012 the SECY-12-0088, which is the cyber security roadmap was issued by the NRC staff. This provided a roadmap for the NRC to consider cyber security at four types of NRC licensees.

These would be the fuel cycle facilities, non-power reactors, independent spent fuel storage

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

installations, also known as ISFSIs, and byproduct material licensees.

There have been other working groups formed to deal with the bottom three that are listed here on this slide. Obviously, we are talking about fuel cycle here today.

This all stemmed from, you know, the reactors kind of took the lead on developing cyber security requirements and this kind of laid out how the rest of the agency should follow along.

The SECY paper discusses a graded approach to develop the requirements commensurate with the risks associated with these individual facilities. Each of these are -- or I should say the licensee types. Each of these licensee types have unique risk considerations with them.

CHAIRMAN BROWN: Would those assessments have been based on their ISAs or --

MR. DOWNS: So non-power reactors it would be research and test --

CHAIRMAN BROWN: At this point?

MR. DOWNS: Are you talking about for the other facility types?

CHAIRMAN BROWN: No, fuel cycle

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

facilities.

MR. DOWNS: For fuel cycle facility types that -- So the recommendations from this roadmap were basically to evaluate cyber security at the fuel cycle facilities and develop a methodology.

CHAIRMAN BROWN: Okay, okay. All right, go on.

MR. DOWNS: Any questions on the other facility, the licensee types here?

(No audible response)

MR. DOWNS: Okay. So kind of overlapping with the efforts on the roadmap as far as the timeline is concerned, an NRC working group began looking at fuel cycle cyber security.

After several visits to various licensees the staff developed an options paper for Commission consideration and that's what the SECY-14-0147 is about there.

This options paper was focused on the increasing cyber threat and the potential consequences associated with the cyber attack.

The focus in the paper was on protecting all functions required by regulation. This is a difference from where we were at then versus where we

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

are now.

At that point we were focused on safety, security, emergency preparedness, material control, and accounting. So we had -- it was a much broader scope that was discussed in the paper.

The staff recommendation in the paper was to issue an order and follow it up with a rulemaking and in that order we discussed very limited cyber security controls but it was for a very, again, a much larger scope of assets.

The controls that were talked about in there were portable media and isolation and the program itself that was discussed in the paper contained a cyber security team, proper training, and some form of detection and response.

One of the problems with this paper was that it, again, with that very broad scope it really didn't take into consideration some of the unique risks, hazards, based upon the different facility types that we have here.

So the Commission received the paper in late 2014 and the three options there again were to issue an order followed by a rulemaking, perform strictly a rulemaking, or take no action at all. Any

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

questions on SECY-14-0147?

(No audible response)

MR. DOWNS: Okay. So in March of 2015 the Commission provided the SRM to the SECY, SRM being a Staff Requirements Memorandum, directed the NRC to proceed directly with a cyber security rulemaking that was to be designated as a high priority and implemented in an expeditious manner.

The SECY was very clear on the work that had been done to date. It wasn't fulsome enough, was the term that they used, so we had to add additional detail and consider some additional things as we went forward, namely that third bullet there, was how to integrate safety and security and apply a discipline-graded approach to the identification of assets.

Again, this keys on the fact that we had a much larger scope of assets that was originally in that, originally being considered in the SECY paper and they really needed to see it scaled down because some of that just wasn't consequence significant. Questions on the SRM?

CHAIRMAN BROWN: My takeaway on that if I wanted to was it's got two points in it, a graded approach to both identification of digital assets and

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

a graded consequence-based approach to their protection?

MR. DOWNS: That's correct. Right, that's the key.

CHAIRMAN BROWN: Okay.

MR. DOWNS: So in early 2015 the NRC staff began work on a draft regulatory basis for a rulemaking. There has been significant interactions with stakeholders on the development of the draft regulatory basis, the final regulatory basis.

This included formal common resolutions, site visits, and as stated here five public meetings.

So it was a tremendous amount of outreach and we appreciated the involvement with the stakeholders because it definitely helped guide the NRC towards the graded approach that we have come up with today.

In March 2016 the staff completed the final regulatory basis, and that was basically to set forth a rulemaking to establish appropriate levels of protection against cyber attacks at the fuel cycle facilities based on facility type and it recommended that along, coincided, or guided by the SRM by the Commission it recommended that graded risk informed performance-based approach for rulemaking.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

It should also be stated that the regulatory basis also took some insights from the power reactor rule implementation, which was 10 CFR 73.54.

Some of those insights that we were looking to apply to our process was to have a defined specific consequence-based process to identify digital assets, felt that we should develop a screening process to determine in-scope assets.

A lot of the, some of the -- The difficulty on implementation of the reactor rule has been with asset identification, so we were trying to really have our hands wrapped around that.

One of the other insights was to add some flexibility to the fuel cycle rule to satisfy the security objective and this would consider things like tailoring controls, you know, cyber security controls, how would you tailor those to fit the processes that are, the diverse processes that are present in our fuel cycle facilities and also how would you, could you potentially credit existing features in lieu of providing cyber security protection.

So that's where in the rule, in the proposed rule, you'll see the discussion alternate

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

means and what we are trying to get at there is sometimes, as we went through in the IROFS discussion, you may have an administrative IROFS in place that would render any effects to a digital component to really not have a consequence of concern.

So providing credit to these other systems that are in place was something that we wanted to be able to do as well. Questions on the reg basis?

MEMBER STETKAR: Yes, I had one. Chapter 8 in the rate basis document is the title cost impact considerations and I got a bit confused as I read through this document, because in a few places, like the introduction to Chapter 8, I see statements saying well, a more detailed cost impact evaluation would be carried out as part of the regulatory analysis in the proposed rule phase and yet in Section 8.6 there seems to be an explicit conclusion that the rulemaking is justified by the costs.

I really couldn't find any compelling arguments regarding the type of regulatory analysis that is typically done, at least over on the reactor side for rulemaking, where you look at objectives and a fairly thorough analysis.

Will that analysis be done as part of the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

rulemaking?

MR. DOWNS: Currently being handled.

MEMBER STETKAR: And suppose the results of that analysis conclude that the rulemaking is not justified because there is no, from any of these facilities there is no measurable benefit, why are we doing all of this now?

MR. DOWNS: I think you've keyed on something here. So in the rulemaking process at the NRC, you know, we do this regulatory basis.

MEMBER STETKAR: And that's essentially a technical basis if I can characterize it that way.

MR. DOWNS: Yes.

MEMBER STETKAR: Well it's a legal technical basis, right?

MR. DOWNS: It's a technical basis to initiate the rulemaking process.

MEMBER STETKAR: Right.

MR. DOWNS: In that rulemaking process you will further refine that technical basis and part of that refinement is consideration of cost.

MEMBER STETKAR: Yes.

MR. DOWNS: That's something that we are actually working on right now and it's part of the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

proposed rule package that will go into concurrence.

You are absolutely spot on though that if during this cost benefit discussion it was apparent to the staff that the rule couldn't be cost justified or it couldn't be legally justified on the basis of adequate protection, or whatever the case may be, then at that point the staff could go forward with the recommendation that the rule be canceled.

What we have found in our analysis to date though is that so far everything is pointing to the rule being cost --

(Simultaneous speaking)

MEMBER STETKAR: And I am assuming at some point we will see that analysis, right?

MR. DOWNS: Absolutely, yes.

MEMBER STETKAR: Okay. So I won't, because of the time, delve into the details of that justification, but I am curious because I am familiar with the regulatory analysis that is done for at least power reactors where they have safety goal screening criteria and people look at that and if you don't meet the screening criteria you don't progress on.

You have to justify that indeed the benefits meet some minimal threshold, if you will,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

before you then go evaluate the costs. Is a similar type of thought process applied here?

MR. DOWNS: Yes, very similar.

MEMBER STETKAR: Okay.

MR. DOWNS: Yes, and that's --

MEMBER STETKAR: So we'll wait to see that.

MR. BARTLETT: Matt Bartlett, NRC Fuel Cycle. So I just wanted to note that we recognize that the reg analysis has two components to the cost argument.

One is a quantitative cost comparison and the other is a qualitative argument, right, so --

MEMBER STETKAR: Yes. And there can be quantitative and qualitative on the benefit side also.

MR. BARTLETT: Okay.

MR. DOWNS: Exactly, yes.

CHAIRMAN BROWN: At this point from what I have seen in the other documents we've had though there is some disagreement on the quantitative cost between industry and you guys at this point.

Are you -- I don't want to go into that now, but at some point we ought to, you know --

MEMBER STETKAR: Regardless. There is

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

always disagreement on both sides of the equation.

CHAIRMAN BROWN: Yes, there's always disagreement, but, you know, I don't want to spend a lot of time trying to do that when you are all still in the process of reconciling the differences and everything else, but that's something.

MEMBER STETKAR: I just wanted to establish for the record that despite the statement in Section 8.6 of what we have been given that the NRC concludes that the cost associated with the cyber security rulemaking would be offset by the benefits is not necessarily a final conclusion of the NRC staff.

MR. DOWNS: You are correct, that's not a final conclusion. It's --

MEMBER STETKAR: That's all I wanted to make sure I understood.

MR. DOWNS: Yes, that's correct.

CHAIRMAN BROWN: Yes, I didn't see that. Where is that? I am looking at Chapter 8 now. Oh, yes, I found it. Okay, yes, yes, yes, yes, yes, thank you. I will highlight that now, I know I read it. Thank you very much, John, as usual.

MR. DOWNS: But similar to that Chapter 6 of the regulatory basis discusses backfit and --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

MEMBER STETKAR: Yes, I didn't want to -- I just wanted to establish that the fat lady hasn't sung yet.

MR. DOWNS: Exactly, right, right.

MEMBER STETKAR: And that since the fat lady hasn't sung I wasn't going to bring up backfit.

MR. DOWNS: Right, and that's --

MEMBER STETKAR: There are questions I'm sure on backfit.

MR. DOWNS: It follows the same premise thought that, you know, that backfit would have to be considered and the final determination hasn't been made.

MEMBER STETKAR: And backfit, to make sure that I do understand this, backfit only applies to Part 70 facilities that are licensed under Subpart H of Part 70, but that's effectively all of your Part 70 facilities, is that right?

MR. DOWNS: It's applicable to all Part 70 facilities, that's correct, yes, yes.

MEMBER STETKAR: I mean that's what I understood. The Part 40 facilities apparently don't have to --

MR. DOWNS: They would fall out of the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

backfit. There was a commitment though by the staff to include them in the cost benefit discussions.

MEMBER STETKAR: Yes. I read that, yes. Okay, thank you.

CHAIRMAN BROWN: I would also assume that if there is a, obviously there will always be a disagreement somehow on the quantitative aspects of this whole thing with industry, that somehow your qualitative assessment is going to be impeccably able to demonstrate that the benefits are worth the cost based on specific threats or the inability to accommodate those threats unless the rule is implemented.

MR. DOWNS: That's a good way to summarize what the regulatory analysis is, yes.

CHAIRMAN BROWN: Going to do, right?

MR. DOWNS: That's what -- That's the goal of the regulatory analysis, yes.

CHAIRMAN BROWN: Okay, go on.

MR. DOWNS: It sets a high bar, but, yes.

CHAIRMAN BROWN: Thank you.

MR. DOWNS: So kind of speaking about this, you know, this slide kind of goes right into what we were talking about here.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

The proposed rule package, which is -- So I should start, we obviously completed the regulatory basis in March of this year. All of these dates had SECY tickets associated with them, so we're -- or I should say all these objectives had SECY tickets associated with them.

The next step is to provide a proposed rule package to the EDO to get it to the Commission for the Commission's review. Our target date for that is to get the package, the proposed rule package to the EDO by mid March of this coming year.

This proposed rule package would include everything that we've just talked about here, the backfit analysis, regulatory analysis, the Federal Register Notice that is associated with the rulemaking, we would include statements of consideration.

With that there would also be a formal comment period after the Commission would release the documents. That formal comment period would be where stakeholders would have an opportunity to question some of those analyses that were performed, some of the values, some of the estimates, those sorts of things.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

I should point out that the actual rulemaking process is led by the Division of Material, State, Tribal, and Rulemaking Programs in the Office of Nuclear Material and Safeguards.

Our Project Manager there is Cardelia Maupin. She has been instrumental in guiding us through this process and, again, we hope to reach, get that proposed rule to the EDO to meet this milestone.

The final rule, obviously it is still a ways off, and this is all speculative upon the, you know, Commission approving the proposed rule package to be put out for formal comment.

MEMBER STETKAR: Are you planning to brief this Subcommittee on the proposed rule package since it's only 4-1/2 months from now before you send it up to the EDO?

MR. DOWNS: We had not planned to do that.

CHAIRMAN BROWN: Okay.

MR. DOWNS: We'll --

CHAIRMAN BROWN: I said okay in the sense that I understand your answer.

MR. DOWNS: Right, understood. No, understood.

CHAIRMAN BROWN: Bear in mind we will have

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

to discuss that amongst the Committee if we would desire to see something.

MR. DOWNS: Absolutely.

CHAIRMAN BROWN: I mean this is, what we are seeing now is literally a draft of where you are going, if I can understand that properly.

MR. DOWNS: It's a fairly well developed draft as far as the proposed rule language goes and the regulatory basis documents. It's kind of the technical crux of the rulemaking effort.

Those have been fairly well developed and given that the working group consists of several different offices across the NRC we are fairly comfortable with these are getting to be fairly near final.

Obviously, there are still pre-decisional, they have a concurrence process that they have to go through, and they'll go through that in tandem with this rule package that would include these other analyses that we have talked about.

That's where the staff -- The effort today is getting those other analyses finalized so that the cost benefit, backfit, those sorts of things, can be presented to the Commission.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

CHAIRMAN BROWN: John, go ahead.

MEMBER STETKAR: Yes, I was going to say from our perspective -- We'll have to talk about it I think more offline, but from our perspective it's only a question of whether we would like to be briefed on the regulatory analysis, the cost benefit analysis, and that justification before it goes up to the EDO or whether we would prefer to wait for the public comments and address it then.

I mean there is, you know, a risk of how the ACRS, the Full Committee, reacts to something if you wait too long.

MR. DOWNS: Sure.

MR. BARTLETT: Matt Bartlett, Fuel Cycle. Just note that the thing we are sensitive to is it's designated as an expedited rule so we have to be sensitive to the SECY dates.

CHAIRMAN BROWN: Yes, we understand that, but the thing is there is about 11 months between the time the package goes to the EDO and the time you want to send the final rule package to the EDO.

So, I mean that's not an inconsequentially small piece of time, it's a matter of where --

MEMBER STETKAR: That's right. That's why

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

I said we need to discuss it offline because there are pros and cons of getting early feedback, at least if not from the Full Committee at least from the Subcommittee in time to make, you know, tweaks, if you will.

CHAIRMAN BROWN: Yes.

MR. DOWNS: Yes, let us know. Let us know what you guys want to do, yes. Okay, so a regulatory program is a little more than just a rule.

We've been talking about a regulatory guide that's currently in draft. A regulatory guide is to provide an acceptable methodology to satisfy the regulatory requirements, and that's the draft regulatory guide has been provided for your review.

There are two other elements here that have not yet been developed, and that is the interim staff guidance document that would provide acceptance criteria for NRC staff to review the cyber security plan that is being submitted.

This kind of correlates to the fuel cycle has a standard review plan, NUREG-1520, that outlines acceptance criteria for all of the other various licensing actions that fuel cycle facilities would produce.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

It focuses, you know, the focus of 1520 is really on the ISA safety aspects primarily, but something similar would need to be developed for the cyber security effort.

I mean that isn't part of the proposed rule package, our plan is over the next, early next year to start development on that and -- Go ahead.

MEMBER STETKAR: Yes, I'm sorry. I was writing things and I was only half listening. The interim staff guide, as soon as you say interim staff guidance, I am curious.

MR. DOWNS: Why is it interim?

MEMBER STETKAR: Yes, why is it interim because you'll have a regulatory guide as part of the, you know, well, I am assuming it's issued in tandem with the rule package --

MR. DOWNS: Correct.

MEMBER STETKAR: -- both in draft form and final form. There is some equivalent of the standard review plan, I think I heard you say, so why does the staff need to develop separate interim staff guidance --

MR. DOWNS: So --

MEMBER STETKAR: When in time will that be

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

applied is what I am trying to get to?

MR. DOWNS: Right, right.

MEMBER STETKAR: Because there isn't any requirement for anybody to do anything until the rule is issued and then there is a time laid out in the rule.

MR. DOWNS: Correct. And that's part of the reason why the interim staff guidance isn't needed to go up for approval with the proposed rule package.

Basically the regulatory guide it's really intended for stakeholder use, for use by the licensees, and it's an acceptable methodology to satisfy the regulatory requirement.

It doesn't have acceptance criteria in there that guides the staff's, the NRC staff's review.

So that's where we need to have this other document that lays out those acceptance criteria.

MEMBER STETKAR: But to me the notion of interim --

MR. DOWNS: Right, yes.

MEMBER STETKAR: Again, I'm more familiar with the reactor world where I have a standard review plan that provides that staff guidance and occasionally, more frequently than not these days, but

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

occasionally interim staff guidance is issued because, for example, in Fukushima, orders were issued, people are doing things, and it takes time to change the standard review plan because regulations haven't been issued.

So interim staff guidance is issued in that sense because there is a need for a stop gap, if you will, the staff is reviewing submittals. What interim --

MR. DOWNS: Why interim?

MEMBER STETKAR: Yes. Why interim? I can understand develop staff guidance.

MR. DOWNS: Ideally we would like to revise the standard review plan and include a section in there.

MEMBER STETKAR: Yes.

MR. DOWNS: That's the ideal world. Right now though we are saying it's going to be an interim staff guidance because the NUREG-1520 is currently, the Commission has stated that NUREG-1520 should not be revised currently because of the ISA considerations that are being developed by -- Who is the group? Well, I forget.

(Off microphone comment)

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

MR. DOWNS: Yes, yes.

MEMBER STETKAR: Okay, but wait, and again, it's not -- I'm just trying to understand. It's not our role to get into administrative issues, but eventually NUREG-1520, if that's the fundamental staff guidance, will have to be revised to incorporate staff guidance for review of things under the cyber security rule.

MR. DOWNS: Yes.

MEMBER STETKAR: So it's going to have to be done eventually.

MR. DOWNS: That's correct.

MEMBER STETKAR: Despite the fact that maybe somebody said don't do it today.

MR. DOWNS: That's correct.

MEMBER STETKAR: I am just hoping that you are not going to do things twice. That's all.

MR. BARTLETT: Matt Bartlett, Fuel Cycle. Often the way these things happen is we develop the interim staff guidance first and then it becomes a new chapter in the standard review plan.

MEMBER STETKAR: I got it. Thanks. I just wanted to make sure I understood why it was called interim.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

MR. DOWNS: And then obviously the third piece of this is the inspection procedure that has not yet been developed that, you know, based -- inspection procedures are very, it will be geared towards that final rule, so we are going to start, begin the process to develop it early in this coming year.

So at this point in the presentation I was going to start discussing an overview of the draft proposed rule. The overarching purpose of the rule is to establish performance-based regulatory framework.

CHAIRMAN BROWN: Hold on.

MR. DOWNS: Go ahead.

CHAIRMAN BROWN: I just want to make sure, we are now transitioning to what we would have started at 1:00?

MR. DOWNS: That's correct.

CHAIRMAN BROWN: Okay, that's fine. I just wanted to make sure I hadn't lost --

MEMBER STETKAR: Don't complain that you are now ahead of schedule.

CHAIRMAN BROWN: I'm not complaining. I'm just so efficient at managing these meetings that we recover promptly and are able to get on with the business.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

MR. DOWNS: You said keep it rolling, so I was trying.

MEMBER STETKAR: You're so good that you didn't even know you were that good.

CHAIRMAN BROWN: I knew I was, I was just making sure I hadn't missed something here and I'm so old I sometimes fall asleep and I don't have anybody beside me to hit me so it works well. Thank you.

MR. DOWNS: Okay. So taking some of those lessons from the experience with the SECY-14-0147 the scope of the proposed rule is limited.

It is focused on active or latent consequences of concern, specific risk-informed thresholds, and vital digital assets. The vital digital assets will be those that, those are the assets that would require cyber security controls be applied to them.

And this whole process, again, it's incorporated stakeholder feedback on the scope and methodology for implementing the proposed rule. In the past 16 months we have had ten public meetings, so there has been significant stakeholder interaction.

This is the structure of the draft proposed rule. There are nine paragraphs so to speak

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

here. Each one has a different purpose, everything from who the rule is applicable to down at the bottom how records are maintained.

So at this point I was basically going to start going through each of the paragraphs to kind of discuss them and field your questions as they pertain.

The applicability section, Paragraph A, describes, you know, the fuel cycle facilities we have been talking about here today, which are those that fall under Part 70 as well as the uranium hexafluoride conversion and deconversion facilities.

When we say Part 70 obviously that would include the enrichment and fuel fabrication facilities. This paragraph lays out the mechanics of the regulatory process.

It says that a cyber security plan would be submitted as a license amended request and a timeframe kind of associated with that is six months after the rule.

This cyber security plan would contain a description of the methodology to identify digital assets and description of the cyber security controls.

We'll get into the plan in a little bit more detail down from one of the following paragraphs.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

So once the NRC receives this cyber security plan the staff would review and consider it for approval. Typically it's a 5-month review time associated with that sort of thing.

This lead time would give the licensees the opportunity to potentially stand up their cyber security team and prepare for implementation of the rule.

Implementation of the plan is expected to be a phased approach where you would perform the identification piece first and then the NRC would probably have a milestone there where it would come out and do an inspection.

The timeline being thrown around with that right now is about six months after the approval of the cyber security plan and then full implementation of the rule would be required 18 months after the NRC approves the plan.

That requirement would actually be part of the NRC approval of the plan, so it would become a license commitment then at that point to have it put in.

CHAIRMAN BROWN: Just one question, and maybe this is better suited for later because when I

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

think of implementing a cyber security plan a plan is a plan, but are there -- What's the right way to say this?

Stuff that has to be installed, I mean a cyber security, to have your cyber security plan and fully implement it means whatever detection, intrusion detection, compensation measures that you have which may be embedded in software, and it can be extensive software products, have to be fully installed, operational blessed, and somehow then have to have some assurance that as attacks or threats change that they have a viable updating process.

And I guess one of my concerns is the updating process if it involves downloading information from the guy that provided the software and he's in Seattle, Washington, and you are in wherever it is, Columbia, someplace, all that information, because that's how virus stuff gets, you know, your intrusion software sticks these days, it's sent to you via the very source you don't want to be connected to, and yet you haven't excluded connection of any of these systems in the guidance.

That doesn't require them to be excluded but you haven't suggested that and there is nothing in

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

the rule that requires that to be isolated from sources that could just wipe you out.

MR. DOWNS: So we'll get into that discussion a little bit when we get into control --

(Simultaneous speaking)

CHAIRMAN BROWN: I saw some stuff, I am just trying to prepare the road here --

MR. DOWNS: Sure, sure.

CHAIRMAN BROWN: -- because one of my major concerns from reading the guidance was alternate means, where you talked about alternate means there was another paragraph, which we'll get there, where you literally said that what many of the things we looked at from a power reactor standpoint in terms of defensive measures in our Reg Guide 5.71 where you isolate and don't allow external access, not insiders threat, but external access, to the systems under any circumstances and there is a certain core set of networks where you don't allow that.

You then said that oh, that's not good enough even if you have other administrative controls to go along with it. There was a paragraph that stated that.

So I am just trying to get down to the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

point where it almost, it becomes so overwhelmingly large and complex that without having some defensive measures acceptable and at least suggested via the guidance that you are really setting yourself up for the most complex set of cyber security updates, monitoring, and goodness and badness factors that become so expensive that they kill you.

So that's one of the areas that I have difficulty with with the guidance. It's very non-specific. I don't want to say ambiguous, but you've got performance specifications and performance objectives but yet no mention or allowance of really building a defensive architecture for the entire facility.

MEMBER MARCH-LEUBA: Yes, and hopefully we are going to talk about this this afternoon.

CHAIRMAN BROWN: Yes. I mean, you know, literally there is functionality and I think of it in terms of functionality. I mean you've got business functionality, you've got process functionality, you've got material accounting functionality, and they don't all have to be connected to the same thing.

You can isolate and separate those so that you can't compromise any one functionality or function

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

from some other function being utilized in the network.

MEMBER MARCH-LEUBA: Yes. I mean --

(Simultaneous speaking)

CHAIRMAN BROWN: I'm just throwing that out on the table as a point I would like to be able, that we're going to have to hit and cover hopefully. Go ahead.

MEMBER MARCH-LEUBA: Yes. I am hoping we will this afternoon because even the guidance talks about denial of service attacks.

CHAIRMAN BROWN: It talks about what?

MEMBER MARCH-LEUBA: Denial of service attacks.

CHAIRMAN BROWN: Right, exactly.

MEMBER MARCH-LEUBA: Which is an explicit recognition that they are going to be connected to the Russian internet, whereas the guidance should say to prevent denial of service attacks you should not be connected to the internet.

CHAIRMAN BROWN: It should say, but it doesn't.

MEMBER MARCH-LEUBA: It doesn't.

MR. DOWNS: So to --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

MEMBER STETKAR: And you shouldn't mix business processes with manufacturing processes or material control processes, you know, from the standpoint of the sabotage, whatever terminology, radiological sabotage, et cetera, and yet you don't --

(Simultaneous speaking)

MEMBER STETKAR: But, again, to keep this going, that's more for the guidance it's not for the rule. The guidance states --

CHAIRMAN BROWN: I didn't -- I said the guidance. Yes, I was talking about guidance.

MEMBER STETKAR: Okay. We're going to talk about the guidance this afternoon.

CHAIRMAN BROWN: I would argue, you know me --

MEMBER STETKAR: Yes.

CHAIRMAN BROWN: I would argue that the rule, this is personal, this is not committee, this is not committee members, subcommittee members, I will have to tell you my bent is rules are more effective than guidance and there are some things like defensive architectures that should be more explicitly covered in the rule.

Now we'll always argue about that, but

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

that's what I have discussed and advocated in the various other power reactor stuff that we have dealt with.

MEMBER STETKAR: And I will weigh in on my personal opinion which is opposed to Charlie's. I believe rules should tell you what ought to be done in reasonably unambiguous terms, not how to accomplish a particular protection, that's the role of guidance.

And, indeed, guidance can be changed, as our understanding evolves rules are more difficult to change. So specifying details of designs and rules is not generally a good idea. We've learned that in the past.

CHAIRMAN BROWN: And John and I would then argue back and forth, back and forth.

MEMBER STETKAR: I just wanted to get that on the record because it is a subcommittee meeting and these are just individual opinions.

CHAIRMAN BROWN: Yes, but I would also argue that you can advocate for defensive architectures in a rule that don't tell you how or what but they provide guidance.

It's more than guidance, it's saying, hey, we really want to make sure we don't set ourselves up.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

So the rule could specify defensive architectures to be considered and evaluated that does not dictate the how you do that but it does at least lay out that that's what we want to do. Now John will provide his counterpoint.

MEMBER STETKAR: Yes, the -- Well, again, this is important for the record also, some of our members aren't here, so they will read this record.

CHAIRMAN BROWN: We do this all the time.

MEMBER STETKAR: The problem putting a particular item like you should consider a defensive architecture in the rule people will look at that as a necessary and sufficient requirement whereas there may be other ways to skin the same cat which are better elaborated in guidance.

CHAIRMAN BROWN: Yes, it's perfectly --

MEMBER STETKAR: So that, you know, and then you get licensees justifiably saying well in the rule you told me I had to look at this and therefore I looked at that and I didn't have to look at this other thing because if you had wanted me to look at that other thing you would have put it in the rule.

And suddenly then you say oh, yes, we should have put that in the rule and you get a laundry

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

list of 35 or 40 things which should have been 36 or 41, and that's the only danger in my opinion of trying to elaborate too much detail about what you ought to look at in a rule, in the rule itself. Guidance, absolutely, that's fair game I think.

CHAIRMAN BROWN: And I would counter that as usual with the thought process that there is always possibly another way where we can achieve the same goal.

In our previous incarnations and other things we have discussed nobody has ever come up with another way yet other than isolation in many circumstances to define anything that would work reasonably.

So since nobody has identified anything in the last eight years, new technology or otherwise, somebody is always going to promise you that my software is so good that nothing will ever get past the firewalls I have built in.

And if -- I mean my boots just don't get big enough to walk through that. What did you call it a few minutes ago Dana?

MEMBER POWERS: I'm sure we can go back to the record.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

CHAIRMAN BROWN: I don't want to go back to say what that stuff looked like, but that's exactly what it would have looked like and I don't think we've got boots big -- Well, we'll go on.

This just gives you a calibration or a little bit of a thought process of information we're going to want to deal with as we go through this.

MR. DOWNS: Yes. Sure. Just kind of to discuss that a little bit though, the overall premise of this rule is to protect against consequences of concern. That's the goal and that's the NRC's mission in licensing.

CHAIRMAN BROWN: Material control.

MR. DOWNS: So, you know, we've laid out, as we'll discuss here, several consequences of concern. The business operations of these fuel cycle licensees are global in nature.

So you are not -- It would be extremely cost prohibitive as well as not in the best interest of their business to require them to have specific architectures of their systems as they've laid out.

CHAIRMAN BROWN: Let me interrupt you for just a second. I have never advocated that the business networks not be connected. My concern is

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

business networks get intermingled with the process and other networks that you may put in within the plant.

It's perfectly reasonable that business architectures are going to have the IT people, are just going to -- They'll just have a whole room full and buildings full of IT people trying to make sure that their books don't get compromised or whatever, okay.

The concern is for those processes involved in handling materials, accounting for materials, utilization of materials, don't get compromised by connection into the business network where they go on.

So when I am talking about architectures that's the type of thought process. It's obvious that business networks are never going to be isolated from their global network.

It would be a travesty for the companies these days. But they shouldn't be co-mingled with processes in the plants. That's all.

MR. DOWNS: So as you have hit on it, they are co-mingled, that's the observation that, in many -
-

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

CHAIRMAN BROWN: That's the problem.

MR. DOWNS: And that is a problem.

However --

CHAIRMAN BROWN: That's the purpose of my point about isolation.

MR. DOWNS: -- to be able to capture that problem from a regulatory perspective it's only a problem if it could potentially cause a consequence of concern.

CHAIRMAN BROWN: As soon as you are connected your consequence of concern is available because if somebody hacks through it they could modify, change, do whatever they want with it and, therefore, that's a problem.

And why shouldn't it be addressed now that you are deciding to address the cyber security threat to these other functions?

MR. DOWNS: Well it would only be a problem if there wasn't adequate cyber security provided, and that's where the adequate -- You know, what do you deem as adequate cyber security?

You know, what this rule does, what the proposed rule does, is it looks at the alternate means of performing that same function. So it may be a non-

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

digital way of preventing that consequence of concern so, therefore, that would be an acceptable means of providing cyber security.

CHAIRMAN BROWN: If the internal plant stuff communicates data via one-way fiber optic little LED serial data links that can't be compromised with software, they are hardware based, that's perfectly acceptable.

MR. DOWNS: Well I --

CHAIRMAN BROWN: I am not arguing about that. The point being is that if they are already co-mingled then you've got a potential problem and you are going to bury yourself in all these other potential solutions.

MR. DOWNS: There are other ways of providing cyber security rather than, you know, just to, you know, isolation one-way data diodes.

CHAIRMAN BROWN: How is that?

MR. DOWNS: Well we've got a list of several hundred controls in our appendices that go through, you know --

CHAIRMAN BROWN: Are they software-based controls and firewalls?

MR. DOWNS: No, there are -- Some of them

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

are, some of them are more than that, and as a total, they function as a total, it's not, you can't single out one individual thing, this goes into that defense-in-depth concept, right.

CHAIRMAN BROWN: If you have all analog systems it works real well.

