Official Transcript of Proceedings

NUCLEAR REGULATORY COMMISSION

Title: Advisory Committee on Reactor Safeguards

Docket Number: (n/a)

Location: Rockville, Maryland

Date: Thursday, June 8, 2017

Work Order No.: NRC-3113 Pages 1-113

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

DISCLAIMER

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

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

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

UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

+ + + + +

644TH MEETING

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

(ACRS)

+ + + + +

THURSDAY

JUNE 8, 2017

+ + + + +

ROCKVILLE, MARYLAND

+ + + + +

The Advisory Committee met at the Nuclear Regulatory Commission, Two White Flint North, Room T2B3, 11545 Rockville Pike, at 8:30 a.m., Dennis C. Bley, Chairman, presiding.

COMMITTEE MEMBERS:

DENNIS C. BLEY, Chairman

MICHAEL L. CORRADINI, Vice Chairman

PETER RICCARDELLA, Member-at-Large

RONALD G. BALLINGER, Member

CHARLES H. BROWN, JR. Member

MARGARET CHU, Member

WALTER KIRCHNER, Member

JOSE MARCH-LEUBA, Member

DANA A. POWERS, Member

HAROLD B. RAY , Member

JOY REMPE, Member

GORDON R. SKILLMAN, Member

JOHN W. STETKAR, Member

MATTHEW W. SUNSERI, Member

DESIGNATED FEDERAL OFFICIAL:

CHRISTINA ANTONESCU

ALSO PRESENT:

SUZANNE ANI, NMSS

MATT BARTLETT, NMSS

MEKONEN BAYSSIE, RES

JIM BEARDSLEY, NSIR

SAMANTHA CRANE, NMSS

JOE DEUCHER, ASLBP

JAMES DOWNS, NMSS

ALAN FRAZIER, NMSS

KAYLA GAMIN, OGC

ADAM GENDELMAN, OGC

WILLIAM GROSS, NEI

JIM MALTESE, OGC

CARDELIA MAUPIN, NMSS

CASEY PRIESTER, NRC Contractor

JANET SCHLUETER, NEI

GREG TRUSSELL, NMSS

JAKE ZIMMERMAN, NMSS

CONTENTS

P R O C E E D I N G S

8:31 a.m.

CHAIRMAN BLEY: The meeting will come to order.

This is the second day of the 644th Meeting of the Advisory Committee on Reactor Safeguards. Today's meeting, the Committee will consider the following, a proposed rule and Draft Regulatory Guide 50.62 on Cyber Security for Fuel Cycle Facilities, future ACRS activities and report of the Planning and Procedure Subcommittee and preparation of ACRS reports.

The ACRS was established by statute and is governed by the Federal Advisory Committee Act, FACA. This means that the Committee only speaks through its published letters.

We hold meetings to gather information to support our deliberation.

Interested parties who wish to provide comments can contact our offices requesting time after the Federal Register Notice describing the meeting and is published.

That said, we also set aside ten minutes for spur of the moment comments from members of the public attending or listening to our meetings.

Written comments are also welcome.

Ms. Christina Antonescu is the Designated Federal Official for the initial portion of this meeting.

The ACRS section of the U.S. NRC public website provides our charter, bylaws, letter reports and full transcripts of all Full and Subcommittee meetings, including the slides presented at the meetings.

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

There will be a phone bridge line. There is a phone bridge line. To preclude interruption of the meeting, the phone is placed in a listen in mode during presentations and committee discussion.

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

At this time, I will turn the meeting over to Mr. Charlie Brown.

MEMBER BROWN: I'm Charlie Brown, I'm the Chairman of this Subcommittee and this morning, we're

going to be doing the Fuel Cycle Facility Rulemaking.

And, in order not to strain the system or the time, I'm going to turn it over to James Downs who will now present NMSS's proposals for the rulemaking.

MR. DOWNS: Great, so good morning, thank you for the opportunity to brief the Full Committee.

I'm James Downs, the Technical Program Manager for Fuel Cycle Cyber Security from the Office of Nuclear Material Safety and Safeguards.

Staff from many different NRC offices have been involved with this effort for the past five years.

With me today are Joe Deucher, a Cyber Security Expert from the support staff for the Atomic Safety Licensing Board Panel and Jim Maltese, a legal expert on Fuel Cycle and Cyber Security from the Office of the General Counsel.

This presentation is intended to facilitate Committee consideration of the proposed rule package and draft regulatory guide on cyber security for fuel cycle facilities.

In developing these documents, the staff considered various approaches while following specific Commission direction.

The documents under your review provide

the history and background of the staff effort as well as the specifics of the rulemaking expected to be considered by the Commission.

Next slide, please?

So, on this slide, there's an agenda for the presentation. We plan to provide an overview of the various documents associated with the proposed rule, everything from the SECY paper through the Draft Regulatory Guide.

These documents total several hundred pages of text, so if we don't get to a level of detail that you're looking for, please stop me so that we can answer your specific question.

It should be noted that the proposed rule package is not expected to reach the Commission until late September of this year. Therefore, this rulemaking remains ongoing and changes may occur as the documents seek review and approval of higher levels of NRC management.

Also, over the next few months, the Committee to Review Generic Requirements, also known as CRGR, will be reviewing the documents.

The staff is committed to keeping ACRS informed of any substantive changes to the proposed rule package or the Draft Regulatory Guide.

Are there any questions on the agenda or schedule forward?

Slide three, here, we've got the obligatory list of acronyms used in the presentation. And, I should also note that there are -- there's a glossary of some unique terminology provided in the Draft Regulatory Guide.

Throughout all the documentation, the staff has made every effort to use plain language. However, cyber security can be a technically complex discussion, so we've attempted to translate where necessary.

Next slide, please?

The diagram on slide four depicts the nuclear fuel cycle. Each phase of this diagram represents fuel cycle facilities performing vastly different chemical and mechanical processes to achieve their business goals.

Needless to say, one of the challenges of regulating fuel cycle licensees is that there is never a one-size-fits-all approach.

These facilities include different types of NRC licensees and even amongst similarly licensed facilities, there may be different safety, security or safeguards concerns.

This is more clearly articulated on the next slide that lists each of the impacted licensees.

But, before we continue, I'd like to stress one thing, when we use the term fuel cycle facility, we are referring to a licensee that more closely resembles a chemical processing plant that has hazards and corresponding regulations that are very, very different from a nuclear power reactor.

Any questions on that?

Okay, next slide?

Slide five shows the specific applicants and licensees that are proposed to be within the scope of this rulemaking. The proposed rule would apply to the applicants or licensees subject to the integrated safety analysis requirements of 10 CFR 70.60 and to applicants or licensees subject to the requirements of 10 CFR Part 40 for the operation of the uranium hexafluoride conversion or deconversion facility.

Overall, the staff has found the deficient to group fuel cycle facilities by their security classifications. Therefore, in the documentation under your review, you'll see terminology like Category I, Category II, Category III or conversion/deconversion licensees.

This corresponds to the different types of

licensed material at various enrichment levels of these facilities.

Category I fuel cycle licensees are authorized under Part 70 to possess or use a formula quantity of strategic special nuclear material as defined by 10 CFR 73.2. Those would be the highly enriched uranium.

Category II fuel cycle licensees are those authorized under Part 70 to possess or use special nuclear material of moderate strategic significance.

Category III are those authorized under Part 70 to posses or use special nuclear material of low strategic significance.

And conversion or deconversion facilities are those source material licensees authorized under 10 CFR Part 40 to perform uranium hexafluoride conversion or deconversion.

This slide provides other characteristics of each specific licensee including the type of operation like conversion, enrichment, fabrication or deconversion and whether the licensee possess classified information or matter.

MEMBER BROWN: James?

MR. DOWNS: Sir?

MEMBER BROWN: Could you just highlight as

to the level of enrichment that's covered under Category I, II or III for those members who may not, like me, who cannot remember what the levels are?

MR. DOWNS: Off the top of my head --

MEMBER BROWN: Anybody who knows.

MR. DOWNS: Yes, I think it's up to --

MR. GENDELMAN: It's 20 percent.

MR. DOWNS: Twenty percent is the --

MEMBER BROWN: With Category I?

MR. DOWNS: Right, that's the 20 percent.

MEMBER BROWN: That's Category I?

MR. DOWNS: Right. And then -- go ahead Adam.

MR. GENDELMAN: Sorry, it's two different standards so that the categories --

MEMBER BROWN: What's your name?

MR. GENDELMAN: Sorry, my name is Adam Gendelman, I'm one of Jim's colleagues in NODC.

There are two different standards, Categories I, II and III in Part 70 refer to total amounts of uranium 235, 233 or plutonium. It's not specifically concerned with the level of enrichment.

So, whether it's enriched to 5 percent or enriched to well over 20 percent in to HEU range, we're looking at the total mass of SNM.

VICE CHAIR CORRADINI: In the facility? In a location? Where?

MR. GENDELMAN: Well, at the facility, licensed -- the facility --

VICE CHAIR CORRADINI: So, anywhere in the facility if the accumulated amount is greater than X?

MR. GENDELMAN: Yes.

MEMBER MARCH-LEUBA: Yes, so, the question I was going to have is where do the -- the facilities that are in the process of being decommissioned and when you get 25 partials Paducah fit into this, they were never under NRC license, but and they are not in and that is because they don't operate now.

But, they have tons. I mean, you look at the cylinder field for one of these places and yes, each of those cylinders has five tons, so it's a category exceed a .5 by the amount of uranium. It's on you list?

MR. DOWNS: Right, that's correct. Paducah would not fall under the scope of this rulemaking.

MEMBER MARCH-LEUBA: Why?

MR. DOWNS: Because it doesn't have an ISA or Part 70, so therefore, it's not included.

MEMBER MARCH-LEUBA: So, they're licensed

by DOE? That does the --

MR. DOWNS: Well, right now, since they're undergoing decommissioning, it's a different -- that's right there. They're going through -- their certification has been terminated so, therefore, they're no longer under the NRC purview.

MEMBER MARCH-LEUBA: And, we're okay with that? I mean, they don't need to have cyber security? I assure you they do, but --

MR. DOWNS: That's right.

MEMBER MARCH-LEUBA: Okay.

MEMBER KIRCHNER: So, I don't have Part 70 with me, could you just give us -- what's the -- what are the break points for the amount of material? The amounts of material?

MR. MALTESE: If you'd like, I can read from the definition of a formula quantity, one moment, formula quantity means strategic special nuclear material, in any combination and a quantity of 5,000 grams or more, so 5 kilograms or more, computed by the formula of grams of U235 and there's a two and a half times factor for the grams of U233 or plutonium.

So, it's somewhat complex. Strategic nuclear material of moderate strategic significance in an amount less than that but more than a 1,000 grams

of material or more than 500 grams -- more than 1,000 grams of U235 or 500 grams of U233 or plutonium or a combination or moderate strategic significance can also be 10,000 grams or more of U235 that's enriched between 10 percent and 20 percent.

And strategic special nuclear material, low strategic significance is less than that, but more than 1,000 grams of U235 enriched between 10 and 20 percent or 10,000 grams or more of U235, less than 10 percent.

And then, there's 15 grams or more of the other material, U233 or plutonium, if that's helpful.

MEMBER KIRCHNER: Thank you.

MEMBER BROWN: The bottom line is it's mushy, it's spread across the types of material as well as kilograms to determine where you fit, that's the way I read the stuff that you said. Is that right?

MR. MALTESE: That's right. As I mentioned, it's on multiple dimensions. It's the type of material, the weight and the enrichment are all variables. But --

MEMBER BROWN: Okay. All right, thank you.

MR. MALTESE: But there's no -- there is

no overlap between the categories.

MEMBER BROWN: All right.

VICE CHAIR CORRADINI: So, this is not -- we need to move on, but I'm just -- since BWST is a fuel for -- it is not for power reactors?

MR. MALTESE: That's correct.

VICE CHAIR CORRADINI: Okay, that's what I guessed. Thank you.

MR. DOWNS: Okay. It's also important to note here that the first paragraph of the proposed rule groups the impacted entities in a slightly different way to provide time frames for submitting a cyber security plan.

Licensees currently in possession of licensed material will be required to submit a plan within six months of the final rule.

Licensees that are currently non-possessing, like Eagle Rock, ACP, GLE and International Isotopes, would not be required to submit a plan until six months prior to the anticipated date of possessing licensed material.

And, applicants currently under review for a license, like MOX, would be required to amend their application to include a cyber security plan prior to a license being issued.