MR. DOWNS: Sure it would. Yes, absolutely. But, unfortunately, again, we can't require that, right. But there are analog systems that licensees could credit in lieu of providing cyber security controls that, you know, would be an effective measure of preventing a cyber attack from causing a consequence of concern.

So that's the premise of, you know, the rule. Our rule is to -- We've kind of accepted the fact that the reconfiguration of licensee systems, as a regulatory body we have very little control over that.

What our cyber security rule looks to do is provide a bubble or a bunker around those systems so that they are adequately protected given the inherent flaws that may be present in them, and that's how we have geared the presentation and the development of the cyber security controls that are

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

present in the guidance document.

MEMBER MARCH-LEUBA: I hope we get into that discussion this afternoon on the reg guide, but most of the industry's cyber security plans are geared towards restoring the service after an attack is identified.

In this case when the attack is identified with a cloud of HF is filling up your building so restoring your service after that is of no consequence to the impact.

And by reading through the reg guide I see that you are following a bank approach to cyber security as opposed to the HF cloud is moving through already.

MR. DOWNS: Right. Preventative, so --

MEMBER MARCH-LEUBA: So we'll talk about it this afternoon.

MR. DOWNS: Well actually the next slide actually gets into that a little bit. So the Paragraph B of the proposed rule lays out the program performance objectives.

As you see here it is detect, protect against, and respond to a cyber attack capable of causing a consequence of concern. The National

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

Institute of Standards and Technology, and I'm going to call them NIST from here on out because it's a mouthful, they published a framework for improving critical infrastructure cyber security.

They published this document in early 2014. They lay out five concepts in their framework-- poor elements that describe functions to organize cyber security effectiveness, and these are identify, protect, detect, respond, and recover.

Again, this is all in reference to critical infrastructure which doesn't exactly capture our fuel cycle facilities, but we took the concepts out of this document and incorporated them into our rulemaking through these performance objectives.

The recover piece of it from a regulatory perspective recovery from a cyber security sense would mean to get the business back up and running, and that's not something that as a regulatory agency we are, you know, concerned about.

That's obviously a business concern that these individual licensees could, you know, look to recover, they would be looking to recover and restore their operations.

The other piece is identify, identify we

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

kind of baked into the rule here. We lay out a process to go through and identify all the various digital assets and screen them out or establish those that are most risk significant that would require protection. Paragraph C are our --

CHAIRMAN BROWN: What --

MR. DOWNS: -- consequences of concern. Go ahead.

CHAIRMAN BROWN: I'll save it for this afternoon.

MR. DOWNS: Okay. So instead of trying to deal with that cloud of HF, you know, after it has been released the rule tries to, it looks to protect against these four types of consequences of concern.

Latent consequences of concern would be those that the compromise of the function occurs via the cyber attack and then lays dormant for a period of time until an initiating event would cause that function to respond, would require that function to respond to prevent a consequence.

So compromise of functions, as I am sure you all are aware, very difficult to detect. So we've laid out these consequences of concern to protect against a latent, that latent concept as well as an

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

active.

An active would be where the cyber attack directly causes the consequence of concern, basically, you know, something over the keyboard or through the malware that's been planted causes the release to occur at that point.

MEMBER STETKAR: Okay. James, just to telegraph for this afternoon, I am sitting here as a surrogate for Dr. Dennis Bley who sent us some comments and said --

(Simultaneous speaking)

MEMBER STETKAR: And I have some comments along the same way. I want to delve into the notion of the scope of those active consequences of concern.

It's better -- I get it. Dennis had some questions in the rule language and I think it's better, from my understanding anyway, to address them in the regulatory guide space anyway.

MR. DOWNS: Okay.

MEMBER STETKAR: I hope somebody is prepared to think about that. Thanks.

MR. DOWNS: Okay. So at this point it should be noted that the existing physical security regulations at fuel cycle facilities are focused on

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

material attractiveness, as we have talked about earlier today, and that would be, you know, theft of low enriched versus high enriched.

It would take a significant amount of low enriched material to cause a concern. So the latent consequence of concern safety and security, even though it says it applies to all facilities the security piece here is focused on the protection of classified information and matter.

It's not focused on the material control and accounting aspects of Category I or Category II facilities. Those are covered up in the latent design basis threat and the latent safeguards consequence of concern.

As you can see these consequences apply only to specific facility types, except for the safety pieces that would be applicable to all.

The intent is to prevent a cyber attack that could cause one of these consequences of concern directly or it compromises a function needed to prevent an event that is associated with a consequence of concern and that whole concept of active latent there.

The consequence thresholds that we are

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

using in the rule are formed by existing regulatory requirements. Earlier Brian went through several of the Part 70 requirements for safety.

As we will see here on the next slide the threshold for the consequences of concern map directly to those existing thresholds, so this isn't a new concept for the fuel cycle facilities. This is something that they have been exposed to in the past.

CHAIRMAN BROWN: So the threshold that you are talking about is like when we get to the table you got, the next page, you are talking about those items that are in the -- like radiological sabotage or theft or diversion?

MR. DOWNS: Right.

CHAIRMAN BROWN: That's the thresholds?

MR. DOWNS: Yes, that would be a threshold.

CHAIRMAN BROWN: Or is it a program that the -- The objectives, I guess if I am, that's what I would have -- Am I correct in assuming that's what you would have called program objectives for these items?

MR. DOWNS: Right. That's correct, yes.

CHAIRMAN BROWN: Okay.

MR. DOWNS: So here is that chart that was

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

just alluded to here. We can kind of go through some of the unique aspects of fuel cycle.

As we discussed earlier is this concept of protecting the worker with very specific thresholds, so that's why in the active safety you'll see that that that 25 rem is for any individual, it's not just outside the control boundary.

Acute chemical exposures, again, we're talking about any individual. It's not just outside the control boundary. Any questions on those thresholds or how they relate to --

CHAIRMAN BROWN: No, I've just got a question on theft or diversion of special nuclear material. I am trying to picture guys walking out of the plant with a bag of uranium hexafluoride or UO₂ if you are in a fuel manufacturer.

Where do you -- That just seems to be a little bit -- Obviously, you have to talk about it or think about it, but it's just --

MR. DOWNS: Again, that consequence of concern would only apply to, that design basis threat would apply to Category I facilities, so you would be talking about highly enriched uranium.

Obviously, there are many layers of

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

defense that are present at these facilities and part of the intent of the rule is to allow those layers of defense to be credited in lieu of providing cyber security for the exact reason that you laid out.

You know, just because a process loses connection or, you know, a denial of service attack or something along those lines, it doesn't mean that the material is going to walk itself offsite.

So that's where it's -- You've got to, you know, there is that interface between cyber security and physical security, we need to have a balance there, and that's what the -- Through the alternate means considerations that's what we are hoping to achieve there.

MR. BARTLETT: And note that these are latent, right. So you're not stealing it by cyber, you're using cyber to facilitate the theft.

CHAIRMAN BROWN: Yes, but still there is, stuff comes in the door and you know how much came in the door --

MEMBER STETKAR: You think you know how much came in the door.

CHAIRMAN BROWN: Yes. Well if it came in on a truck I would imagine, you know, you'd have to

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

have a latent threat that succeeded in not identifying something at Honeywell that got on the truck and then it -- but it wasn't what you thought it was and you got in and when you checked it it wasn't what you thought it was and then when it's finished being utilized it wasn't what you thought it was and you didn't know it the whole time.

MEMBER MARCH-LEUBA: Yes. Following that line of thought I have an issue with the language in the rule and this is -- when it says loss on NMC&A for SNMs, I won't spell everything, there is a failure mechanism or an attack mechanism which I can see in which you compromise the MC&A and I gain access to the database.

That tells you how many, seeing they move from here to here, and immediately I remove one of those there and I ship it to my office in downtown Baghdad and if I have control of the computer I can modify all that.

So when the language says loss of MC&A it implies you lose completely your ability to do it. You really should say compromise because it goes into -- You understand I can go into -- You see the movies when the guys go there and say, okay, ship that

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

container to my garage in Los Angeles.

MR. DOWNS: Sure, sure.

MEMBER MARCH-LEUBA: And the guys will go there and ship it via FedEx.

MR. DOWNS: So the compromise piece is actually included in the -- If you look at the rule language there in C(1) the compromise is up in the top part of that paragraph.

So it's the compromise as a "result of a cyber attack" and blah, blah, blah, blah, blah, "of a function needed to prevent one or more of the following."

So if it's a function needed to prevent the loss of MC&A, of SSNM, that would, that's how we've captured it there, but I hear what you are saying.

If you just focus on the (iii) or the (ii) there it doesn't capture that compromise piece, it's just because it's rolled up in the top of that paragraph.

MEMBER MARCH-LEUBA: Yes. I mean it would make it more clear that it's not just losing your ability of tomorrow recording new events, but losing your ability of keeping chain of control of what was

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

there because these facilities are extremely automated.

I mean almost a robot handles the cylinders and the computer tells it to load this one on that truck.

MR. DOWNS: Depends on the facility.

MEMBER MARCH-LEUBA: Yes.

MR. DOWNS: But there are facilities like that, that's true, yes.

MEMBER MARCH-LEUBA: There is nobody thinking about oh, how come this is going to Baghdad. The computer told it so.

CHAIRMAN BROWN: Well wouldn't they have to put the five pounds in a shielded box so that you couldn't measure any radiation levels that went out?

MEMBER MARCH-LEUBA: No. No, it wouldn't be going to a foreign country because it would need an export license, but you can ship it to --

CHAIRMAN BROWN: Well even out of the facility. I mean I can't see shipping it to your garage, Jose.

MEMBER MARCH-LEUBA: Well those cylinders come out of the facility all the time in trucks.

CHAIRMAN BROWN: Yes.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

MEMBER MARCH-LEUBA: I'm just changing the shipping notice.

MR. DOWNS: But there are manual checks the licensee performs.

MEMBER MARCH-LEUBA: Yes, I am sure it will be harder to do.

MR. DOWNS: It's not -- Yes.

MEMBER MARCH-LEUBA: But that's why we are --

CHAIRMAN BROWN: My part of this argument that I would get into is how do we apply our cyber security rule and guidance to not be so intrusive and so encumbering that you drive the cost so far out of sight that it's just not a good idea?

And I was only commenting, and Jose as well, on some of these theoretical things just to make that point. I mean the guidance is extremely, extremely detailed from a big picture standpoint.

And by the time I finished reading it it was almost things were still, it was almost everything had to be turned into a vital digital asset.

Now I am exaggerating, okay, that's the way I do business just to have fun. And I can't comprehend, you know, that every one of these things

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

has to be encompassed under this umbrella or that I have to review, I don't know, 10,000 computers within a facility in order to accomplish this end result that's all.

It's just almost -- It almost looked like a one size fits all so I am trying to encourage you all to tell us why it's not a one size fits all and why it is easy for the licensees to be able to apply this guidance and rule. Pardon, John? Go ahead. Was that you? Go ahead.

MEMBER STETKAR: Well it's --

CHAIRMAN BROWN: We're not shy.

MEMBER STETKAR: -- not clear that it was intended to make it easy, but --

CHAIRMAN BROWN: Well we'll get into it in the guidance. We're talking about the rule right now. Okay, go ahead.

MEMBER STETKAR: All right.

CHAIRMAN BROWN: Thank you.

MR. DOWNS: Okay. So the next slide here.

CHAIRMAN BROWN: Oh, we will break at 1:00. We are ahead of schedule.

MEMBER STETKAR: We'll break at noon.

CHAIRMAN BROWN: I'm sorry, what did I

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

say, 1:00? Yes, I would never make it to 1:00, I guarantee that.

MEMBER STETKAR: They can't get through three slides in seven minutes.

MEMBER MARCH-LEUBA: We can break --

MR. DOWNS: I mean this is a good stopping point if --

CHAIRMAN BROWN: This is a good stopping point?

MR. DOWNS: Yes, because I am in between paragraphs here and I'll start laying out the program next, so --

CHAIRMAN BROWN: Yes, you're going -- The next is the cyber security program, right?

MR. DOWNS: Right, yes.

CHAIRMAN BROWN: Okay. We'll go ahead and break now until 1:00 o'clock and we will reconvene at 1:00 o'clock. We are recessed. Thank you, John, I appreciate that.

(Whereupon, the above-entitled matter went off the record at 11:52 a.m. and resumed at 1:02 p.m.)

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

A-F-T-E-R-N-O-O-N S-E-S-S-I-O-N

(1:02 p.m.)

CHAIRMAN BROWN: We're going to reconvene.

And we will proceed with -- Mr. Downs will proceed with the rest of his elaboration.

(Off the record comments)

CHAIRMAN BROWN: Oh, it'd be a great idea.

Okay, we are B- what did I say we were doing?

Reconvening, exactly right. We are restarting. And we'll proceed. James, you can go ahead with Ellis and all kinds of good stuff. And by

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

the way, we've been joined by our consultant, Myron Hecht, on the phone line.

MR. DOWNS: Cool, sounds good.

CHAIRMAN BROWN: Okay.

MR. DOWNS: Okay, thank you, Charlie. So we left off with Paragraph D of the proposed regulation which discusses the requirements for the cyber security program. Again, the goal here is to meet the performance objectives that were -- the program performance objectives that previously outlined the -- to protect against and respond to a cyber attack.

To do that, there's a requirement for licensees to establish and maintain a cyber security team that is adequately staffed, structured, trained, qualified, and equipped to implement the cyber security program.

That cyber security team really is the hub, as we've designed this proposed regulation. They are the ones that are going to be doing many of the tasks that are outlined through it. And our guidance elaborates on that.

That would be one. (d)(2), establish and maintain a set of cyber security controls for each

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

applicable type of consequence of concern. Controls are unique by facility type. And the reason for that is because the consequences of concern are unique by facility type.

Not everybody has to protect against the DBT. Not everybody has to protect against the safeguard considerations as we've laid out in Cat II.

CHAIRMAN BROWN: Do you have an example of cyber security control, what you mean by that?

MR. DOWNS: Sure. We can flip any -- so the way that the draft guidance document is arranged, the controls are present in Appendices B, Bravo, through F, as in Frank.

Each one of those chapters, the Chapter Bravo is overall controls that are applicable everywhere for all vital digital assets. The remaining Appendices, C through F, are specific to the individual consequences of concern.

So what you can do is look at (c)(2), for example, account management procedures. There's a long list there of performance specifications that would require the application of measures to address these performance specifications. Some of them may be as simple as assigning an account manager which is

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

more of an administrative type specification.

Something a little more technical could be monitoring the use of VDA accounts. How that monitoring is done could actually be some form of a database or, you know, a cross check, or something of that nature.

CHAIRMAN BROWN: Let's go back to B, since that's the VDAs, right?

MR. DOWNS: All of these are VDAs. All these appendices would only be applicable to VDAs.

CHAIRMAN BROWN: I'm trying to B- in Appendix B there were 48 items.

MR. DOWNS: Correct.

CHAIRMAN BROWN: With upwards of 9, 10, or 11 bullets per item of things to do, protect, what have you. And if you go to C, there's another -- in other words, that works out to be several hundred. And then if you do the counting in some of the other ones as well, it works out to lots, and lots, and lots of specific items.

I mean, is there supposed to be a checklist where you go down, and now you're going to demonstrate that they comply with each and every one of these, or meet each and every one of these, or

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

whatever it is?

MR. DOWNS: In essence, yes. That's correct. There would be your implementing procedure for each vital digital asset would capture the measures that have been taken to satisfy these performance, yes, the performance specification.

And the reason these controls are necessary goes back to the conversation we were having earlier that, you know, we can't force anybody to re-architecture the system. So therefore, in order to protect it, these are the elements that come into play.

MEMBER STETKAR: I think we'll get into this more when we get into the guidance itself. But the implication is that that big, long laundry list of things is, A, necessary and, B, sufficient. I suspect neither of those is absolutely true.

So creating large checklists with the implication that checking off all the boxes is, I can't say required, because it's regulatory guidance, and that by checking off all those boxes, you are adequately protected, oftentimes has led us into situations where we've discovered we weren't. So we'll discuss that more, I think, when we get into the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

guidance itself.

CHAIRMAN BROWN: Yes, I'm actually B-

MEMBER STETKAR: It seems pretty onerous, but that's guidance, it's not the rule. We've got to get through the rule first.

MR. DOWNS: Correct.

CHAIRMAN BROWN: Well, he referenced the appendices which, that's when I B- when he did that, just pulls one out. And some of them have even more than that, 48. And I didn't have any big, you know, gross disagreement for what I would call the top level, big, bold bullets, you know, which were general area topics that people should address. But it was the proliferation of sub-bullets that got me thinking about it, that's all. Go ahead and B

MR. MALTESE: I'd say that, well, I'd say two points might be worth making at this point. One is that the list of controls in the guidance does represent a list that the NRC finds acceptable to use for vital digital assets, not to say that licensees cannot propose other controls that we would review and also that not every control will be applicable to every vital digital asset.

MEMBER STETKAR: We'll get to the guidance

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

when we B-

CHAIRMAN BROWN: Yes, let's B- I agree with --

MEMBER STETKAR: The implication is that if I have a list of 243 things in the guidance, I have to sit down and say I'm not going to apply this, because today we have this sort of thing. And that takes a heck of a lot of time and effort, not only by me, as a licensee, but by the staff.

And the staff will say, well, I don't agree with the fact that in Paragraph 37 you put a comma in there. And could you please explain why you put a comma there, because you might interpret that as a way of not complying. So we'll get to it when we get to the guidance. The guidance is very onerous.

MR. DOWNS: Okay. So here with the rule language, again, the (d)(2) just established B- is the requirement to establish and maintain a set of controls for each applicable type of consequence of concern.

So by that, we mean Category I facilities would have a list of controls applicable to the design basis threat consequence of concern. It would also have a list of controls applicable to the active

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

safety consequence of concern.

And it would have another list for the latent safety and security consequences of concern and with the assumption that those controls would be graded in such a manner that the DBT, and we talk about this in the guidance, the DBT threat is of a higher significance. So therefore, those controls will be more robust.

Let's see, just as an aside, the controls here were modeled after the controls from the NIST Special Publication 853 and NIST SP 882. Eight hundred, fifty-three is applicable to federal information systems. Eight hundred, eighty-two is the guide for industrial control security.

Those standards establish control sets organized by low, moderate, and high impact. And what we did was we tried to model, in the guidance document, we tried to model our example controls after the corresponding impact levels associated with those consequences of concern.

The NIST controls are written generically.

So as the rules require the security controls be described, you would have to make them specific, so the licenses would have to develop applicable B- make

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

them pertinent to the applicable consequences of concern at their site.

Any questions on controls, anything pertaining to the rule? No.

MR. HECHT: This is Myron Hecht. Can you hear me?

MR. DOWNS: Yes.

MR. HECHT: Oh, great. Okay. When you discuss the reg guide itself, will you be talking about how you've decided which controls are applicable to which kind of facility and why, for example, you have 148 controls in Appendix B, and you have a few less in Appendix C, and a few less in Appendix D and E. I think it goes down to 91 in Appendix E. Will you be describing your overall approach in deciding which controls apply?

MR. DOWNS: We can definitely go into that. That discussion can get a little in depth very quickly, but we can try to state some of our overall guiding principles.

CHAIRMAN BROWN: I'll interrupt here. What I suggest we do is, when we get to the reg guide itself, we'll B- a couple of examples to help us focus your thinking, not necessarily what B- obviously we're

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

not going to go through every one. But some examples just to illustrate the thought process would be useful at that time, I think.

MR. HECHT: Okay, great.

CHAIRMAN BROWN: Is that okay, Myron? I don't want to go through the laundry list, just to get a little bit of their thought process, to get an example of they came up with B-

MR. DOWNS: Well, I made a note here on Slide 58 to go into that when we get there.

CHAIRMAN BROWN: Okay. That's good.

MR. DOWNS: Okay. So back to the proposed rule requirements, Paragraph (d)(3). This is identify digital assets and support systems that, if compromised, could result in a consequence of concern. The intent here is to document these assets, digital assets, so there's kind of a hierarchy here. Digital assets are associated with the consequence of concern.

That's not saying that those assets will be required to have cyber security applied to them. Vital digital assets are a subset of the digital assets. Only vital digital assets will be required to have cyber security applied to them.

And this process here in identifying and

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

determining -- identifying digital assets, determining the vital digital assets, this is kind of the process to get to that subset.

So documentation of digital assets, which is the larger set, is required by the rule. The reason there is primarily for configuration management type concerns over the life of the facility. Certain alternate means may be modified or eliminated, and the adequacy of the identification of those assets could come into play. So that's what it really boils down to. It establishes that baseline set of digital assets related to a consequence of concern.

There is the note here, as we previously discussed, that assets are part of a classified system, a creditor authorized by another federal agency are excluded from the rule. And this is because we considered protections provided by those other federal agencies are acceptable to meet the intent of the rule.

So (d)(4), determine vital digital assets, again, you take that set of digital assets, determine the subset of vital digital assets. The key here is the alternate means.

For digital assets performing a function

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

for which an alternate means can be credited, those assets would not be considered vital. So vital digital assets have no alternate means to perform the function that they're credited for.

CHAIRMAN BROWN: And you'll be able to provide some examples of what you mean for that when you get into the guidance?

MR. DOWNS: Sure. I actually can provide a real quick example right now. In a process line that's processing UF6, you may have several digital components to that process line that could, if compromised, those digital components could create an overpressurization to that line.

So therefore, you could potentially cause a release of UF6, tripping one of the thresholds for a consequence of concern. That's the sort of analysis that's done in the ISA through the process hazard analysis piece. Those digital systems there could be credited as IROFS, potentially.

The fact that they're compromised may or may not B- I should say, so an alternate means then, instead of protecting all of those digital assets, there could be something very simple as an overflow tank is provided. So that if the line were to

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

overpressurize, the volume of that line would go into an overflow tank and remain contained.

CHAIRMAN BROWN: A relief valve in a containment tank then.

MR. DOWNS: Exactly. Right. So therefore, that would be an acceptable alternate means. So therefore, none of the digital assets on that line would be required to be protected. They would not be identified as vital digital assets.

MEMBER STETKAR: James, and I don't B- tell me if it's better to discuss it in the context of the reg guide as opposed to now. You brought up an example. I have questions about other examples, but I don't know whether it's better B- were you going to talk about the identification of vital digital assets alternate means, and boundaries of digital assets as part of the reg guide?

MR. DOWNS: Yes, we'll, okay, go to the next level of detail, surely.

MEMBER STETKAR: I will wait for that then.

MEMBER MARCH-LEUBA: Sorry to bring up too much detail, but in the case you just were describing, where you have an overpressurization in there, in the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

centrifuge cascade, what the plan to do is you adopt two tails. So they just open up the tail valve, and close the product valve, and then dump it out.

Now, if I gain control of that pressure regulator, PLC, that's maintaining the pressure, and I get control to the valve that opens the tails, then it becomes B- if I have access to those too, then it becomes a critical asset.

How do you identify those? Because you just told me those pressure regulators are not critical asset.

MR. DOWNS: Well, so this gets into the second bullet here on the screen. Alternate means must be protected from a cyber attack. So if there was some way that the overflow tank could B-

MEMBER MARCH-LEUBA: There is a valve that opens the overflow tank.

MR. DOWNS: Exactly, right.

MEMBER MARCH-LEUBA: And I have obtained cyber security access to the pressure regulator, and the valve.

MR. DOWNS: Exactly.

MEMBER MARCH-LEUBA: Then that suddenly becomes a critical function.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

MR. DOWNS: Definitely. So B-

MEMBER MARCH-LEUBA: If I was --
centrifuges, bad things happen.

MR. DOWNS: Sure.

MEMBER MARCH-LEUBA: So how do you, I
mean, obtaining access to one of them is not bad.
Obtaining access to two of them is bad.

MR. DOWNS: Exactly.

MEMBER MARCH-LEUBA: The safe thing is to
make them both critical.

MR. DOWNS: Right. So what we've done is
that really, in essence, only one would need to be
protected. Because if you had B-

MEMBER MARCH-LEUBA: One of the two?

MR. DOWNS: One of the two, right. So if
you were to identify the overflow tank as an alternate
means, in order to meet the requirements of the rule,
that alternate means would need to be protected from a
cyber attack. So therefore, you would protect that
valve associated with the tank.

MEMBER MARCH-LEUBA: Yes.

MR. DOWNS: Alternatively, you could say,
well, I'm not going to identify the tank as an
alternate means. The benefit to us would be we're

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

going to protect the other assets.

So again, this is the flexibility in the rule as to how the licensees want to proceed. They have that option as to which assets they want to protect. They, you know, just need to B- if they can identify that an alternate means is present and can credit it, that it's protected from a cyber attack, then that's acceptable to us. Or they could just protect the asset, the other asset.

MEMBER MARCH-LEUBA: Yes. I see where things can fall on the ground and you never pick them up. That analysis will have to be very thorough.

MR. DOWNS: Yes, yes. The last bullet on this slide, the terminology, we tried to make the terminology in this rule different from the terminology in the reactor rule. We're not using the term critical digital asset here. That was just more or less for an ease of communication.

We didn't want overlap, you know, between guidance documents thinking that what was done on the fuel cycle side of the house is applicable in reactors or vice versa. So that was just the reason that we chose different terminology.

Okay. Requirement (d)(5), this

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

requirement ensures that each vital digital asset is protected against a cyber attack by doing two things.

One is identifying the controls applicable to the associated consequence of concern.

So again, here you've got a vital digital asset. We're going to B- how do you protect that vital digital asset? You're going to identify the applicable controls. Then, two, you document those controls in written implementing procedures.

Implementing procedures, in the NIST world, you could say they're somewhat equivalent to information system security plans, ISSPs. There are some similarities there. But the bottom line is that you need to be able to document the measures taken to address the performance specifications of the identified controls.

(d)(6) provide intercompensatory measures, and measures are degraded. This is kind of a forward looking thing. You know, obviously things happen in facilities, and you need to take interim compensatory measures.

We just are looking to have that ability there, that the licensees have the ability to provide B- they have procedures in place to consider the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

interim compensatory measures and whether they are applicable to a certain situation. And if they are, they need to be documented, tracked to completion, and available for NRC inspection.

That's the last measure here on the B- or provision for the cyber security program. Are there any questions on the program, hopefully?

CHAIRMAN BROWN: Do you envision interim compensatory measures to be procedural or could even be other equipment that could be then put in service or B-

MR. DOWNS: It could B-

CHAIRMAN BROWN: Have you made any B-

MR. DOWNS: It could be anything, really.

CHAIRMAN BROWN: So you haven't really defined it anywhere?

MR. DOWNS: I mean, the guidance document talks about it a little bit. The key here is just that they're documented and tracked to completion and obviously that they also meet the program objectives, the performance objectives.

There's not B- as you said, talking about the various controls, you could see some of the controls are administrative in nature. Some were more

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

technical in nature. So the interim compensatory measures could be all over the map, as far as what they pertain to.

MR. HECHT: This is Myron. Can I ask a couple of questions?

CHAIRMAN BROWN: Go for it.

MR. HECHT: Okay. Number one, on the aspect of the program itself, I didn't see any provisions in the controls and leading up to the regulation concerning custom developed software.

On the reactor side, if there's a basically critical software, there are very explicit guidelines in the Q/A section of 10 CFR 50 concerning how that's done. And there's nothing here about that.

CHAIRMAN BROWN: Are you talking, Myron, are you talking about in the rule?

MR. HECHT: No.

CHAIRMAN BROWN: You're in the reg guide?

MR. HECHT: There has to -- what I'm wondering is that shouldn't there be a place in the rule for that?

MEMBER STETKAR: Myron, you weren't on this morning. This is John Stetkar. My opinion is that the more stuff you put in a rule the worse off

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

the rule becomes. Because people will use it as a necessary and sufficient checklist. And I don't think you want rulemaking to do that.

Regulatory guidance is intended to serve that purpose. So if we want to discuss details about what's in and what's not in the regulatory guide, that's good, under the regulatory guide. But, you know, what you want in the rule, and what Charlie wants in the rule, and what I want in the rule will suddenly become a list of, you know, six things. And it's not good to start listing six things, because maybe there ought to be seven, or 12, or three. So we had a lengthy discussion of that earlier.

MR. HECHT: Okay. Well, that implies that there's a place where custom developed software would fit. Where would it fit?

MEMBER STETKAR: In the regulatory guide somewhere.

MR. HECHT: So which of these six B-

MEMBER STETKAR: When we start to talk about the regulatory guide, that would be a good question, I think.

MR. HECHT: Well, it should fit into one of these B-

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

MEMBER STETKAR: We're not talking about the regulatory guide.

CHAIRMAN BROWN: Well, hold on, hold on, hold on. What did you say, Myron?

MR. HECHT: I say it should be traceable to one of these six elements of the cyber security program.

MR. DOWNS: Sure. I can kind of trace it back, if you like. So what you would have there are custom developed software. I'm assuming this is custom developed software that controls a specific process. Okay, so --

MEMBER STETKAR: That's as good as any other?

MR. DOWNS: What you would have in that situation is would that custom developed software, would that be a vital digital asset or not? And that determination is based off of whether or not it has a consequence of concern.

And those consequences of concern could range B- we've gone through those ad nauseum at this point, so you know what the consequences of concern are. But the bottom line here is if that is determined to be a vital digital asset, then you would

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

need to apply the cyber security controls to it.

MR. SHINN: And let me just add, this is Mike Shinn, NSIR contractor, there are controls in the reg guide for the development of software as well as vital digital assets that provide the B-

CHAIRMAN BROWN: Well, there's a listing for custom software. I saw the words custom software somewhere.

MR. SHINN: Correct.

CHAIRMAN BROWN: I just don't remember where.

MR. SHINN: That's correct. It is in the reg guide.

MR. HECHT: Okay. So we know it's in the reg guide. But the point is, unless it's traceable to the rule, the reg guide provision doesn't really have the same force as if it is traceable. So that B-

CHAIRMAN BROWN: Well, Myron, what they're trying to tell us, and I was on, you know, I've read your stuff, and I was kind of on this same sheet of music also. But they're tracing back on a global basis to a global set of consequences of concern rather than specific details relative to the listing we have in a reg guide or anything like that.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

So I'm not saying that's necessarily the best or only, but that's the discussion or the argument they've used, or not argument, the points they've made in some of the other discussions that we've gone through.

So that we've effectively got -- the way I interpret that is, if you look at the rule, you've got either the consequences of concern, or you've got meeting some item in what I would call the program development and/or the planned development, or configuration, that those are global type traceability issues as opposed to specifics where you pick up certain items back in the reg guide.

You've kind of, you've globbed them all together as a big hunk back in the reg guide as opposed to poking a specific thing. So that's the way I read it. I'm not sure how to deal with that one yet. But that's a pretty general type of traceability.

MR. HECHT: Okay.

CHAIRMAN BROWN: All right?

MR. HECHT: Yes, thank you.

CHAIRMAN BROWN: All right. No, that's good. Thank you.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

MEMBER MARCH-LEUBA: I have a qualification question. In my mind, when I was reading asset, I was identifying it with a piece of hardware, I mean, a computer, a PLC, a microphone. You used it as a software? Software would be an asset? I mean, if I load Excel on one of those computers, suddenly we have to deal with Microsoft Office as an asset?

MR. DOWNS: So the software obviously would key on the asset at which it was loaded to and was actually performing the function that could be compromised.

MEMBER MARCH-LEUBA: So when you say asset, you mean a computer?

MR. DOWNS: For the most part, yes. We've got a definition, I think, of what a digital asset is.

MEMBER MARCH-LEUBA: I'm easily confused.

MR. DOWNS: No, no. I think B- no, it's a good point. I mean, obviously the software itself, software just sitting somewhere doesn't do anything, right? You need something to put it in motion. So, yes, it would be that function, right. The function is what we're looking to protect.

CHAIRMAN BROWN: The functionality of the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

software that you're talking about.

MR. DOWNS: That's right.

CHAIRMAN BROWN: That's already coded in some memory unit.

MR. DOWNS: That's right. Okay. Paragraph E, this is where we get into the requirements for the cyber security plan. Just to be specific here, this is the document that the licensee would submit for NRC review and approval. It's site-specific, and it describes how the program performance objectives are met. And that's the detect, protect, and respond piece that we've been talking about.

Part of this also would get into the incident response. By incident response, we mean cyber security incident response. This is different from the event response that's already present at the fuel cycle facilities today as far as emergency response goes.

This is, you know, the cyber security is, it's a specific element associated with cyber attack.

So the plan would either describe how the requirements of the section are satisfied, how the program is managed, and focus on that incident response piece.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

The supporting documentation, it talks about policies, implementing procedures, all these other items that form kind of the arms and legs of the cyber security plan. Those would all be maintained onsite for inspection. Any questions on the plan?

(Off the record comments)

MR. DOWNS: Yes, that's a good point. So Matt just brought up the controls, we talked about the documentation of controls. The controls would actually be in the plan itself. It's the B- there would be B- we've got a template in one of the appendices in the guidance document that just lays out some of the considerations, just a general format for what a security plan can look like.

And it discusses the methodology for identification. It discusses the controls that would be applicable. It discusses alternate means a little bit in there as well.

So it's, again, this document is, since it's going to be incorporated into the licensing basis for each of these facilities, this would be a citable document by NRC inspectors. So when the staff reviews it, you know, once it's submitted for staff review, the staff needs to make sure that it's enforceable

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

going forward, it's at the right level of detail. And that's what we're trying to provide by guidance on that in the regulatory guide.

Okay, Paragraph F, this establishes requirements for configuration management. There are -- obviously, we want to ensure that -- the intent is to ensure that facility modifications are evaluated prior to implementation and that these modifications would not adversely impact the program performance requirements.

Obviously, a facility modification could do any number of things. You could have a new process. And in adding that new process, you could add an additional digital asset that was previously not considered. You could potentially remove an alternate means that was already credited.

So these are the sorts of things that we talked about in configuration management. The key piece here is that the system, the configuration management system must be documented in written procedures and available for inspection by NRC staff.

So this is B- most of these facilities have some element of configuration management in place already.

It's just establishing that cyber security

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

considerations need to be a portion of that overall configuration management process.

MEMBER STETKAR: James, I had a question.

When I read this paragraph of the rule, this is now the rule, I stumbled across it a couple of times. And I went back, and I read the corresponding part of the rule for the power reactors.

And in particular, let me say, it says, "The licensee must utilize the configuration management system to ensure that changes to the facility, including modification of an existing digital asset identified through Paragraph (e)(3) of this section, are evaluated prior to implementation."

And it goes on.

Why do we need that comma offset phrase? The first time I read it I said, well, gee, they're just talking about modifications to the vital digital assets. And then I went back, and I said well, no, it says "ensure that changes to the facility" are evaluated.

When I read the regulatory guidance, it seems to be clear that any change to the facility, regardless of what I touch, needs to be evaluated. And unfortunately, in the power reactors, I think we

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

missed it. Because the power reactors' guidance specifically says just look at the critical digital assets.

So in the rule language, why do we need the including modification of an existing digital asset identified through Paragraph (e)(3) if the intent is that somebody needs to evaluate any modification to the facility by changing that light bulb?

MR. DOWNS: So the reason that that was in there was because, on the power reactor side, it focused on the critical digital asset.

MEMBER STETKAR: It didn't focus, it exclusively focused on it.

MR. DOWNS: Sure, right. And so our intent here was to B- now notice, this isn't a vital digital asset. This is existing digital assets. So this is the larger group. This isn't the subset. So that's where we wanted to make sure that the focus was, at least at that larger group level, the digital asset level. These would be the B

MEMBER STETKAR: (e)(3) says, "Identify digital assets that, if compromised by a cyber attack, would result in a consequence of concern identified in

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

Paragraph C." That's what it says.

MR. DOWNS: Right. And then (d)(4) gets into the vital piece which is the next step down. So what we were trying to do there was, and maybe we muddled the waters instead of making a clarification which, you know, so our intent was to focus that we're at that larger digital asset level, even though you may not be providing B-

MEMBER STETKAR: So I've done that. I comply with (d)(3) and I comply with (d)(4). So I now have my box of digital assets. And you're telling me I only need to look at modifications of those? I don't need to look at the modification to the plant that brings in a whole new control system.

MR. DOWNS: No, it'll be including modifications to digital assets. So you would need to look at overall. But the point here is that, on the reactor side of the house, you're only focused, if I want to B- you would only be focused on vital digital assets --

MEMBER STETKAR: Right.

MR. DOWNS: -- on the reactor side of the house. Here we're focused on, you know, it includes digital assets as well. We were trying to just get a

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

level of focus beyond the vital piece. I mean, the bottom line here is, I mean, I understand your comment. It's something that we can definitely look at.

MEMBER STETKAR: When I read the guidance, the guidance seemed, the regulatory guidance --

MR. DOWNS: Right, right.

MEMBER STETKAR: -- seemed more, I hate the term holistic, but I can't come up with a better word, more comprehensive or less restrictive. I didn't B-

MR. DOWNS: I agree, yes.

MEMBER STETKAR: I just want to make sure that somebody reading the rule, because that's the law, doesn't interpret this as saying by law I only have to look at this stuff that I put in this box over here. And by law, I don't need to look at any other things that I do to the plant.

MR. DOWNS: Right. And --

MEMBER STETKAR: Because the regulatory guidance isn't the law.

MR. DOWNS: It's a good point. And emphasizing these particular assets that should be included in the review of changes to the facility was

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

not meant to exclude any other changes to the facility that should also be looked at.

MEMBER STETKAR: And I'd suggest you step back and take a look at that rule language and make sure that it can't be misinterpreted as unduly constraining your intent. Because the regulatory guidance is the regulatory guidance.

MR. DOWNS: Right, right.

MEMBER STETKAR: And depending on how I read that, I could perhaps try to twist it different ways. Thanks.

MR. DOWNS: Thank you.

MR. HECHT: This is Myron. Can I ask a question?

CHAIRMAN BROWN: Go ahead.

MR. HECHT: Okay. We were talking about modifications to digital assets. And I looked up the term digital assets in the glossary. And it refers to a device, specifically an electronic device or organized collection of devices that either processes information, communicates data, or are programmed to manipulate licensed site machinery.

So what happens if I completely change the software configuration of that device, or I just

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

insert, on the other hand, an new anti-virus file?
Where do we set the limits on what constitutes a
modification of the facility if it's only if I replace
a device, or if I change anything for the software?
Or is software excluded because of the definition of
device -- of digital asset refers only to the device?

MR. DOWNS: So the intent wouldn't be to
exclude the software change there. I don't know if -B

(Off the record comments)

MR. DOWNS: I'm sorry, repeat.

MR. HECHT: It seems to me that it would,
because it says device. And software, I don't think,
is a device.

MR. DOWNS: So in the rule language
though, in Paragraph F, are you making a change to the
facility?

MR. HECHT: No. I'm changing software of
one kind with software B- with a later version, or
completely changing out the operating system, or
anything in between.

MR. DOWNS: I could see an argument for
that either way, to be honest. So that B-

MEMBER STETKAR: I think this is another
example of making it pretty clear what the intent of,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

in the rule, the guidance can elaborate on that intent but making sure that the rule language doesn't leave people vulnerable to misinterpretation of the rule.

And then, as you hear, some people interpret the word asset as, you know, something I can actually touch. Other people will say, well, a change, you know, my interpretation of a change to the facility would be, sure, if I change the software I'm changing the facility. Other people might not.

MR. DOWNS: Right. Well, it's a good comment. We'll have to take it back and consider B- I don't know, I'll be honest, I don't know if our guidance document addresses that.

MR. SHINN: It does, yes. I mean, certainly the intent --

MR. DOWNS: I think the guidance B-

MR. SHINN: -- is what everyone has talked about here, right.

MEMBER STETKAR: When I read the rule for, this is just me personally, I read the rule first. And I wrote down this question. And then I wrote a note to myself after I read the guidance document. I said, you know, Section 9, which is the appropriate section, seems to be -- more clearly indicate the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

intent. But I still had a question about the rule itself. Because ultimately, that's what people will go to bat against.

MR. DOWNS: Yes. The trick will be how to capture that in succinct language within the rule --

CHAIRMAN BROWN: Including modification of digital of assets. We certainly eliminate that particular notion of it.

MR. DOWNS: Well, again, I think Myron's point is that, by definition here, the digital asset is identified as a device. He said B-

CHAIRMAN BROWN: Well, I think B-

(Simultaneous speaking)

MR. DOWNS: -- on that device.

CHAIRMAN BROWN: Well, I could argue against that. Because I'm not saying I'm right, but if you read that definition, it also says it's a device for our program to manipulate. You know, programming it, it kind of gives you an assumption of software B-

MR. DOWNS: Yes, I agree.

CHAIRMAN BROWN: -- if you want to call it that.

MR. DOWNS: Right.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

MEMBER STETKAR: Let me read it again, what it says. It says, "The licensee must utilize a configuration management system to ensure that changes to the facility" -- I will now omit something B- "are evaluated prior to implementation and do not adversely affect the licensee's ability to meet the cyber security program performance objectives in Paragraph B of this section."

Now, one can then argue is installing new software a change to the facility or not?

CHAIRMAN BROWN: Yes.

MEMBER STETKAR: But it gets away from this notion of whatever glossary or dictionary you use that a digital asset is something that I can, you know, physically B-

CHAIRMAN BROWN: Yes, but it also says if I change the door on one of the rooms I have to go evaluate it. I mean, that can be B-

(Simultaneous speaking)

MEMBER STETKAR: It does, and that's the danger of that all inclusive.

CHAIRMAN BROWN: Exactly.

MEMBER STETKAR: On the other hand, there are other parts of the regulations that say if I make

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

changes to my facility I need to do, you know, it's a 50/59 type evaluation for a power reactor. I ought to do that if I make a change to my facility and assert that, you know, it doesn't affect the safety of the facility.

CHAIRMAN BROWN: And the only way I would see that out of that is if you deleted the including and just say changes to the facility which could result in a change in the consequences of concern identified in (a) and then go on after that. And that just covers what we were trying to protect against itself. That's all. And again, if you work on that one awhile, you can probably find a way to milk that B

MEMBER STETKAR: You guys are real smart about writing rule language. You get the comments.

MR. DOWNS: Absolutely. Yes, something we're not going to take back. Thank you.

So the next paragraph is the review, the periodic review of the cyber security program. Some recent stakeholder comment influenced the staff to divide this up into two different sections.

We've gone all over the place with this. Originally, we had planned to require an annual review which seemed a bit onerous, especially for Cat III

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

facilities that, you know, have a lower level of material tracked than is generally associated with them.

So what we ended up doing, we split it up into two requirements. 10 CFR 73.46(g)(6) actually has annual review requirements for Category I facilities, the security programs associated with them. So our intent here is basically to lump the cyber security requirements into that annual review as well. So that will be a corresponding change to B- we're proposing a corresponding change to 73.46(g)(6).

For all other facilities, which will be Cat II and Cat III facilities, Part 40 facilities, the proposed rule has a triennial review, so every 36 months.

The purpose of the review is to audit the effectiveness and adequacy of the cyber security program. And that would include the implementing procedures as well as a vulnerability consideration.

The point of this review is twofold. One, it's to make sure that the, if the configuration management is working properly, that you've got the proper cyber security controls that have been applied to these new processes.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

And the other side of this is also, as you're probably all aware, the cyber security threat will change over time. What one vector to -- you know, today's vector may not be tomorrow's vector. And things that we've never thought about today could be vectors tomorrow. So this is where this vulnerability evaluation comes into play.

And the process of documenting this evaluation also would make sure that it's tracked and addressed in a timely manner and fed to the licensee's plant manager and corporate management to make them aware of the changes every three years.

Any questions on the review, periodic review piece?

(No audible response)

MR. DOWNS: Okay. Moving on to event reporting and tracking. The fuel cycle facilities that exist today already have reporting requirements for many of the thresholds that we've talked about for consequences of concern.

They're going to be notifying us if one of these consequences of concern were to happen. So what we're doing here, the intent is to basically add on notification that, within 24 hours of discovery, that

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

it was a cyber attack that was involved with this event, the licensee was required to notify the headquarters operation office.

There's also tracking requirements here as well for lesser type, well, I shouldn't say lesser, but it's a failure or compromise of vulnerability degradation that results in a decrease in effectiveness of the cyber security control. We call these logables.

Most of our facilities have a log now where they have this -- that they'll record these sorts of things. And basically, that's just so that the inspectors can come through and see what's kind of B- what's been going on. And again, those events would be recorded and then tracked to resolution. And not B-

CHAIRMAN BROWN: Question?

MR. DOWNS: Go ahead.

CHAIRMAN BROWN: How do you know you can really identify that you've had a cyber attack, particularly if it's latent and doesn't cause anything to happen for a month?

I mean, some of these will sit there, and just sit there, and sit there until somebody turns on

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

a specific machine or somebody's accessed the function for the 14th time. There's a, you know, sense that malware or whatever you want to call it was inserted into the system. The detection of a cyber attack is pretty ambiguous.

MR. DOWNS: Right. The intent here isn't to provide notification of the attack. Notification would be required only if an event were to occur. And then in the process of B-

CHAIRMAN BROWN: Well, how do you know something didn't just break?

MR. DOWNS: Well, you're absolutely right.

CHAIRMAN BROWN: Sometimes it takes a lot longer than an hour to figure out whether something broke or not.

MR. DOWNS: Well, the hour isn't in regards to the event occurring. The hour is with, specifically here, it's within one hour of discovery that an event is the result of a cyber attack. So you've gone through, you know, you've had the event, you're going through the root cause analysis for the event.

And you discover then at that point that, hey, wow, this was actually a cyber attack that caused

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

this to happen. So that would be your point of discovery. So you've got an hour from then to notify the others.

But if I'm not mistaken, this is similar to the reactor reporting requirements, right?

MR. BERGEMANN: Well, so again, you could have an event, a safety event that occurs. And there's already existing regulations that -- this is Brad Bergemann from nuclear, NSIR CSD.

So you have an event, safety event or something. And they are requested to call it in by existing regulations. Potentially, two, three months later, after possibly sent in, you know, the hardware or something off to be analyzed, then you could find out that it was some sort of cyber attack that caused the event.

And, yes, it may come in as just some failure of a piece of equipment. And they wouldn't know what the reason or cause of the failure was until months later, possibly. And then they would still, based on that initial event, once they find out if it was a cyber attack, they would follow-up with that information.

MR. DOWNS: So by following up they would

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

amend the initial event report to say that it was due to a cyber attack.

CHAIRMAN BROWN: And you took so long to answer that I forgot my other question. But it was a --

(Laughter)

CHAIRMAN BROWN: -- real plus to --

MR. MALTESE: Good job, Brad. Well done. And to James' point about reactor reporting requirements, 73.77 is the cyber security event notification rule which also requires notification to the NRC within an hour of discovery of a cyber attack that adversely affected safety functions.

MEMBER STETKAR: I know, Charlie, I went back, and I compared the reactor with this. And that one hour reporting was conceptually B-

CHAIRMAN BROWN: The same?

MEMBER STETKAR: -- the same, one hour within, you know, just the, in the words of the late, great Peter Boyle, the holy crap moment.

As you characterized it, the logables that the requirements are a little different in the reactors versus this rule. These are a little bit less onerous, if you will. Okay?

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

CHAIRMAN BROWN: Okay.

MR. DOWNS: And every good rule has a records retention piece. There it is. And I don't know what more to say about that. You have to maintain superseded (phonetic) records for three years. Basically, it just goes through and details B-

CHAIRMAN BROWN: Oh, I remember.

MR. DOWNS: -- for the record.

CHAIRMAN BROWN: The problem is you kept talking long enough that I remembered.

(Laughter)

MR. DOWNS: That's a minus for me.

CHAIRMAN BROWN: Let me phrase this properly. Detecting the fact that you had a cyber attack is extremely B- can potentially be very, very complicated and difficult to untangle.

And the implication, to me, is the likely B- John's going to hate this word, but I'm going to use it anyway in this case B- likelihood of the need to address one of these.

If this happens often, that's a problem for other reasons, okay. If it happens once every year and a half, that means you've got to maintain a staff of extremely, extremely capable people at each

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

site in order to sit around whatever, you know, playing game boy or what have you -- I'm teasing a little bit there B- to be available in the event of something happening where they can dig into it, and then root out the cause, and identify. And that's difficult.

MEMBER STETKAR: That's why God invented consultants.

CHAIRMAN BROWN: So you're going to call in your consultants who do this routinely around the country that I didn't see -B I guess I didn't think about the use of contractors. I'm thinking about, after looking at you all's cost, you know, derivations and how low they were, and looking at NEIs and seeing how high they were, I was trying to find out is there B- I'm not arguing one's right, wrong, or anything else. That's not the point.

It's just that all the IT departments in major facilities I've ever seen have more people working on them in that area than anything else, just about the engineers disappear, and the IT operation takes over. And again, I'm probably exaggerating. But it's a difficult task, to say the least, to find people who can really do that.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

MR. DOWNS: Sure. And if I'm not mistaken, the Department of Homeland Security actually offers some of that service, that you can bring them in. DHS, ITS are B-

CHAIRMAN BROWN: That gives me a great feeling if B-

MR. DOWNS: I'm just saying that, you know, if you suspect a cyber attack, they can come in and, you know, take a look at what's happened. And the benefit there is that that interaction is actually held in some confidence. So it's not required to be reported to a regulatory body such as the NRC. That's the benefit for the licensee.

The downside for a regulatory body, such as the NRC, is that, you know, we don't have a good feel for what the current number of attacks at our facilities, the current number of successful attacks. They're not required to report that currently.

But having this rule making requirement in here, having the requirement for reporting, gives us some operational event experience that we can start, you know, kind of getting a better landscape for the threat as it specifically pertains to the fuel cycle facilities.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

CHAIRMAN BROWN: I don't disagree with the concept of reporting. Don't get that wrong, okay. It's just the difficulty of figuring out and the tact required to do that. And if you plan on having a roving team of contractors, I guess maybe that's one way of doing it. All right, go ahead.

MEMBER SUNSERI: So hopefully, sorry, you know, let me --

CHAIRMAN BROWN: Go ahead.

MEMBER SUNSERI: -- offer my opinion on this. Since you already said there's a different reporting requirement for within one hour of a cyber attack to report that, right? It's 10 CFR 70.53 or whatever you said, right?

MR. BERGEMANN: Well, so for the fuel cycle, based on their consequence of concern, if they had, like, a criticality or something, that would be called in under B-

MEMBER SUNSERI: So my incongruity with this is it says when known. So this doesn't say within one hour of an event decide whether it's a cyber or not. It says when known --

MR. BERGEMANN: Correct.

MEMBER SUNSERI: -- report within an hour.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

CHAIRMAN BROWN: When discovered.

MEMBER SUNSERI: Yes, right. So this could be, you know, months later. So then my question for you then, if it's something that can happen one month later why, all of a sudden, is this urgency to report it within one hour when the very next statement is the 24-hour reporting for failures of whatever. It just, it seems like the 24-hour reporting would cover the intent of what this one-hour thing sometime way after the fact.

MR. DOWNS: So the 24-hour, the requirement there in (h)(2), it's just the licensee must record the following. So there's no reporting to the NRC. It's just writing it down in the log and making it available for inspections. So that's (h)(2).

(h)(1) was actually, again, I mean, you nailed the timeframe, you know, pretty close there. It could be significantly after the actual event occurred that you have that aha moment where you say, oh, this is as a result of a cyber attack.

I don't think that an hour seems like a very short period of time to pick up the phone and call the NRC. However, I would be surprised if it

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

ends up being, I mean, how do you actually measure the time from that aha moment to when the report is received? It kind of B- there's got to be some flexibility in there slightly. The reason we said an hour is just to stay consistent with the reactors. And there's already guidance out there on that, on how to proceed with that.

MEMBER MARCH-LEUBA: Just for fun, and I guess search, cyber security attacks on my phone right here. These are the cyber security attacks that's happening right now on the phone.

MR. DOWNS: Right.

MEMBER MARCH-LEUBA: They're all originating from the -- originating from where it's affecting me too. And you can now load it in your browser anytime you want.

CHAIRMAN BROWN: Well, I've just reviewed my phone and --

(Simultaneous speaking)

MEMBER MARCH-LEUBA: I'm super protected on that one.

(Laughter)

MR. DOWNS: So again, the point here though is that B-

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

(Off the record comments)

CHAIRMAN BROWN: And I agree with you. So I don't have one.

MR. DOWNS: And some of our licensees have said to us that their systems are being attacked 1,000 times a day --

CHAIRMAN BROWN: Yes.

MR. DOWNS: -- you know, kind of thing. And that's just what's, you know, an attack could be as simple as just, you know, pinging an address. But what, you know, the key here is is that it's tied to than consequence of concern. So it's either one of those thresholds.

CHAIRMAN BROWN: Yes. Well, my computer must not be very important then. Because since 2006, that's ten years, my virus software has detected and removed three threats.

MR. DOWNS: Do you have it plugged in?

CHAIRMAN BROWN: Yes.

MR. DOWNS: I was just, okay, I just wanted to B-

(Laughter)

CHAIRMAN BROWN: It's off most of the time. It's off most of the time, I'll agree. That's

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

one of the B- I've considered unplugging it and unplugging the Internet connection every night also. But I just, you know, had to have some humor in here, that's all. I'm contrasting Jose's humor.

MEMBER MARCH-LEUBA: No, it's not humor. It's you take the laptop to an open network on an airport or on B-

CHAIRMAN BROWN: Well, I don't do that either.

MEMBER SUNSERI: -- just in a cell box (phonetic), and you are attacked continuously.

CHAIRMAN BROWN: Yes, yes.

MEMBER SUNSERI: I have just one more.

CHAIRMAN BROWN: Go ahead, Matt.

MEMBER SUNSERI: Just before we leave this. I mean, you know, I know you tried to create fidelity between this and the reactor side. But, you know, don't, for the sake of fidelity, do something that doesn't make sense though, right. You know, don't carry forward something. Maybe the reactor guys will change their viewpoint on this one hour thing if common sense prevails or whatever. So that's all I offer.

CHAIRMAN BROWN: The problem is that the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

one hour is written into the rule for the reactors. It's 73.77 or something like that. I said I went back and B-

MEMBER SUNSERI: Yes. Well B

CHAIRMAN BROWN: I stumbled over the one hour here also. And I said well, geez, man that B-

MR. DOWNS: Seems awfully fast?

CHAIRMAN BROWN: Seems awfully fast, given the fact that you might not have that, as you characterized it, aha moment for B-

MR. DOWNS: Yes, but you still B-

CHAIRMAN BROWN: -- a considerable amount of time. The same would apply for the reactor folks though.

MR. DOWNS: Exactly right.

MR. BARTLETT: But it would almost seem like the issue isn't with the one hour but with the discovery, right. I mean, the reason there's a delay is because the discovery hasn't happened, right?

MEMBER SUNSERI: Well, you're going to get in a huge debate if you start thinking about that. So when is the discovery? Before the root cause is done, when the root cause is signed off, you know, when the first report of the analysis comes in. I mean, you

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

know, that's a big judgement call right there in itself.

So, you know, in either case it's going to be some time delayed, probably more than an hour from when it actually happened, right. So, I mean, so if that's the case, then why does it all of a sudden turn on an hour clock.

MR. BERGEMANN: Well, let me just add, for the one hour, like, for the cyber attack, for the reactors, the event has happened. And it's already been called in under a safety or security event.

At that point, they don't know it's been a cyber attack. They're required to call something in if they've had an adverse impact to a safety, or security, or AP system. So as they call in, they say we've had this event occur.

Yes, two or three months later, they would possibly call up and say, oh, we now have discovered, through forensics, that it was the result of a cyber attack, not just some random failure, or electrical, or something like that.

CHAIRMAN BROWN: Are they required to report an event in B- forget the cyber.

MR. BERGEMANN: Correct.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

CHAIRMAN BROWN: You have B-

MR. BERGEMANN: Yes.

CHAIRMAN BROWN: They already have an event reporting.

MR. BERGEMANN: Right.

CHAIRMAN BROWN: Not necessarily a cause.

MR. BERGEMANN: Right.

CHAIRMAN BROWN: But an event reporting requirement.

MR. BERGEMANN: Correct.

CHAIRMAN BROWN: That provides some, I presume, some type of hazard, or casualty, or whatever --

MR. BERGEMANN: Correct, yes. But it could be I ran a test on safeguards actuation and B-

CHAIRMAN BROWN: And it didn't work.

MR. BERGEMANN: -- the functions didn't B-

CHAIRMAN BROWN: They worked slower, they worked snarky, or they, you know, I use a lot of technical terms here. You have to report that.

MR. DOWNS: But let me just kind of flip this a little bit though. Say that there's an actually active consequence of concern that a cyber attack has directly caused, and that it's obvious to a

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

licensee that we are under attack, and it is directly causing this to happen.

If this rule requirement were to be 24 hours, or a week, or something to kind of correspond with probably the more common case, right, of the latent piece, then the licensee wouldn't be required to pick up the phone necessarily to tell us about it until significantly after that event were to happen.

CHAIRMAN BROWN: But what are you going to do about it if they do call you?

MR. DOWNS: Well, there's the possibility that that could be, that that same attacker could be attacking another fuel cycle facility or also have a nuclear power plant in its cross hairs. And that could be valuable information for law enforcement officials to have. And that's the B-

MEMBER MARCH-LEUBA: Exactly. When any level happened, they grounded all the planes. If you get a cyber attack, ongoing, that was a nuclear facility, they'll be calling every nuclear facility and saying hey, guys, start looking out your windows.

MR. DOWNS: That's the benefit of the hour.

CHAIRMAN BROWN: While you go to

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

disconnect them from everything.

MEMBER MARCH-LEUBA: It should be five minutes. It should not be an hour.

CHAIRMAN BROWN: There's a rather unique solution to your problem if all of your memory is UVPROM. And once it's burned it can't be changed. You ever heard of that? That's ultraviolet B-

MR. DOWNS: Right, right.

CHAIRMAN BROWN: That's the way we did it in our program when we first started. All of our programmable read only memory was UVPROM. If you wanted to change it, you had to pull the whole chip out and put in a new one, very effective for controlling access.

MEMBER STETKAR: Especially if you had infinite resources available.

(Laughter)

CHAIRMAN BROWN: Well, no, the real key is to write software that works. Therefore you don't have to change it, and you don't have to put any virus software in it. How about that? That makes it really simple. I just love these suggestions.

MR. DOWNS: Okay, so at this point in the presentation, we were going to start getting into the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

draft regulatory guide. So before we leave, were there any other questions on the actual rule language before we move on?

(No audible response)

MR. DOWNS: Okay. So we're going, again, moving on to the draft reg guide, I'm going to turn the bulk of the presentation here over to Matt Bartlett and the rest of the working group.

MR. BARTLETT: So I'm going to begin the, thank you, so I'm going to begin the draft reg guide discussion. Like James said, my name is Matt Bartlett. I'm a project manager in fuel cycle.

So start with just an overview of the format of the draft reg guide. So note that we followed the standard research template for the format. It has five sections which are the introduction, discussion, staff regulatory guidance, implementation, and then the glossary, references, and appendices. So that's just the standard format.

The bulk of the guidance is actually in Section C. And then the controls are located in the appendices. So that's where the bulk of the meat is located.

Next slide. The introduction portion has,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

it's just, like, essentially a paragraph long. It's a purpose statement. It essentially identifies that the goal is to establish, implement, and maintain the cyber security program.

And then it states the performance objectives which again are to detect, protect against, and respond to a cyber attack capable of causing a consequence of concern, applicability at the fuel cycle facilities, and then there's a section on which regulations are impacted. So this would be a change to 73.53, as we've already discussed.

And there are some corresponding changes to Part 40 and Part 70, but they're relatively small changes. Related guidance is 5.70 which is guidance on the DBT. And then it makes the statement that this is just one approach to meeting the rule, this guidance.

Okay, next slide. On the discussion section, it has a section that has the reason for the development which is to implement a cyber security program to meet the performance objectives.

This section also has several paragraphs that run through the background. And it essentially starts at 9/11, and then works through the development

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

of the DBT, and then the reactor rule, then the development of the road map, and then ultimately the SECY-14-0147, and the SRM which was the genesis of this rule making.

CHAIRMAN BROWN: You're talking about reasons for development right now, right? That's B

MR. BARTLETT: Yes. This is just, it's essentially the discussion section of the reg guide. And it's essentially a boiler plate format that just kind of introduces the guidance.

CHAIRMAN BROWN: I guess, this is for an educational B- for information, is fundamentally the question. Has there been, since it's now been 15 years since 9/11, and have there been any explicit examples where our fuel cycle facilities have been attacked, impacted, adverse effects, adverse processes, interrupted, special nuclear material found unaccountable because of a cyber attack? Or are we still working in the zeros here?

MR. BARTLETT: So the official response is we don't know. Because there are no reporting requirements associated with everything B-

CHAIRMAN BROWN: And you're sure you would not have heard about it? I find that very hard to

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

believe.

MR. BARTLETT: That said, again, our licensees have reported, you know B-

MR. BERGEMANN: We've had, this is Brad Bergemann from NSIR. I know of one attack that's been reported from a fuel cycle facility to us.

CHAIRMAN BROWN: So we're using a sledge hammer to start to smash a miniaturized ant.

MR. BERGEMANN: I would B-

CHAIRMAN BROWN: I'm just trying to address this head on as to what B- I'm not saying we don't need something. That's not the point. My point of the question is the depth of this, and breadth, that's been proposed is pretty extensive and, by your own admission, is going to require considerable effort, argue about the level of effort.

And I'm just trying to figure out what problem am I solving with this rule as opposed to a simpler potential approach. I don't know what that would be. Maybe I could probably come up with something, like using UVPROMs but, you know, well, again, I'm just trying to get my handle on why, what problem are we really solving.

MEMBER MARCH-LEUBA: Let me do B-

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

CHAIRMAN BROWN: I'm aware of B- just a minute, Jose, and you can go. I'm aware of the stuff that's happened in industrial sites, you know, switch gear tripping and all kinds of things happen in the electrical world, controls world, and some in the industrial world that you hear reported.

But I haven't, in all of our B- at least the eight years on this committee, haven't heard any, you know, nibblings or rumblings of this having some mounting, terribly adverse effect in our fuel cycle facilities. So I guess that's the genesis of my question. Now, Jose, thank you.

MEMBER MARCH-LEUBA: Can I do John's job and say that this is a subcommittee meeting, and all you're hearing here is individual member comments.

CHAIRMAN BROWN: I know that.

(Simultaneous speaking)

MEMBER MARCH-LEUBA: I'm referring to Michael.

CHAIRMAN BROWN: Oh, okay. All right.

(Laughter)

MEMBER MARCH-LEUBA: You being the head of the committee carries more weight. We can argue about the B-

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

(Simultaneous speaking)

MEMBER MARCH-LEUBA: -- size of the hammer but not about why we're doing it. This is extremely important, and I will wait and then trust in the team to implement it. This needs to be done. And it's a serious problem. And I support them doing the rule making 100 percent.

CHAIRMAN BROWN: Just shows you the agreement we have on this subcommittee.

(Laughter)

MEMBER STETKAR: I think that I'll weigh in and kind of parrot some of Dennis Bley's comments that I have here also. I personally, and I don't think Dennis either, if I can speak for him, disagrees with the notion that there ought to be attention paid to cyber security threats against these facilities.

On the other hand, treating them all equally without regard to the risk, the risk now, not consequences, I mean risk afforded by each, I think that's why you may be hearing some of the pushback here.

And I don't claim to have the magic solution to how we get that real risk informed approach such that we start to focus on the threats to

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

the facilities where the consequences are more significant. Because we've already established the fact that threats could be happening, you know, constantly.