Were there any other questions on the impacted entities before I move on?

Slide six provides an overview of the SECY paper that the staff intends to provide to the Commission for consideration of the proposed rule.

The SECY paper contains the high level response to the Commission direction provided in the SRM to SECY 14-0147.

In that SRM, the Commission directed the staff to proceed directly with the rulemaking and designate it as a high priority with the final rule being completed and implemented in an expeditious manner.

The Commission also stated the staff should augment the work performed to date and develop in a more fulsome technical basis for the proposed rule and ensure that cyber security is considered as an integrated aspect of overall site security.

The SECY paper highlights specific topics that are discussed in greater detail within the documents associated with the proposed rule package.

The purpose of the current phase of this rulemaking is to publish a Federal Register Notice that solicits formal comments on a proposed rule package and the associated draft regulatory guide.

Are there any questions on the purpose of the SECY paper?

MEMBER SKILLMAN: I do.

Jim, my question has to do with the use of the word fulsome. I read that word over and over again and I said that's a word that we don't commonly use in our day to day discourse.

It kind of conjures up a thoroughness, adequacy. Why was that word selected?

MR. DOWNS: That was actually directly out of the SRM. So, that was language that the Commission selected. And, the staff interpreted it the same way as you, completeness, adequate, more robust.

Up to that point, the staff had done some preliminary groundwork and we thought we had a basis for orders at that point. But, the Commission felt that the staff didn't establish a basis for orders and that's, therefore, directed us to proceed to that rulemaking.

So, they were emphasizing the fact that once you've done, you know, your technical base and that you've established to date wasn't adequate and you need to go a little bit deeper with -- in the rulemaking.

MEMBER SKILLMAN: Thank you.

MR. DOWNS: Slide seven provides an overview of the Federal Register Notice. This is a fairly traditional FRN that contains several questions on the proposed rule which are answered in the discussion section. These are often referred to as Statements of Consideration.

At the very end of the FRN is the actual text of the proposed regulation. I'll get into the specifics of some of those proposed requirements within the next couple of slides.

But, again, the intent of the FRN is to solicit formal public comments on a proposed rule package and the associated regulatory guide.

Are there any questions on the structure of the FRN?

Slide eight provides an overview of the proposed rule. The NRC currently lacks a comprehensive regulatory framework for addressing cyber security at fuel cycle facilities.

The staff has observed that fuel cycle facilities rely upon digital assets for the performance of important safety, security and safeguards functions.

For fuel cycle licensees, there is no regulatory requirement to consider the potential

consequences that a cyber attack could cause by compromising these functions.

The proposed rule, if approved, would require fuel cycle licensees to detect, protect against and respond to a cyber attack capable of causing a consequence of concern.

To do this, licensees would be required to establish a cyber security program that addresses these consequences which I'll discuss in my next slide.

MEMBER KIRCHNER: I have one question before you go on. Some of the facilities of most concern, obviously, deal with what in the DOE world that's called SNM which is a different definition.

But, and usually classified the facilities operations. It's communications and such have to meet security requirements as such for handling and storing and using classified information.

So, how do you reconcile this with what already exists in that world, in the classification world?

MR. DOWNS: So, back on slide five --

MEMBER KIRCHNER: With my concern being, where does it become redundant?

MR. DOWNS: So, on slide five, we've

highlighted some of the -- each of the facilities and whether they have classified information or matter.

Those facilities that have classified information typically have a classified computer network that is authorized by the Department of Energy, NNSA, Naval Reactors, one of those three entities.

So, the goal through this rulemaking has been to develop regulations that don't have dual regulation associated with them. We don't want to, as you were pointing out, we don't want to step into DOE territory, NNSA and Naval Reactor territory.

Because, we feel like they've done a pretty good job with the requirements that they've got on those classified computer networks.

So, there's an exception in the proposed rule that would say that if you've got a classified computer network that's authorized by another federal agency, the digital assets residing on that network are except from this regulation.

MEMBER KIRCHNER: Thank you.

MR. DOWNS: Okay, slide nine highlights the four types of consequences of concern that are defined by the proposed rule. These would be the latent design basis threat, a latent safeguards and

active safety and a latent safety and security.

These consequences are based on specific thresholds and formed by the existing regulations referenced on the slide.

Not every consequence of concern is applicable to every fuel cycle facility. For example, the latent design basis threat consequence of concern would only be applicable at a Category I fuel cycle licensees.

Overall, the consequences of concern provide the basis to apply a disciplined graded approach to the identification and protection of vital digital assets.

One question the staff is accustomed to getting is what's the difference between an active and a latent consequence of concern?

So, that's one of the questions that we've discussed in the Federal Register Notice.

An active consequence of concern is when the compromise of a digital asset from a cyber attack directly results in a radiological or chemical exposure exceeding the thresholds set forth in the proposed rule.

Note that the active designation is only valid for safety consequences.

In the case of a latent consequence of concern, a digital asset is compromised, but there is no direct impact on safety, security or safeguards until a secondary event occurs. And, by that, I mean an initiating event separate from the cyber attack.

For a latent consequence of concern, the compromised digital asset would no longer be available to provide the function needed to prevent the consequence from the secondary event.

MEMBER BROWN: One thing on the active, just to make -- you called it a direct impact or it's for the active concern -- consequence or concern.

By direct, I also interpreted that to mean immediate. Is that -- do those go hand in hand or not?

MR. DOWNS: There is --

MEMBER BROWN: To me, if based on the way you've describe latent, it almost sounds like direct has to mean the attack comes in, it initiates an action itself to some degree as opposed to sitting around for a while waiting for something else to happen. So, that's the word immediate came to mind as I was reviewing this.

MR. DOWNS: I think that's a fair conclusion there that, you have to be careful with

immediate because it doesn't necessarily mean that you press a key on a keyboard and something, you know, there's an immediate exposure at that point. It may take some time for a pressure and a process to fill such that a release would occur.

But, it's a direct cause and effect. It's -- you're not -- there's no -- the key difference between active and latent is that for latent, there's a secondary event that has to happen.

MEMBER BROWN: Well, wouldn't the -- when you talk about it, may have to wait for a pressure or a temperature or something, that's waiting for another initiating event. So, I don't --

MR. DOWNS: No, I don't --

MEMBER BROWN: -- I can't quite --

CHAIRMAN BLEY: Could I jump in and try and correct me if I don't hit what you're saying.

I think the way they interpret it, and the way I've interpreted as I read it is, if it's inevitable given where you sit right now that it happens, it's immediate if, in fact, some other intervention has to happen later, then it's latent. It's sitting there, it doesn't do anything until something further that isn't a direct consequence of what's already started.

MEMBER BROWN: That was my --

CHAIRMAN BLEY: That's the way you interpreted it, too.

MEMBER BROWN: No, my concern was he made the comment, the active, it might come in, but then you may need say a pressure to get to some range or a temperature to get to some range which now moves it out of the active, to me, into the latent. You're waiting for some plant condition to occur which is now not direct anymore, it's latent. It's waiting for something in the process to occur before it --

So, that's the nuance I've been struggling with that as I've read it.

CHAIRMAN BLEY: And, to me, if it was already on that trajectory, it was --

MR. DOWNS: That's --

CHAIRMAN BLEY: It's your words, so I wondered what you meant.

MR. DOWNS: That's right, you're absolutely right. If it's on that trajectory, if there's an intervening action that could, you know, if there's an item that's relied on for safety that could potentially stop that event from occurring, then you've prevented the consequence of concern from that cyber attack.

MEMBER BROWN: So, you still define it as active?

MR. DOWNS: That's correct. It would still be active.

MEMBER BROWN: Because there's something that would take care of that.

MR. DOWNS: A good example of a latent consequence of concern would be if say a facility has access control by several different badge readers, that sort of thing, a cyber attack were to take down that access control.

The material isn't going to walk itself off site, you need another event to occur, you need that adversary to come to obtain the material and walk it off. So, that's the difference, the nuance there.

MEMBER BROWN: Okay, thank you.

Anything else? Go ahead.

MR. DOWNS: Okay, the three outer boxes on slide ten summarize the specific provisions of the cyber security program that would be required by the proposed rule.

These provisions would support the overall program performance objectives and correlate to the steps the licensee would take to implement their cyber security plan, identify, protect and maintain.

Combined with the consequences of concern, this approach limits the burden on fuel cycle licensees by allowing them to focus their efforts on protecting only risk significant digital assets.

Because the thresholds for the consequences of concern are informed by existing regulatory requirements, licensees can utilize existing analyses to facilitate the identification of digital assets.

Acceptable approaches to excluding digital assets are demonstrated in the regulatory -- in the draft regulatory guide.

The proposed rule also avoids a standalone focus on cyber security by allowing licensees to credit alternate means of preventing a consequence of concern in lieu of implementing measures to address cyber security controls.

An alternate means could be something like a guard who performs the same function as a badge reader or an overflow tank on a process line that prevents a release capable of causing a chemical consequence.

Several fuel cycle licensees have indicated they expect to primarily document alternate means and plan to have few, if any, vital digital

assets.

Only vital digital assets which would be those not having an alternate means to prevent the consequence of concern would require protection using cyber security controls.

The staff has developed the Draft Regulatory Guide to provide additional guidance on an acceptable cyber security program and we'll be discussing that in the coming slides.

Are there any questions on the proposed cyber security program?

Okay, slide 11, the staff has prepared a Draft Regulatory Analysis to examine the benefits and costs of the proposed rule. It is generally accepted that security related events have undeterminable frequencies.

Therefore, many of the benefits of the proposed rule are not easily quantifiable. Although many analyses for security regulations assume a frequency of one, for this Draft Regulatory Analysis, the staff has stated that the proposed rule cannot credit a specific change in the frequency of a consequence of concern from a cyber attack.

This forced the staff to perform a qualitative assessment in the Draft Regulatory

Analysis consistent with applicable NRC guidance.

By considering various attributes, the staff determined that the proposed rule would increase assurance of safeguards and security, reduce risk to public and occupational health, reduce risk to property damage and improve knowledge, regulatory efficiency, licensee production reliability and public confidence.

The draft of the regulatory analysis measures the estimated costs of the proposed rule relative to a hypothetical baseline of NRC undertaking regulatory action.

The total undiscounted cost of the proposed rule to the fuel cycle industry is estimated at roughly $5 million per licensee over the 25-year period of analysis considered.

This figure was informed by industry estimates for both the implementation and continuing costs of the rule.

A final note on the Draft Regulatory Analysis, the staff felt it would be beneficial to provide a discussion on the current cyber threat as it relates to the vulnerabilities that this rulemaking would address.

Appendix B of the draft regulatory

analysis discusses the general nature of the cyber threat and provides examples of both active and latent consequences resulting from recent real world cyber attacks on industrial control systems that are analogous to those at fuel cycle facilities.

The staff believes that this discussion supports the benefits documented in the -- for the proposed rule.

Are there any questions on the Draft Reg Analysis?

Next slide?

Slide 12 provides an overview of the Draft Backfit Analysis. In accordance with the backfitting requirements in 10 CFR 70.76, most of the entities impacted by this rulemaking are afforded backfit protection.

The exception being future applicants and current Part 40 licensees.

The Draft Backfit Analysis prevents the staff's evaluation of the proposed rule and examines its impacts relative to the current regulatory framework.

Based on this analysis, the staff has determined that the proposed rule would constitute a backfit which is justified in part based on the

adequate protection exception and in part based on the cost justified substantial increase and overall protection of public health and safety.

The Draft Backfit Analysis basically bins each provision of the proposed rule based on whether it would be required for adequate protection or whether the proposed rule -- whether the provision would be a substantial increase in protection.

Within the Draft Backfit Analysis, the staff has provided a threshold analysis to better quantify the cost justification for the substantial increase in protection.

And that really boils down to the provisions related to the safety consequences of concern.

The undiscounted costs for the substantial increase in protection was calculated to be a total of roughly $14 million for the industry over the 25-year period of analysis.

The threshold analysis considers that $14 million figure relative to the averted costs of potential safety events caused by a cyber attack.

This threshold analysis basically provides a break even point in relation to several different events, each with a range of consequences including a

threshold exposure to a single individual to numerous individuals.

Are there any questions on the Draft Backfit Analysis?

MEMBER SKILLMAN: Yes. Why are the Part 40 license holders excluded from backfit provision?

MR. DOWNS: So, with the backfit provisions being in Part 70.76, they're only applicable to the Part 70 licensees. There are no backfitting provisions provided in Part 40.