But I just, you know, this is a point to kind of reemphasize this notion of a risk-informed process that perhaps focuses more on both parts of the risk equation, the frequency and the consequences, than what the guidance does.

The rule, this again, my personal opinion, the rule, I think, seems to be appropriately cast in what needs to be addressed in terms of areas of concern. But how folks can do that most effectively may need some thought.

MR. DOWNS: So if I could, when we're dealing with a security rule, frequency is a very, very tough conversation to have.

MEMBER STETKAR: It is. On the other hand, you know, I'm a power reactors guy. I can't speak as the great Dana Powers can about, you know, chemistry. But we have many hazards in the power reactors area where frequency is also very, very difficult to address.

I'm thinking about, oh, earthquakes, I'm

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

thinking about external flooding that nobody has yet gathered much information where we can estimate reasonable frequencies. I'm thinking about some fire phenomena that people are still arguing about how you model certain types of phenomena.

So just saying that we can't do something about frequency is just too easy a way out. You can always do something about frequency. And you may not need to do something that's very precise about frequency. You may be able to very easily dismiss a set of potential risks, despite the fact that there might be quite broad uncertainties about the occurrence frequency of threats that would result in those consequences.

MR. DOWNS: So --

MEMBER STETKAR: If you start thinking about it from that B- rather than thinking about it from I have this facility, and I've identified an IROF that's part of some sequence that has no notion of risk, if I start from the back end and think about, well, what are the things that can really get me in trouble.

MR. DOWNS: So in the cost-benefit analysis associated with the regulatory analysis, we

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

get into a little bit of the discussion on frequency.

MEMBER STETKAR: Good.

MR. DOWNS: And what we do there is, well, you're not going to like what I thought.

(Laughter)

MEMBER STETKAR: Honestly, I might not like it, but it's good that you're at least B-

MR. DOWNS: Right.

MEMBER STETKAR: -- addressing it.

MR. DOWNS: So what we've done there is we've looked at the cyber security threat landscape as it existed 14 years ago when those inter-compensatory measure orders were issued and, basically, the intent of those orders and what the threat landscape was at that time.

We have a feel on what the landscape is today. Obviously, this rule was written for not only today but also for future, you know, over the life of these develops.

The real difficult piece to talk about is what's the threat going to be in ten years, what's it going to be in 20 years? Is there going to be a pathway where if something's plugged into an electrical socket it could be hacked, possibly. Who

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

knows?

So what the staff has come up with is, given that B- considering the lay of the land, and of the cyber threat, and various examples that we cite, you know, worldwide examples, both of an active consequence of concern as well as latent consequences of concern, obviously not at fuel cycle facilities, we don't have a tangible flag to wave and say it's happened. So therefore, we're doing a rule.

Well the fact is, if it's happened, we're probably just doing an order. We're probably not going to a rule making. So the rule making is trying to get ahead of the event prior to it happening. So the bottom line here is the assumption in the regulatory analysis on a frequency, the frequency is one.

MEMBER STETKAR: Well, but the assumption is that somebody creating that attack has equal motivation to attack and create any conceivable -B they have equal motivation to have a worker inside a plant breathe some sort of chemical mixture as they do to diverting materials from a Category I facility. And it's not at all clear that those motivations are quite the same.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

The implicit argument here is that all consequences are equal. And therefore they are all equal targets for cyber attacks.

MR. SHINN: So I would say B-

MS. ANTONESCU: Would you identify yourself?

MR. SHINN: Yes, Mike Shinn, NSIR contractor. So we don't consider all consequences to be the same. You'll see there is a grade in terms of the degree of protection we expect different types of VDAs to have based on their consequences. So if it's got a greater consequence, there are more things you need to do to protect it. If it's got a lower consequence, there are less things you need to do.

But to your point, we actually aren't assuming that necessarily the system is being targeted. The attractiveness of a digital asset isn't always a function of it being attacked. We definitely see adversaries, as you described, that just attack things because they're there. They're targets of opportunity.

So we also have to take into consideration that you may have an adversary that has no idea that this is a fuel cycle facility. And they're just

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

banging away at something, and you have a consequence that occurs from that.

So we definitely don't consider all the consequences to be the same. You know, certainly the risk thresholds that already exist for these facilities are what we use to define the consequences of concern. So these are events that they already have to prevent. We're just simply saying this is another potential initiator.

And the other variable we haven't had a chance to talk about yet is we also considered the capabilities of the adversary as it relates to that consequence.

So we don't say for a Cat III facility that we expect them to defend against the same type of adversary that a Cap I defends against. A Cat I has a certain attractiveness to an adversary that has a greater level of resources, time, motivation.

And so for those consequences of concern, there are additional things that those sites will need to do to defend against that type of a threat versus just somebody in their basement banging away on a keyboard. That's a different consequence of concern and has a different set of lower threshold controls

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

than we would expect you to apply.

MEMBER STETKAR: On the other hand, Mike, and maybe we should wait until we get into the controls, when you say different levels, we're talking about differences between B- and I have the math here someplace, but let's say differences between 170 and 155.

MR. SHINN: Sure.

MEMBER STETKAR: We're not talking about 170 versus, like, three B

MR. SHINN: Yes.

MEMBER STETKAR: -- in terms of the number of controls that I need to address.

MR. SHINN: True.

MEMBER STETKAR: So in truth, there is some difference. But the differences aren't --

MR. DOWNS: But if I could, if you actually compare it control by control, there's also a difference in the level of robustness B

MR. SHINN: Correct.

MEMBER STETKAR: -- associated with it. So Control Number 1 for a Cat I and Control Number 1 for a Cat III, yes, they're controls that are B-

MEMBER STETKAR: True, true.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

MR. DOWNS: But the robustness is different. So the level of resources to implement that control for a Cat III would be less than what would be required for a Cat I.

MR. SHINN: And just to give you one simple example, so there're some controls for Cat I that involve two manuals (phonetic) that we don't have in Cat III. It's a tiny change in language, but a substantively different degree of protection, and resources, and what not.

So whereas it's fair to say the numbers, you know, don't differ by an order of magnitude. The quality of differences between the controls are fairly different. But you also have to remember that these controls only apply if you have a VDA. So it's possible you could have a licensee that has none.

The alternate controls make it such that a cyber event won't lead to any of these consequences of concern. And then the controls only apply to the VDA. So there may only be one, two, three assets, dependent on the type of site that you're talking about.

You know, we definitely agree with all the concerns that you have. And I think we took them into

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

consideration trying to address a reasonableness as well as a flexibility to this.

We didn't have a chance to mention it yet, but this is very similar to what we do on the reactor side where you can credit an alternative for a control. So a control may say do X, and you can say, well, you know, I have somebody who walks into the room and checks it every hour, so I don't need to do this digital thing.

MEMBER STETKAR: I'm waiting until we get to Slide 6 -- Slide Number 50 for that. So we'll get into that a little bit later.

MEMBER MARCH-LEUBA: Not if I can avoid it. There was an argument about frequency going on here. And I heard James saying frequency is one. I heard John implying the frequency probably is ten to the minus six.

I'm with James, okay. You're thinking of a high school student in the basement of his mother's house finding an IP by mistake and starting a game of thermal nuclear war, you know, the 1980s movie.

That's not how it happens. This is government power, I mean, really bad actors out there being in every single IP, every way, several times, to

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

find out what they are B- what vulnerabilities they've got. And if you're in and you're open (phonetic), you'll get in it. The probability is not one per year, it's one per day.

MR. PRIESTER: Casey Priester, CSB contractor. And that was the point that I was going to make, is every IP address in the world is being attacked constantly. So the frequency of attacks is one. It's the frequency of successful attacks that is the unknown. And that is what we're trying to address with this rule. Because that's the real issue. They're attacking all the time. It's just they haven't been successful to date --

MEMBER MARCH-LEUBA: Yes, and these bad actors B

MR. PRIESTER: -- that we know of.

MEMBER MARCH-LEUBA: Yes. And these bad actors are all there trying to find soft targets and storing them for whenever they need them.

CHAIRMAN BROWN: Yes. But the way they've written this, they have to be able to detect all those attacks.

MEMBER MARCH-LEUBA: Well, that's what I disagree.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

(Simultaneous speaking)

CHAIRMAN BROWN: -- detect. And that's a huge, that's a huge effort to run through that. I'm being, you know, devil's advocate. It's pretty clear in this circumstance, but I went and looked at Appendix B, C, and D. And there's a lot of these things, for instance, the account management procedures, they're about as extensive for one as they are for two or three of the other ones.

I just did a number count of the stuff without looking at the details. But there were a lot of requirements regardless of which category of facility you were looking at.

MEMBER MARCH-LEUBA: The argument you're making, Charlie, and I support it 100 percent, is that the only way to prevent this is not the way they've gone, but it's just some scissors and cut the cable. It is cheaper to rerun all those critical assets through an internal Internet, internal line, and disconnect it from the outside, and try to implement all this.

CHAIRMAN BROWN: Yes. And protecting yourself from an internal -- an insider threat is much easier than beating yourself to death on the hackers.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

Of course, they don't want to do that. John doesn't want to do that.

MEMBER MARCH-LEUBA: It's less expensive.

MEMBER STETKAR: I think, you know, let them decide what's the cheapest way to skin the cat.

MR. DOWNS: That's exactly, hopefully B-

MEMBER STETKAR: In some sense, you know, I support that. Let the fuel, you know, let the owner/operator decide what's the most effective way to meet the requirements.

MR. DOWNS: And B-

MEMBER STETKAR: I'm just B-

MR. DOWNS: Sorry.

MEMBER STETKAR: I'm just trying to advocate a notion, because we, as an agency, support risk-informed. And again, I always say risk is frequency and consequences. Regulation that, without some notion of frequency, you know, we could be going down a path where we're not being necessarily very effective in our regulation, looking at real risk.

You know, I always use the argument that we don't protect facilities against meteorite strikes, despite that fact that the consequences would be pretty doggone onerous, because everybody believes

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

that a meteorite strike is of sufficiently low frequency that we don't care. But if you just looked at the consequences, it wouldn't be a good day.

And this is actually, John, a circumstance where, even though I would advocate cutting the wire, and Dennis mentioned it in his comments as well, you know, for the facilities, there's not a lot of facilities here to deal with, I mean, when you look at it.

Doing a risk assessment of those activities could create a problem and then developing your plan to address it from that standpoint as opposed to we're just going to blanket the entire process. That's B-

MR. DOWNS: Well, Charlie, I've got to say that I think the rule actually outlines a process to do that and for the licensee to do that analysis, to document the analysis, and the NRC to come in and inspect it. We're not saying that they have to have vital digital assets. As a matter of fact, the early indications are is that many of the licensees are saying that they are not going to have any vital digital assets.

CHAIRMAN BROWN: So they're going to be

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

all analog?

MR. DOWNS: Well, they have adequate --

CHAIRMAN BROWN: Oh, okay. I'm sorry they could be digital assets but not vital.

MR. DOWNS: Not vital. That's right. So you've got a situation then where it's just making sure your configuration management over time, that none of them become vital, right.

And the other aspect is that you're not going to be throwing a whole bunch of controls at assets that don't need them, in other words. And through this process, the alternate means consideration will be such that you've identified alternate means that may be administrative or other, you know, features of protection that act in lieu of the cyber security controls.

So the intent, the staff's intent with this rule was to provide licensees as much flexibility as possible. Now, I'm sure the, you know, as you've seen in the industry letters, the concept there of cost, ongoing costs to maintain the program when you've got zero vital digital assets needs to be considered.

And that is something that the staff is

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

looking at. We are trying to minimize the costs associated with the ongoing activities if there're, you know, no vital digital assets.

You know, in essence, you know, you talked about having a huge team of cyber security folks onsite, you know, for the event that possibly could occur, you know, that they're just sitting around waiting for something to happen.

CHAIRMAN BROWN: Good job.

MR. DOWNS: And we're trying to scale, in the guidance, we're trying to provide that clarifying language that the program is scalable to the number of vital digital assets that you've got. It's not going to be, you know, we don't expect this to have, you know, a team of ten cyber security experts sitting around if you don't have any vital digital assets.

But you have to have some sort of controls. The staff's position is that you need some controls in place to make sure that the configuration management piece of this doesn't create something in the future. So that's the B-

CHAIRMAN BROWN: Well, but then you go on in the reg guide, and you say that although the design and configuration of a digital asset, digital asset

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

may have some inherent protection, e.g. air gapped, non-Internet facing, stand-alone, and protected by a firewall data diode, virtual local area network, tunneling, or cross domain solution. These are not acceptable alternate means.

MR. DOWNS: That's correct.

CHAIRMAN BROWN: And I'm trying to figure out why a stand-alone digital asset becomes a vital digital asset.

MEMBER MARCH-LEUBA: But you're just vulnerable to this cyber threat.

(Simultaneous speaking)

MR. DOWNS: John's got it, right there. That's it.

CHAIRMAN BROWN: That's a vital digital record. I'm holding up a thumb drive. It's not going to be doing anything while you're holding it.

It's an internal threat. I'm sorry, that is an internal threat, malicious guy that wants to compromise you. And there are administrative procedures that we use at power reactors that try to take care of that specific thing. Why isn't that good enough for a fuel cycle facility?

MR. DOWNS: We're not saying that it's

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

not. But what we're saying is B-

CHAIRMAN BROWN: You just said, you just said in here, stand-alone, protected by a firewall, that's a stand-alone device.

MR. DOWNS: No, no, no. What we're saying in there is that that isn't an acceptable alternate means. So in other words, just because you don't have connectivity to the Internet, doesn't say that, oh, well, because I'm not connected, therefore I've got an alternate means. No, you need to consider the other pathways at which the compromise could happen to that alternate means.

CHAIRMAN BROWN: But every B-

MR. DOWNS: The pathway B-

CHAIRMAN BROWN: But every asset is accessible by a person.

MR. DOWNS: That's true. And that person may not be maliciously acting and putting that USB in there. But the point is that if that asset is required to be considered a vital digital asset and have the controls applied, the fact that it doesn't have Internet connectivity actually satisfies a tremendous number of the controls.

You can credit that, because of your air

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

gap, you can go through your controls and use that to say this measure satisfies these proponent specifications. And it's just a matter of documenting that. Now, the portable media is one aspect that introduces a potential attack that, well, that hasn't been addressed.

So yes, there's a control for portable media. So you have to apply portable media controls like you do on a reactor to make sure that that vital digital asset is adequately protected.

MEMBER STETKAR: Charlie, if I read, and this is one area where I'll weigh in that, if I kind of read between the lines, you're using your experience in the Navy and what we've heard from the power reactor side.

What I hear the staff saying, historically, that some of these facilities don't have the control over the portable media. They don't have it, and they claim that they don't need it, because they're good enough. And that's kind of a specious claim.

CHAIRMAN BROWN: But I agree with you on that. But I would argue that that B- portable media is obviously a concern, no matter how you slice it.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

And I have no problem with people dealing with registering and accounting for the portable media that are allowed inside any particular boundary condition or boundary area. That's a very smart thing to do.

But if anything we've learned in this B- and I've spent 22 years developing this stuff, and the one thing we learned is control of access. You don't allow electronic access anywhere, period. And Number 2, you control who can get it. Number 3, you control what they can carry in with them. So they never get inside the boundaries with anything.

So, I mean, that doesn't mean it can't happen. I mean, you know, maybe the guy could stick it in his ear, and you wouldn't detect it, or something like that. I don't know.

But to me, if NRC wants to implement protection rules, make them so that they can be easily accomplished and not crush everybody in terms of getting to the endpoint with administrivia, people, and paperwork, and everything else. That's all. I'm not, you know, it's a point of view.

MR. DOWNS: Sure.

CHAIRMAN BROWN: You know, and B-

MR. DOWNS: And I appreciate B-

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

CHAIRMAN BROWN: And all I'm going hear always, well, if we get too prescriptive on this, what's going to B- oh, there are other ways to do this. And we don't want to stifle innovation and ingenuity. And it's baloney if you want to, in my opinion, if you want to be like we were, make sure nobody got in and discombobulated your stuff. That's a good word, by the way. I don't know what that means.

And that's the point I'm trying to make. And it's easy. It's easy to do, not costly, and very focused. And you can pick -- the business stuff, fine, separate it out. Put it out somewhere. Just don't let any of the vital stuff connect to it. Make your networks isolated for functions. Don't pile them all together. I mean, you made a B- you all made an observation in here that multiple devices can be connected together to provide B-

MEMBER STETKAR: Charlie?

CHAIRMAN BROWN: I'm rural (phonetic).

MEMBER SUNSERI: In a sense, you are. In a sense of time, I hope they ask NEI why the facilities wouldn't do that on their own.

CHAIRMAN BROWN: Well, if we can get to

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

them. I'm happy that B- you heard that. Is NEI still here? Do you hear me?

(Off the record comments)

CHAIRMAN BROWN: Can you address that?

MEMBER STETKAR: Why don't we wait until they're on the B-

CHAIRMAN BROWN: All right. Well, let's get rolling so I can have them dispute me, why nobody wants to do this.

MR. DOWNS: One thing just to add here real quick is that, you know, you talk about the controls being just overly burdensome, that it's a large number of controls. And I'm not going to dispute that it's not a B- yes, it is. There's a lot to think about here. But the point is that this is the industry standard for how cyber security is applied.

CHAIRMAN BROWN: Well, but B-

MR. DOWNS: When you say that all you have to consider is portable media, I think that, you know, the folks that developed these standards at NIST, that NIST, they would tend to disagree with you. So that's B-

MEMBER STETKAR: Of course they would.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

And I'm not, I don't deal with the stuff, and Lord knows I don't want to. When you say this is the industry standard, that implies that every one of those controls are necessary at every single facility.

Or is that B- does the industry, and I don't care what the industry is for the moment, consider that as a useful checklist of things that I ought to think about?

When I read through this, if I consider the useful checklist of things, I'd say, well yes, you know, my facility, I need to employ controls Number 1, and 37, and 29, and, you know, a variation on 68 for the following reasons.

But I don't have to sit down and write a page of justification why I did not apply the other 165 of them. Right now, the guidance says I have to write down that page of why I didn't. And if it doesn't, that's the way I interpreted it. I think -B

CHAIRMAN BROWN: Yes, that's the way I read it.

MEMBER STETKAR: I think that Dennis' comments and Myron, if he ever speaks up again, had the same B-

MR. HECHT: I'm here.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

MEMBER STETKAR: -- that a tremendous burden of going through each one of those, point by point, bullet by bullet, for my particular facility, and justifying now, in writing, for something that is subject to inspection, and question, is a fairly large burden.

MR. DOWNS: So they do this presently with federal information systems. And it is not a page on each one.

MEMBER STETKAR: It is not?

MR. DOWNS: It is a very succinct statement for each one.

MEMBER STETKAR: Okay.

CHAIRMAN BROWN: That's right. But those are taxpayer dollars which nobody --

MEMBER STETKAR: Let's, well, wait. One of my concerns, quite honestly, is getting into this checkbox mentality where, if I'm not forced to think about that and write a page about it, today I, John Stetkar, decided that I would not implement this control for the following reasons.

I found, in the past, that if I that thoughtful process, occasionally I'll question things. And sometimes that questioning is good. If I develop

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

-- but if I have to do that for 300 of these things, I get into the nope, nope, nope, nope, nope, nope checkbox stuff. And I don't really think about anything.

I think about the one thing that I thought perhaps in the beginning, yes, I want to focus on portable media because, yes, I realize I have a problem with portable media, and really put some thought into that one control. Because a priori, I've already made the decision about what's important.

So simply by creating a very long list of things that someone must go through, and as you characterized, in kind of a pro forma notion, check off the boxes, could be contrary to what we really want people to do anyway.

MR. DOWNS: So I personally have never implemented a cyber security control. However, I have folks on my team that have. That's why I want to defer to, Joe, you want to answer B-

MEMBER STETKAR: Joe's been sitting B-

MR. DEUCHER: Yes, I have, waiting to jump in. But just, we've had such a great conversation. First of all, this is Joe Deucher with NMSS in cyber security.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

And what I would bring up is, having done this internally for NRC on both the, what was called the Digital Data Management System and the Licensing Support Network, for those of you who aren't familiar with the Yucca Mountain program, the idea behind this, when we're dealing with these NIST controls is, again, it's a performance measure.

And you're going through, and you're identifying, and looking at your system, or your digital asset in this case but -- digital asset, excuse me. And you're looking at these individual requirements and seeing whether or not it's necessary or not.

On the back end of all of that, you're doing a verification. There's a verification to determine do vulnerabilities still exist. And I'm asking myself is my system protected? Is my vital digital asset protected after I've done all of these individual items?

And a lot of times, when we look at it, we look at the list of controls. It can be very, very onerous, as we've said here at the table. But in reality, a lot of this stuff, if I'm looking at, say, a typical computer that's got software on it, it's got

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

an operating system, it's got a program, a lot of these features my very well be built in. And it's just a matter of me turning something on.

And these are, as we'll go forward we talk about the individual measures that folks would be doing. And it's just a fact of identifying, okay, what measure am I using, what am I turning on, and just being able to record that and have that.

And as we discussed in the rule language earlier, that would then be documented in the implementing procedure.

And on the federal side, it's just a list.

It's a list, it's a thoughtful list, because it gives enough for a reviewer, in this case, it would be done internally with the NRC, with the Office of -- the Chief Information Officer's office. You would go through, and you would be able to identify, and be able to answer those questions, and see, from the list that you've established, have I met the criteria. And it's just a simple list. And then we've got this verification on the end of it that we've confirmed it.

And then going forward, as the system is operating, because we'll talk about, in terms of some of the controls that are identified, we have to do

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

ongoing maintenance, which means we have to ensure that we continue to meet the requirements, which I think gets to some of the points that Myron was making in terms of, you know, whether or not we're updating software, we're making changes.

The controls themselves for a vital digital asset would address that. So our hope with this is, between the controls themselves at the, one could argue, the worst case scenario, that I actually have to implement controls, versus the other side of it where we may very well have a process line that's got lots of digital assets associated with it.

But again, because of the alternate means that's associated, whether it's a holding tank, whether it's speed limiters, whether it's by design that not enough will flow through the process at a given time, we see that there's a lot of flexibility to be able to address this and still address the cyber threat effectively.

CHAIRMAN BROWN: Unless the speed limiters itself were controlled and connected to the network.

MR. DEUCHER: But even in that case then, you know B-

PARTICIPANT: That's right. The protected

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

B-

MR. DEUCHER: Right. Then we can talk about protected by a cyber attack.

CHAIRMAN BROWN: You went through your list of stuff which, you know, you all did this, and you all did that, and such and such. And the point is, what problem are you solving, and did you solve it?

In this case, when we look at these three facilities, or four, whatever they are, what risk is there that we're B- what are we attacking? I mean, I was one of the 2 million people from OPM that had my entire Social Security numbers, every piece of data I have ever put into the system in 47 years was inputted into -B is now out in the public somewhere. That made me very, very happy.

And I'm sure they went through their checklist and checked it all off. It didn't work. It's aggravating unless you know what problem you're trying to solve.

Here you have an opportunity. These people do certain things. They have certain consequences for certain things that happen. You address the risk for what those consequences are, and

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

you implement the controls necessary to alert you to those consequences, you know, to the loss of that control.

I think that's kind of the point we're making relative to, you know, a risk-informed or a risk-evaluated approach to doing this to try to simplify the whole process and apply controls where they're needed. John, if I said something wrong, I don't always phrase this properly. So B-

MR. DEUCHER: I appreciate B-

CHAIRMAN BROWN: I'm a deterministic guy.

MEMBER STETKAR: I was going to say, for the record, I'm just speechless that I heard him use risk twice in one speech.

CHAIRMAN BROWN: Well, as opposed to reactor trip systems and safeguards, I think this is a really B- this is a prime opportunity to utilize these tools.

MEMBER STETKAR: But again, I'm interested to hear from the industry. Because one of the reasons B-

CHAIRMAN BROWN: You all want to stop and we'll get into it?

MEMBER STETKAR: No. Just because there

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

are other things that I think we need to discuss.

MR. DEUCHER: I feel like we left a point that you made, Mike Shinn, and our NSIR contractor that you mentioned, John, the adequacy of the controls. It's not just a checklist.

And as you may recall from the reactor side, both on physical and cyber, it's a performance-based rule, right. We want you to consider what new things has the adversary come up with? It can't be a static list, right.

So I would like to draw your attention to there are some controls in here that deal with what Joe was talking about, what we call security control assessments, that you use an independent assessor to consider the adequacy of the control and if this occurs on an even more periodic basis than what we discussed.

So there are things that happen maybe every 30 days, every 60 days, or they may be triggered by an event. The vendor says, hey, there's a problem.

Or DHS says there's a new capability that the adversary has. So you need to go back out and reconsider these things.

There's a dynamic performance piece of

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

this that's not really a checklist. Because we don't know what the adversary might come up with tomorrow. So our objective was to capture all of the known effective measures that the global cyber security industry says, yes, you should do these things, and filter out the things that are irrelevant to these facilities, and then build in this performance piece as well so that it's not just a checklist.

MEMBER STETKAR: Yes. Mike, the only thing I'm -- and I hear what you're saying. The only thing that I am trying to raise is that you said, well, you compiled everything that, I've forgotten the words, but it's in the transcript, list of things that people should be doing or something like that.

My concern is getting into a situation where a licensee, because of the regulatory interaction now, is placed in a situation where they need to do that thing, like write a paragraph. I today decided that I'm not going to do this for the following reasons, for every last, blessed one of those things, and then be subject to regulatory questions about, well, wait a minute, why did you put that parenthetical phrase in there? Or why shouldn't you think of this differently, which can be resource

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

intensive both for me as a licensee and from regulating, you know, rather than -- I certainly agree that there are some controls that are very, very useful. And different controls may be more or less useful for different facilities.

It's just this notion of is it necessary for me, as a licensee, to explicitly address each one of those? And for any of them that I'm not implementing -- implementing them is fine, yes, I'm implementing this, and here's how I'm implementing it.

Great. But for all for the other ones that I'm not going to implement, justify for each one of those, subject to inspection, and questions, and so forth, why I didn't do that, and why I didn't do it today.

And then six months from now, as the threat has changed, why I'm still not doing it, you know, six months from now, or a year from now, or three years from now, or whatever.

MR. SHINN: So, Mike Shinn, NSIR contractor. Certainly we don't tell them what the degree of documentation is that they need to provide.

We're certainly not telling them they need to produce a lot. The intent is there should be an answer. When you inspect, and you ask a question, why didn't you do

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

this, there should be a story to tell.

And this is my -- I'm going to change gears. As someone who has gone out and inspected plants, all I'm looking for is an answer, right. I never said bring me a stack of paper, right. If the answer is reasonable and supportable, we move on.

And I think that's certainly our intent here, is to communicate that in terms that hopefully everyone understands. And maybe that's something we need to take back and think about.

But we're certainly not looking for them to produce volumes of paper or what, in my industry, sometimes we jokingly call the paper fort. You know, you generate all this paperwork, and you build it up around the computer. That's not helpful.

But there needs to be a reasonable amount of documentation. And I would say, in the same vein that we would require for any other program that we regulate, there is a certain amount of documentation that we would expect to see. And we wouldn't expect to see any more or less for this program than we would for any other program we regulate.

MR. BERGEMANN: Correct. And this is Brad Bergemann. And just to add to that, so on the flip

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

side is when there is no documentation. And you ask, well, why wasn't this implemented, it draws more questions, and especially if the staff has changed, and they don't know that initial decision of why it wasn't implemented, you know, it's somebody new there.

And they don't have an answer. And that happens, staff changes, things change.

MR. HECHT: Can I contribute something to this?

CHAIRMAN BROWN: Have at it.

MR. HECHT: And that is with respect to the justification for not including specific controls.

You have appendices for the cyber security plan. You have an appendix for implementing procedure.

Can I suggest that you also have an appendix, including some examples of what you might expect is reasonable, or not including the cyber control and that you make up a scenario, you make up a specific plant, and you show that. And might I also suggest that you also provide the same kind of documentation for how you justify an alternate means?

MR. DOWNS: Myron, this is James Downs. Absolutely. That was one of the takeaways from a recent discussion with stakeholders, is that there

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

needs to be some more examples in the guidance document.

And along with that, you hit on the alternate means piece. The other is how, give an example of how you would document this list of digital assets that we've been talking about. That's something that the staff has taken, and it's on the list to be added to the draft reg guide prior to going out for public comment. So it's definitely something we're looking into.

MR. HECHT: Okay, good. Thank you.

MR. DOWNS: Thank you.

MEMBER MARCH-LEUBA: I think those examples would be really valuable. But I'm questioning whether they should be in the guidance or on a separate document and included by reference.

MEMBER STETKAR: It doesn't make any difference if it's a separate document that's endorsed in the guidance or if it's in the guidance. It's, you know --

MEMBER MARCH-LEUBA: The guidance is already 170 pages long.

MEMBER STETKAR: That's all right.

MR. DOWNS: We can always make it two

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

volumes if we need it.

MEMBER MARCH-LEUBA: I mean, it's 3:00 o'clock already. I'm hoping to get to Appendix G, the only example in there. I have some serious problems with it.

MR. DOWNS: Well, I'll be the first to admit it. Appendix G was something that we put together fairly quickly and hasn't gone through a lot of revisions.

MEMBER MARCH-LEUBA: I can't wait until we get there.

MR. DOWNS: I appreciate what you're saying there, yes.

MR. BARTLETT: Okay. So I'll go ahead and move forward with Slide 3 --

CHAIRMAN BROWN: Okay. Let me B- a calibration here for just B-

(Off the record comments)

CHAIRMAN BROWN: No. But we're almost to the break, but that's not --

MR. BARTLETT: I can finish --

CHAIRMAN BROWN: -- that's not his point. No, we're going to finish. We'll finish this. I just, you've got 61 slides. And we're going to finish

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

this. And I think I can do the math, that there will be 18 left as long as the last one's not at the end.

And we are actually not too bad off for time. And I want to make sure we make time enough for NEI to make their statement. I don't know how much B-how much time do you need for your statement anyway?

(Off the record comments)

CHAIRMAN BROWN: Oh, I'm sorry, did you hear me okay, sort of?

(Off the record comments)

CHAIRMAN BROWN: Okay. I just wanted to make sure he had enough time to give his statement and possibly answer some questions if somebody questions his statement, and if we've got anybody on the phone also. So I want to leave a little time. I don't want to end up this thing at 6 o'clock. I'd prefer to end it around 5:00 at the latest. So we've got two hours, so we should be able to do that.

We've had a lot of really good discussion so far which I think has encompassed some of the broader concepts and issues without digging or drilling down into what I call some of the nitty gritty of specific steps, which is normally not overwhelmingly productive.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

Because these bigger concepts are one of the ones I really wanted to make sure we covered. And I think we've kind of gotten there. So anyway, let's go ahead and keep it moving. And this is just the B- there's only one slide on this?

MR. BARTLETT: Yes. I can finish this in one minute here.

CHAIRMAN BROWN: Okay. We'll take a break at 3 o'clock then when you come up.

MR. BARTLETT: Yes, that should work. So just to conclude what's in the discussion section, so it's also B- the discussion has an overview of the major topics that are covered in the guidance, just at a very high level.

It's also got a table in there that identifies the timeframes for implementing the rule. James already went through those. It's essentially 180 days for the licensees to develop the plan and then 150 days for the NRC to review it and approve it.

And then once that happens, then there would be six months for the licensees to document digital assets, and then 18 months for full implementation.

The discussion section also has information

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

on how the guidance relates to IAEA guidance, international guidance. The IAEA guidance is basically cyber security principles, and it's reactor focused. It's just a paragraph in there.

MEMBER STETKAR: Non-facility focused, in other words.

MR. BARTLETT: Right, right. And then it also makes reference to the fact that the controls and the cyber guidance were drawn from NIST 853. They were informed by that standard.

MEMBER STETKAR: How often does NIST update the standards? Because they're on, like, Rev 4 of B- I've forgotten which one they're on, REV 4 B

MR. BARTLETT: Anybody know?