MEMBER SKILLMAN: What do the Part 40 license holders say?

MR. DOWNS: Well, I'm sure they'd like to have backfit provisions, but --

(LAUGHTER)

MR. DOWNS: So, the requirements in 70.76 were brought around -- brought about during the Subpart -- when Subpart H was added to Part 70, basically when the ISA requirements were put in there, the Commission said that, you know, backfit provisions would also be required.

Part 40 really hasn't been changed in a while. So, it's -- those same requirements, those same provisions aren't there.

MEMBER SKILLMAN: Is there dialogue from

their attorneys saying, hey, with this change in regulation, we're kind of like the Part 70 people and we want to be treated the same way?

MR. DOWNS: Not to my knowledge. But, again, given that Part 40, there is not a whole lot of change to Part 40.

Typically, if you don't have a change to the regulation, then you don't even really consider backfitting.

MEMBER SKILLMAN: And, still they have to classify their assets as VDAs or not and go through the process?

MR. DOWNS: That's correct.

MEMBER SKILLMAN: So, there is a burden on them regardless?

MR. DOWNS: That's correct. And, the Draft Regulatory Analysis measures that burden and communicates those costs very clearly.

However, given that the regulations aren't there for the backfit provisions, we -- you know, it's not something that the staff has to justify really.

MEMBER SKILLMAN: Okay.

MR. DOWNS: But it is discussed.

MEMBER SKILLMAN: I understand, thank you.

MR. DOWNS: Okay?

Next slide, please?

Slide 13 provides an overview of the Draft Environmental Analysis. The Draft EA examines the potential environmental impact of the rulemaking. It considers the same alternatives presented in the regulatory analysis and concludes with a finding of no significant impact for the proposed rule.

Keep it pretty short and sweet with this one. Are there any questions on the Draft EA?

Okay.

So, now, we'll get into the Draft Regulatory Guide which can also be referred to as DG 5062.

Slide 14 highlights the overall structure of the document which follows the standard layout of a typical NRC regulatory guide.

DG 5062 is somewhat unique given that it has a number of appendices that we'll discuss in the coming slides.

The Draft Regulatory Guide provides an approach that the staff will consider acceptable for meeting the proposed rule.

It must be emphasized that the guidance does not demonstrate the only acceptable approach.

The staff looks forward to further public

discussion of the demonstrated approach and potentially clarifying or expanding the document.

Are there any questions on the structure of the Draft Reg Guide?

Slide 15 provides the --

MEMBER BROWN: Just maybe you can address this when you talk about the rest of the stuff, but you made the comment that the draft guide provides the standard and the methods acceptable to NRC.

MR. DOWNS: Provides a method.

MEMBER BROWN: A method.

MR. DOWNS: Correct.

MEMBER BROWN: But, does not preclude something else. However, when you look at the specifics of the rule itself, after you go through the latent consequences and you're in the program part of the rule, it very specifically says you will identify all digital assets, all, it's not -- it doesn't give you any, you know, any outs.

So, whatever other methods somebody wants, they are still subject to categorizing each and every digital asset and then making some determination as to where it falls relative.

So, the consequences of concern and/or whether it's a vital digital asset.

So, when you say I'm giving them license to do something, the allowance to do something else, that seems, to me, to be a little bit off -- yes, I don't -- I'm not trying to be pejorative, I'm just -- but it doesn't seem to track.

Somebody comes in and wants to do something that doesn't result in categorizing each and every digital asset but subdivides them, you can't do that. You've got to address all of them.

So, to me, the rule overrides any suitable type of way of reducing the level of effort that they have to deal with. That's the way I read it.

Because the rule is the rule and the guide is, yes, you can do it, but you don't have to, et cetera, et cetera. But, the rule still governs in this circumstance.

So, to me, that's just -- that's my thought process relative to the comment that you are allowed to do something else. I might not --

MR. DOWNS: Let me help you with our thought process because what you've said there demonstrates a misunderstanding of the rule.

We are not requiring the identification of all digital assets. We are requiring the identification of digital assets that have a

consequence of concern.

MEMBER BROWN: But, don't you have to look at all of them in order to determine that?

MR. DOWNS: Not really, no. Because the benefit of having some of these existing analyses is that the licensees are familiar with where the digital assets are that could potentially have a consequence of concern.

MEMBER BROWN: It means they have to look at all of them in order to determine whether they have a consequence of concern.

MR. DOWNS: Well, I don't think that a fax machine that's tied into a land line, you know, in a business operations would need to be considered.

So, I don't think that it's fair to say that a licensee would have to consider all --

MEMBER BROWN: Be careful.

CHAIRMAN BLEY: Can I try something? Because we've got a -- we had a long discussion about this in the Subcommittee.

MEMBER BROWN: Yes.

CHAIRMAN BLEY: And, what you're saying kind of makes sense to me, but it seems a little different than the previous discussion.

Let me try an example. If I went to my

facility and I went through it and there were not sufficient materials that could lead to a consequence of concern in two-thirds of my facility, I could take that off the table then --

MR. DOWNS: Absolutely.

CHAIRMAN BLEY: -- and only look at the digital assets in the places where, in fact, there was the physical possibility of getting a consequence of concern.

And, there was some -- the discussion earlier didn't quite go that way, but if that's the way it is, I'm much more comfortable with --

MR. DOWNS: That is 100 --

CHAIRMAN BLEY: -- what you're doing.

MR. DOWNS: -- 100 percent the way that it is.

The licensee can propose a methodology in their cyber security plan that could take that approach and screen out a large portion of the facility that has no consequences of concern associated with it and that would be an acceptable methodology and the draft regulatory guide discusses that approach as being acceptable.

MEMBER BROWN: Dennis's elaboration mentioned -- used the words didn't have a quantity of

special nuclear material. It was a low level.

But, how -- there's no differentiation in terms of if you've got some special nuclear material, then if lower them some, what is that level where they don't have to do it? Is that going to create an argument?

I mean, if you've identified the general level in terms of how the facility is classified, but in terms of where that material is located withing in the facility.

I mean that gives you the idea that we could take our thousand kilograms or one kilogram or whatever it is, I'll distribute it through four different buildings and it'll be below some number. But there's no categorization of what that would be.

I'm still a little bit off the chart, not off the charts, but lack of understanding where this flexibility is allowed. Because there's just not enough specificity in what that level of material --

It has no material, that's easy, but what if they've got some? Because part of this whole rule makes it very clear when you go through the consequences, is material accountability and where it is, what it is, how much you've got, what you start with, what you end with, all that type of stuff.

And, that's covered in each one of these latent I guess really, the first two consequences of concern. So, I -- it still seems to me there is a not quite the flexibility you envision based on the way this is categorized, the way the rule is written right now.

MR. DOWNS: So, the --

MEMBER BROWN: I'm not trying to detail how to fix that, but all I'm saying, in my own mind, that's something that makes it more difficult for the industry to comply without a greater effort than you envision.

MR. DOWNS: So, given that there are existing programs and plans that discuss these specific thresholds that are laid out in these consequences of concern, the focus isn't necessarily on is there material there, the focus is on whether or not there could be a consequence of concern.

So, therefore, just because you have one kilogram of material, that really doesn't have a bearing on whether there could be a consequence of concern.

Those consequences of concern are -- have already been analyzed in existing programs and plans that the licensees have in place. So, they know where

in their facilities, these consequences of concern could occur at.

So, the whole point here is that they can, as Mr. Bley pointed out, you can focus in on very specific areas of the facility instead of using the -- focusing in on the facility as a whole.

If the licensee would want to do a full analysis and do the, you know, examine the entire facility, that would be an acceptable approach.

But, given the flexibility that this proposed rule would give licensees, the licensee could propose a methodology that focuses in on only those areas of the facility that have these consequences of concern.

MR. DEUCHER: And, again, this Joe Deucher with ASLBP.

Getting back to the notion of the graded approach, as you look at the consequences we have listed here, you mentioned material control and accounting as an example. That's only an item as a consequence in design basis threat which specifically speaks to the type of material, the level of the material and its characteristics.

So, you'll see that we built flexibility in by aligning it with the existing regulations where,

for your active safety and your latent safety and security, again, it's focused more towards the facility type as well without mentioning the facility type by name.

But, each facility could look at their particular situation, their ISA, their other documents that they have and make an informed decision, okay, where do we need to look first, because they already have that -- those conclusions addressed in order to meet these existing requirements.

And so, it's not that they're going to have to take a step back all the way to step one and say, we need to look at where we have material throughout the facility.

The only one that really needs to specifically with our consequences, needs to look at material in and of itself would be the Category I. But they already have to do that as a result of the design basis threat.

MR. DOWNS: And, just to add on, Joe --

MEMBER BROWN: Hold it, hold it.

The safeguards, one says, unauthorized removal of special nuclear --

MR. DOWNS: That's what I was going to -- correct.

MEMBER BROWN: That's Category II, so --

MR. DOWNS: But there are no existing Category II licensees. That's where I was going to go with that.

MEMBER BROWN: But, that doesn't make -- the rule -- but you're calling it out even though there aren't any, it makes no difference. So, you can't make an argument you could have a Category II, you could have somebody apply for a license to Category II, so it's not -- your words are not consistent. It really applies to both Category I and Category II.

And, just because there aren't any doesn't mean it's not going to be a burden. That it's not going to have an unnecessary effort. That's --

MR. DOWNS: So, just to kind of put material control and accounting to bed, Category I and Category II facilities have very, very specific material control and accounting requirements.

And, they have very, very specific fundamental nuclear material control plans that account for every gram of that material that's present in those facilities.

Therefore, they know the locations, they've done these existing analyses and they can

easily use that to inform their methodology for the proposed rule.

And, that's where you -- that's why we've divided up design basis threat, latent design basis threat, that's Category I.

Latent safeguards, that's Category II.

So, it's a fair point that there are no Category -- just because there are not Category II facilities now, doesn't mean there are not going to be any in the future.

The point is, is that the requirements for nuclear material control and accounting are very, very specific for both of these types of licensees.

So, therefore, it will easily inform this proposed rule.

We haven't gotten any push back from Category I facilities concerning material control and accounting.

Previously, we did have some material control and requirements down in the latent safety and security several years ago when we were talking about the proposed rulemaking.

We had a lot of feedback from Category III facilities saying that would be overly burdensome. And, we looked at it and we agreed that, yes, it would

overly burdensome.

But, beyond that, the amount of Category III material that would be required to cause a significant consequence was such that it just wasn't feasible that that amount of material could be diverted or stolen from, you know, in regards to a cyber attack.

So, the proposed rule has evolved over time to account for some of these -- the things that we're talking about, especially in the consequences of concern.

MEMBER BROWN: Any other discussion?

MEMBER KIRCHNER: While this slide is up, you are considering a MOX facility. And, I was just looking at the second bullet under safety, 30 milligrams or greater intake of uranium.

So, you're treating plutonium as acute chemical exposure?

MR. DOWNS: So, the -- we would be focusing on the radiological properties of the plutonium, that's the 25 rem to any individual and then the acute chemical exposure piece, that's correct. That's where you would be focused on that.

MEMBER KIRCHNER: Thank you.

MEMBER CHU: I have some comments, yes.

I remember in our Subcommittee meetings, there was a lot of discussion about it could be very burdensome, this could become a big paperwork exercise.

And, it seems like the proposed rule is trying to address that issue, am I correct? You are more flexible than our Subcommittee meeting or there was no change?

I just don't know whether there were changes since our Subcommittee meeting because there was a lot of discussion about, you know, I kept thinking of my personal experience of the bad QA program.

You can get into that kind of exercise and the payback becomes very small after a while, it's all paper exercise. Your vital digital asset, you start, you know, documenting things and then are you really addressing the significance concern? Don't know.

You know, it's like the low level people start all getting into this exercise.

So, I want you to give us assurance that, you know, you do understand that potential concern.

MR. DOWNS: That's correct.

MEMBER BROWN: James, before you go on, I just -- correct me if I'm wrong, she said she wasn't

sure what from Subcommittee until now whether stuff has changed.

The rule, as I understand it, based on the reading from the Subcommittee meetings, is -- and I did compare it word for word with the FRN and it hasn't change.

MR. DOWNS: That's correct.

MEMBER BROWN: There -- as a result of our Subcommittee meetings, there were a number of comments, a few comments, that were observations we had made during the Subcommittee meeting where they did translate that into the Draft Reg Guide.