MR. DEUCHER: This is Joe Deucher. Typically, it's about between three and four years, give or take, maybe five years. In fact, they're coming up on a revision now. They're drafting Revision 5.

And what they've also done is they've created the industrial B- we talked about the 882, which is for industrial control systems. That's designed to overlay on top of the 853 which are the general IT cyber security controls.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

So if you wanted to protect industrial control systems, and you were just a business out in the world, you could take the two of those together in order to be able to protect your devices.

They're also working on another product coming out this year that's designed for Internet of things type devices, or what they would consider cyber physical devices, which I think is going to operate in the same way. You'll just take it, and you'll overlay it on top of the 853.

MEMBER STETKAR: So I'm going to ask the obvious question that if we're endorsing on regulatory guidance, Rev 4, of something that's a moving target, does it endorse Rev 4 or does it --

MR. DOWNS: We do not.

MEMBER STETKAR: You do not. Oh, that's right, you don't. You only have B- you say it's informed by it, but it's not --

MR. DOWNS: Okay.

MR. DEUCHER: Right. One of the other things, just to add, this is John Deucher again. There is also ISO and other standards bodies have cyber security standards now.

One of the nice things with the 853 and, to

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

a certain extent what we're doing, is trying to show some traceability between the two. And so the idea of being that a licensee, if they wanted to, if they've already established -- because again, they all have some degree of voluntary effort.

They may very well have standardized on a different cyber security set of controls that this is traceable to those other standards. And they could go ahead and make alterations with what they have in order to be able to meet what we've come up with as a reasonable approach.

CHAIRMAN BROWN: Go ahead.

MR. BARTLETT: So this may be a good place to break, if you want to do this where we start getting into the body of the actual guidance.

CHAIRMAN BROWN: Yes. Okay, we'll take our prescribed 15 minute break here at 3 o'clock, return at 3:15, as Mr. Skillman would say. He was by that clock.

(Whereupon, the above-entitled matter went off the record at 2:59 p.m. and resumed at 3:17 p.m.)

CHAIRMAN BROWN: We're now back in session. I'll turn my microphone back on. So you're next. I'm trying to save his ears. I blasted them a minute ago.

(Laughter.)

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

I saw his eyeballs roll when I hit the phone. Go ahead, Matt. Thank you.

MR. BARTLETT: All right, so we're on Slide 44, Staff Regulatory Guidance Section C. So this is where the body of the guidance is. There are 12 sections to this. It essentially addresses each piece of the proposed rulemaking. This section is 31 pages of the guidance, and the appendices are another big piece of it. But this is where we should have the most interesting discussions.

So next slide.

Okay, this slide just reemphasizes general requirements. Okay. It's a different slide than I've got.

Okay, the general requirements. The general requirements provide an overview of the major aspects of the cyber security program. Licensees would start by creating a team as we've got it set up. They would start by creating a cyber security team. The team would be responsible then for developing the cyber security plan. And the plan would describe the program and identify the cyber security controls. So the controls that we have in this guide they could just adopt those or they could propose alternate controls.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

But the plan would be where they would define what controls they're going to use to protect their vital digital assets.

Then they would do an analysis of their facility to identify the digital assets that could cause a consequence of concern and then they would further screen those to determine which ones are vital.

Once the list of VDAs is created, the team would implement the controls and develop implementing procedures. If the controls can't be put into place, the licensee would need to implement interim compensatory measures as a way to protect against the consequence of concern.

And then the cyber security team would need to manage the program over time. So that's just general summary of the process.

CHAIRMAN BROWN: One question I had.

MR. BARTLETT: Next slide. Thank you.

CHAIRMAN BROWN: I think this is the right one. Is there a definition of an adequately structured staff trained, qualified and equipped? I mean am I just naive because I'm not a big IT guy or is that 15 people? Is it ten people? Is it training that's every three months? You have to constantly have something

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

going on because of the -- in the IT world?

MR. BARTLETT: So what we envisioned in terms of on the team for the creating of the program, it would be facility dependent and vital digital asset dependent, but we envisioned in the cost, in the regulatory analysis that it would essentially be two cyber security experts, a facility expert, and then a manager and then potentially security -- a security person.

MR. DOWNS: Now again, these individuals wouldn't be dedicated to that team. They could have other duties at the facility. It's just a matter of the team would be established to be able to maintain the -- perform the analysis that's required by the rule. And then as Matt was saying maintain the program.

CHAIRMAN BROWN: But they would be the people that if you had a suspected thing or something when you wanted to determine, they would be the ones you would call on? If I think of the cyber security team, they're all trained and expert or whatever you want to call them. So you're thinking four or five people then or something in that nature?

MR. DOWNS: Yes. It would be about four or

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

five, but again, those folks, it's not like they're fire fighters sitting around the firehouse. They could be fire fighters that are also gardeners and engineers and that sort of thing, but they're volunteer fire fighters. When the time comes when they need to perform that function, they're available to do that.

CHAIRMAN BROWN: Well -- go ahead.

MR. DEUCHER: I was going to say -- this is Joe Deucher with NMSS. Just to let you know, you asked the question regarding training and we do expect that they would -- that there would be annual training for the cyber security team members.

CHAIRMAN BROWN: I'm not arguing against that. I just -- obviously, you're going to do some of that. But then it goes on and says "and equip to manage the cyber security program." I presume that would include whatever assets are defined as needing to be monitored?

MR. DEUCHER: Well, in terms of equipment, what we're really talking about is the tools that they would need in order to be able to perform cyber security duties. It could include vulnerability, scanning software. It could include any sort of digital forensics materials that they would need. More

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

along the lines that the resources that they would need in order for them to be able to perform their duties on those vital digital assets.

CHAIRMAN BROWN: But if you're scanning, doesn't that mean that you're doing this real time, all the time, trying to detect threats that are coming in or see all the little hits coming in all the time so you determine well, geez, I'm being constantly attacked or not as Jose so amply identified a few minutes ago on his --

MR. DEUCHER: It actually depends upon the device. Like, for example, if they had say a network device and they had a border. You would have a protection system in there. It would involve a fire wall and perhaps a security information manager. But if we talk about a system that is stand alone, you may as a part of -- again, a vital digital asset that's a stand alone, you may have as a part of its ongoing maintenance program that every so many months I vulnerability scan the device just to see if based upon any new vulnerabilities that have been identified out in the field that may affect that device and then I would need to go ahead and make changes or updates to it.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

CHAIRMAN BROWN: Somewhere I saw numbers people think there might be vital digital assets in the neighborhood of several hundred or so at the facilities. And I'm just thinking if you've got to constantly be sure of what their state is, that means people to go be doing that. You just don't -- that's just not -- you don't do it in your sleep, obviously.

MR. DEUCHER: A lot of this can be automated. It can be set to run remotely. It just depends upon the device in question.

MR. DOWNS: And as far as the numbers are concerned, the numbers that we've seen would be for the larger group of digital assets, not vital digital assets, digital assets. We've seen numbers as high as 15,000 at a licensee.

CHAIRMAN BROWN: In just digital assets?

MR. DOWNS: In digital assets. As far as the number of vital digital assets, it should significantly drop from there.

MR. BARTLETT: We've discussed 5 to 12 vital digital assets at a facility.

MR. DOWNS: And again, if certain -- if the unclassified network accreditation is considered as an exception for the rule, the prevailing thought is that

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

some licensees may have zero. So in which case, the guidance isn't clear on this and this was a comment from stakeholders is that the guidance needs to reflect that the number of individuals on that team can be scalable to the number of vital digital assets and that's something that we're looking to add into the guidance.

CHAIRMAN BROWN: So just digital assets aside from those -- after you've separated out the vital. Say you had several hundred digital assets. Nothing needs to be done with those. They just kind of exist. Is that right?

MR. DOWNS: The documentation exists and especially it's important for the configuration management purposes, if you've got a number of digital assets and no vital digital assets, that means that you've identified alternate means of maintaining those functions for all those assets. So therefore, the configuration management piece would be that those alternate means are maintained. If something changes with them, that that process is reevaluated. That's kind of the concept there.

MEMBER MARCH-LEUBA: Not to pick on anybody. Each centrifuge has its own micro controller

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

on it and I fail to see where the alternate asset could be if I can get to the micro-controller and make it malfunction, meaning that right there I would have, I don't know, 10,000, 20,000 assets that are critical?

MR. DOWNS: So I don't want to speak specific to a certain licensee, but controls for centrifuges are typically on classified networks. Is that not correct?

MEMBER MARCH-LEUBA: Yes, absolutely.

MR. DOWNS: So therefore, they would be excluded from this rule, from the effects of the rule because those are protected under the guise of the classified network and in accordance with the requirements of --

MEMBER MARCH-LEUBA: So they're already doing it right.

MR. DOWNS: Yes, exactly.

CHAIRMAN BROWN: What?

MEMBER MARCH-LEUBA: They're already doing it right.

CHAIRMAN BROWN: Theoretically.

MR. DOWNS: They are adequately protected as far as the NRC.

MEMBER MARCH-LEUBA: Those classified

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

networks --

CHAIRMAN BROWN: As far as the NRC is concerned they're already adequately protected.

MR. DOWNS: Right. You have to go talk to DOE to get any more specifics on that.

CHAIRMAN BROWN: Okay. All right, thanks. Go ahead.

MR. BARTLETT: Next slide. Okay, so the cyber security performance objectives we've discussed already. They are to detect a cyber attack capable of causing a consequence of concern, protect against a cyber attack capable of causing a consequence of concern and respond to a cyber attack.

So just a couple of items that are identified in the guidance. By detect, we're talking about licensees would need to have the necessary equipment, material procedures, sensors to analyze anomalous activity. They would need to maintain a baseline understanding of the facility's normal network system behavior so that they could compare it to abnormal activity that could happen.

Detection would also involve being able to take lessons learned from detection and then apply it to their systems and then utilize relevant threat

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

intelligence from external sources to inform their detection process.

MR. DOWNS: And just to clarify one thing, we kind of glossed over it, but the key here is a cyber attack capable of causing a consequence of concern. So if a site has no vital digital assets, that would imply there that a cyber attack could not cause a consequence of concern. So therefore, the monitoring would be extremely limited.

CHAIRMAN BROWN: It's difficult to see that you're actually always going to know what I need to detect to ensure I know that a cyber attack is occurring. And number two, since I don't know the nature of the cyber attack that is attacking, how do I know that I can protect against it if it's implementing or utilizing some techniques of which I don't have programmed into my detection.

I'm kind of doing a circular argument here, but it seems to me every time I see what's going on with the stuff that works in what I call the commercial world, it's after the fact. McAfee comes out with something to protect against the latest thing. People have found out it's already caused a problem because they didn't know that it was going to happen. So now

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

they come out with some upgrades to their software to say now we're going to make sure this doesn't happen to you. Luckily, it didn't happen to you initially.

So it seems to me you're always in a defensive mode or a -- what's the right term? Responsive, after-the-fact mode in all of this stuff.

MR. BARTLETT: From the perspective of the rule, we would consider a vital digital asset protected when it has the controls that have been approved in the plan applied to the vital digital asset.

CHAIRMAN BROWN: No, I understand that, except I don't see how that necessarily gives me any comfort that it's going to be safe that I can detect the one that nobody knows about yet.

MR. DEUCHER: This Joe Deucher with NMSS. To get to your point, one of the things in order to be proactive, we talk about understanding network traffic.

There are a lot of techniques and tools out there available for me to see where I'm sending information to. And I can plug that information in to security event managers, other technologies, and the folks who are sitting there monitoring this. And they can get a good idea of what should be happening on a normal day.

If their monitoring program is in effect, and capable

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

and operating, I should be able to tell if I'm getting traffic from some place I shouldn't be.

So if I'm communicating out to say some place in Russia or some other location that I normally won't communicate to, that's going to show up. And businesses do this around the world today. It's a capability that's available and it's just for us, it's just a matter of us spelling that out and providing that as one approach in the guidance to be proactive.

It's understanding how your daily traffic is from a network perspective and also how your system should operate. You could have awareness to your employees that the individual, vital digital asset they're working on, is it running slowly and the specific training that the employee is given is that hey, if it's running slowly or if it's running out of spec, call somebody. And then at that point, there may be an attack under way.

It's those sorts of activities that they would build in as a part of this program for them to be proactive. And that's on top of the fact that you have the protections in place that the various measures again, the reactive activities as well as the somewhat proactive administrative controls, whether it be media

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

protection or some other restriction of account log out or where certain types of accounts can be utilized.

And then the third leg of this stool which Matt's going to talk to you in a moment is the idea of response is that if we are being attacked and we've identified that we're being attacked, how do we stop it? How do we stop it before it moves over into the consequence of the concern happening? And from the staff's perspective, it's taking all three of these together, them operating together and integrated that gives us an effective cyber security program that's going to address this.

MR. PRIESTER: And to just add, this is Casey Priester, CSD Contractor. This is the notion of the defense in depth that's built into the way that the controls are designed. So in the example of say an attack that gets past McAfee because McAfee doesn't have the correct signature, doesn't have an updated signature for it, then your intrusion detection system might trip on anomalous network behavior which then can be flagged by your network operations staff. But let's say that gets passed up. Then it gets to the host that it wants to get to. It has host-based protection that disallow the use of certain privileged commands and it

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

will send an alert in the event somebody tried to do that with the incorrect credentials.

So you're talking about multiple layers and an attack that can bypass four or five discrete layers with different techniques for analysis is -- you're talking about a diminishing probability at that point.

MEMBER MARCH-LEUBA: Does the rule require to have this network monitoring because the way it is implemented in this building I'm sure somewhere in this -- probably on this floor, there's a war room with a guy with seven monitors overlooking, really looking at all the statistics on the network where things are going. And I had an opportunity to observe that in the lab because I used to park next to guy that worked in the war room and when we came on the way and we are talking all the time.

And, funny thing where he's saying I'm really worried about this because it's Christmas. Christmas is coming. And the bad guys know we are not here. And then when I come back in January, I have to fix up all the messes.

So unless you have that guy looking at those seven monitors, you're not really protected. Now having a guy looking at seven monitors in every plant

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

in a building like this is a minor cost. But in a plant like that, it's a big cost. That would be probably the largest cost of the whole thing. And he can only work Monday through Friday, 9 to 5. Bye, guys. I'm going to come on Saturday morning.

MR. DEUCHER: One of the things again, this is Joe Deucher with NMSS, that Casey started to touch upon is the tools and examples you were giving were all automated. And it winds up being something that this person who was working can build and configure to be operating for him or her when they're not around. So the thresholds are established. They're not there. It's Christmas. They're gone on vacation. They've got somebody designated that it's sending alerts to. And alerts can be sent out to let folks know that on the off hour something is happening. We're seeing something anomalous and it's hitting different devices and things aren't behaving the way that they should.

These tools are available. They're automated and designed for exactly the situation you're talking about, so that it's not burdened on just one individual and then when they're not there the resource isn't happening.

MEMBER MARCH-LEUBA: All day I have been

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

defending this side of the table and now I'm going to defend this side of the table.

(Laughter.)

That's a big expense with very little probability of payoff because the attack we are trying to prevent -- this guy over here, somebody here is a guy looking at seven monitors in this building. He's trying to prevent somebody sucking up a whole hard drive and taking it to an undisclosed location to look at it and see if there is something valuable in it. That's easy to detect.

The attack you are warning about here is downloading a few kilobytes of malicious code into somewhere it happens one ping and never happens again until he gives -- so network monitoring is not going to detect that.

MR. SHINN: Mike Shinn, NSIR Contractor. And that may be the case which is why we don't say in the rule you must do that, right? It's a performance-based rule because it's going to differ by each facility. I mean even the ones that are in the same business, the facilities are nothing like each other. The technologies they use, their processes and so on. So they're each unique. They're each different. How

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

they're going to solve this problem is going to be different.

There are technologies that are entirely preventative. That is to say they wouldn't allow the system to deviate from its normal behavior. Right? Maybe it just causes the device to not function. Maybe a licensee says that's adequate and they can credit that across the other controls.

We're trying to make this program as flexible as we can because there's this complete diversity across every single licensee that we have. They all do something different and even the ones that do the same thing do it differently and they use different technologies which is why we are not being prescriptive in the rule because in some cases maybe that works because we do have some licensees that are part of large global companies that have SOC's and they already have this capability and maybe that works for them. Maybe another licensee, the type and technology they're using, it's not necessary. It's not going to solve the problem. They're going to do something different. Maybe they just unplug it as Charlie described. They make it very simple.

So we're trying to make this as flexible as

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

we can. But the other challenge we have is on the reactor side, we actually have far simpler technology.

On the fuel cycle side it's all modern, 21st century, as you well know from just the facilities you've been to. They're ethernet based. They're programmable. They're sophisticated modern technologies.

So we have this range of things we have to protect against everything from computers running Windows to Siemens micro controllers that are custom built for that particular facility. So we have to make the program as flexible as we can to address both the - - just the wide variety of sites and technologies, as well as the huge range of solutions that a licensee potentially could use to solve the problem.

MEMBER MARCH-LEUBA: Okay, so again this is a personal request, nothing from ACRS or an ACRS member. Do me a favor. When you re-read this, make sure it says that. Because when I read it, I mean it's 170 pages. And you all know how we read it, but it says "thou shall have a software monitoring network program." And that could be interpreted as you need to have a war room with a guy with seven monitors. I would argue that the payoff for that investment is very low.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

MR. PRIESTER: So just to kind of complete that thought, Casey Priester, CSD Contractor. The rule states that you have to be able to detect a cyber attack. Now in the case where you're saying that well, my concern is not going to be an attack that propagates across the network. So having the guy with seven monitors is a big waste of money. Okay, so now you've determined that that attack pathway is not viable and you can then use that as part of your justification while you have a lower network monitoring capability.

In the meantime, I'm going to say can you detect a cyber attack that's 16 kilobytes of data that you're so terrified about? Do you have a means to detect that? And what is it? It's up to you come up with that and that's the one that's going to be the most important detection capability, but you still satisfy the requirements of the rule to have that detection capability.

MR. DOWNS: Jose, I hear what you're saying is from what you read and from what we're saying there seems to be a disconnect.

MEMBER MARCH-LEUBA: That is correct. Correct. Please review the Reg. Guide and make sure that what we're saying --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

MR. DOWNS: Is reflected in the Reg. Guide.

MEMBER MARCH-LEUBA: It's not part of the law.

MR. DOWNS: Fair enough.

MR. SHINN: We completely agree. What it should say is for each security control when you have a VDA, you should do one of three things. Either you're going to implement it or you do something that it solves the problem otherwise, what Casey and you were just discussing, or you can demonstrate that it's not necessary. So if that's not clear, we'll go back and look at it and make sure that's the case, but that's certainly precisely the way that we've expect the controls to be analyzed. They're not prescriptive requirements. They are solutions to problems that you should consider.

CHAIRMAN BROWN: Okay.

MR. BARTLETT: Okay, so respond to the last item, the last bullet on this slide. In order to have a response program, the licensee would need to establish procedures and resources for response to cyber attacks. So those would have to be established.

The order of response is spelled out. It should be first to place the digital asset into a safe

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

condition; second, to stop the attack; and then third, preserve evidence of the attack for investigation.

The response should also have the ability to test the response capabilities regularly and to address weaknesses that are identified.

Next slide.

MR. HECHT: This is Myron. Can I ask some questions before you go on?

MR. GIBSON: Please.

MR. HECHT: Okay, number one, with respect to the discussion of network monitoring, I don't see how you can get by without it, quite frankly, because you'll need it in just about any environment. But that brings up the question of whether -- you said SOC before which is Systems Operation Center, as far as I can tell. And that is something that's remote.

Is it acceptable for somebody outside the facility and that could be a network monitoring service provided by a third party to do that in your opinion?

MR. DEUCHER: Yes. This is Joe Deucher with NMSS. Yes, that would be. It's entirely incumbent on the licensee. They have choices. If they wanted to go ahead and go with an outside service provider and there are several out there to outsource

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

that service in order to have that, they certainly can do so. It's just what's going to suit their needs.

Again, the only area where there would be an issue or concern is so long as they don't run afoul of any of the requirements under 10 CFR 95 for any of their classified networks. So they would have to have that demarcation that they were only looking at their unclassified systems and not trying to attempt to outsource that monitoring.

MR. DOWNS: The other element here, too, is I think that the cyber security controls when it prescribed for digital assets associated with specific consequences of concern, those controls actually get into the off-site communications associated with that.

So for example, a design basis threat consequence of concern, I believe it's very, very limited, if not -- it may even prohibit offsite communication for the DBT consequence of concern.

And as you go down the list, this is an example of the grading that's present in the controls.

You know, a category 3 facility with a safety concern would be potentially in the lower end of that scale, so therefore you would be able to have this offsite communication that we're talking about.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

MR. HECHT: Okay, and just a comment. There's been a response to Jose's I guess general theme, not specific question. The point of advanced persistent threats is to be able to act in a way so that traffic monitoring won't detect what you're doing.

So there are -- this is what nation states do. And network monitoring won't be a complete solution and that points back to the importance of having your threat analysis and subscribing to these services and the assessments, the review of the adequacies of the controls to getting to that point. Particularly for the advanced persistent threats, they are at least as capable of the -- as the facilities for attacking probably much more.

And that also points to the futility of using a probabalistic approach. As hard as it is to predict an earthquake, it's a lot harder to predict human behavior when it's a lot farther in the future.

MR. DOWNS: Myron, this is James Downs. I completely agree there with what you've saying that the one aspect that you brought up with advanced persistent threat, those adversary characteristics would only be applicable to certain licensees within the fuel cycle industry. That's something that the design basis

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

threat would take into consideration, but that isn't something, given the material track in this present CAT 3 facility that they would be held to that same standard. So again, this is another great example of the grading that is present in the controls in the appendices. You should be able to -- if you look through the controls, you will be able to see how that's differentiated in there.

MR. HECHT: I'll have some questions about that later.

MR. DOWNS: Look forward to it.

CHAIRMAN BROWN: Let's move on.

MR. BARTLETT: Next slide. Okay, so now we talk about the responsibilities of the cyber security team. The primary responsibility of the team is to ensure that the performance objectives of detect, protect, and respond are met. That includes setting up the cyber security program which would be the development of the plan.

There are 16 individual items that are identified that the team would be responsible for in the reg. guide. They range from protective VDAs and associated support system from cyber attacks. I won't read them all, but you can read the list that the cyber

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

security team would be responsible for.

The make up of the team, we already discussed that briefly. It would essentially be a program sponsor, so it would be like your senior executive program manager; cyber security specialists, two of those; and then technical staff in safety and security. These staff would need to be trained and appropriately qualified.

MR. HECHT: This is Myron. I had a question on that as well. What happens if the team doesn't have a sponsor? Does this mean it deviates from the guidance and instead only the manager is the real point of contact with the NRC? And what happens if the team has a different certification than CISSP?

I guess my point is is that you may have used those assumptions in doing your costing, but don't you think that's overly prescriptive? Or why is it?

MR. DOWNS: So let me address the issue of the management piece of this, that you don't have an executive individual involved. The staff's intent there was to have some impact for the cyber security team to have some influence over the budget that they're allotted. And that was the executive piece of this. We wanted to be able to make sure that the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

concept and the rule where it discusses being adequately equipped and such, obviously there are budgetary concerns with that and we felt that if you didn't have a representative that could speak towards those needs that the cyber security team may not be adequately equipped at that point.

If it could be demonstrated that a mid-level manager had some of that budgetary influence, then yes, this is why we put it in the guidance document. We're trying to give one example of how to meet the rule. The rule itself doesn't say that you have to have an executive level individual in there. It just says that the team has to be adequately equipped. So that's kind of the connections that we were making.

As far as the other point on the --

MR. DEUCHER: Do you want me to?

MR. DOWNS: Yes, Joe, yes.

MR. DEUCHER: Myron, this is Joe Deucher with NMSS. Regarding the question that you raised for training, we listed just the CISSP, the Certified Information Systems Security Professional, as one example.

It would be incumbent upon each licensee to

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

determine what level of training that they thought their cyber security employees should have for their individual facility. I mean there are plenty of external certifications available that provide differing levels, but certainly in the same field or spectrum of the type of experience and understanding that they would need in order to perform their duties adequately. And we were just throwing one out there that certainly from a holistic perspective of what we're looking for in a cyber security program and for an expert, the CISSP is one that covers all of the various disciplines associated with cyber security versus say a certified ethical hacker where you're dealing more with the technical aspects or a certified auditor where you're dealing more with the accreditation pieces.

CHAIRMAN BROWN: We need to move forward.

MR. HECHT: But don't you think you ought to be more abstract and what properties of the CISSP is needed and similarly instead of saying that you need to have a sponsor, if in fact the issue is adequate for these -- forces then why don't you just specify that -- has adequate resources to do its job.

MR. DOWNS: That's a fair comment. We

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

appreciate that and it's something we'll have to take back and look at revising the guidance on.

Next slide, please.

Okay, so the cyber security plan we've talked about some. It needs to be -- the cyber security plan would be developed by the licensee and submitted to the NRC for our review and approval. It would be incorporated by license amendment to their license, so it would be tied down as a licensing document.

We do have a rough template in Appendix A that illustrates what would need to be in a plan. I went through the reg. guide and it identified a number of things that would need to be described in the plan.

The list includes the cyber security team, controls, identification process for digital assets, incident response, how the program is maintained, etcetera. So the plan would just have to spell out how the program, what's going to be in the program. And a key thing to note is it would be tied down in the license.

At this point, I'll turn the presentation over to Joe Deucher.

MR. DEUCHER: Yes, this is Joe Deucher, NMSS. We're going to be speaking about the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

consequences of concern which I know we've spoken about already today. Just to reiterate, these are risk-informed concerns that we've identified that are based on existing NRC thresholds that the rule is tied to in terms of what events are of significance with respect to the rule and what we are trying to prevent and what we are trying to protect against. We have them related to the individual facility types that the NRC has so that we have your Category I facilities are associated with as an example design basis threat. Category II would be associated with the safeguards consequence of concern. And then down from there to our Category III and our Part 40 facilities being associated with the safety and security, both active -- excuse me, the active safety and the latent safety and security consequences of concern.

The idea again, this is risk informed. So when we look at this list, we see that the design basis threat latent consequence of concern is the most robust. It is the most comprehensive. It is the strictest of our requirements and again that falls in line with what they're trying to protect against. So we set that threshold and that's why we have built all that we have on the control side as we'll talk about

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

later on into that particular one. And then it falls down from there when you look at the safeguards consequence of concern, all the way down through the other two consequences.

I will point out one difference between the active consequence and the latent is in terms of a concept. What we see is that between the two as a latent consequence of concern we do have an aspect of timeliness involved. When we look at an active consequence of concern, we're saying that this particular consequence, it happens based upon the cyber attack occurring. The cyber attack occurs. The device is compromised. The consequence occurs. So in terms of timeliness, it's an immediate. We have an immediate action versus the latent consequence of concern where there has to be two actions. One, we have the compromise that eliminates the function that the individual device has. And then we have a second event coming along that actually shows us that the function is no longer available and can't do what it needs to do.

So one of the things that we're taking advantage of in terms of the latent is this aspect of timeliness. And one of the things that we're looking

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

for in terms of the licensees as they're looking at these consequences of concern, this is mainly on the safety consequence of concern when we look at the latent safety and the latest safety security is that the other programmatic activities that the licensee has may very well catch this latent consequence of concern as opposed to the active consequence of concern, since the active is immediate. And that's why there's a difference in the granularity of the controls that we have between those two in response to that, so we are trying to take advantage of those other programs that exist.

The other thing that I would say is that in terms of consequences of concern that we have, if multiple consequences of concern are associated with a given area or given digital asset or vital digital asset, it would be the highest consequence of concern would be the one that would address all of the associated requirements.

So in the case of if we have a safety consequence and we have a DBT consequence in the same area, it would be the DBT consequence that would encompass all of the requirements in that particular area.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

And again, just finishing this out, as we say here, we've got the types of consequence of concern are ordered highest to lowest based upon the comprehensiveness of the associated controls.

MR. HECHT: This is Myron again. With respect to the III and IV categories, it's hard to understand the difference between the two because one says the device is disabled -- let's just say the VDAs associated with preventing a safety security violation and the other one is that the device is disabled and as a result some exposure occurred.

And it seems to me that in order to have an exposure you have to disable the VDA controlling the safety device. Why is there a difference? And why wouldn't disabling of the device that is basically a safety measure doesn't cause an immediate -- isn't active in both cases?

MR. DOWNS: Myron, this is James Downs. So let me just give you an example of an active consequence of concern. This could be a situation where you've got a crane that's lifting a liquid UF6 cylinder. That crane could have several IROFSS associated with it with the structural integrity of the crane, the robustness of the cylinder and in the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

process hazards analysis you would decipher that that crane, that cylinder could withstand one drop and it wouldn't rupture.

Okay, so the piece that may not be considered is that crane has a wireless controller to it. If you hacked into that wireless controller, you could feasibly take that cylinder and pick it up and drop it again and pick it up and drop it again and pick it up and do that until the cylinder fails. Okay? This is theoretical, obviously.

So that's where a cyber attack directly would cause a consequence, the consequence being the release of the UF6 in that cylinder to cause a -- to trip one of the thresholds that we've talked about.

The latent side of this would be if the function to prevent the consequence of concern was disabled and just sat there over a long period of time until a secondary event like a fire flood, earthquake, process hazard upset came along and would require the activation of that function, that function wouldn't be available because it's been compromised. So that's the big difference between active and latent.

MR. HECHT: It seems to me that if your control was doing the prevention of that crane

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

controller, and that failed, that would be a latent safety concern or would it be an active safety concern?

MR. DOWNS: Well, it potentially would be an active because if the malicious actor gained control over that crane, then at that point they could directly cause the consequence of concern. So there's very little time built in there for detection or reaction. So that's why the controls, the examples of the controls that we've given are more robust for that active example than what you would have for the latent example.

MR. HECHT: Well, let me just say that in the safety thing, the absence of a fire extinguisher is pretty -- where it's required is considered a problem even though no fire is attributed to that. Is that latent or is it active?

MR. DOWNS: That would be a latent example there because you've -- if the function of it relied upon was that fire extinguisher being present, the malicious actor didn't cause the fire. They just removed the fire extinguisher.

CHAIRMAN BROWN: Let's -- I don't want to belabor the active and other thing. We really do need to move on right now, if you don't mind. This is a bit

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

of nuance down in here between III and IV. So --

MR. HECHT: I think that's where a lot of them are going to be and I would just say that maybe some more examples might help.

CHAIRMAN BROWN: I appreciate that. That's a very good comment from that standpoint. Nobody would disagree. I certainly don't disagree with that. Examples are pretty sparse.

Let's go on to the next slide.

MR. DEUCHER: This is Joe Deucher again. Under identification of digital assets in this section, we have provided a methodology for identifying digital assets and determining vital digital assets.

Again, what we're looking to do is have licensees look in their various plant areas for consequences of concern, where they are. Look at digital assets associated with that, identify those that would have a direct, if compromised, have a direct action to cause that consequence of concern, either as active or latent. And then be able to list those. And then from that list look around and determine whether or not there are any alternate means that may stop that consequence from happening if that digital asset was compromised. Anything left over would then be

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

considered a vital digital asset requiring cyber security controls and programmatic activity.

And again, when we talk about an alternate means that's acceptable, what we're looking for is we're looking for something that number one is protected from a cyber attack. It's something that has the resources necessary. It's actively maintained and properly maintained. And can be activated in a timely manner and also takes into account the cumulative effects of a cyber attack. And where we bring this into play, a good example of this is if I say that I've got a controlled area where I've got an intrusion detection system. And if that intrusion detection system were to fail, well, I say well I've got a regular guard patrol and I'm going to take credit for that guard patrol. I need to make sure that I have enough guards on staff that if several intrusion detection systems fail, that the guards can go to those areas to be able to meet this and for them to take credit for the alternate means.

And then in terms of vital digital asset when we get down to that, these vital digital assets are the ones that would actually need cyber security controls to be looked at and ultimately measures to be

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

instituted in order to protect the digital asset. Now -- excuse me, the vital digital asset.

Now when we look at that vital digital asset, we can set its boundary and when we talk about a boundary, it's what are the individual components and features, software, if we're talking about software, individual hardware devices that would be included. And this is where we've built flexibility in for the licensee for them to say I could take an entire network and make that a vital digital asset if indeed I have multiple network devices.

They also have the ability through what we call grouping or what would also be considered typing to where if I have a particular programmable logic controller that I'm using and maybe I have one that's a similar design across the entire plant, they could go ahead and protect that in kind. And again, what this is designed to do is from a documentation standpoint and from an overall just implementation standpoint, it's going to cut down on what they ultimately need to do because they'll be able to take advantage of the economies of if I'm doing one thing and I'm doing it for say 10 or 15 different devices, I take advantage of the resource savings that I have there.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

Does anybody have any questions on this slide?

MR. HECHT: This is Myron.

CHAIRMAN BROWN: Myron, John wants to have some questions. Let him go.

MR. HECHT: Absolutely.

CHAIRMAN BROWN: Thank you.

MEMBER STETKAR: And again, I'm being the surrogate for Dennis, I had some questions. As I read through this and tried to think through how one defines vital digital assets and acceptable alternate means.

Let me pose a couple of examples first and see if I get a couple of answers. So I've done an integrated safety analysis on my facility and I have these I'll call them scenarios that result in my undesired consequences of concern. And suppose in my integrated safety analysis I've identified two digital assets, both of which must fail to achieve the undesired consequence of concern. Now I've also examined these digital assets and I found that they don't share any common hardware. They don't share any common software. They don't communicate with one another and they don't share any support systems. So they are two separate things. They're both vulnerable

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

to cyber attacks because they've got USB ports.

My understanding is neither of these is a vital digital asset because neither one of them individually will result in the undesired consequence of concern. Is that correct?

MR. DOWNS: No, that would be incorrect.

MEMBER STETKAR: Okay, why is that incorrect? I need to understand why that's not correct.

MR. DOWNS: It's incorrect because in the actual rule itself it states that a digital asset is vital is no alternate means that is protected from a cyber attack can be credited for the consequence of concern.

MEMBER STETKAR: Okay.

MR. DOWNS: So therefore you don't have that -- by adding that USB port on there you have the pathway to enter it, so you're vulnerable to that cyber attack. So that would not be protected.

MEMBER STETKAR: So as long as -- I make sure that -- it's not that digital asset X is vulnerable to cyber attack vectors one, two, three, four, five. And digital asset Y is vulnerable to attack vectors six, seven, eight, nine, ten, the fact

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

that they are both vulnerable to a cyber attack makes them not acceptable alternate means to one another. Is that --

MR. DOWNS: That's correct.

MEMBER STETKAR: Am I getting that?

MR. DOWNS: That's correct. Now you would only have to protect one of those. If you protect one, if you provide cyber security protection to one of those and it becomes a vital digital asset --

MEMBER STETKAR: But the key is it must be protected from any conceivable cyber attack, not just the cyber attacks that can affect -- let's say I want to take credit for a digital asset Y as my alternate means. And I know that asset X is vulnerable to as I said, one, two, three, four, five. I must protect digital asset Y from any conceivable cyber attack, not just one, two, three, four, five.

MR. DOWNS: That's correct. You would have to protect it as if it were a vital digital asset.

MEMBER STETKAR: Thank you. That helps.

MEMBER MARCH-LEUBA: Would you say then that any and all unprotected assets, if they are unprotected, they're assumed to fail. You have to assume that they have been compromised, even if you

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

have to use two different attacks.

MR. DOWNS: That's correct.

MEMBER STETKAR: Thanks. That helps that one. Let me make a note here because I can't remember what day it is. Okay.

Now let me take again my ISA scenario where I have -- I'll just call them two IROFSSs. They may or may not be digital. Maybe one is digital, maybe one is analog. But they share an electric power system that is vulnerable to cyber attack.

As I read the guidance, it says I identify vital digital assets and then I look for their support systems. It doesn't say that I separately look at support systems and see if they might -- once I have completely analog IROFSSs, but the electric power system is subject to cyber attack, how do I identify that? Is my electric power system now a vital digital asset?

MR. DOWNS: So in ISA space that actually should have been addressed in the consideration of common cause failure because the power supply --

MEMBER STETKAR: Okay, I should have done that, but if I read the guidance, my interpretation as I read the guidance says I identify vital digital assets and then I look at their support systems.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

MR. DOWNS: That's true.

MEMBER STETKAR: But neither of my IROFSs in the sequence is a vital digital asset. They're both analog things. They're not even digital.

MR. DOWNS: That's true.

MEMBER STETKAR: So I don't have a vital digital asset that I've identified. How do I identify that electric power supply as a vital digital asset?

MR. DOWNS: So have you had these assets identified to have a consequence of concern?

MEMBER STETKAR: Yes. But remember, they're analog.

MR. DOWNS: So if they're analog, would they fall under the scope of the rule?

MEMBER MARCH-LEUBA: In his example, there is a digital controller to the relay of the interest of the plant that can keep the power.

MEMBER STETKAR: You know, my whole electric power system inside my plant.

MR. DOWNS: So if your vital digital asset the IROFSs in that case or would it actually be the power supply?

MEMBER STETKAR: See, I don't know how people will apply this. That's what I'm asking about

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

when I get -- because as I read the guidance, again, I'm just reading the guidance and the guidance says if I identify a vital digital asset I look for its support systems. And it then goes on and says well, I could group the support system with that vital digital asset, or I could decide to treat the support system separately, but the trigger for me seems to say I have to identify first a vital digital asset before I go look for the kind of thing I'm looking for.

MR. SHINN: Mike Shinn, NSIR Contractor. So I think the answer to that is part of -- in the case of the ISAs that digital asset would have already been identified. And you use the ISAs as part of the process of identifying the consequences of concern.

MEMBER STETKAR: No, no, no. I'm asking -- I'm now sitting. I have this blank piece of paper here and I have an ISA that's got all of these sequences out there. You say that digital asset has already been identified and I'm asking what digital asset?

MR. SHINN: So if I understood your hypothetical, you have a digital component or series of components that controls the electrical power to some analog devices that are part of an IROFS.

MEMBER STETKAR: Yes.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

MR. SHINN: So that digital asset should have already been identified as part of that ISA because it can cause that consequence -- malicious attack aside, you lose the electricity, it doesn't function.

MEMBER STETKAR: Okay.

MR. SHINN: That would be our expectation.

MEMBER STETKAR: Thanks. I got it. As long as that's clear, let me ask a third thing here in terms of now if I focus on adequate alternate means. A couple of examples in the guidance notes that include manual or automatic fail safe features or processes, process stoppage in a timely manner before the consequence of concern can occur.

So can I take credit now for personnel actions to be an acceptable alternate means?

MR. DOWNS: Yes.

MEMBER STETKAR: Okay. How do I determine that those manual actions are adequately -- that they're both feasible and reliable?

MR. DOWNS: There is some inspection guidance on the fuel cycle side of the house that gets into the robustness of IROFS and other credible means of protection. There's a little bit of discussion in

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

that.

MEMBER STETKAR: In the interest of time, let me do a couple of things.

MR. BERGEMANN: I mean the criteria would be to prevent the consequence of concern.

MEMBER STETKAR: Right. I understand the criteria. I'm asking about both feasibility and reliability of those --

MR. DOWNS: How do you know that operators --

MEMBER STETKAR: How do I know that the people can do what I'm crediting them to do within the time that's available for them to do it, whatever it is, and that I have reasonable assurance that more than 50-50 they're going to do it for more than 10 percent or whatever that they're actually going to accomplish that?

I don't know how much detail you want to get into. There is guidance available in the Agency for doing that type of an assessment in NUREG-1852 and in NUREG-1921. Now that guidance was written in particular for power reactors for response to fire events, but it's generic guidance. It looks at time available to perform an action. It looks at time

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

required to actually do that, assessing whether people can actually accomplish what they're supposed to do within the available time window and then it looks at margins in terms of assessing reliability.

I don't know whether that belongs in this regulatory guidance, but certainly you do identify the fact that the personnel actions can be credited as acceptable alternate means. And you might want to emphasize the fact that those actions should be demonstrated to be at least feasible if not feasible and reliable. There's a lot of -- I'm not advocating doing some sort of formal quantitative human reliability analysis, but the Agency does have guidance in terms of looking at available time margins as a surrogate for reliability, if you will.

MR. DOWNS: Yes, and actually, I happen to be very familiar with that. In a former life I was a fire protection engineer over at NRR.

MEMBER STETKAR: Well, there you go.

MR. DOWNS: It's right up my alley. I appreciate the comment.

MEMBER STETKAR: Okay, thanks. Those are my three, Charlie.

CHAIRMAN BROWN: Now I'm waking up now. I

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

listened to all of them.

Myron, are you there? Myron? No. Myron, are you there? We'll come back. You want to check to make sure the phone didn't get disconnected? I haven't heard any snap, crackle, and pop here for a few minutes, so -- all right, why don't you go ahead.

MR. DEUCHER: Okay, again, just one last point that John did mention was with respect to support systems, again with a vital digital asset, we would expect that any support systems that aid in its function would need to be analyzed to determine if the removal of it or what its impact would have on the vital digital asset. And if it turns out that the support system is vulnerable to cyber attack, you either include it or you protect it separately.

MEMBER STETKAR: I got that directionality. I was looking for --

MR. DEUCHER: Right, the other piece.

MEMBER STETKAR: The other piece.

MR. DOWNS: Just before we move on, would you think examples like that would be beneficial in the reg. guide?

MEMBER STETKAR: I think an example like would be really useful because the problem is people

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

read guidance, both licensees and staff reviewers will read that guidance and certainly look for the directionality that Joe mentioned that I mentioned previously. Here's a vital digital asset. It relies on AC or DC power from these sources. Are they vulnerable? It relies on ventilation of room cooling because of its location. And that's fairly clear from what's in here. What's not quite as clear, especially if the ISA itself has not necessarily explicitly identified the electric power system. It might have a circuit breaker in it or something. I don't know the level of detail what people put in these things.

MR. DOWNS: For IROFS, it's pretty good. We have what's called an IROFS boundary package that's available on site for inspection that includes all of the elements that are required for that IROFS to function properly. So they're fairly well documented, but I appreciate the direction.

MEMBER STETKAR: But I think something to just trigger something -- let's say your whole plant, ventilation --

CHAIRMAN BROWN: Hold on, Myron, hold on. Can you hear me?

MR. HECHT: Yes, I can.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

CHAIRMAN BROWN: Hold on for a second.
John was having a discussion as you came back on.

MR. HECHT: Right.

MEMBER STETKAR: Your whole plant
ventilation cooling system, for example, was digitally
controlled, let's say --

MR. DOWNS: Right, right.

MEMBER STETKAR: To just alert people that
they need to think about from that direction, despite
the fact that we might write off everything because
they explicitly thought about going analog or whatever.
Thanks.

MR. DOWNS: Thank you.

CHAIRMAN BROWN: Okay, Myron.

MR. HECHT: Okay, I have two questions
related to the -- one was related to the concept of
grouping. And the other one was related to the concept
of inheritance. And I guess the first thing I'd like
to ask is -- you spoke about the example of an
enrichment facility with thousands of centrifuges in
it. Could the entire centrifuge control network be
considered one VDA?

MR. DEUCHER: This Joe Deucher. Yes. That
is correct. You could do it either way. You could do

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

it by type which means that each individual centrifuge could be considered a VDA and you come up with a common set of controls and measures to do them all. Or you could make the entire network one VDA. It just depends upon -- what we're thinking would go into this is how are these being maintained now, what IT services they may be receiving. And it would probably parallel -- or the licensee could parallel what they're doing in terms of on-going maintenance and operations, how they would approach cyber security with it.

MR. HECHT: What if I made all 15,000 digital assets in my facility into one digital asset, one VDA. What prevents me from doing that?

MR. DEUCHER: Nothing. This would be analogous to developing an IT system -- my experience has been with IT systems in the Federal Government and we had -- I'll take the licensing support network which dealt with the Yucca Mountain evidentiary documents. That was a farm of I believe 30 different servers with multiple different software packages. And it was housed in its own hosting facility and it was considered one distinct system. Even though you could have taken four or five functions out of it made those individual systems.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

It's really again, it's up to the licensee and their operations and maintenance what makes the best sense for them.

MR. DOWNS: And Myron, this is James Downs, just to add on to what Joe was saying, you could take all 15,000 and put them -- and group them as one, but that assumes that there's some level of connectivity between those 15,000. If you were to take 15,000 assets that were completely unrelated and completely unconnected and try to group them together, it could be challenging to address the controls in a single implementing procedure for all those 15,000. You would have a lot of different exceptions. It could be done, but that implementing procedure would be very complicated at that point. But again, it's a flexibility that we're allowing licensees to choose how they want to pursue it.

MR. HECHT: So in principle, these requirements aren't as onerous as they might first appear because even though we might have a lot of computers hanging around the plant, they could be essentially divided into zones and each zone could be considered a VDA.

MR. DOWNS: Possibly, yes, you could do it

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

that way, yes.

MR. DEUCHER: That's correct, or you could consider the computer itself to be a VDA and it's just a VDA type. So they're all the same type so they would get essentially a software image with all the protections they needed. And you would just have one software image and one implementing procedure for all those computers, similar to what's done in federal IT systems.

MR. HECHT: Okay, my second question was with respect to inheritance. So you have, let's just say your Siemens family controllers and some of them have different interfaces and some of them have different functions and they're all running the same, I guess, they have many things in common. How does that work with respect to writing implementation procedures or defining controls?

MR. DEUCHER: Well, with respect to controls and this is a great segue to the -- if you bear with me, Myron, to the next slide, when we're talking about controls, controls are performance specifications. So essentially what we're trying to do is we're trying to deal with individual what would be called threat vectors. And the control family is again

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

our controls are informed by the NIST controls and the NIST controls are designed to cover all the possible threat vectors that you could attack a given system with.

And so the individual controls themselves are performance specifications. And then what I do is I would add a measure to meet that specification. Now when we start talking about inheritance, what we're getting into is, let's say that I've got a couple of Siemens controllers and let's say that they're tied to a SCADA system as an example. And that SCADA system is managing these controllers or maybe one of the controllers has management authority over the other.

When we talk about inheritance, what we're saying is whatever I've potentially done for the one controller, if there is a relationship between the two, let's say that one is feeding the other its information and it only talks to that other controller, that I could put measures to protect that first controller and those measures could be inherited by the second controller. That's the notion of inheritance. It's a one-to-one relationship between two vital digital assets where I'm using protections on one to protect the other.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

Now when I want to further take out this example, when I start talking about common controls, what I'm talking about there are measures that I might do at a higher level to cover multiple vital digital assets. One could consider if these things were all attached to a network. Again, if I had a SCADA management server or computer, I could then go ahead and put the various protections on that management computer and use that to then protect these other devices that they would take the inheritance because the argument being that the individual logic controllers only talk to that SCADA computer. They don't talk to anything else. There's no other way to get to them so if I protect the SCADA computer, I've protected these individual logic controllers.

MR. HECHT: But one example of inheritance might be a firewall which will prevent vectors from the external environment.

MR. DEUCHER: Exactly. And again, when we talk about the individual controls, we're talking about the communications controls where we're trying to protect system communication. The firewall in that instance would be an inherited controller. Again, if I'm doing it for multiple VDAs it's really a common

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

control because everything that's attached to it can take advantage of it and in that instance I am protecting this particular threat vector with this measure and I can take credit for it. So again, when you look at how onerous these controls and the efforts that we're looking for licensees to do, in reality, we're building in this flexibility that depending upon the design of their facility, there's lots of different choke points that I can put things at to be able to take advantage of, so I'm not having to individually protect each vital digital asset for every single threat vector that exists that's being addressed by the controls.

MR. HECHT: Well, then how I write the implementation plan for the -- asset and the inherited control situation?

MR. DEUCHER: This is the beauty part. For that, all I have to do is reference the implementing procedure for that other device. So as long as I'm able to refer back to that other device's implementing procedure, that it exists, that it's -- it could be either in a parent system or another vital digital asset. I'm referring back to that other implementing procedure. I have met my requirement or again, one

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

approach to meeting the requirements.

MR. HECHT: Okay, then how with the Siemens controllers we have them behind a firewall. One has one kind of --

CHAIRMAN BROWN: Hold it, Myron, Myron. We need to slow down on this a little bit, okay. We're getting way down at this level, way down in the depths of programming, inheriting, and all that other kind of stuff. I don't want to necessarily cut you off, but I need to cut you off on this one. We need to get moving.

MR. HECHT: Can I just make one final comment there? I just want to say that Appendix G with your implementation control has the simplest case and I think you have to consider a lot of other cases to make it clear what the grouping common and inheritance are about and how you would write those controls.

CHAIRMAN BROWN: That's a good conclusion.
Thank you.

MR. DEUCHER: Let me just make one final comment and then we'll move on to the next slide. One thing -- and I'll be quick. When we're dealing with the controls and we're dealing with the measures, we want to be very clear to licensees that for vital

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

digital assets you can't use one control to meet the requirements of another control. Each individual control needs to be individually addressed. We can't swap one for the other saying that I don't need to do this one because I did this other one over here.

The only way that I can eliminate a control is to say that it's not applicable that the threat is not present because each individual control is designed to deal with a specific threat. And with that I'll move on to the next slide.

CHAIRMAN BROWN: Don't worry, based on earlier conversations and I'm not going to --

MEMBER STETKAR: Just for the record I need to define an acronym. You often referred to SCADA computers and things like that? Supervisory Control and Data Acquisition. Thank you.

CHAIRMAN BROWN: Thank you.

It's a public record.

MR. DEUCHER: No, I completely understand.

CHAIRMAN BROWN: I was looking for that as a matter of fact since I knew it and forgot it. All right, let's go on. We need to keep moving along here.

MR. DEUCHER: Absolutely, and I'll make this brief. What we ultimately -- this results in the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

creation of what are called implementing procedures. The implementing procedure is the equivalent of what would be a systems security plan. It's going to identify the measures that I need to take for a particular vital digital asset. It's going to identify those that I didn't take. It's also going to include how I verify the controls or I should say that the measures did indeed work. This is something that they would have in their documentation. It would be kept on site, but available for inspection.

And when we talk about interim compensatory measures which have been mentioned earlier today, those would come into play then when I'm going through the verification process or these measures that I've implemented to address the cyber security controls. If something doesn't work, in order for me to operate that device, that vital digital asset, I need to have a compensatory measure in place.

CHAIRMAN BROWN: What you really mean is compensatory measures are required when the basic functionality has been degraded. Measures and measures, I'm trying to define the difference between the two words here.

MR. DEUCHER: Yes, that's exactly right.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

CHAIRMAN BROWN: Okay.

MR. DEUCHER: So it's something temporary.
You track it until completion.

CHAIRMAN BROWN: I understand that.

MR. DEUCHER: Okay. Great. If there are
any other questions?

MEMBER STETKAR: I have one. Sorry,
Charlie.

CHAIRMAN BROWN: That's all right.

MEMBER STETKAR: I think this is going to
be my last one. In this particular section, there's a
note that says that licensees should document
justification and an appropriate management approval
for an interim compensatory measure that would be kept
in use for more than one calendar year from the date of
adoption. I hung up on that only because we've lived
through decades of licensees instituting interim
compensatory measures for lack of compliance with fire
protection, regulations, and I was curious why we're
sort of tacitly saying that we can keep interim
compensatory measures in place for at least a year.

MR. DEUCHER: Well, if you like, I can
answer with a quick example. Let's say you've got a
logic controller and your intention was that we're

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

going to password protect the logic controller and we're going to put actual -- use the features in the logic controller in order to be able to protect it so no one can tamper with it.

There's a recent example where a logic controller that needed to be updated by the company in order to deal with the vulnerability. A vulnerability now existed where you could break in and you could defeat the password system that was on board and then you could go ahead and take over that device.

The update would not work on this model logic controller because it didn't have the memory protections in place. So if you already had a measure in place that said I'm going to take advantage of what's built into the logic controller and all of a sudden you now find out that my options are I either have to replace the logic controller or I have to protect it in some other fashion, that's where an implementing procedure could come into play that could take a longer period of time because it may very well be that the licensee decides okay, in order to replace this logic controller, I actually have to go through and re-engineer the line and look at the performance characteristics of what I'm going to replace it with.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

And that's where this sort of scenario that we looked at where we would need to give them some flexibility, but at least to have it documented and show that internally within the cyber program it's taking notice of this and somebody approved that this is going on.

CHAIRMAN BROWN: Okay, next slide. Whose turn?

MR. DEUCHER: This fine gentlemen over here.

CHAIRMAN BROWN: I did a quick look at the next few slides and it looks like we did some fairly extensive discussion on some of these earlier. So if you can look at those and recall in your young memory bank as opposed to my old memory bank where you can calibrate this like that and say hey, look, we spent a lot of time on this and go on, okay?

MR. BERGEMANN: Right. Okay, the next slide is -- this is Brad Bergemann from NSIR. So the next slide is configuration management. We did talk about this a little bit during the rule language.

One thing to note, even if you're a site that does not initially identify any VDAs, you still want this program in place. So when there's changes to the facility or digital assets that are Part B

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

consequences of concern, there's some sort of analysis done by the technical experts in those fields and that cyber person to look at to make sure this change would not either affect the alternate means that you're relying on or introduce a new vital digital asset.

CHAIRMAN BROWN: So if all plants, if they don't have any digital assets or vital digital assets, they have to have a security program, a security program plan, a security team, a security --

MR. BERGEMANN: Well, they don't necessarily --

CHAIRMAN BROWN: -- configuration team.

MR. BERGEMANN: Introducing cyber within their current configuration management program to continually in the future analyze changes.

CHAIRMAN BROWN: You said configuration management program meaning not necessarily cyber, but their facility configuration management program.

MR. BERGEMANN: Correct. Correct.

CHAIRMAN BROWN: All right.

MR. BERGEMANN: Through stakeholder interactions, that was pretty much the consensus they already had some program in place.

CHAIRMAN BROWN: I got it.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

MR. BERGEMANN: We're just adding cyber to it. Any questions on that still?

CHAIRMAN BROWN: Not from me anyway.

MR. BERGEMANN: The next slide is review of the cyber security program and as James talked about earlier for the CAT 1s, the intent was to keep it consistent with what they're currently doing for their physical security program. So their cyber security program would be reviewed along with that physical security program annually. And there's other criteria involved with that and that we would just keep it consistent with what's currently being done at the CAT 1. For the CAT 2s and 3s, that would be performed every 36 months, every 3 years and it would look at your implementing procedures, any comp. measures, the program overall configuration management, cyber security team, and just evaluate the controls in place and just look at their effectiveness and if there's been any changes to the threat or controls that are no longer needed.

CHAIRMAN BROWN: Okay.

MEMBER POWERS: I understand for CAT 1, you're doing it just for consistency. You're already reviewing one, might as well do the other one while

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

you're at it. What motivates the triennial?

MR. BERGEMANN: So I think the point there was some of their other programs have the three-year review and also I think that's kind of with the NIST guidance is every three years.

MEMBER POWERS: Software modifications, of course, they're faster than that.

MR. BERGEMANN: Software modifications.

MEMBER POWERS: Yes, operating systems, things like that undergo more frequent upgrades than triennially.

MR. DOWNS: That's a great point, so what you have there is a situation where the configuration management piece of it would be monitoring those elements that are involved with the vital digital assets. However, you're not doing that comprehensive review except for every three years.

And typically, what the NIST program recommends that you do it incrementally over the course of the three-year period so that you're looking -- you don't have to do it all at once. It's not a huge effort every three years. You're doing a certain percentage -- 33 percent one year of the SS-33 and working around that. The number is there. You missed

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

one percent.

MR. DEUCHER: And when we're talking about the review, it's looking at the measures that you took.

It's also looking at the controls that were in place, just looking at your foundation of your program overall to see if the assumptions that you made at that point going forward are still valid. Do you need to make any changes? Do you need to make any plan amendments which would then be submitted to the NRC for approval?

And then going forward, do you continue on, as James said with the configuration management system which would look at the individual updates, the individual changes they made --

MEMBER POWERS: I was kind of finished for why we were doing three years. I mean the first one is a convenience. It's not motivated by any technical factors. You're there. You might as well do all of them at once and get it out of the way.

And it's not orthogonal to the rate at which changes might be made. In a three year, it's less obvious why that was selected. It's Category 3.

(Laughter.)

MR. DOWNS: Another influencing piece of this is I believe on the reactor side it's every two

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

years. Yes. So originally, we had aligned this rulemaking, the -- what was going to be all of our facilities every two years to be consistent with the reactor side of the house and what our stakeholders pointed out to us was and what we realized is that the risk profiles associated with the CAT 3 facility are dramatically different than that associated with the reactor.

MEMBER POWERS: Why not take five?

MR. DOWNS: That's a good question. Why not do five. So what we did was, as Mike pointed out, it's every three years per NIST, so that seemed to be an acceptable, an industry -- a globally industry acceptable standard, so therefore we just went with three. But I could see a stakeholder comment saying why not do five? And try to provide some justification for it, but staff position right now is that three is in line with other industries and that's what -- that's our story and we're sticking to it.

MEMBER POWERS: You're appealing to authority. There's no technical basis.

MR. DOWNS: Absolutely, absolutely. Yes.

MEMBER POWERS: So I might as well ask it her for her.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

MR. DOWNS: What we should do and I'll take this back is look into the reasons that NIST has established that three-year period.

MEMBER POWERS: I sure would because she's got -- she'll pick that one up almost instantly. I think their PHAs are reviewed every five years.

MR. DOWNS: I'll have to look, I'm not sure.

MEMBER POWERS: Yes, you want to make sure your story is pretty glib on that one.

MR. BERGEMANN: Any other questions on that slide? All right, well, moving right along. Event reporting and tracking. We did talk about this. So we're pretty much relying on existing regulations for these events, the consequence of concern events.

CHAIRMAN BROWN: Why don't we go to the next slide? We've spent a lot of time talking about your 1 hour and 24 hours and all that other kind of stuff.

MR. BERGEMANN: All right, next slide is record keeping and --

CHAIRMAN BROWN: You spent 32 seconds on that one last time.

MR. BERGEMANN: Probably too much.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

CHAIRMAN BROWN: Too much. and you said all good programs have record keeping.

MR. BERGEMANN: Right.

CHAIRMAN BROWN: And you went on. So we can go on on this one also. Okay, good.

MR. DOWNS: All right, Appendix B.

MEMBER MARCH-LEUBA: Hold on, hold on, just keep a section D on data implementation. Maybe I'm reading the wrong rule, the wrong guideline.

CHAIRMAN BROWN: What are you doing?

MEMBER MARCH-LEUBA: There's a section data implementation, right, in there.

MR. DOWNS: You're correct. We did skip over that.

MEMBER MARCH-LEUBA: And I have a question.

CHAIRMAN BROWN: What did we skip over?

MEMBER MARCH-LEUBA: What am I not understanding there because under use by the NRC staff says under no circumstances are we planning to use this guide or even ask that it be applied voluntarily. I mean what am I missing here?

MR. DOWNS: So basically what this is, that section there says that this is a guidance document and it doesn't set regulatory requirements. So therefore,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

the staff can't say it's in the reg. guide, you have to do it. That's really what it gets to.

MEMBER MARCH-LEUBA: Maybe you should just shorten it, because it really is -- several times.

CHAIRMAN BROWN: Boilerplate. Why can't we go on? It's in every darn reg. guide we get. It is exactly the same.

MR. DOWNS: But I agree with you, it should be three sentences rather than --

CHAIRMAN BROWN: Well, we're doing it in no sentences.

MEMBER MARCH-LEUBA: We are doing it, and we are not using it, don't even try to use it.

CHAIRMAN BROWN: John, you look like you're going to punt, let's move on.

MR. BERGEMANN: Appendix A is going to be a security -- cyber security plan template that would be submitted to the NRC. Some of that will be boilerplate language and then there will be some site-specific considerations that they'll have to address.

The controls that are in the reg. guide can be used and submitted with the cyber security plan if they choose to use those. And once again, that plan would be submitted to the NRC for review and approval.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

CHAIRMAN BROWN: Just one question again relating back to one comment you couldn't substitute one control for another. I guess my flavor on this is if you decide to use the reg. guide and you have 144 controls spread through these various B through Fs, you have to document based on the way the guide reads, why you did what you did, the descriptions, all these -- rest of the boilerplates that's in --

MR. BERGEMANN: That would be in the procedures. The actual plan would just be hey, we're using these controls, B through whatever --

CHAIRMAN BROWN: But you have to document what each control, how it's executed or implemented in your thing, right?

MR. BERGEMANN: Not in the plan. Only in the procedure.

MR. DOWNS: The implementing procedure, associated with that vital digital asset.

MR. BERGEMANN: The plan would just basically be the template of the control B-

(Simultaneous speaking.)

CHAIRMAN BROWN: Appendix B in other words.

MR. DOWNS: Correct.

CHAIRMAN BROWN: Which says controls

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

associated with --

MR. DOWNS: Right, literally you would --

CHAIRMAN BROWN: You'll still have to take a piece of paper and write down all this stuff for each and every control, for each vital digital asset. We touched on this a little while ago. John mentioned it I think.

MR. BERGEMANN: Oh, for the -- that's for the implementing procedure. So you have a VDA and you've got to implement the controls or address the controls.

CHAIRMAN BROWN: And you can't pick and choose. You've got to go and say why you didn't or why you did and whatever else the process goes along with it.

MR. DEUCHER: That's correct.

CHAIRMAN BROWN: Okay, all right.

MR. BERGEMANN: That's not in the plan.

CHAIRMAN BROWN: I got your point.

MR. BERGEMANN: Any other questions on the cyber security plan template?

All right, next slide.

MR. DEUCHER: Okay, this is Joe Deucher again with NMSS. When we're talking about the actual

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

controls themselves, we did provide, as we've spoken to, the set of sample controls that licensees could use as one approach.

The Appendix B includes what we would consider the controls that all vital digital assets would need to address. What we tried to do is essentially boil this down so that you would be able to use Appendix B and then depending upon the consequence of concern you were dealing with, one of the other following appendix, four, Appendix C through F, together with a particular vital digital asset and you would have your road map for the protections that you needed to go ahead and put into place.

Again, as we say here, the licensee can choose to adopt the appendix and just attach it to their cyber plan. Or if they want to they can develop their own controls. And again, there are other control sources out there. They just would need to show that and demonstrate that the controls provide the capability to address the cyber attacks and keep them from causing a consequence of concern.

Next slide, please?

Does anybody have any questions on --

CHAIRMAN BROWN: No. Next slide.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

MR. DEUCHER: Okay, and again, the difference here with Appendix C through F is its consequence of concern specific, so Appendix C is going to be the most robust, most complete because it's dealing with the latent design basis threat and as we go through E through F, they become less comprehensive, less robust. And again, the same rules apply. Licensees can either adopt them or they can choose to develop their own with justification.

CHAIRMAN BROWN: Hold on. Whoever is on the speakers up there, you're shuffling papers and we can hear it, so kind of mute your input if you don't mind, please.

MR. HECHT: Sorry about that.

CHAIRMAN BROWN: That's all right. We got it. Go ahead.

MR. DEUCHER: Does anybody have any questions on this slide?

CHAIRMAN BROWN: No, go on.

MR. DEUCHER: Great. Next slide.

MR. BERGEMANN: Brad Bergemann with NSIR again, and the last piece, Appendix G. Something that we kind of came up with at the last minute and we're working on is developing an implementing procedure,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

probably this criteria and maybe a template. We want licensees to be able to use -- they have their current way they write their procedures, but we would definitely want certain things in the implementing procedures for the vital digital assets to be addressed in those. And come up with that criteria.