Particularly regarding the parts on identifying digital assets and vital digital assets and air gaps and/or boundary conditions and stuff like that.

So, they did, in terms of how you evaluate how they can be used, was extensively revised, as a matter of fact.

But, the rule is the same as we saw before so that's -- I just wanted to make sure we understood and flexibility in the Reg Guide can't override if there are certain specific things required by the rule, you have to follow those regardless of what the Reg Guide says.

That's all -- that's my only difficulty here is a little bit of the -- the way the rule is written as opposed to what's in the Reg Guide, will the industry individuals actually have the flexibility that they think they have, that's it's perceived that they have. That's all.

So, now, I'll let James go ahead and answer your question.

MR. DOWNS: And, Charlie's right on, the rule hasn't changed since the Subcommittee briefings.

What has changed, and as Charlie point out, is the guidance. The rule itself is, as most performance based regulations are, it allows for a great deal of flexibility.

Some of the feedback that we've gotten from, you know, stakeholders, is that the -- that flexibility is great, but what are you really looking for and does it mean that, oh my gosh, we need to go to the nth degree, as you pointed out, to document all of these vital digital assets?

So, one of the purposes of the Draft Regulatory Guide, especially Appendix G I believe it is, the very last appendix, is to provide an example of the level of implementing -- the level of documentation associated with implementing the cyber

security program that the proposed rule -- it would satisfy the proposed rule.

So, our goal is to not have this be a huge paper exercise and a tremendous burden on licensees. That's one of the lessons that we've learned from just general cyber security implementation across, you know, as the cyber security industry.

We've learned several lessons from the reactor side of the house as well. That's why we've got some very specific consequences of concern in this rule.

We're trying to really limit the -- truly make it a risk informed rule by focusing in only on those digital assets that are -- we call vital which would have that significant risk impact.

So, we're really trying to narrow it down. And, again, we provide that additional flexibility by allowing documentation of alternate means. It's not just that, hey, this vital digital asset has this consequence of concern associated with it. Well, if there's a non-cyber way to prevent that consequence of concern, great, credit it as an alternate means and you don't have to worry about applying the cyber security controls to that.

MEMBER CHU: Thank you.

MR. GENDELMAN: This is Adam Gendelman.

I would add two things, first, and this sort of was very consistent with my experience as I've acclimated to the rule for lack of a better term is the consequence of concern is the analytical frame.

And so, whether or not materials in a particular part of a facility may not actually drive whether you could or couldn't screen out, say, large parts of the facility.

There may be part of the facility that has some material, but you could, nevertheless, analytically demonstrate that there's no consequence of concern associated with it.

Likewise, there could be part of a facility with no material, but that's where all your security hardware is, your access control system, your cameras, et cetera where there may, indeed, be something that at least required further analysis.

And, I think also just in the broader frame, to your point about, you know, how much flexibility do you have? As we say, you know, as a performance rule, but I was actually sort of, I wouldn't say surprised.

But, I mean, the rule is like two pages long. Consider that in the context of other NRC

requirements, 50.55(a), something like that where, you know, we go into painful, bloody detail in terms of exactly what our expectations are.

And, the reason that's the way the rule is structured is, beyond have an adequate program, have a team, have training, there is, I would say, a great deal of licensee flexibility to meet those requirements.

The Reg Guide says, here's one way. And even to the extent that the Reg Guide says, we don't think a particular approach would be an acceptable way to meet our requirements.

And the licensee comes in and not withstanding that initial position, demonstrate to satisfaction that this what we thought was not okay approach does in fact meet the requirement, then they have an acceptable program.

Because it's the rule that they have to meet, not the Reg Guide.

MEMBER BROWN: I don't know how much you're going to be talking about this specific Appendix G, but for the Members who are unfamiliar with this a little bit, Appendix G walks through an example of a system in the plant process type stuff in the plant, and then proposes how you would then go and

evaluate that including alternate means to determine what are the levels that you have to address.

And, when you go through that example, which is it's got to be the simplest little process system you can imagine. It has almost no technical, I don't want to say substance, but technical difficulty, very easy to understand.

But yet, when you go through it, it's develop a table. Here's the categories, describe each thing. Document, document, document, document, document until you get to the end.

There's a considerable amount of description that has to be -- and the things that have to be identified. It's a very simple system with no complexity, yet there's a considerable amount of what appears to me, necessity to document why this relatively simple approaches to doing things require fairly -- could be an elaborate amount of documentation.

You don't know because it's just -- you don't see the details.

Including implementing procedures that have to be involved that then have to be monitored and continually reviewed.

So, that's -- I'm not trying to be -- I

understand the need for this. I'm just trying to be skeptical enough that we don't miss providing the best level of flexibility we can out there but yet still accomplish the same goal.

So, I mean, and I appreciated the Appendix G, that was very useful in terms of taking the guidance and the draft guide and then trying to see how you would apply it with alternate means from the previous paragraphs in this guide.

I mean, that's just -- you can go on now. I think I've now milked this one enough unless somebody else has a comment.

Go ahead, move on, James.

MR. DOWNS: Okay.

Slide 15, here are the topics discussed in Section C of the Draft Regulatory Guide.

As you can see, the organization mirrors the requirements of the proposed rule.

Feedback from industry stakeholders as well as the Digital Instrumentation and Control System Subcommittee informed the refinement of several of these topics.

As I previously stated, several licensees have indicated they expect to primarily document alternate means and plan to have very few, if any,

vital digital assets.

So, in the guidance, the staff recently clarified that it would be acceptable to satisfy many of the proposed program requirements with a level of effort, scalable to the number of vital digital assets.

For example, DG 5062 does not specify an exact number of individuals on a cyber security team and neither does the proposed regulation.

But, the guidance does state that, if initial implementation -- if the initial implementation process identified few vital digital assets, staffing may be reduced to a level capable of maintaining the program performance objectives.

For licensees with no vital digital assets, this would imply that staffing of the team could be limited to only what is needed to perform configuration management, periodic reviews and event reporting.

I know I've just scratched the surface of Section C of the guidance document, but I think our time would be better utilized if I open it up to any questions.

I do plan to discuss more technical topics like control of access and defense of architecture

when we get to the appendices of the guidance.

Are there any questions on Section C?

Okay. Slide 16 provides an overview of Appendix A of the Draft Regulatory Guide. This appendix contains a template for a licensee cyber security plan.

The cyber security plan would be required to be submitted to the NRC for review and approval.

The cyber security plan as is clearly articulated in the proposed rule describes how a licensee would identify digital assets and determine vital digital assets.

Without prior approval of this methodology, there would be no licensing basis or regulatory framework for the NRC to evaluate the licensee's analysis.

Furthermore, the cyber security plan also formalizes an enforceable commitment by the licensee to utilize a configuration management system, perform periodic reviews of cyber security and report events caused by cyber attacks.

Regardless of whether a licensee does or does not have vital digital assets today, the cyber security plan provides NRC with the basis to ensure that future operation of fuel cycle facilities remains

adequately protected against cyber attacks.

Are there any questions on Appendix A of the Regulatory Guide?

Slide 17 provides an overview of Appendices B through F. The appendices contain cyber security controls that the staff will consider acceptable for meeting the proposed rule.

Appendix B contains controls that would be generically applicable to all vital digital assets.

Appendices C through F contain controls that would be applicable to specific consequences of concern, therefore, not every appendix would be applicable to every licensee, similar to the consequences of concern.

For example, Appendix D contains controls for vital digital assets associated with the latent safeguards consequence of concern which would only be applicable to Category II fuel cycle facilities.

A licensee can choose to adopt the controls in the guidance by referencing them in their cyber security plan or a licensee can develop their own controls.

The key with developing a unique set of controls would be for the licensee to demonstrate that the program performance objectives are all addressed.

A licensee would satisfy a cyber security control by taking measures to address the controls performance specifications.

A measure is a capability, item or action that provides protection from a cyber attack vector. There are numerous attack vectors to consider, so addressing the applicable cyber security controls may take numerous measures.

The staff utilized an industry accepted approach to ensure that each of the cyber security controls actually adds value.

The controls in the draft regulatory guide were informed by the National Institute of Standards and Technology special publications, frameworks and profiles on cyber security.

This industry accepted approach has been recommended by recent Executive Orders and the controls developed by most other organizations have crosswalks that map back to NIST.

Each control in the Draft Regulatory Guide documents its traceability back to a NIST control.

The staff tailored NIST controls by establishing parameters that are suitable to each of the specific consequences of concern.

For example, a vital digital asset

associated with a design basis threat consequence of concern would have remote access addressed in its control C7.

Basically, that control prohibits any remote access.

A vital digital asset associated with a latent safety consequence of concern has the same topical remote access address in F7 which allows remote access, but only through a specifically configured boundary control device.

This graded comprehensiveness is reflective of the overall risk informed approach proposed for fuel cycle cyber security.

MEMBER BROWN: We had some discussion during the Subcommittee meeting relative to wireless remote access.

And, I'm trying -- I've forgotten now whether the guide -- nothing prohibits that right now. If they wanted to use wireless, they can. Is that --

MR. DOWNS: I think it depends on the consequence of concern. So, at your Category I facility where you have that design basis threat consequence of concern, I believe that we've got a control there that actually rules out wireless and --

MEMBER BROWN: I don't remember that.

MR. DOWNS: And, part -- that's also consistent with the NNSA, Naval Reactors and Department of Energy approach to the classified systems that are present on those facilities as well.

So, but as you get down to some of the other consequences of concern such as that latent safety security, there are -- I believe there are ways to do wireless there, but it's through very specifically -- it's with the specific controls in place, you know, very specific standards that you have to follow.

MEMBER BROWN: Okay, thank you.

MR. DOWNS: Okay, so I know this slide's a little hard to see, hopefully, you've got it in front of you, it makes a little easier.

Slide 18 shows how the controls provide a layered approach to security. This approach was specifically informed by the NIST framework from proving critical infrastructure which organizes a strategy for cyber security similar to the program performance objectives from the proposed rule.

Categories subdivide the objectives into outcomes closely tied to programmatic needs and particular activities.

Across the top of the table are 18

families that organize cyber security controls. Within each family are specific controls that may involve aspects of policy, oversight, supervision, manual processes, actions by individuals or automated mechanisms.

This table shows how the relation between the control families and the overall objectives. Notice how something like access control, which is under the performance objective, I'm sorry, the protect objective, is accomplished by controls from several different control families.

Performance specifications to achieve a defensive architecture are also provided by many of the controls -- are provided by many of the controls contained in the Draft Regulatory Guide.

On this table, each of the categories associated with a protect objective, align with a defensive architecture.

In previous meetings with the Digital Instrumentation and Control System Subcommittee, it was apparent that some members would prefer requirements prescribing a network structure that bakes in cyber security.

Unfortunately, requiring a specific network architecture does not address all cyber

security vulnerabilities.

The proposed rule adheres to the Commission direction of applying a disciplined graded approach for the identification of digital assets and a graded consequence based approach to their protection.

The proposed methodology also aligns with the industry accepted NIST strategies for protection which provide a hardened shell around networks.

Furthermore, fuel cycle facilities have business needs that are not necessarily conducive to the reconfiguration of existing networks.

The approach in DG 5062 would be less burdensome for fuel cycle facilities to achieve and has been demonstrated to be effective.

Obviously, there are benefits of having features like air gaps and network segmentation.

The Draft Regulatory Guide discusses how these features can be credited to address cyber security controls and the controls are designed to cover the spectrum of attack vectors in such a way that a layered approach to security would exist, including detection and response measures.

Are there any questions on the controls?

MEMBER STETKAR: Yes. This is a great

slide. It illustrates my biggest concern with this. This slide illustrates the mentality that, if you don't have enough boxes in a spreadsheet, you can get better security by subdividing the boxes. And, Appendices B through F support that notion.

I've got hundreds and hundreds and hundreds and hundreds of hundreds of things that I can check off and as long as I can find a box that I can check off, I'm good, by definition, because somebody else created those boxes.

If I don't have a box, I create another box.

So, how does this whole thing support a systematic assessment of risk? Checking off box mentality? And, as I said, one of these boxes doesn't fit it, I subdivide it so that I find enough that I can put a dot in it and, therefore, I'm good.

So, explain that to me. I've got pages and pages and pages of Bs and Cs and Ds and Es and Fs that got all subbed up things created by other people, the esteemed NIST folks who like to create boxes. So, tell me how this is promoting safety?

MR. DOWNS: Safety or risk, what are we talking about?

MEMBER STETKAR: Don't get me started on

risk.

MR. DOWNS: Well, you said risk, that's why I just --

MEMBER STETKAR: Okay.

MR. DOWNS: -- wanted to make sure that --

MEMBER STETKAR: How am I systematically identifying the risk for my facility by checking off these boxes? I'll just start there.

MR. DOWNS: You're not, not at all.

MEMBER STETKAR: Okay, thank you.

MR. DOWNS: The risk with the facility is informed by the other proposed requirements of the proposed rule.

We've already gotten -- once you're down to this level of applying controls, you've already established that there is a potential consequence of concern that cannot be addressed by an alternate means.

Therefore, it is very, very real that a cyber security -- that a cyber attack could cause that consequence of concern.

Therefore, how do you defend against that cyber attack? That's where you get into the boxes.

MEMBER STETKAR: By checking off boxes?

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

methodology that NIST has put out there and it's been proven to be effective.

MR. DEUCHER: And, again, this is Joe Deucher with ASLBP.

When you talk about the boxes themselves, the details that are in each individual box, it corresponds to a potential threat that exists, a method of attack, a way to defend yourself, a way to ensure that the measures that you put into place cannot be compromised themselves, that you can ensure their accuracy, whether it be through, as examples, audit logs, access control.

Again, it's the detailed specifications of what I need to meet in order to defend myself. So, we're getting really into the technical details.

MEMBER STETKAR: And, that's my whole point, Joe, is that, if you keep subdividing boxes small enough, you can eventually find a box that you can put a dot in, but you've kind of lost the big picture, maybe two boxes would have been enough.

MR. DEUCHER: Well, in one respect, and the point is well taken, in one respect, when you go back to the left side of this, that's really where --

MEMBER STETKAR: Right.

MR. DEUCHER: -- you see the program

activity and that cross, is what we're hoping that -- and our goal with the rule itself is for the licensees to be focused on that, that overall, from a programmatic standpoint, that you're looking across the entirety of your facility. You're looking at these consequences, you've identified the areas that there are issues and you're looking at it from that 10,000-foot view.

But, then, at the same time, you're able to drill down in and when you're actually getting into the nitty-gritty of protecting a particular vital digital asset, that you're also looking at the individual elements that you need to have in order to effectively protect it.

So, it's like we have two different levels of processes going on at the same time. Something very, very detailed, but at the same time, in order, to your point, not to lose sight of the big picture of addressing the consequences, addressing the risk and making sure, going forward throughout the life cycle of these devices or as well, the life cycle of my process, that I am ensuring that I'm not missing something.

And, we feel confident that what we've put together covers both. And, it's also nice that it's

aligned with where industry is today, where industry sees itself going tomorrow in order to ensure that you're protected against an attack.

MR. DOWNS: And, the other thing to point out, too, is that a single measure may address multiple cyber security controls.

For example, I know in the Subcommittee meetings, we've talked about, you know, that standalone networks, we've talked about, you know, isolation and network segmentation.

Those features may address multiple performance specifications in the controls. So, it's not that you have to have for each box that a control has got that you have to have a unique measure to satisfy that box.

So, you may be -- and the Draft Regulatory Guide goes into how that -- how you can credit multiple measures with certain elements of protection.

MEMBER STETKAR: I mean, I don't -- I'm not familiar with the facilities. I'm not familiar with how people are proposing to implement this guidance, my concern reading through it is that the guidance could be interpreted as promoting kind of a checklist mentality where people have so many things that look like this, that they focus most of their

effort on trying to find a box to put a dot in without doing the sort of things that you just said orally.

Stepping back and saying, well, you know, looking at the facility and saying, I have various, I'm going to call them vulnerabilities, how can I best solve this problem rather than saying, well, I've got a dot in this one, this box for this one and I've got a dot in this other box for this other one and as long as I can find enough dots in enough boxes, I'm, you know, by definition, I'm okay.

MR. DOWNS: And, I think for what you just --

MEMBER STETKAR: That's the concern.

MR. DOWNS: But, what you just pointed out there is one of the reasons that cyber security professionals are very well paid because they save -- they can save significant, you know, money to who they're working for by knowing -- by keeping that higher level perspective and being able to apply, you know, certain features of protection to multiple controls.

MR. DEUCHER: And, specifically in the rule, that's where, when we talked about the -- and I may be jumping ahead, the configuration management and the overall life cycle management aspects of the rule,

that's where we see being able to refocus this to that level where we're looking at risk, we're looking at consequences, we're looking at, as we're making changes to the plant, taking a step back and saying, okay, how does this affect our cyber security?

How does this affect what we've done thus far and what changes do we need to make or do in terms of actions or specific measures in order to keep the level that we've established going forward?

So, it's our goal with the mix that we have in place that they're able to take care of the detailed aspects, but at the same time, be looking strategically at their cyber security to be able to maintain effectiveness. At least that's the hope.

MR. DOWNS: And, in addition --

MEMBER STETKAR: Well, yes, sure. Obviously, it's the hope. Again, the devil's in the details and as long as the guidance -- I don't see the guidance necessarily keeping the focus at that level simply because of all of the boxes, if you will.

Anyway, that's enough, you know, it's --

MEMBER SKILLMAN: Yes, I'd like to join John Stetkar's comment from a little different perspective.

Forty-six years ago, the NRC required

licensees to develop a QA program. Before about 1971, there wasn't one.

And Appendix B to 10 CFR 50 was promulgated and all licensees were required to develop a program.

And, for those who were there before and after, in the after environment, the organizations started with two and then four and then ten and then 15 then a 100.

It began with good intention and I don't for instance suggest it hasn't earned its pay, it has. But the cost was huge, raising the question, what's the value?

Another example, there was a time many years ago, when you went to a nuclear power plant, you would have three operating teams or four operating teams, depending on how the shifts were organized.

There was a maintenance team. There was an admin team. And, there was a relatively small security team.

And, if you go to one of the plants today, you will find that that security team is one of the largest organization on site. It's a consequence of our culture and the consequences of how we've chosen to defend these plants.

So, we started with the security plan that grew and grew and grew and grew.

With each one of these boxes, each one of these blocks, there's going to be a man or a woman who's going to have to sit down and make an evaluation, go after almost every digital device in these classifications of plants.

I agree, that work has been done in many cases. But, this is going to be a huge administrative burden. And, I have hunch, based on what I've seen in my career that this will only grow because the digital threats continue to grow and to be more complex.

So, here's my question, what conscious or what conscious thinking has gone into how to reign this in, how to prevent this from becoming an exponentially growing issue for the people that have these assets?

What is being done to say, how do we contain this and prevent this from continuing to become a larger and larger and perhaps unmanageable juggernaut?

MR. DOWNS: So, the key with this proposed rule is in the consequences of concern. A digital asset is not required to be protected unless it has a consequence of concern and there is no alternate means

creditable to prevent that consequence of concern.

The feedback that we've gotten is that most licensees are going to have very, very few vital digital assets.

I don't think that -- I'm sorry.

MEMBER KIRCHNER: The danger is that, I'll say it for the record, that you encourage a response that games the system and deflects from the mission that you want them to accomplish which is to, whether we're going to call it safety or risk, that should be the framework that you do this within, not a box chart like this.

I would like to observe that the word governance shows up under identify. I don't know why it's there. Governance usually means management. And so, management will look at something like this and they'll say, low and behold, I'm responsible for governance and there's a dot for every little box there.

So, I better put together a plan that goes from access control to systems and information integrity.

Then, as management, I would have exercised good governance because I've checked all those boxes.

I'm very perplexed with a chart like this.

MR. DOWNS: The chart, just to -- oh, go ahead.

MR. DEUCHER: Yes, so, two parts to that. Okay? The gamesmanship, as you talked about, the -- a vital digital asset would, as defined by the rule, the proposed rule, a vital digital asset would have a consequence of concern and is susceptible to a cyber attack. So, therefore, the staff feels like it should be protected.

If it's not a vital digital asset, it is inherently protected from a cyber attack because no consequence of concern could result from that cyber attack, whether an alternate means has been credited or whether that digital device has no consequence of concern.

So, therefore, the objective of this rulemaking is to protect digital assets from a cyber attack. Thus, it's protected.

MEMBER KIRCHNER: I agree. And, what you said verbally is good, no disagreement from me. But what this chart infers and what I think my colleagues are leaning towards is that this drives you to an administrative bureaucratic response rather than a focused response on the key assets that you're trying

to protect.

MR. DOWNS: You don't even get to this chart until you have a vital digital asset. There are no cyber security controls for assets that are not considered vital.

MEMBER KIRCHNER: Okay. So, let's assume I have one, then I assume I'm management. Management is responsible usually for governance.

I see a dot on this chart for every control family.

MR. DOWNS: That's correct.

MEMBER KIRCHNER: So, basically --

MR. DOWNS: Governance -- I'm sorry.

MEMBER KIRCHNER: -- you're saying, I have this digital -- maybe it's a simple controller on a chemical process line, so I need to go through this table from alpha to omega, that's essentially what you're implying by having a chart like this.

MR. DOWNS: So, you will not find this chart in our Draft Regulatory Guide. This chart was intended to facilitate discussion at this meeting.

MEMBER KIRCHNER: Well, it has then, thank you.

(LAUGHTER)

MR. DOWNS: And, just to be clear on

governance, the terminology reflected in the category column of this chart is terminology that is specific to NIST.

MEMBER KIRCHNER: That's right.

MR. DOWNS: The NIST term of governance is applicable to each of the control families and, by that, it's a written procedure or policy that overall addresses that control family.

Again, our specific controls speak to those policies and procedures. So, therefore, that concept of governance applies to every control family. However, it basically means that you've considered it in the NIST framework.

Joe, do you want to expand on governance at all?

MR. DEUCHER: Right, exactly. I mean, IT governance is just that, it's the policies, it's the procedures that you would have as associated with an individual system in the NIST parlance.

Again, in our parlance, it's vital digital assets.

This chart that you're looking at was our effort to show that, based upon our conversations from the digital instrumentation and control subcommittee that the notions of defense of architecture, defense

in depth, those concepts are inherent in the individual controls, the performance measures, if you will, that we're looking that licensees would apply to their various activities and devices that they're going to put in place in order to develop cyber security protection.

The chart itself, if you look to the left hand side, that's the part of the NIST cyber framework. So, that's the --

MEMBER KIRCHNER: I'm aware of that.

MR. DEUCHER: Right. And so, specific in our rule, we've taken, identified and made it a great portion of protect. We have detect and respond. We don't deal with recovery as a part of our rule.

So, but the intent of this was just to show that the notions that came out of the Digital Instrumentation and Control Subcommittee meetings, we've considered them, but they are in place at a detailed level in our document in the appendices.

The idea being that a licensee could go ahead, whether they're using our controls, whether they're using their own controls, something associated with NIST or derived from another certifying organization, they'd be able to come up with the same levels of protection that address the same concerns

that were raised in the Subcommittee meeting.

We were just trying to put it out here in a graphical format. Because, again, the idea of behind our controls is that there are these various areas of threat that the different control families address and the threats addressed by the control families then cut across the different things that a licensee could do, whether it be actual actions, whether it be physical components that they would put in place or procedures that they would do.

So, again, it's this integration between the two that we wanted to show. And we wanted to show that it was in there.

MEMBER KIRCHNER: Thank you.

MEMBER SKILLMAN: I would like to get my question answered. My question was, was there a conscious effort to contain the expansion of this? In other words, going in, was there the view or a guidance to the individuals who are involved that was in some, let us be careful we don't let this thing become so large that its value is no longer returning a reward?

MR. DOWNS: I apologize, Mr. Skillman, I did get sidetracked there.

So, to answer your question directly, yes,

there was a conscious effort. The conscious effort was in limiting the number of vital digital assets, identifying only those requiring protection -- cyber security protection only for those vital digital assets that would have a consequence of concern, right, that's the definition of vital digital -- consequence of concern and no alternate means of protection.

So, therefore, if you're looking at is the protecting strategy, was that out of control? I don't feel that -- I think the protection strategy as we've been discussing here is geared to each of the specific attack vectors that could be present to that vital digital asset.

It's a methodology that is accepted industry wide from a cyber security perspective and it has been endorsed by, you know, obviously, Executive Orders as well as, you know, different standard bodies that have taken this NIST approach and put it into use.

So, that's -- we feel like we've limited it. The application of the protective strategies and the strategies are each -- each of the strategies adds value because they address a specific attack vector that could be present.