MEMBER MARCH-LEUBA: So is this the time to start criticizing the specific examples?

MR. DOWNS: You can.

MEMBER MARCH-LEUBA: I see in there in one of the paragraphs you give credit to the fact that the asset is inside a LOCA cabinet. When we finish and there is more time I'll tell you a very funny anecdote when I found out that every cabinet in the United States uses the same key and because -- the clear example is when you see these maintenance technicians, they don't carry a four-inch ring with 150 keys. They carry only one. So the fact that it is locked is -- shouldn't even be credited. And even if it was a different key, those keys are this long, have only three pins and you get on to You Tube and figure how to open it. You just need a paper clip and a screwdriver. Even I can open it. So also credit is given for the door=s alarm. The only alarms that trip are the ones

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

that when the intruder doesn't know they are there.

It's the same with the tampering indicating devices and alarms. If the intruder knows it's there, that alarm is useless. So giving credit to those two things in your example is a bad -- set in the licensee is --

And going fast, the very last bullet, it says that you have to verify that the DVA has combustible fuse such that all ports except network connection are disabled. And you verify this by plugging in a USB device. So you're closing all the ports and you're leaving the USB open? That's the worst thing you can possibly do. I see the expert saying yeah. Remove that sentence. This example is terrible. It's directing the licensees to do some things that they shouldn't do. Scratch it and start all over and provide us with three or four more which are real and --

CHAIRMAN BROWN: I'm trying to find Jose's example. Is that the one on page G1 where it talks about the access control and alarm system performs a functional capability to contacts-generated intrusion, etcetera, etcetera?

MEMBER MARCH-LEUBA: Yes.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

CHAIRMAN BROWN: Okay.

MEMBER MARCH-LEUBA: Under the very last paragraph on the very last page.

CHAIRMAN BROWN: Very last page. ZZ.

MEMBER MARCH-LEUBA: It is an example.

CHAIRMAN BROWN: I got it, the USB device. Okay, got it. Thank you.

I guess Jose is finished and you can go on. I'm not sure this is -- go ahead, this last slide.

MR. DOWNS: Last slide.

CHAIRMAN BROWN: If you're just going to say these words, that's not useful for very much.

MR. DOWNS: No, I understand. So it's kind of a recap and hopefully -- we've kind of discussed a little bit of this as we've gone through. But again, we've got a wide variety of existing process architectures present in our fuel cycle facilities. Some are robust. Some maybe not so much. The proposed regulatory requirements for fuel cycle cyber security are based off of the potential consequences associated with those processes.

The licensees aren't tied down to any specific digital designs for these processes because they have evolved over time.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

CHAIRMAN BROWN: Neither are these.

MR. DOWNS: I'm sorry?

CHAIRMAN BROWN: Neither are these fundamentals either.

MR. DOWNS: Well, that's true, but the point here is that -- as kind of an anecdotal here, systems aren't built with physical security. The physical security, the guards, guns, and gates are designed around them. It's the same concept here with cyber security. We can't really control what that licensee has for their proprietary system that's designed to produce whatever widget it's designed for.

What we're saying is is that the methodology that we've outlined here under the proposed rule takes that process and protects it in a bunker, so to speak, such as the threats that are trying to get into that bunker will be unsuccessful in producing the consequences of concern.

CHAIRMAN BROWN: And my argument is that there are some fundamentals that transport into your world as well, like independence of various functional assets, provides a valid, very valid protection against access and control of access, internal and external. Those are the two big ones.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

MR. DOWNS: Sure, absolutely.

CHAIRMAN BROWN: It was mentioned earlier that at your first network, I've forgotten the gentlemen. He's not here now, that talked about the first network was compromised and you got down, you had your second network and then you had your third thing at the device or whatever it is which are all complex intrusion detection programs that has to be maintained, upgraded and everything else which is kind of really kind of building yourself the most complex arrangement you can. It's a little bit different than a defense in depth type --

MR. DOWNS: It's providing defense in depth.

CHAIRMAN BROWN: I understand that, but it's also -- it's not blacksmith technology. It's nightly variable technology that requires upgrading in order to maintain its effectiveness, whereas, in defense in depth, we normally refer to in the reactor plants from the power plant type thing are kind of built in and they are there and they don't change.

MR. DOWNS: Right.

CHAIRMAN BROWN: Anyway, that's the only point of making use. Hopefully, you guys would think

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

about this. These are fundamentals we've emphasized and seems to me they are applicable in some of the development of the way these people apply their logic to their vital digital assets and how they do things. So anyway, that's the last slide, right?

MR. DOWNS: Yes, sir.

CHAIRMAN BROWN: Before we go on to anything else, I think we have NEI would like to make a statement.

MR. ASHKEBOUSSI: Nima --

CHAIRMAN BROWN: Angle it more.

MR. ASHKEBOUSSI: Nima Ashkebousi, Nuclear Energy Institute. So thank you for the opportunity to provide comments on industry's behalf. This was certainly a very comprehensive discussion today, a significant look back at the history of the rulemaking. And we're in alignment with NRC. We understand the cyber security threat. Unless you're living under a rock, you know that this is a real threat and what we're seeking is a rule that is risk informed, performance based, graded and in line with historical regulatory approaches to the framework for protecting special nuclear material and is not overly burdensome to implement. That is what we are seeking here today.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

So I'd just like to hit on five items of interest that we submitted into a letter last week to the subcommittee. The first two items look at high level policy issues regarding the rulemaking, the first being the departure from the historical treatment of special nuclear material as a security threat. So historically, Category 3 material, UF6 and low enriched uranium, has not been considered a sabotage target.

There's a current rulemaking on-going right now with Part 73 that we affirmed this position that LEU and UF6 are not sabotage targets. And this rule is a departure from that in terms that a cyber attack is an adversary tool. It does not make the material more or less attractive. So we see this as a significant policy issue that we see the Commission meeting to weigh in on as this is brought forth to them.

Staff did address it somewhat in the final regulatory basis, but we think that it's not going there and are seeking direct Commission input on this issue.

The second item is related to an existing petition for rulemaking that NEI submitted in 2014. This is a petition on the reactor cyber rule that seeks

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

to align the critical digital assets to the design basis threat. So items directly related to radiological sabotage.

So the staff's regulatory basis is silent on this petition and we want there to be a realization that there is a direct linkage between this existing petition on the reactor side and this current rulemaking on the fuel cycle facility side. It may be different time lines for how they proceed or move forward, if the petition is granted or not granted, but there needs to be a realization that there's issues there existing in that petition that impact this fuel cycle facility rulemaking.

MEMBER STETKAR: Are you saying for these facilities that this rulemaking should be aligned only with the design basis threat for Category 1 facilities?

MR. ASHKEBOUSSI: That is --

MEMBER STETKAR: I'm trying to understand the nexus between what you're saying on the power reactor side and --

MR. ASHKEBOUSSI: Right. So Category 1 facilities are the only ones that implement the DBT. If the petition is granted that only looks at digital assets related to the DBT, transferring that to this

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

rulemaking would only make this rule applicable to Category 1 fuel cycle facilities.

MEMBER STETKAR: At least I understand where you're coming from. Thank you.

MR. ASHKEBOUSSI: That's where we're seeking clarification on.

CHAIRMAN BROWN: Just -- I want to make sure I understand what you all just concluded. If I took the rule as it is presently written, based on what you all just said that consequences 2, 3 -- no, 3 and 4 would disappear, or 2, 3, and 4 would disappear.

MR. ASHKEBOUSSI: Correct.

CHAIRMAN BROWN: You're only going to address Category 1.

MR. ASHKEBOUSSI: What we're saying is that yes, if the Commission makes the determination that yes, the original cyber rule for reactors was only intended to apply to those assets related to the DBT, then we would seek equity between that determination and this rulemaking.

MEMBER STETKAR: I'm going to get into security-related stuff. Does the DBT for Category 1 facilities span the notions of safety that was Category 2, 3, but the --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

MR. DOWNS: The consequences?

MEMBER STETKAR: The consequences.

MR. DOWNS: Three and 4?

MEMBER STETKAR: Three and 4.

MR. DOWNS: No, so that's why at a CAT 1 facility you'd be looking at the consequences of concern of the DBT-1 as well as 3 and 4. It would all be --

CHAIRMAN BROWN: But it would just be Category 1 plants?

MR. DOWNS: That's correct.

MEMBER STETKAR: But the DBT -- I just want to make sure that I understand it, the DBT does not -- does the DBT, design basis threat, address worker safety on offsite public safety?

MR. DOWNS: No.

MEMBER STETKAR: Thank you.

MEMBER MARCH-LEUBA: That was going to be my question to you, but related to this is you are making a blanket statement that in the past we have considered LEU not to be a problem.

The staff is proposing on the side saying, why didn't you evaluate what the consequences to the worker chemical ingestion and see if it can kill

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

somebody and therefore, it is a problem.

MR. ASHKEBOUSSI: So to give you an analogy, so that situation currently exists. Right now you could have an individual take a hammer and destroy and IROC and lead to a consequence of concern. That's not something that the licensees are required to protect under Part 73. It's the CAT 3 licensee.

So you may have the same asset that you require to protect against the cyber attack that you don't require them to protect against someone bashing it in with a hammer. That's the disconnect that we're trying to -- that's a policy issue that we're seeking clarification on.

MEMBER MARCH-LEUBA: I'm going back to the previous example, we aren't protected against meteorite strikes either. We are not perfect.

MR. ASHKEBOUSSI: We're not perfect, but these are assets that were specifically identified to protect against consequences and yet, there's still determination that they're not a sabotage target.

So just to reiterate what the NRC staff presentation said earlier, licensees are already implementing cyber security programs. They've extended significant resources to protect assets, not just for

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

business purposes, but for the DBTs and for the security orders that were issued after 9/11. So there significant work under way that's already been done in this area.

So just to move back to the rule, next item for clarity that we're seeking is the scope of streaming of the digital assets. So I heard some positive statements today, but based on the last version of the draft reg. guide we saw is that it's an excessively burdensome process to go through all digital assets to make the determination of what's vital and what's not vital. So we seek clarity as the rule moves forward in that regard, especially when you look at some Category 1 facilities having up to 13,000 digital assets that are associated with a consequence.

That can be an excessively burdensome process. The end results, we see no VDAs or a very small handful of VDAs or starting from this very broad scope, getting to a very, very small number, the process outlined right now seems excessively burdensome.

So the next item is in regards to unclassified accredited systems. So staff has excluded the accredited classified systems by another federal agency from this rule and we're seeking for them to

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

make the finding that accredited, unclassified systems should also be scoped out of this rule. Those licensees with a CAT 1 facility that implement those DOE, your NNSA, naval reactor programs, protect those unclassified network systems at the same levels that they do with the classified side. We're using the same NIST standards.

So we know that staff is working with naval reactors in NNSA to reach to this conclusion, but that will have a significant impact on those licensees. We may reach the situation where without that they could have up to 800 vital digital assets if unclassified accredited systems are scoped out, we expect to reach zero for some of those licensees.

MEMBER STETKAR: But just to make sure from the staff, we heard what seems like days ago, but this morning that that's still in play. Is that correct?

MR. DOWNS: That's correct. That's currently being evaluated.

CHAIRMAN BROWN: In other words, what he just asked for, it's unaccredited, unclassified systems that's scoped out also.

MR. DOWNS: Well, not the way the rule is right now.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

CHAIRMAN BROWN: Right now, but is that still on the table?

MR. DOWNS: It's still under consideration, absolutely. And it's just a time issue as to whether or not we're going to be able to complete that evaluation prior to the milestones that the SECY has established.

CHAIRMAN BROWN: But is it important to complete that?

MR. DOWNS: Well, what it will do is it will have a tremendous bearing on the cost effectiveness associated with the rule. So in our regulatory analysis document, right now we would consider those assets to be scoped in. There will be costs associated with that and we would present it as such.

CHAIRMAN BROWN: It would be a positive thing if it got cheaper, right?

MR. DOWNS: No question about it, yes.

MR. DEUCHER: One of the challenges just to add is we are waiting for draft guidance and requirements that DOE, NNSA, and naval reactors are in the process of developing. And one of the concerns is what that schedule is currently shaping up to be and it

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

may very well be outside of the scope of the rulemaking schedule that we're currently on.

MR. ASHKEBOUSSI: It's important for us to see that result sooner than later and ideally before the SECY goes up to the Commission.

MR. DOWNS: We agree.

MR. ASHKEBOUSSI: Time might be tight to do that, but that's ideal for all that. The Commission will see the --

MR. DOWNS: We are working towards that.

CHAIRMAN BROWN: It seems incongruous to say we don't have enough time to make it less expensive and less onerous.

MR. DOWNS: So the Commission has directed a high priority expedited rule.

CHAIRMAN BROWN: I understand we're going it as bad as we can and as hard as we can because we have got a priority designation.

MR. DOWNS: And remember, this is just a proposed rule phase, so obviously if this were to go forward without this exclusion, the NRC could expect a formal comment based on this which would have to be considered and further evaluated which would allot more time. That would be the worst case scenario.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

CHAIRMAN BROWN: All right. Go ahead, finish.

MR. ASHKEBOUSSI: It's important for us to get that resolved also to avoid dual regulation between two agencies over the same system.

The last point I want to make is the need to have a pathway for licenses with no vital digital assets. As this rulemaking has progressed and if we reach the resolution of the unclassified accredited system, we expect licensees, many licensees to have no vital digital assets. And the way the rule is laid out right now, they first have to create this cyber security plan, then create the cyber security team, then start the analysis to determine if there's vital digital assets or not. And that's a very costly process to create that plan and set up that team.

We've provided some of those cost estimates in a letter to NRC. So we are seeking a way to have licensees do the analysis up front to reach the conclusions if there are vital assets or non-vital assets and then proceed with the development of a plan for the cyber security team. Creation of those teams, training, set up, doing the documentation of the plan is an extensive expense in light of no vital digital

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

asset.

The last comment I wanted to make since it was brought up by committee members is some of the industry cost estimates. We base those cost estimates of a reading of the draft regulatory guide and the draft rule and like some of you, we thought it was excessively prescriptive and potentially hard and excessively burdensome to implement in certain areas. So we stand by our estimates, based on Category 1, licensees already have an understanding of what it takes to implement cyber security programs under other government agencies and what it takes in general when applying for new NRC programs. So we provided that to staff for their information as they moved forward on the reg. basis.

I know the question of air gap systems came up. Several licensees' systems are already air gapped and just as an example of excessive costs, there should be an easier way for a licensee that has an air gap system to satisfy the requirements of the rule other than going through all of the control tests and documenting. I think that there's probably an easier path forward. So thank you for the opportunity to provide comments.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

NRC staff has gone above and beyond their -
- the minimum requirements for this rulemaking and I think that every meeting that we've had with them has led to a better product and we look forward to continue working with them as the rule progresses. Thank you.

MEMBER MARCH-LEUBA: You mentioned air gaps, what percentage of the licensees have air gaps?

MR. ASHKEBOUSSI: I --

MEMBER MARCH-LEUBA: It's 1 or it's 90 percent?

MR. ASHKEBOUSSI: I believe it's at least 50 percent. I don't have an exact number.

MEMBER MARCH-LEUBA: This is obviously our preferred implementation method, right?

MR. ASHKEBOUSSI: It may be more than that. I don't have a direct --

MEMBER MARCH-LEUBA: The rule should encourage that implementation. When people do the good thing, you should reward them.

MR. ASHKEBOUSSI: So all of the Category 1 facilities have air gaps and that's three right there. And I'm sure that almost all of the CAT 3s have at least some portions of their systems air gaps.

CHAIRMAN BROWN: Around the table --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

MEMBER STETKAR: Usually ask for public comments first.

CHAIRMAN BROWN: That's where I was going.

Myron, do you have any other comments? Is there anybody out there? Is there anybody in the audience that would like to make any public comments? I'm hearing none. Is the phone line open?

Is there anybody out there on the phone line listening in? If so, would you please say something to let us know that you're there?

MR. KENT: Yes, I can hear you guys. This is Aaron Kent with MOX services.

CHAIRMAN BROWN: Okay, do you have any comments?

MR. KENT: I would like to say thank you to you guys. I sat in all day and I think this was a very, very useful meeting. It makes a lot of the hard work that everybody has put into it feel like it was good work and good effort. So thank you for that.

CHAIRMAN BROWN: Thank you. Is there anyone else on the line?

MR. BURKSDALE: Yes, this is Michael Burksdale. I kind of want to reiterate exactly what Aaron said. This has gotten better every time we've

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

had a meeting and seems to be going in the right path and I really appreciate all of the effort and some of the guys, especially James Downs and crew in trying to help us get to a better state. This has been a very, very good conversation.

The only one thing I would like to add is just around the cyber security staff, I know that there were some comments made earlier about what those individuals may or may not do, part time, full time, volunteers, they could be fire brigade. They could be something else. Do you seriously really think into that in what you're stating because when you start talking about cyber security staff and you start talking about Tier 1, Tier 2 analysts, security operation centers and the actual expertise at a level of technical expertise in order to pull off these capabilities, it's not going to be something that you're going to go and grab someone like at the volunteer fire department when you need them. When you're talking about this kind of monitoring and this kind of threat vectors and the things that we're looking for this is really, really in-depth stuff and it's the things that people spend a lot of time trying to research and keep on the current technologies.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

So let's not -- I wouldn't say that the cyber security staff will be someone that's exactly what I would say could be borrowed when needed and I will say it's a lot of time getting the staff that we do have. We pretty much max them out all the time because that's how we run a business efficiently. So I just want to kind of reiterate that because that's kind of important in relation to the conversation today.

And again, thank you all. I really appreciate it. It's a good, good topic.

CHAIRMAN BROWN: Thank you. Is there anyone else on the line? Hearing no response, we'll close the line.

And with a deep breath, we'll go around the table here and if there's any observations, I'll start with Matt.

MEMBER SUNSERI: Thanks, Charlie. The only comment I have is I've heard a couple of times that says we're under a time -- I'm going to say demand because we have an expedited rule. I would just suggest where I come from, the background I have, we never let time pressure overcome quality. So let's make sure we produce a quality rule and recognize that there's a time frame, but we shouldn't let the time

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

pressure not allow us to produce a quality rule. Thank you.

MEMBER CHU: Thank you for the presentations. This is the first time I have ever attended a cyber security presentation.

I have a couple of comments or questions. The first one is I thought I heard somebody say earlier from the staff, say you guys are going to be preparing a regulatory analysis document? Okay. The reason I ask that is just because I think it's a very complicated rule. There are a lot of requirements. So I'm very curious to see what the regulatory analysis document says because usually for a new rule, they look at options they have looked at, the cost benefit. So I'm just curious to see why you pick what you pick. It's a very complicated rule.

The second comment may be baseless. I don't know. A key element of your rule is you identify each vital digital asset and then you identify potential sources of cyber attacks. You call cyber attacks vectors, right? And then you put in controls to provide protection. I understand the logic. But I was thinking, you know, with the cyber attack people getting so good and so innovative and creative and then

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

I was thinking in the next few years whether your controls will be enough to keep up with the new kinds of cyber attacks down the road. But there are technologies advancing very quickly. So that's just sort of comment.

CHAIRMAN BROWN: Dana. Margaret, you're done. I'm sorry. Okay. Dana?

MEMBER POWERS: No comments.

CHAIRMAN BROWN: John?

MEMBER STETKAR: No comment. Thanks for a good discussion, comprehensive. The only question I have for the subcommittee is one of what should we as a subcommittee recommend in terms of bringing this issue to the full committee and what's the appropriate timing for that?

I mean we've had a good discussion today. We know that the regulatory analysis is in progress. There's been some discussion of enhancing the guidance perhaps with additional examples and things like that.

I honestly don't know what is the most appropriate time for the full committee to weigh in on this. Should the full committee weigh in before the March submittal date to the EDO of the package or -- that would give the committee the opportunity to

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

formally recommend in a timely fashion to the Commission anything that the committee decides to highlight which would be timely. Or should the committee wait until the Commission looks at the package and in principle agrees that it should be submitted for public comments?

I honestly don't know. I mean my general preference personally is on something like this to get the committee involved earlier than later, especially if the committee has something that they feel is of significance that the Commission should consider during their deliberations, but that means that we face some logistics in terms of working with the staff to make that happen in a timely manner before middle March.

CHAIRMAN BROWN: We would have to have a full committee meeting. It would have to be presented at the February --

MEMBER STETKAR: We'd most likely need another subcommittee meeting to delve into details before that.

CHAIRMAN BROWN: It would have to be in January which would assume that maybe we have the regulatory analysis available.

MEMBER STETKAR: We don't need to do the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

planning, but I think that we as a subcommittee before our full committee P&P need to --

CHAIRMAN BROWN: This week.

MEMBER STETKAR: That would be by Friday of this week, recommend some sort of decision.

CHAIRMAN BROWN: I agree with you.

MEMBER STETKAR: I don't think we need to make that decision right now unless we want to.

CHAIRMAN BROWN: Well, if we're going to talk about it Friday, I guess when P&P is, then we've got to have some concept or at least idea -- the one document we haven't seen is the regulatory analysis which contains, I guess, a fair amount of the detail for making a judgment as to how deeply we want to go, the justifications, etcetera.

Trying to get it in February for a full committee meeting, that would presume that we'd need a subcommittee meeting in late January which right now there are none on the schedule, so the schedule is open in order to be able to do it that I don't know what the status again, of the regulatory analysis is, whether is it done, almost done?

MR. DOWNS: It's nearing the beginning of the concurrence process.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

MEMBER STETKAR: Say that again?

MR. DOWNS: The plan is, here's the plan, the plan is to get it into concurrence actually starting next week and by in the concurrence, the package has to be processed into ADAMS and all this with the administrative review. The time frame for office director concurrence would be early December, I believe. I'd have to look at the schedule, but that's kind of the key date.

Once it goes to the office directors, office concurrence process, obtain OGCNLO. That may be of more value. So OGCNLO would be -- is anticipated in late January which the office concurrence process would go mid-December time frame.

So by the end of December we expect to have office concurrence. At that point we'll go to OGC for their review for no legal objection. At that point, that would be -- I would be confident that there are not going to be any more changes.

CHAIRMAN BROWN: In late December.

MR. DOWNS: Well, I would say after OGC to be completely honest. So mid-January.

CHAIRMAN BROWN: Okay, OGC is going to be in early January or late December?

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

MR. DOWNS: Early, mid-January would be OGC. It just depends on how quickly the package goes through the process.

CHAIRMAN BROWN: Late January we could do a subcommittee meeting -- it would be late January, third week or something like that.

MEMBER STETKAR: We don't need to do the actual details of the planning right now. We do need to have some recommendation for the full committee to consider. Not necessarily on schedule dates.

CHAIRMAN BROWN: No, I understand that.

MEMBER STETKAR: Bigger picture is --

CHAIRMAN BROWN: The picture is --

MEMBER STETKAR: -- basically is the full committee going to weigh in --

CHAIRMAN BROWN: -- before it goes to the EDO the first time.

MEMBER STETKAR: Right. Or are we going to wait until --

CHAIRMAN BROWN: Well, we can discuss it this week and find out what we -- see what the full committee thinks they want to do and then we'll let -- work with the staff to see where we go.

MEMBER STETKAR: Other than that, I'm done.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

CHAIRMAN BROWN: Right now, the plan was to have full committee and then have a report in December, beginning, but that seems to me --

MEMBER STETKAR: My opinion is that's premature.

CHAIRMAN BROWN: Premature, given what we've heard today.

MEMBER STETKAR: The only question is --

CHAIRMAN BROWN: -- critical changes that could come out.

MEMBER STETKAR: I think a December -- I don't know what the committee could say in December that might not still be somewhat in a state of flux. In other words, so sending something to the EDO in December on something that's still in motion doesn't sound like a very productive use of our time or the staff's time because you have to respond to ACRS letters and all that kind of thing. So in my opinion it would be does the committee decide that we want to weigh in in a timely manner for that mid-January sort of deadline or not.

CHAIRMAN BROWN: That's 7 February. We've got a topical report. That's a planning issue. We can talk about that tomorrow, I mean Friday. Or whatever

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

it is, P&P, about the general schedule.

Jose?

MEMBER STETKAR: It is relevant, by the way though because if we're not going to have a committee brief, full committee briefing in December, we absolutely need to make that decision in our planning meeting this Friday, because the Federal Register notice is on agendas for our full committee meeting. So that's why I brought it up.

CHAIRMAN BROWN: That's one on my mind as well. It's a matter of what we do. So if we can make a decision on it Friday, P&P, then we have enough time to inform the staff. I agree with you. I just think it's premature right now based on the flux and the changes and things like that that you all are still evaluating. If you've got a draft version of the regulatory analysis, even as it goes to OGC --

MEMBER STETKAR: I wouldn't --

CHAIRMAN BROWN: I'm just some -- later.

MEMBER STETKAR: I don't care about OGC as -- well. You know.

(Laughter.)

MEMBER STETKAR: But in a sense, as long as you have -- that you're reasonably well advanced on

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

technical concurrence from the various offices, that's the important point. And I have no idea where the offices are on this point.

CHAIRMAN BROWN: We'll have to figure that out tomorrow.

MEMBER MARCH-LEUBA: So let me finish and get the microphone from John. I wanted to thank you guys. You have done an excellent job and I feel a lot better now than I felt at 8 a.m. this morning after -- when I received the 170 pages, I was convinced it was just cut and paste from other guidance and nothing really -- there's a lot of thought that has gone into this.

One positive thing I come up with is what we just heard that over half of the I&Cs actually have air gaps on their systems. That is the best way to address a network intrusion is not having a network. And that has to be rewarded. Whenever kids behave properly, you give them Halloween candy. So please make sure that you review the language of the rule and the language of the guide so that that is not only allowed, but encouraged. It is the best thing we can do is to have an air gap.

So with that concept another request,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

again, is a member of the -- in the regulatory language, we have this loss of nuclear material control and accounting.

CHAIRMAN BROWN: What was that again?

MEMBER MARCH-LEUBA: Loss of nuclear material control and accounting. I think compromise is a word that reflects more what we're thinking. And it forces the licensee to think more broadly than just losing the ability of controlling, but compromising what databases you have in the past. Other than that, excellent job.

CHAIRMAN BROWN: Okay, I have no other -- I forgot I turned it off. You told me to. You're giving me my direction here.

MEMBER STETKAR: For the record, I'm the official microphone holder.

(Laughter.)

CHAIRMAN BROWN: He's been watching green lights all the time. I'm not going to amplify. I've said all I'm going to say. You heard most of my comments.

I do agree with Jose as we've made the emphasis on the air gaps and types of ways to -- whatever we reward, that's a good thing for those

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

already there, but I would have even wanted to encourage, not mandate, but encourage defensive measures that reduce the opportunity for folks to create problems. That's the idea. And then let the licensees do what they want, but understand that that makes it simpler for them if they do something that is more defensive and there's other aspects of the air gap thing. It's not just one. It's multiple air gaps in isolation of functional systems.

I guess our conclusion, we haven't got the full committee to agree yet. We will talk this out during our planning efforts later this week.

MEMBER STETKAR: You may want to show up for our planning and procedures discussion. It will -- I don't have our agenda in front of me, but it's -- it will be on Friday. It's usually first thing in the morning, but Christina, do you have it? Check with Christina. It's typically our first thing on Friday morning.

MS. ANTONESCU: I'll let you know.

MEMBER STETKAR: And you may want to be there in case something comes up during the discussion.

CHAIRMAN BROWN: Yes, you might have the information. We are uncomfortable with trying to write

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

a report right now based on the way the discussion went today. It's kind of a --

MR. DOWNS: Too much in flux.

CHAIRMAN BROWN: Too much in flux. And if you come to listen to us, we will possibly like to know how this impacts our ability to get another subcommittee and full committee meeting. And I don't want to discuss it now, but you all have got your schedule and you have to provide some information or insight as to the impact on you and that which may impact how we make our decision.

MR. DOWNS: I plan on being there Friday. I appreciate it.

CHAIRMAN BROWN: And Christina will tell you when. Other than that, there's no other comments.

The meeting is adjourned. Thank you, all. Good program.

(Whereupon, the above-entitled matter went off the record at 5:32 p.m.)