MEMBER SKILLMAN: Thank you.

MS. MAUPIN: This is Cardelia Maupin, I'm with NMSS Rulemaking Group.

And, as a part of this rulemaking, we've conducted over 11 public meetings. And, a part of those public meetings, we looked at the controls. And, I can tell you that, when we first started this effort, there were a whole lot more.

And, we heard from the stakeholders and their comments. And, we've tailored back.

And so, what you're seeing today and what James is trying to explain to you is that, we have, you know, heard from our stakeholders and we believe we have appropriately, in most instances, reflected that input that we got from them.

And, our stakeholders have indicated that they appreciated the large number of outreach activities that we've had on this rulemaking far greater than any other rulemaking that we've had.

I just wanted to put that on the record.

MEMBER SKILLMAN: Thank you.

MR. DOWNS: And, just to add on to what --

MEMBER SKILLMAN: Thank you.

MR. DOWNS: -- add on to what Cardelia said there, we anticipate that there will continue to

be a tremendous amount of interaction with the stakeholders.

And especially on the controls, the staff is committed to providing, assuming the approval to publish the proposed rule and Draft Regulatory Guide is granted in the Federal Register -- you know, publication of the Federal Register Notice, we will continue to have that outreach and we are committed to, again, seeking more feedback on the controls.

And, there's going to be a lot more discussion about this.

The whole point of this proposed rule, again, is to solicit that sort of feedback.

CHAIRMAN BLEY: James, I'd like to weigh in on this just a little.

When I read through the appendices, I looked at them as if I've done a top level down approach and I need to develop controls for a particular asset, this is kind of a laundry list of things I might do.

When I look at the chart you brought with you, it kind of implies one has to go through all of these things and do lots of this.

I don't think that's the intent. This chart is very uncomfortable, and one can find places

where there are interactions among things all over it that one would question.

I think it, for me, it adds more confusion than help.

But, if the intent is what I suggest, that could be made more clear if the intent is, as was discussed by several members earlier, that once I have identified an asset, I have to go through all of these and do them all, that's an unworkable situation.

And, if the impression is that, for several of our people, the impression is bound to be that for others.

So, you know, if you can make that clearer.

MR. DOWNS: Sure. So, again, I'll emphasize that you will not find this chart anywhere in the guidance document.

MEMBER STETKAR: James?

MR. DOWNS: Go ahead.

MEMBER STETKAR: Right, you've emphasized that. So, if I'm a Category III facility, as I understand the guidance, I must go -- use Appendices D, E and F for my controls. You don't have to look it up, it's in there.

That's on all facilities, so I'm a

Category III facility, I'm not a I or not a II.

MR. DOWNS: That's right.

MEMBER STETKAR: And, if I count up the number of controls in D, E and F, I come up to 212.

Back in November of last year, I asked you specifically the question that Dr. Bley just raised. Do I now need to go down through each and every one of those 212 controls and justify whether I applied, whether I didn't apply it, why I didn't apply it?

The answer at that time was, the intent is that I must address each of those potentially applicable cyber security controls and explicitly document why I applied it directly, why I may have tailored it or did not apply it to each of my critical VDAs.

And, if that is the intent, that's the checklist mentality that I'm concerned about.

CHAIRMAN BLEY: And it becomes unworkable.

MEMBER STETKAR: It's unworkable.

CHAIRMAN BLEY: And it becomes such a mass of documentation that nobody can find --

MEMBER STETKAR: So, if that's the intent on the record from our Subcommittee meeting in November that doesn't seem to be the intent that you're trying to portray today.

MR. DOWNS: So, you emphasized -- you stated there that Appendices D, E and F, E and F are specific to two different consequences of concern.

So, yes, you're correct that D would be applicable to all vital digital assets at a Category III facility as it would be in all facilities.

Appendix B is applicable to any vital digital asset.

The appendices -- the other two appendices you referenced, again, since they're specific to consequences of concern, you would only be applying one of those appendices --

MEMBER STETKAR: Okay.

MR. DOWNS: -- to. So, but I can't really --

MEMBER STETKAR: Reduces it to 50 or 70 or 80 or something. So, either I have a 133 or I have 127, if I've added -- close enough.

MR. DOWNS: But, you are correct that each -- you would have to go through, and as we stated in the Subcommittee, you would have to address each of the controls and document how it's been addressed. That's correct, that is the NIST approach to cyber security.

MEMBER STETKAR: That's the agenda.

I just wanted to make sure that hadn't changed.

MEMBER SUNSERI: One question over here.

CHAIRMAN BLEY: Reminiscent of the FME approach to safety. That's troublesome.

Go ahead.

MEMBER SUNSERI: Yes, I suppose if I went through my review of all my assets and I identified a vital digital asset and was faced with doing these appendices and controls or providing an alternate means of protection which would eliminate it from being a VDA, right, then that would be satisfactory compliance with the rule?

MR. DOWNS: Absolutely, 100 percent.

MEMBER SUNSERI: Okay, thank you.

MEMBER BALLINGER: Yes, along those lines and with respect to what Dick was saying, there's a fundamental difference between Appendix B and this.

Appendix B is now fixed, this is going to be evolving forever because the digital threats and things like that are also evolving forever.

I mean, my idea of a digital -- critical digital asset is my computer, my TV and my sprinkler system for my lawn, and I get updates for security about once a week on all of those.

And so, I think that what might happen is that what Matt was saying is that people will look at this and say, holy mackerel, I'm going to find a way, an alternate protection method. And, that takes all this off the table, is that right?

MEMBER BROWN: Well, it all depends on what's acceptable as an alternate method.

Mike, go ahead, yes, I'm going to finish up here when you're down.

VICE CHAIR CORRADINI: No, I was going to at Charlie.

So, I have not, I didn't attend the Subcommittee meeting, but I've just been watching the interaction.

So, does the Reg Guide give examples of alternatives?

MR. DOWNS: Yes.

VICE CHAIR CORRADINI: Can you give me one?

MR. DOWNS: Sure.

VICE CHAIR CORRADINI: Because I started in the business about the time of Appendix B QA and I avoided QA for the very reason that it became a checkbox mentality.

So, what are some examples that you would

avoid doing this?

MR. DOWNS: so, say if I've got a process that could potentially, that the release of the chemicals in that process could potentially cause a consequence of concern.

On that process line, there are various pressure temperature controllers that are digitally controlled that have an interface that could potentially be accessed via cyber attack.

The over pressurization of that system, again, causing the release, you could have some sort of a containment around that system that could be a physical containment that could be credited as an alternate means.

So, regardless of whether or not, you know, the cyber attack causes that over pressurization to occur, you've still got that containment structure in place.

So, therefore, you know, whether it's a tank or whatever it is --

VICE CHAIR CORRADINI: Okay.

MR. DOWNS: -- you would credit that as an alternate means.

VICE CHAIR CORRADINI: So, but if I were to reverse, I mean, again, I don't know any of this,

so I'm just watching you guys go after the discussion.

If I -- if the real threat is the fact that I'm communicating with the outside world, isn't the easiest thing to stop communication with the outside world, period, end of story? Am I missing something?

MR. DOWNS: So, that's one attack vector. Another attack vector could be that there's portable media that's placed on to that digital asset and so that you could, you know, if you have portable media coming into the site, that portable media could be the conveyance method for the attack as well.

VICE CHAIR CORRADINI: Okay.

MR. DOWNS: So, it's -- there are several different attack vectors to consider here.

MR. DEUCHER: Oh, and just to clarify, for some of the licensees, they do need network communication with the outside world just to do their business, especially in the area of the Category III of the fuel fabrication facilities.

So, it's almost a situation where they can't get around it. They would have to deal with having communication with outside vendors, suppliers and customers.

VICE CHAIR CORRADINI: Sorry, this is the

Subcommittee discussion and Charlie will tell me to be quiet eventually.

But, communication with the outside vendors and things doesn't mean that I'll allow people to get in and noodle with my processes.

MEMBER BROWN: Only if the circumstance occurs if you co-mingle your process with the business process that's on your network.

VICE CHAIR CORRADINI: Fine, okay, okay, fine. Thank you.

MEMBER BROWN: So, let -- I'm going to try to categorize this a little bit based on all of this discussion.

And, I don't -- I'm not asking anybody to agree with me or disagree, I'm going to merely present my thought process.

MEMBER STETKAR: Charlie, before you do that --

MEMBER BROWN: Yes, go ahead.

MEMBER STETKAR: Can I ask --

MEMBER BROWN: Go ahead.

MEMBER STETKAR: You mentioned earlier, I think, that during your meetings with the various stakeholders, that they've indicated that the vast majority of -- or they're -- let me see if I can

recall the discussion, that they have indicated that they will be implementing alternate means.

Do you have any sense whether those alternate means are in your simple example, if your design hardware related alternate means, you use, you know, a confinement as one approach.

Or, are they approaching it by people, do you know?

MR. DOWNS: So, based on the site visits that the staff has done and just some of the sense of -- obviously, the analysis hasn't been done by the facilities.

MEMBER STETKAR: Yes.

MR. DOWNS: So, the sense that we're getting, it's a combination of both.

MEMBER STETKAR: Okay. See, I draw the analogy between this and the problems that we've been facing in fire protection for commercial and nuclear power plants for along time. People couldn't meet the regulations.

So, you found people standing around staring at cables all the time. You know, they addressed it on a people problem and that was judged for a long time to be an acceptable interim alternate means, if you will.

People have now done more comprehensive evaluations as part of their risk informed approach to fire protection.

And, in many cases, they stepped back from those things and said, hey, we can solve a heck of a lot of these problems by putting in a creative alternate system for cooling the reactor coolant pump seals, for example.

We didn't necessarily recognize that when we focused at each individual cable where we had somebody staring at it. But, when we stepped back from the whole problem, it was more effective to use this more global solution, if you will. And, that's good.

So, I was just trying to get, you know, just saying that, well, people are going to take an expedient way of providing alternate means and those are manual actions or additional increased training and oversight or having two bodies to stare at a cable or something like that doesn't necessarily solve the problem.

That's why I was trying to get a little feedback from what you've heard.

MR. DOWNS: Right. So, one of the benefits of the guidance, and I know you brought that

up in the Subcommittee meeting as well, and we have included some of the considerations of manual actions.

And, but again, the flexibility that the proposed rule would apply is that a licensee could address that situation, they could address alternate means in numerous ways.

The key with an alternate means, and it's defined very clearly in the proposed rule, is that it's -- it prevents the cyber attack from causing a consequence of concern.

MEMBER STETKAR: I'm sorry, Charlie, you can summarize now, I'm done.

MEMBER BROWN: Yes, okay, let me -- I'm just trying to put this back in my own, you know, particular thought process is that, the whole issue involved in all of this is fundamentally comes down to control of access, to the whatever is inside the plants.

There's two means of control of access, external or just internal. If you exclude one, then you've simplified the process to -- for instance, if you have no remote connections then you submit it, you've simplified the process to only have to deal with internal controls.

MEMBER MARCH-LEUBA: Yes, Charlie, I have

a --

MEMBER BROWN: Let me finish.

MEMBER MARCH-LEUBA: -- offering an opinion.

MEMBER BROWN: Let me finish, you can have whatever opinion you want, I'm telling you want mine is.

When you get down to internal access, then it's a fundamentally a matter of configuration management and control of access to those assets which have to be managed for the configuration whether you bring in portable media who can go use that portable media on the specific process, asset that you're dealing with.

So, if you look at it from a top level down as opposed to the micro piece level up, there are ways to reduce the burdensome nature of what you do.

Controlling somebody's access to changing the configuration of a particular process computer or a network internal to the plant is far easier than trying to protect yourself against every external cyber threat.

You've provided two examples in your regulatory analysis about recent cyber attacks. One was with a utility, I believe a water utility where

the conclusion when they finished for the people they brought in, the utility brought in, was they violated some very, very specific circumstances.

They did not -- they had everything connected externally. They co-mingled supervisory and scata type systems or supervised control systems, with their business systems and everything else and their conclusion was they should have isolated all of those.

One of the other ones, they -- and they weak authentication mechanisms even on the internal stuff.

For the other example, the fundamental issue was they were trying to control substation operations in an electric utility and they noticed that they were getting some unusual results.

And, again, they had passwords that were sitting right on the network, unencrypted passwords is the way I read it.

So, I mean, your examples in the regulatory analysis, you made it more crisp to me in terms of looking at this in that some allowance for a more top down approach as opposed to a I have to evaluate each and every detail within the threat vectors from external, which are very complex and lead to the very things that Dick and others have talked

about in terms of how do you protect those.

Because, I mean, I can't even use my laptop that NRC gives me if I don't have it being updated everyday and I'm not even here every day. It keeps getting locked up on me and I have to call in and spend an hour and a half on the phone with their IT services trying to get it updated.

MR. DOWNS: It's controlled your access --

MEMBER BROWN: They've controlled my access, exactly right.

(LAUGHTER)

MEMBER BROWN: So, I mean, fundamentally, you know, we've made this thing complex and I think you run into the circumstances we're trying to document and trying to constantly update all these processes because you allow all these types of access.

And, I'm not saying you need to exclude them, my only point being the Reg Guide and the rule should be more open to allowing a vendor or a manufacturer to put a giant bubble around something, whatever it is, because controlling access --

And, I know in my program, when I try to control access to the reactor plant stuff and everything else, we don't allow any access. And, if the person goes down to work on the cabinet, they've

got to open it up. They've got to have somebody standing by and so it's a simple procedure. It's not complex, you know, assessments of 120 controls that you had listed in one of these appendices.

And, that's where my basic hangup has been with this. I don't disagree with the need for a rule, it's a matter of how the rule is configured and how the industry is required to comply with that rule.

So, anyway, I'll finish, that's my little summary.

Now, Jose, fire away.

MEMBER MARCH-LEUBA: I was waiting for you to turn off the green light.

MEMBER BROWN: Oh, okay, I'll turn off the green light.

MEMBER MARCH-LEUBA: Okay. I want to offer a dissenting opinion. I mean, controlled access is very important. It is crucial, but it's not the end of it.

The bad guys are extremely creative, they are very, very, very smart guys thinking about ways of bypassing people.

And, this is what Appendix B is trying to say. I mean, I'm really in Appendix B and this is the way you will set up your network if you thought of

setting up a network. You wouldn't do it any other way.

Because, you have to have defense in depth. You have controlled access. You have authentication, but you also include all the other things.

You have to ensure that the Java update gets pushed when the Java update needs to get pushed. Better yet, you don't have Java if you don't need it.

And, that's what Appendix B says and it's a complex thing and that's why they pay IT guys their money.

But it needs to be then, so I don't see the complexity to this.

Back to Dick's comment, the response are very ecstatic. Response won't change.

Appendix B is a big problem with -- because the purchasing of stuff all the time. Once they do their cyber security for a plant, it's going to stay like that until they have to change the Windows desktops for Macs.

And, at that point, you're going to have some process that ensures that those Macs don't have the Java updates in place.

So, I don't see this as a tremendous

imposition on the facilities. I mean, they need to have it.

MEMBER SKILLMAN: I would simply respond that the sophistication of the threats coming in over the threat vectors continues to change.

And, as you point out in your own words, the sophistication increases. And so --

MEMBER MARCH-LEUBA: And --

MEMBER SKILLMAN: So, this becomes quite candidly a game of protection needing more protection needing yet more protection.

MEMBER MARCH-LEUBA: I'm familiar with one of these plants, there are two guys sitting in that room doing this job and that's their job and they're not going to fire them. They're going to have two guys, but there are never going to be 200.

CHAIRMAN BLEY: Charlie, I'd like to clarify something that I said earlier, clarify my optimistic reading, support John but also support what James said.

The Section 7.2 of the guidance is, in fact, very clear. It says, we've got these appendices. If you decide to use those, then for each applicable appendix, you have to do each of the things that's there or say why you don't.

Alternatively, if you don't use those appendices, you have to set up performance specifications of the controls that you're proposing that will detect, protect against and respond to cyber attack.

So, it's pretty clear and it gives you a pretty clear option and I guess, depending on your own sophistication and how risk thinking you are oriented and how checkbox oriented you are, you can take your choice.

MEMBER STETKAR: And, whether you can convince the regulator that your alternative --

CHAIRMAN BLEY: That remains to be seen, yes. But, you can put -- but you need to put together a darn good argument for that.

MEMBER STETKAR: That's right.

MEMBER BROWN: I won't disagree with this. I agree totally, but 7.2 does that and I did not bring that up because, if you -- when you read 7.2 and you contrast it with what the rule says in terms of digital assets, there's no differentiation.

I mean, the rule talks about digital assets and critical and vital digital assets. And that some other alternative that doesn't agree with the rule cannot be subsumed by the Reg Guide.

That's what I've been taught the last nine years, that the Reg Guide is guidance but you're trying to override the rule by doing something --

CHAIRMAN BLEY: But, you can't override the rule, period.

MEMBER BROWN: That's my problem, is the rule specifies addressing digital assets and does not include some allowance for some other methodologies as --

CHAIRMAN BLEY: The rule doesn't tell you how to do it, though.

MR. DOWNS: It doesn't, that's true. That's a very true statement.

MEMBER BROWN: I'll go back. It depends on how you want to interpret the words that say identify digital assets that, if compromised, would result in a consequence of concern. Very specific.

CHAIRMAN BLEY: Yes, but it doesn't tell you how to do it.

MR. DOWNS: It doesn't tell you how to protect them, right, it says the controls or establish controls, it doesn't say what those controls --

MEMBER BROWN: In ten years, I bet you if you try to run that one by the NRC and you'll run into a giant stone wall. Because I've -- it's this

accretion of what's expected as you go forward.

I'm just concerned about that. I've given my opinion.

CHAIRMAN BLEY: Indeed.

MEMBER BROWN: And, I'm very sensitive to the fact, I've watched this type of stuff grow until it's out of control. I saw in some areas of the program I was with, it was 17, you know, 18 years ago and I tried to eliminate that and get it down to the simplistic stuff when I had to apply these systems in the ships and go upgrade them.

And we had no remote access. We didn't allow them to do it any other way and --

CHAIRMAN BLEY: If one of the guys running one of these facilities does what you said, he doesn't have any. I hope that -- that's not easy.

MEMBER BROWN: Hope springs eternal in the human breast. And, right now, my hope is not very -- I'm not very convinced that that hope is allowable.

It's a great discussion. I mean, this was the purpose, one of the reasons I wanted to get here today and infect everybody was to ensure we had --

CHAIRMAN BLEY: You'd better be careful next month.

MEMBER BROWN: Yes, that's all right. I'm

working hard, if I pass out, just pour water on my head.

MR. DOWNS: I may not make the next meeting. I don't know which way to lean.

MEMBER BROWN: But, I wanted to ensure that we had this general discussion as part of this because I think it frames the overall Committee frame of reference as to how we'd like to go forward with this and without the spirited discussion which we've had so far, I don't think we would have -- the members who have not been on the Subcommittee, I don't think would have had a full appreciation of what we went through during the Subcommittee meetings which were very, very useful in terms of starting to get this issue in focus.

So, James, go ahead. Nobody else has any more, I think we're finished with this particular approach and let James go ahead and finish up.

MR. DOWNS: Okay. So, slide 19 provides and overview of Appendix G of the Draft Regulatory Guide.

Appendix G contains an example that demonstrates implementation of an acceptable cyber security program, including identifying digital assets, determining whether those assets are vital,

defining boundaries for vital digital assets, addressing the controls and performing configuration management.

In each step of the example, there are examples of acceptable documentation provided.

Feedback from the Digital Instrumentation and Control Subcommittee was used to develop Appendix G.

Also, the staff believes that this appendix, when used in tandem with the guidance in the body of the Draft Regulatory Guide clarifies the level or burden for many of the proposed program requirements, especially for the identification and screening of digital assets.

Are there any questions on Appendix G?

MEMBER KIRCHNER: Just, on that example, James, I'm thinking about your alternate means. You suggest there that you have a vital digital asset. It's controlling a process, the disruption of that process could lead to radiological or safety consequences.

Then you say, if you have a containment around it that is not controlled by a digital asset, if that could be designed, I don't know, that that would be acceptable.

But, is that, in reality, is that actually going to pass muster?

MR. DOWNS: It would -- a lot of facilities have these sorts of items relied on for safety already in place.

MEMBER KIRCHNER: Yes, I know, most of the facilities have.

So then, and I'm struggling why we're going through this exercise.

MR. DOWNS: Because, for some digital assets, those having a consequence of concern, they may not have those -- that defense in depth measures in place or those items relied on for safety that they can credit.

So, therefore, if they can't credit those alternate means, as we referred to them, then they would be required to provide protection from a cyber attack.

MR. DEUCHER: And, it also takes into the account the fact that, as modernization were to occur, as they may be replacing parts going forward into their facilities, a lot of this stuff is going to go from analog to digital, especially with things like the Internet of things, these, you know, sensor associated components that can talk to one another in

order to tell their health and status, it's going to create the possibility for there to be openings for potential cyber attack as modernization happens.

MEMBER KIRCHNER: You really think somebody is dumb enough to connect into the Internet of things or the cloud to run their processes?

MR. DEUCHER: Well, it's not necessarily --

MEMBER KIRCHNER: You've got to be kidding me.

MR. DEUCHER: It's not necessarily the Internet itself, it's the fact they are -- they can talk to one another inside the facility. And, actually, I'd rather not discuss the vulnerabilities that we've observed --

MEMBER KIRCHNER: I agree with you.

MR. DEUCHER: -- with some of that stuff.

MEMBER KIRCHNER: Yes, oh, okay, I'll drop it, too.

But, what I was searching for was, when you integrate this with your defense in depth for your standard safety analysis for the plant, I would just personally treat the digital asset that controls the process that might lead to a vulnerability as under that -- examine it under that and treat it accordingly

without having a separate rule.

Thank you.

MR. DOWNS: And, that would be one approach. However, the current regulations do not require the safety analyses to include malicious actors in as part of that analysis.

So, therefore, this is where the proposed rule is coming from.

MEMBER KIRCHNER: And, we're skirting something, but I'll just submit that any good safety analysis would figure out that they had a vulnerability whether it was malicious or not.

MEMBER BROWN: You want to go on, James?

MR. DOWNS: Sure.

MEMBER BROWN: Okay, please.

MR. DOWNS: Okay, last slide here.

In conclusion, the proposed rule would provide risk informed performance-based requirements that promote common defense and security and provide reasonable assurance that public health and safety remain adequately protected as the risk and complexity of cyber attacks continue to grow.

Furthermore, the proposed rule would also promote clarity, effectiveness and openness in the regulatory process by providing the opportunity for

formal comment on a transparent and comprehensive regulatory framework that fuel cycle licensees could consistently implement.

The staff looks forward to the ACRS letter regarding the proposed rule package and Draft Regulatory Guide.

Obviously, we hope that the Committee will endorse the publication of the documents for formal public comment, but I'd like to thank each of you for reviewing this action.

I have firsthand appreciation for the depth and breadth of the information provided. So, speaking on behalf of the NRC staff, we sincerely appreciate your time and feedback.

With that, I conclude.

MEMBER BROWN: Okay. Are there any comments from the public in the audience? Yes?

Go to the mic and give your name, please.

CHAIRMAN BLEY: Name and affiliation.

MEMBER BROWN: And affiliation, thank you very much, Dennis.

MS. SCHLUETER: My name's Janet Schlueter from the Nuclear Energy Institute and thank you for the opportunity to comment.

MEMBER BROWN: Oh, hold it. Can you tilt

that? Yes, that's fine, try to speak a little louder for the transcript. Tilt the mic up towards your mouth a little bit.

MS. SCHLUETER: I'm Janet Schlueter, is that better? Okay. From the Nuclear Energy Institute. Thanks for the opportunity.

And, I would like to say thank you to the NRC staff, as Cardelia and others mentioned, we have had several public meetings.

But, more to the point, thanks for releasing the seven documents in advance of this meeting publically because it gave us a chance to take a look at where the staff is, how the thinking has or has not evolved, if you will, since we last saw these documents back in February.

And, it is an exhaustive set of information. And so, we've had to, you know, pour over them as you have in the last week or so. And so, we've just made some preliminary observations.

First of all, I'd just like to reiterate, as we have said before in our other, you know, earlier letters to you and to the NRC staff that, cyber security is clearly an extremely important aspect of our safety and security programs.

These facilities have corporate cyber

security programs in place so not only do you have corporate programs which are there for business continuity purposes and protection of their assets and programs, but the CAT I facilities are subject to the DOE accredited program, some of which we've discussed.

And then, of course, now you have the overlay of a potential NRC rule.