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

Fuel Cycle Cyber Security Rulemaking

ACRS DI&C Subcommittee Briefing

November 2, 2016

Agenda

- Overview of fuel cycle facility licensees
- History of fuel cycle cyber security
- Overview of draft proposed rule language
- Overview of draft regulatory guide

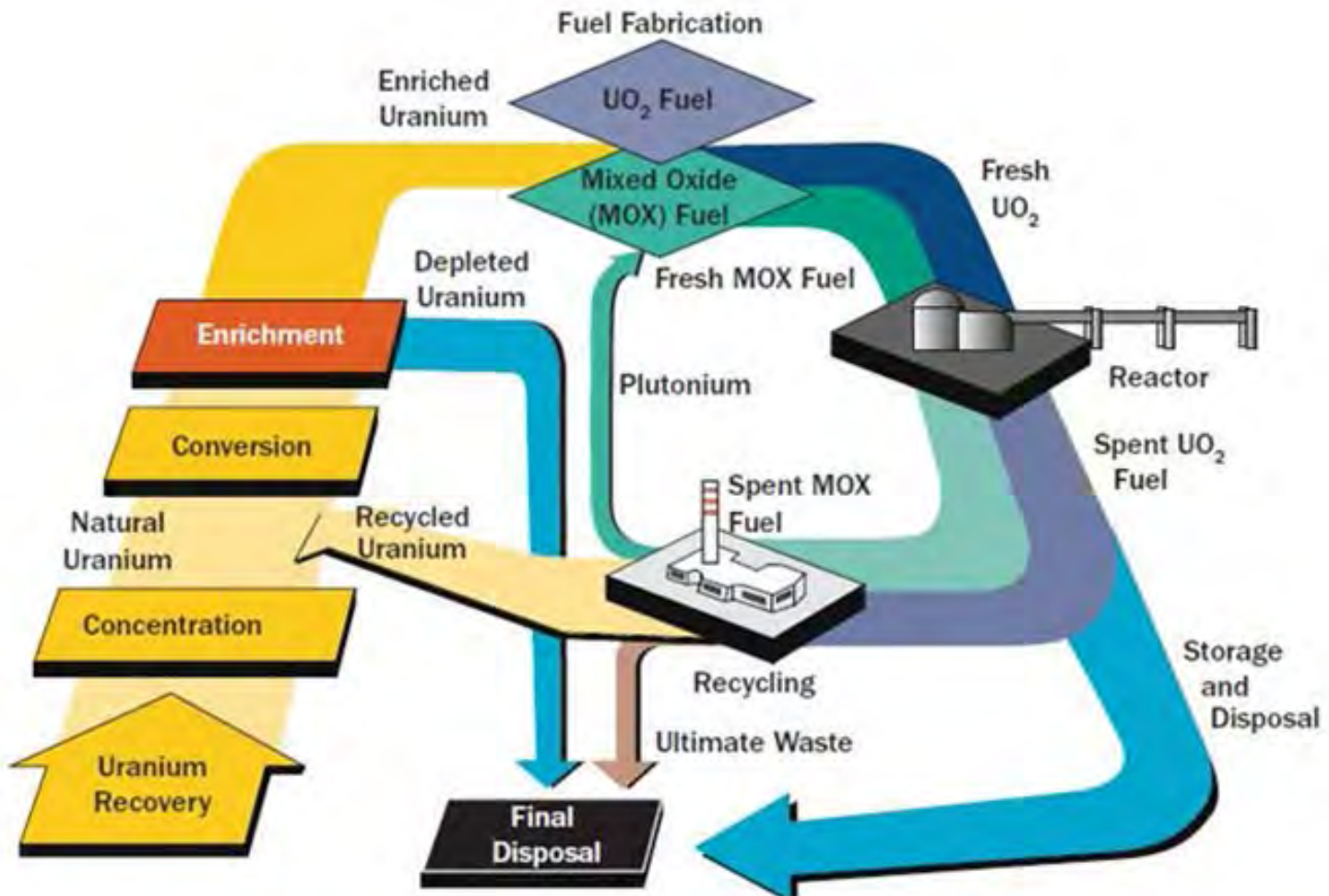
Acronyms used in this presentation

- 10 CFR: Title 10 of the *Code of Federal Regulations*
- IROFS: item relied upon for safety
- MOX: mixed oxide
- NRC: U.S. Nuclear Regulatory Commission
- SNM: special nuclear material
- SSNM: strategic special nuclear material

Overview of fuel cycle facility licensees

- Facility types
- Process fundamentals
 - Conversion
 - Enrichment
 - Fuel fabrication
 - Deconversion
- Regulatory framework
 - Safety
 - Physical security
 - Material control and accounting
 - Safeguarding classified information and matter

Overview of fuel cycle facility licensees – facility types



Overview of fuel cycle facility licensees – facility types (continued)

Licensee/License Applicant	Material Present	Location
Uranium Conversion		
Honeywell International	source material (Part 40)	Metropolis, IL
Uranium Enrichment – Gas Centrifuge		
Eagle Rock Enrichment Facility	SNM (Category III), classified information/matter	Idaho Falls, ID
URENCO USA Facility (LES)	SNM (Category III), classified information/matter	Eunice, NM
American Centrifuge Plant	SNM (Category III), classified information/matter	Piketon, OH
Uranium Enrichment – Laser Separation		
Global Laser Enrichment Facility	SNM (Category III), classified information/matter	Wilmington, NC

SNM = special nuclear material

Overview of fuel cycle facility licensees – facility types (continued)

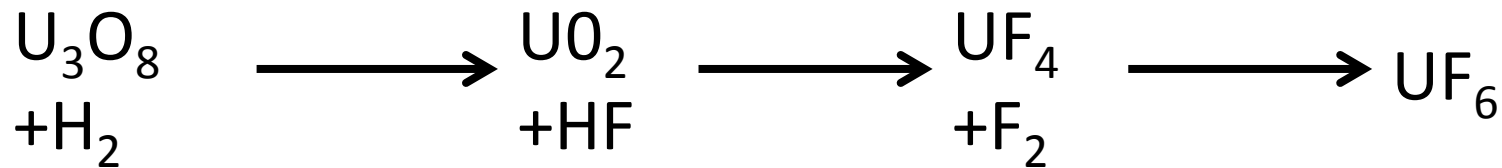
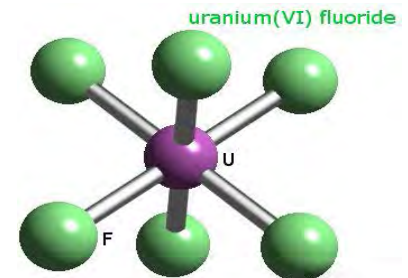
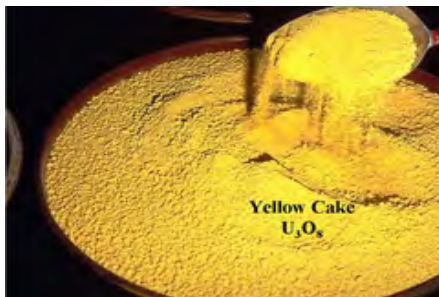
Licensee/License Applicant	Material Present	Location
Fuel Fabrication – Commercial Use		
AREVA	SNM (Category III)	Richland, WA
Global Nuclear Fuels-Americas	SNM (Category III)	Wilmington, NC
Westinghouse	SNM (Category III)	Columbia, SC
Fuel Fabrication – Nuclear Navy & Research Reactors		
BWXT	SSNM (Category I), classified information/matter	Lynchburg, VA
Nuclear Fuel Services	SSNM (Category I), classified information/matter	Erwin, TN
Fuel Fabrication – Mixed Oxide		
Shaw AREVA MOX Services	SSNM (Category I), classified information/matter	Aiken, SC
Depleted Uranium Deconversion		
International Isotopes	source material (Part 40)	Lea County, NM

SSNM = strategic special nuclear material

Overview of fuel cycle facility licensees – process fundamentals

Uranium Conversion

40.31-82 Application for specific licenses



Overview of fuel cycle facility licensees – process fundamentals (continued)

Uranium Enrichment

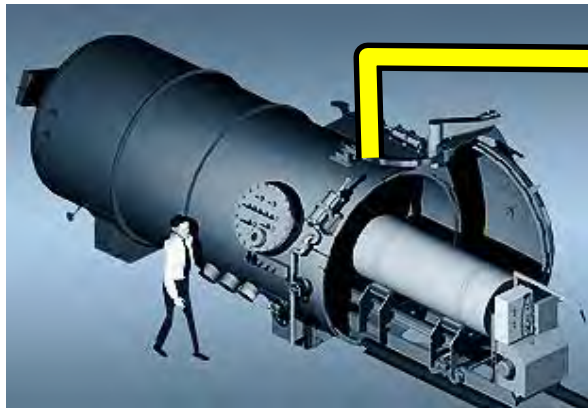
Source Material

Enrichment

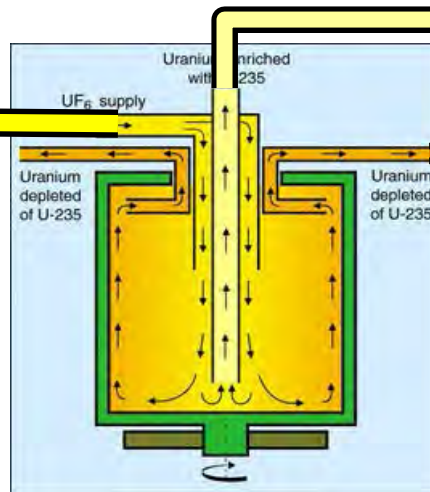
Source Material

Special Nuclear Material

Gas Centrifuge



UF_6
Natural



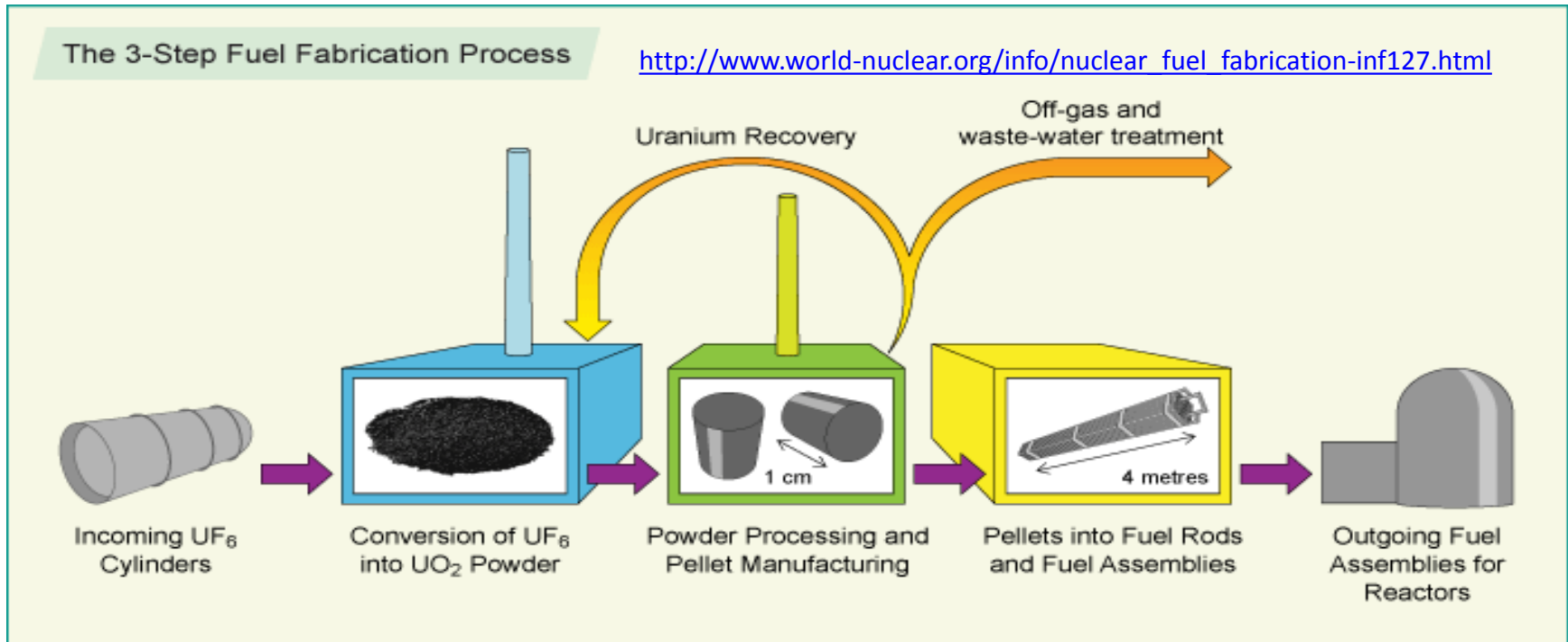
UF_6
Depleted



UF_6
Enriched

Overview of fuel cycle facility licensees – process fundamentals (continued)

Fuel Fabrication – Commercial Use



Enriched UO₂
Natural or Depleted UO₂



Overview of fuel cycle facility licensees – process fundamentals (continued)

Fuel Fabrication – Nuclear Navy and Research Reactors

- High enrichment fuel that typically involves > 90 wt % ^{235}U
- No current NRC licensed enrichment program for producing highly enriched uranium

Fuel Fabrication – Mixed Oxide

- Input: surplus weapon-grade plutonium and uranium oxide
- Processes: dissolution, purification, conversion, powder blending, pellet production, rod production, assembly, various support systems
- Product: MOX fuel pellets in power reactor fuel assemblies

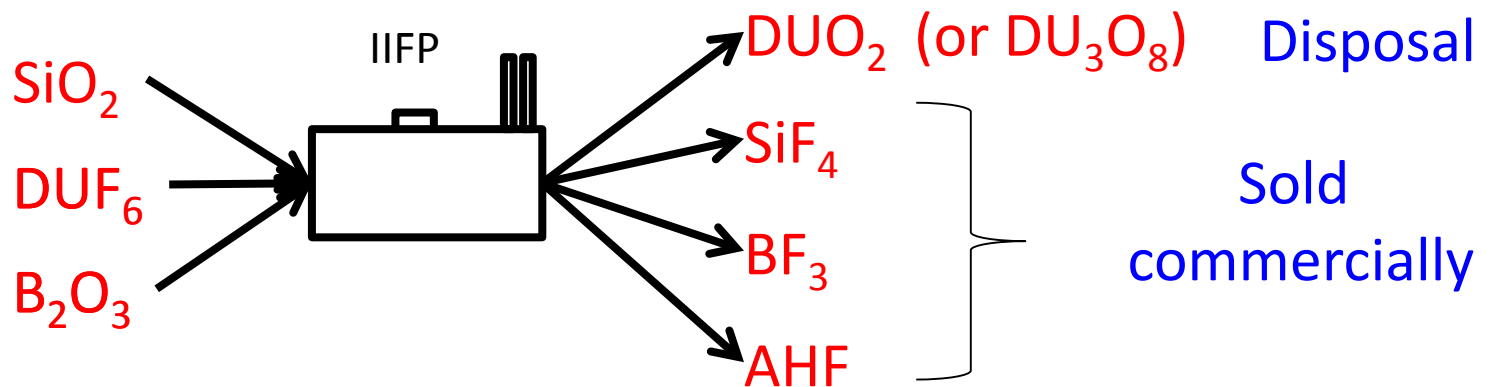
Overview of fuel cycle facility licensees – process fundamentals (continued)

Depleted Uranium Deconversion

Receive: DUF6 from enrichment facilities



Processing: Chemical Deconversion of DUF6



Overview of fuel cycle facility licensees – regulatory framework

Diverse facility types, processes, and safety/security considerations require a regulatory framework that is very different from nuclear power reactors.

- 10 CFR Part 40 (safety)
 - Conversion
 - Deconversion
- 10 CFR Part 70 (safety)
 - Enrichment
 - Fuel Fabrication
- 10 CFR Part 73 & security orders (physical security)
- 10 CFR Part 74 (material control and accounting)
- 10 CFR Part 95 (safeguarding classified information/matter)

Overview of fuel cycle facility licensees – regulatory framework (safety)

10 CFR 70.61

- Specific thresholds for:
 - High consequence events
 - Intermediate consequence events
- Limit risk of nuclear criticality
- Designate engineered or administrative items relied on for safety (IROFS)

Overview of Integrated Safety Analyses

- Licensee provides methodology to consider accident sequences (threshold, event frequency, and IROFS effectiveness)
- Does not consider a malicious actor
- NRC review of digital instrumentation and control is risk-informed
- Most licensees have some digital IROFS but alternate means to prevent consequence may also exist

Overview of fuel cycle facility licensees – regulatory framework (safety) (continued)

70.61 Performance Requirements	Highly Unlikely	Unlikely	Not Unlikely
High Consequence Publ Dose > 25 rem Worker Dose > 100 rem Publ U intake > 30 mg Publ Chem: Irreversible+LongLasting Worker Chem : Endanger life	Acceptable	Not Acceptable	Not Acceptable
Intermediate Consequence Publ Dose 5 - 25 rem Worker Dose 25 - 100 rem Publ Chem: Mild Transient effects Worker Chem:Irrever+LongLasting Env releases > 5000 Tbl 2 10CFR 20	Acceptable	Acceptable	Not Acceptable
Low Consequence Publ Dose < 5 rem Worker Dose < 25 rem	Acceptable	Acceptable	Acceptable
Under normal and abnormal conditions: Nuclear process must remain subcritical			

Overview of fuel cycle facility licensees – regulatory framework (physical security)

- Interim Compensatory Measure Orders: Contain additional physical security requirements beyond existing regulations
 - one provision to address cyber vulnerabilities
 - applicable to all fuel cycle facility licensees and UF₆ conversion/deconversion facilities
- Regulations applicable to Category I fuel cycle licensees
 - 73.1: Contains the design basis threats
(includes cyber attack)
 - 73.20: High assurance performance objective and requirements
(physical protection systems to protect against the design basis threats)
 - 73.45: Performance capabilities of physical protection systems
 - 73.46: Physical protection systems, components, and procedures
- Regulations applicable to Category II and III fuel cycle licensees
 - 73.67: Performance objectives and requirements
(physical protection systems to protect SNM of low and moderate strategic significance)

Overview of fuel cycle facility licensees – regulatory framework (material control and accounting)

- 74.41: Material control and accounting for SNM of moderate strategic significance
 - applicable to Category II fuel cycle facility licensees
- 74.51: Material control and accounting for formula quantities of SSNM
 - applicable to Category I fuel cycle facility licensees
- Performance objectives pertaining to:
 - SNM losses
 - ongoing confirmation of quantities and locations of SNM

- 10 CFR Part 95, “Facility security clearance and safeguarding of national security information and restricted data”
 - applicable to all fuel cycle facility licensees with access to classified information or matter
- 95.29, “Establishment of restricted or closed areas”
 - physical security measures to prevent unauthorized access and removal of classified information or matter

History of fuel cycle cyber security

- Current cyber security requirements for fuel cycle facilities – security orders
- NRC Cyber Security Roadmap (SECY-12-0088)
- Cyber Security for Fuel Cycle Facilities (SECY-14-0147)
- Staff Requirements Memorandum to SECY-14-0147
- Regulatory basis for rulemaking
- Rulemaking schedule

History of fuel cycle cyber security – current requirements for fuel cycle facilities

- Currently no cyber security regulations are codified in 10 CFR for fuel cycle facility licensees
- Interim Compensatory Measure orders (issued in the 2002/2003 timeframe) instructed fuel cycle facility licensees to evaluate computer and communications networks for vulnerabilities, related to emergency response and offsite personnel, and address as necessary
- 10 CFR Part 73 was revised in 2007 to explicitly include cyber attacks in the design basis threat (applicable only to Category I fuel cycle facility licensees) but did not establish specific security requirements for protecting against cyber attacks or establishing a formal cyber security program
- Fuel cycle facility licensees have implemented some voluntary measures for both business and safety considerations

History of fuel cycle cyber security – NRC Cyber Security Roadmap (SECY-12-0088)

- Established the approach for evaluating the need for cyber security requirements for four categories of NRC licensees and facilities:
 - fuel cycle facilities
 - non-power reactors
 - independent spent fuel storage installations
 - byproduct materials licensees
- Recommended a graded approach to developing cyber security requirements commensurate with the inherent nuclear safety and security risks associated with the different types of licensees and facilities

History of fuel cycle cyber security – Cyber Security for Fuel Cycle Facilities (SECY-14-0147)

- Stated that cyber security requirements for fuel cycle facility licensees need to be enhanced because of an increasing and persistent cyber security threat, the potential exploitation of vulnerabilities through attack vectors, the inherent difficulty of detecting the compromise of digital assets, and the potential consequences associated with a cyber attack
- Concluded that if compromised by a cyber attack, the availability and reliability of safety, security, emergency preparedness, and material control and accounting functions required by NRC regulations could be adversely impacted in a manner undetectable until the function fails to perform when needed
- Provided the following three options for Commission consideration:
 - issuance of a facility-type security order to fuel cycle facility licensees followed by a rulemaking (NRC staff-recommended option),
 - a rulemaking, or
 - no action

History of fuel cycle cyber security – SRM to SECY-14-0147

- The Commission directed the NRC staff to proceed directly with a cyber security rulemaking designated as a high priority and that the final rule should be completed and implemented in an expeditious manner
- The staff should augment the work performed to date to develop a more fulsome technical basis for a proposed rulemaking and interact with the stakeholders in developing the proposed and final rule
- The technical basis should address the need to integrate the regulatory consideration of safety and security and the necessity to apply a disciplined, graded approach to the identification of digital assets and a graded, consequence-based approach to their protection

History of fuel cycle cyber security – regulatory basis for rulemaking

- NRC staff conducted extensive interactions with stakeholders on the development of the draft regulatory basis and final regulatory basis (e.g., formal comment resolution, site visits, and five public meetings)
- In March 2016, the NRC staff completed the final regulatory basis for cyber security at fuel cycle facilities
 - Set forth a rulemaking for fuel cycle facility licensees to establish appropriate levels of protection against cyber attacks that could result in a consequence of concern based on the facility type (i.e., Category I, II, III, or 10 CFR Part 40 conversion/deconversion facilities)
 - Recommended a graded, risk-informed, performance-based approach for the rulemaking to develop appropriate cyber security requirements for fuel cycle facility licensees

History of fuel cycle cyber security – rulemaking schedule

OBJECTIVES	TARGET DATES	SECY DATES
Complete the regulatory basis	03/22/16 ACCOMPLISHED	03/24/16
Proposed rule package to the NRC Office of the Executive Director of Operations	03/15/17	03/17/17
Final rule package to the NRC Office of the Executive Director of Operations	02/01/18	06/11/18

History of fuel cycle cyber security – NRC program development

- Regulatory Guide (currently in draft)
 - An acceptable methodology for fuel cycle facility licensees to satisfy regulatory requirements
- Interim Staff Guidance (not yet developed)
 - Acceptance criteria for NRC staff to review the cyber security plan
- Inspection Procedure (not yet developed)
 - Objectives for NRC inspectors to evaluate implementation of the cyber security plan

Overview of Draft Proposed Rule Language

- Establishes a performance-based regulatory framework for protecting against cyber attacks at fuel cycle facilities
- Scope is limited:
 - active or latent consequences of concern
 - specific, risk-informed thresholds
 - controls needed only for vital digital assets
- Incorporates stakeholder feedback on the scope and methodology for implementing the proposed rule

Overview of Draft Proposed Rule Language (continued)

- a) Applicability
- b) Cyber security program performance objectives
- c) Consequences of concern
- d) Cyber security program
- e) Cyber security plan
- f) Configuration management
- g) Biennial review of the cyber security program
- h) Event reporting and tracking
- i) Records

(a) Applicability

- Fuel cycle facility applicants and licensees – conversion, deconversion, enrichment, and fuel fabrication
- Date to submit cyber security plan as a license amendment request (e.g., 6 months after final rule)
- NRC reviews and approves cyber security plan (5 months is standard review time)
- Implementation of cyber security plan – phased approach under consideration:
 - Vital digital assets identified (e.g., 6 months after NRC approves cyber security plan)
 - Full implementation (e.g., 18 months after NRC approves cyber security plan)

(b) Cyber security program performance objectives

- Detect cyber attacks capable of causing a consequence of concern
- Protect against cyber attacks capable of causing a consequence of concern
- Respond to cyber attacks capable of causing a consequence of concern

(c) Consequences of concern

- Four types of consequences of concern
 - Latent - design basis threat (applies only to Category I facilities)
 - Latent - safeguards (applies only to Category II facilities)
 - Active - safety (applies to all facilities)
 - Latent - safety and security (applies to all facilities)
- Intent is to prevent a cyber attack that:
 - directly results in a safety consequence of concern (active); or
 - compromises a function needed to prevent a safety/security/safeguards/design basis threat event associated with a consequence of concern (latent)
- Consequence thresholds informed by existing regulatory requirements

(c) Consequences of concern (continued)

LATENT – DESIGN BASIS THREAT

The compromise, as a result of a cyber attack at a licensee authorized to possess or use a formula quantity of strategic special nuclear material, of a function needed to prevent one or more of the following:

- | | |
|---|------------------------------|
| • Radiological sabotage; | 10 CFR 73.1(a)(1) |
| • Theft or diversion of formula quantities of strategic special nuclear material; or | 10 CFR 73.1(a)(2) |
| • Loss of nuclear material control and accounting for strategic special nuclear material. | 10 CFR 73.20
10 CFR 74.51 |

LATENT – SAFEGUARDS

The compromise, as a result of a cyber attack at a licensee authorized to possess or use special nuclear material of moderate strategic significance, of a function needed to prevent one or more of the following:

- | | |
|--|--------------|
| • Unauthorized removal of special nuclear material of moderate strategic significance; or | 10 CFR 73.67 |
| • Loss of nuclear material control and accounting for special nuclear material of moderate strategic significance. | 10 CFR 74.41 |

ACTIVE – SAFETY

One or more of the following that directly results from a cyber attack:

- | | |
|--|------------------------------|
| • Radiological exposure of 25 rem or greater for any individual; | 10 CFR 70.61 |
| • 30 mg or greater intake of uranium in soluble form for any individual outside the controlled area; or | 10 CFR 70.62 |
| • An acute chemical exposure that could lead to irreversible or other serious, long lasting health effects for any individual. | 10 CFR 40.31
10 CFR 70.22 |

LATENT – SAFETY AND SECURITY

The compromise, as a result of a cyber attack, of a function needed to prevent:

- | | |
|---|------------------------------|
| • Radiological exposure of 25 rem or greater for any individual; | 10 CFR 70.61 |
| • 30 mg or greater intake of uranium in soluble form for any individual outside the controlled area; | 10 CFR 70.62 |
| • An acute chemical exposure that could lead to irreversible or other serious, long lasting health effects for any individual; or | 10 CFR 40.31
10 CFR 70.22 |
| • Loss or unauthorized disclosure of classified information or classified matter. | 10 CFR Part 95 |

(d) Cyber security program

- (1) Establish a Cyber Security Team
 - Management structure
 - Adequately staffed, trained, qualified, and equipped
- (2) Establish and maintain a set of cyber security controls for each applicable type of consequence of concern
 - Controls are unique by facility type
 - Controls provide performance specifications

(d) Cyber security program (continued)

- (3) Identify digital assets and support systems that could result in a consequence of concern, if compromised
 - Intent is to document these digital assets
 - Digital assets that are part of a classified system accredited/authorized by another federal agency are excluded (existing protection)
- (4) Determine vital digital assets
 - Digital asset performing a function for which an alternate means can be credited is not designated as vital
 - Alternate means must be protected from a cyber attack
 - Terminology intentionally different from 10 CFR 73.54

(d) Cyber security program (continued)

- (5) Ensure each vital digital asset is protected
 - Identify the controls applicable to the associated consequence of concern
 - Document written implementing procedures for measures taken
- (6) Provide interim compensatory measures when measures are degraded

(e) Cyber security plan

- Site-specific cyber security plan
 - Describe how the program performance objectives are met
 - Submit for NRC review and approval
- (1) Plan must describe how the requirements are satisfied, the program is managed, and incident response is provided
- (2) Supporting documentation maintained onsite

(f) Configuration management

- Ensure facility modifications are:
 - Evaluated prior to implementation
 - Do not adversely impact program performance requirements
- A facility modification may:
 - Add a previously unconsidered digital asset
 - Remove an alternate means for a digital asset that may create a vital digital asset requiring cyber security controls

(g) Review of the cyber security program

- (1) Annual review for Category I facilities in accordance with 10 CFR 73.46(g)(6)
- (2) For all other fuel cycle facilities, a triennial review must document, track, and address internal findings, deficiencies, and recommendations that result from:
 - Analysis of program effectiveness and adequateness;
 - Review of implementing procedures; and
 - Vulnerability evaluation

(h) Event reporting and tracking

- Follow existing regulatory requirements for notifications to the NRC
- When known, inform the NRC within 1 hour that the notification is a result of a cyber attack
- 24 hour reporting requirement for:
 - (1) Failure, compromise, degradation, or vulnerability in a required cyber security control
 - (2) Compromise of vital digital asset for nuclear material control and accounting at Category I or II facilities

(i) Records

- Retain supporting documentation as a record
- Maintain records for inspection
- Maintain superseded records for 3 years

Overview of Draft Regulatory Guide

A. Introduction

B. Discussion

C. Staff regulatory guidance

D. Implementation

Supporting glossary, references, and appendices

A. Introduction

- Purpose & applicability
- Applicable regulations
 - 10 CFR 73.53
 - Conforming changes to 10 CFR Part 40 (§§ 40.31 and 40.32), Part 70 (§§ 70.22 and 70.32), Part 73 (§ 73.46(g)(6))
- Related guidance
- Purpose of regulatory guides

B. Discussion

- Reason for development
- Background
 - Overview of each section in draft regulatory guide
 - Table B-1 has timeline for phased implementation
- Harmonization with international standards
- Documents discussed in staff regulatory guidance

C. Staff regulatory guidance

1. General requirements
2. Cyber security program performance objectives
3. Cyber Security Team
4. Cyber security plan
5. Consequences of concern
6. Identification of digital assets
7. Cyber security controls
8. Implementing procedures and interim compensatory measures
9. Configuration management
10. Review of the cyber security program
11. Event reporting and tracking
12. Recordkeeping

C.1 General requirements

Provides an overview of each rule concept

1. Cyber Security Team
2. Cyber security plan
3. Identifying digital assets
4. Addressing performance specifications of cyber security controls
5. Implementing procedures and interim compensatory measures
6. Managing the cyber security program

C.2 Cyber security program performance objectives

10 CFR 73.53(b)

- Detect a cyber attack capable of causing a consequence of concern
- Protect against a cyber attack capable of causing a consequence of concern
- Respond to a cyber attack capable of causing a consequence of concern

C.3 Cyber Security Team

10 CFR 73.53(d)(1)

- Responsibilities of the team
- Makeup of the team, training, and qualifications
- Management structure and relationship to operations

C.4 Cyber security plan

10 CFR 73.53(e)

- Reviewed and approved by NRC as a license amendment request
- Template for the plan is provided in Appendix A
- Documents program requirements for establishing and maintaining:
 - Cyber Security Team; and
 - Cyber security controls specific to each of the applicable types of consequences of concern
- Describes measures for:
 - Management and performance of the cyber security program; and
 - Incident response to a cyber attack affecting vital digital assets

C.5 Consequences of concern

10 CFR 73.53(c)

- Details are provided for each consequence of concern
- Shows relationship of facility types to the consequences of concern
- Vital digital assets that have more than one type consequence of concern associated must address performance specifications associated with the cyber security controls of only most severe consequence of concern
- Types of consequences of concern are ordered (highest to lowest) based on the comprehensiveness of the associated cyber security controls

C.6 Identification of digital assets

10 CFR 73.53(d)(3)

- Provides a methodology for identifying digital assets and determining vital digital assets
- Discusses the characteristics of an acceptable alternate means that can be credited for digital assets
- Describes vital digital assets and associated boundaries, support systems, and potential grouping

C.7 Cyber security controls

10 CFR 73.53(d)(2) and (d)(5)

- A cyber security control is a performance specification established to provide an element of protection against specific cyber attack vectors
- A cyber security control is addressed by taking measures to protect against the cyber attack vector(s)
- Different cyber security controls are addressed by applying various measures that are needed in combination to adequately protect against the cyber attack vector(s)
- A specific cyber security control should not be considered adequately addressed by the measures taken to address another cyber security control (i.e., one control should not credit another)

C.8 Implementing procedures and interim compensatory measures

10 CFR 73.53(d)(5)(ii) and (d)(6)

- Implementing procedures are required to document the measures taken to address the performance specifications associated with the cyber security control
- Interim compensatory measures are required when measures are degraded
 - Demonstrate the cyber security program performance objectives are met
 - Interim compensatory measures are temporary, until a permanent measure can be approved for use

C.9 Configuration management

10 CFR 73.53(f)

- Requires that licensees review additions or changes to the facility, or an activity associated with a consequence of concern or vital digital asset, to assess the impact on cyber security
 - Modifications to existing vital digital assets or implementing procedures may be required prior to making the planned change
- Cyber security considerations should be integrated into the facility design and maintenance process
 - This is an ongoing effort

C.10 Review of the cyber security program

10 CFR 73.53(g)

- Complete a comprehensive review of the cyber security program annually (Category I facilities) or triennially (all others)
- The review could result in changes to the program or any vital digital assets, as well as a review of supporting documentation and analyses

C.11 Event reporting and tracking

10 CFR 73.53(h)

- Follow normal NRC event reporting along with:
 - Notifying the NRC within 1 hour of discovery that an event is the result of a cyber attack
 - Updating an existing event report upon discovery that the event involved a cyber attack
- A licensee must record the following events within 24 hours of discovery and track them to resolution:
 - Failure, compromise, degradation, or vulnerability in an applied cyber security control
 - Compromise of vital digital asset for nuclear material control and accounting at Category I or II facilities
- Voluntary notifications regarding non-reportable cyber security events are encouraged

C.12 Recordkeeping

10 CFR 73.53(i)

- Retain supporting documentation as a record
 - Examples of records are provided
- Maintain records for NRC inspection
- Maintain superseded records for 3 years

Appendix A: Cyber security plan

- A cyber security plan is required to be submitted for NRC review and approval
- The template provides specific licensee actions and requirements regarding cyber security
- Cyber security plan must consider site specific conditions
- The applicable cyber security controls must be included in the plan submission and should follow the format of Appendices B – F
- Should the licensee choose to not utilize the NRC template for their cyber security plan, the licensee must demonstrate the requirements in 10 CFR 73.53(e) are addressed

Appendix B: Controls for vital digital assets associated with all consequences of concern

- Contains cyber security controls that NRC considers applicable for vital digital assets associated with all consequences of concern
- The licensee can choose to adopt the appendix directly and attach it to their cyber security plan
- Should the licensee choose to develop its own controls, it must demonstrate that the controls provide the capability to prevent a cyber attack from causing a consequence of concern

Appendix C – F: Additional controls for vital digital assets based on consequence of concern

- Contains additional controls that, in combination with the controls from Appendix B, NRC considers adequate to effectively address cyber security for vital digital assets associated with a particular consequence of concern
- The licensee can choose to adopt these appendices (as applicable) and attach them to their cyber security plan
- Should the licensee choose to develop their own controls, it must demonstrate that the controls provide the capability to detect, protect against, and respond to a cyber attack capable of causing a consequence of concern

Appendix G: Example implementing procedure

- Simplified example can be used by fuel cycle facility licensees to assist with developing site-specific implementing procedures for vital digital assets

Discussion of fuel cycle cyber security and the fundamental principles of design architecture

- Control of access (internal and external)
- Defense-in-depth
- Redundancy
- Independence
- Deterministic performance
- Simplicity