So, we have lots of things sort of at play here and we spend a lot of resources, you know, in the cyber security arena today.

We have reviewed, as I mentioned, just the documents that were released. We do have some preliminary concerns.

I think that we have found that the concerns that we've expressed in our recent letter to -- or our October 2016 letter to the Committee remain. There's nothing new there as far as our concerns regarding policy issues that need to be resolved prior to the staff sending this paper up to the Commission.

And, I'll touch on a couple of those just briefly.

I think the best way to maybe demonstrate our concern is to go back to slide nine which has the chart there on the consequences of concern.

So, while as Mr. Brown indicated, we don't

really see much change in the rule language or scope. The Reg Guide is voluminous. It seems to be growing to some degree.

We have a cost estimate to try to implement this rule that far exceeds what the staff has estimated. And, one might say that perhaps we even low balled it now that we're continuing to get further insight into the Reg Guide and consider how it will be implemented.

So, the cost is quite high, we estimate, to implement this rule.

But, more fundamentally, if we look at that top box, I think this is where our position on this rule and the need for this rule just fundamentally, we are in a different place than the staff is.

And, this is where the essence of our differences lie. And, what I mean by that is that, through Part 70 rulemaking about 17 years ago, and even through the post-9/11 security orders, the staff and the Commission made a determination that the regulatory framework is really focused on the DBT and the fact that the CAT IIs and IIIs which fall into the next three blocks are not required to protect those assets from a physical attack.

So, in this rulemaking, the staff is actually sort of expanding that regulatory footprint, expanding that scope such that cyber attacks are being protected against in a manner that is different than the regulatory framework that's been previously established for physical attacks.

Okay? So, regardless of the initiating event, we do not believe that this rule should go beyond that top box, the design basis threat. And, that is the CAT I facilities.

Based on fundamental principle and policy that the Commission has a regulatory framework in place that has identified the primary consequence of concern as the DBT.

Now, those facilities, CAT Is, have DOE programs in place. The staff has acknowledged that they will recognize or accept the DOE classified programs. They're working on the unclassified piece.

We appreciate the staff moving in that direction, the progress that they're making in that area. But that the jury is still out. That question is still open.

I think what we're discouraged by is a couple of things.

One, that the policy issue of this very,

very principle, very fundamental regulatory framework issue is not going to be resolved or isn't being really fully vetted with the Commission before this rulemaking proceeded.

In other words, the staff is going to have to put up to the Commission a paper that involves a very fundamental policy question that could, in fact, change the scope of this rule dramatically.

And, as I know you're aware of and is in our letters, I'll remind you of a Petition for Rulemaking that NEI filed on behalf of the power reactors that has the same fundamental policy issue addressed in it.

And, the staff acknowledges that, if that Petition for Rulemaking on scope for the power reactors is granted, they will have to make a determination as to how and whether the scope of this rule would be impacted by that petition resolution. Assumably, it would be narrowed in scope.

Now, in my opinion, the staff should be making that determination now so that the Commission makes a fully informed decision when they get that paper in September.

And, I would say that, you know, the paper, in the staff's defense, it's been pushed out

for several reasons, now it's the CRGR, they've also had a lot of interactions and so forth, but these policy issues are not getting addressed and resolved prior to sending that proposed rule up which is now scheduled for September to the Commission.

They are fundamental in the scope of this rule and the Commission is going to get a product potentially, that will not have those issues answered, DOE accredited systems, Petition for Rulemaking, rule scope.

So, as stakeholders and licensees, we're running the risk that the NRC puts out a proposed rule, we spend another exhaustive amount of time, as you probably will, in reviewing it. And then, somewhere down the road, either between the proposed rule or the final rule or worst case, final rules already on the streets and we're implementing, the scope of the rule gets narrowed and we have this whiplash effect where we have been put through this exercise and then the scope of the rule gets narrowed and it all has to be dialed back.

So, bottom line, policy issues need to be resolved, Reg Guide is voluminous, it's overwhelming. We believe, based on our preliminary review, that there is a lot of information there that goes beyond

the rule and that the rule should be limited to those facilities that are subject to the DBT to be consistent with the current regulatory framework for physical attack.

Thank you.

MEMBER BROWN: Is there any other comments from the audience?

(NO RESPONSE)

MEMBER BROWN: Is there anyone on the phone line --

THERON: Open.

MEMBER BROWN: -- that would like to make a comment? Is there anybody on the phone line?

(OFF MICROPHONE COMMENTS)

THERON: Bridge is open.

MEMBER BROWN: The bridge is open, okay, thank you.

We're sorry for that buzz, but if you're out there and want to make a comment, please identify yourself.

(NO RESPONSE)

MEMBER BROWN: Okay, hearing no comments from the phone line, I'll turn it -- are there any final comments from members or are we done?

(NO RESPONSE)

MEMBER BROWN: Hearing none, Dennis, I'll turn it back to you.

CHAIRMAN BLEY: Thank you, Charlie.

MEMBER BROWN: Can I make one -- I think -- I just -- I wanted to thank the staff. I think they've done a -- two Subcommittee meetings, very detailed discussions. Issues have been brought up and I just wanted to thank them for a good job. I apologize for not getting that in.

CHAIRMAN BLEY: Thank you.

We will reconvene for PNP at 10 minutes till 11:00. At this point, we are off the record for the day and we are recessed until 10:50.

(Whereupon, the above-entitled matter went off the record at 10:35 a.m.)

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

Fuel Cycle Cyber Security Rulemaking

ACRS Full Committee Meeting

June 8, 2017

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

Agenda

- Overview of the proposed rule and associated documents:
  - SECY paper;
  - *Federal Register* notice (FRN);
  - Draft regulatory analysis;
  - Draft backfit analysis;
  - Draft environmental assessment; and
  - Draft regulatory guide.
- SECY ticket for sending the proposed rule to the Commission was extended to September 30, 2017.

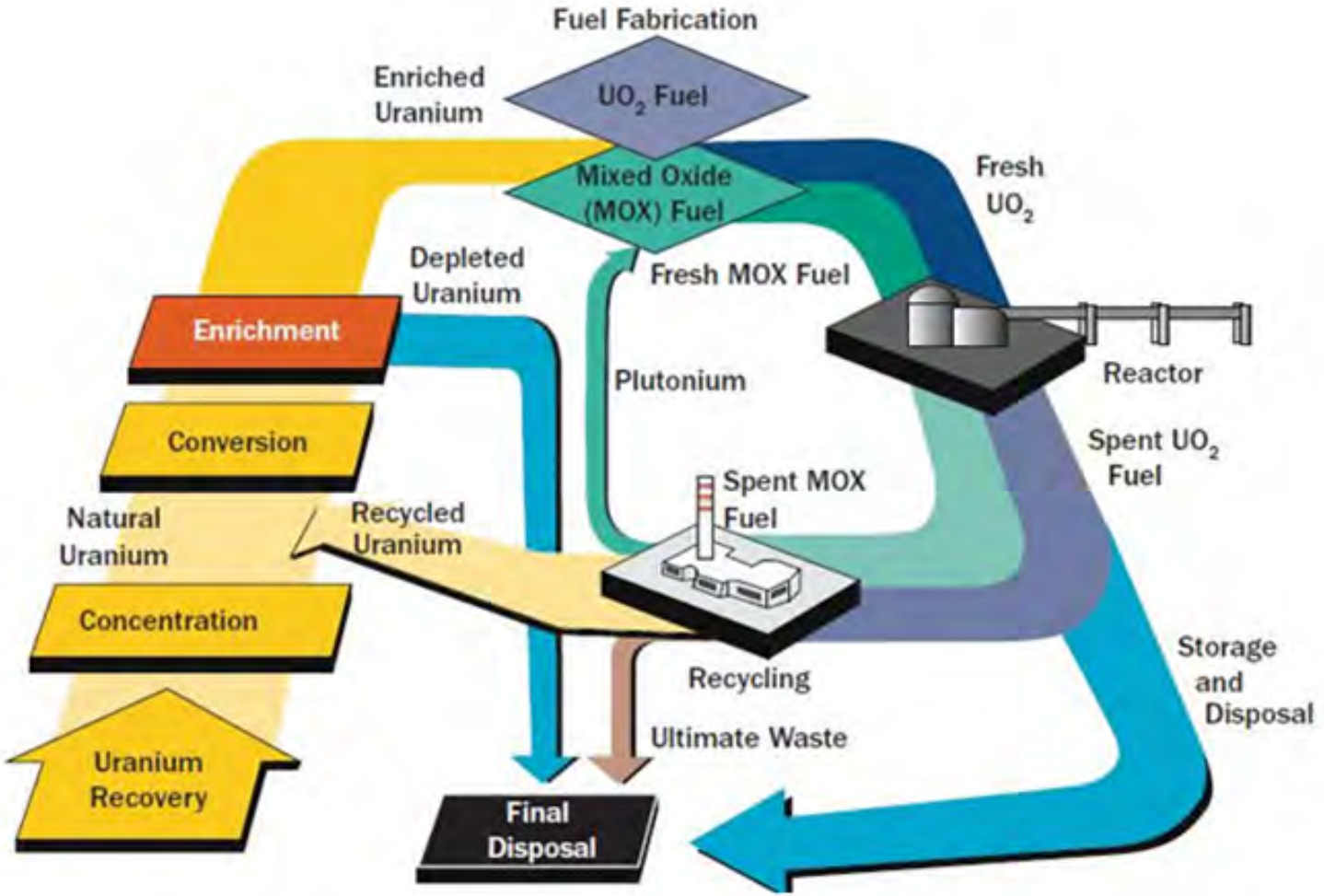
U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Acronyms

- 10 CFR: Title 10 of the *Code of Federal Regulations*
- ACRS: Advisory Committee on Reactor Safeguards
- EDO: NRC's Executive Director for Operations
- FRN: *Federal Register* notice
- NMSS: NRC's Office of Nuclear Material Safety and Safeguards
- NRC: U.S. Nuclear Regulatory Commission
- SECY: NRC's Office of the Secretary
- SNM: special nuclear material
- SSNM: strategic special nuclear material
- VDA: vital digital asset

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

Overview of impacted fuel cycle licensees – facility types



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

Overview of impacted fuel cycle licensees – facility types (continued)

Licensee/ License Applicant	Material Present and Operation
Category I (10 CFR Part 70)	
BWXT	SSNM (fabrication), classified info/matter
Nuclear Fuel Services	SSNM (fabrication), classified info/matter
Shaw AREVA MOX Services	SSNM (fabrication), classified info/matter
Category II (10 CFR Part 70)	
None	
Conversion/Deconversion (10 CFR Part 40)	
Honeywell International	source material (conversion)
International Isotopes	source material (deconversion)

Licensee/ License Applicant	Material Present and Operation
Category III (10 CFR Part 70)	
Eagle Rock Enrichment Facility	SNM (enrichment), classified info/matter
URENCO USA Facility	SNM (enrichment), classified info/matter
American Centrifuge Plant	SNM (enrichment), classified info/matter
Global Laser Enrichment Facility	SNM (enrichment), classified info/matter
AREVA	SNM (fabrication)
Global Nuclear Fuels-Americas	SNM (fabrication)
Westinghouse	SNM (fabrication)

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

Overview of SECY paper

- NMSS is forwarding the proposed rule for the Commission's consideration by way of a Commission decision-making paper (known as a SECY paper) submitted through the EDO.
- The SECY paper contains a high level summary of the proposed rule with background information.
- Specific topics discussed in the SECY paper:
  - Key features of the proposed rule;
  - Implementation of the proposed rule;
  - Coordination with ACRS;
  - Consideration of NRC's strategic goals and objectives;
  - Stakeholder interactions; and
  - Implementing guidance.
- SECY paper provides staff recommendation that the Commission approve the proposed rule for publication in the *Federal Register.*

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

Overview of FRN

- Announces the public availability of the proposed rule and solicits comments.
- FRN includes:
  - Executive Summary;
  - Details on obtaining information and submitting comments;
  - Background information on the proposed rule;
  - Discussion of the statements of consideration;
  - Discussion and text of proposed rule;
  - Availability of associated documents; and
  - Administrative sections.

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

Overview of FRN – proposed rule text

- Proposed 10 CFR 73.53 would require FCF licensees to establish, implement, and maintain a cyber security program that detects, protects against, and responds to a cyber attack capable of causing one or more of the consequences of concern.
- Proposed conforming changes to 10 CFR 40.31, 40.35, 70.22, 70.32, and 73.46(g)(6).

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

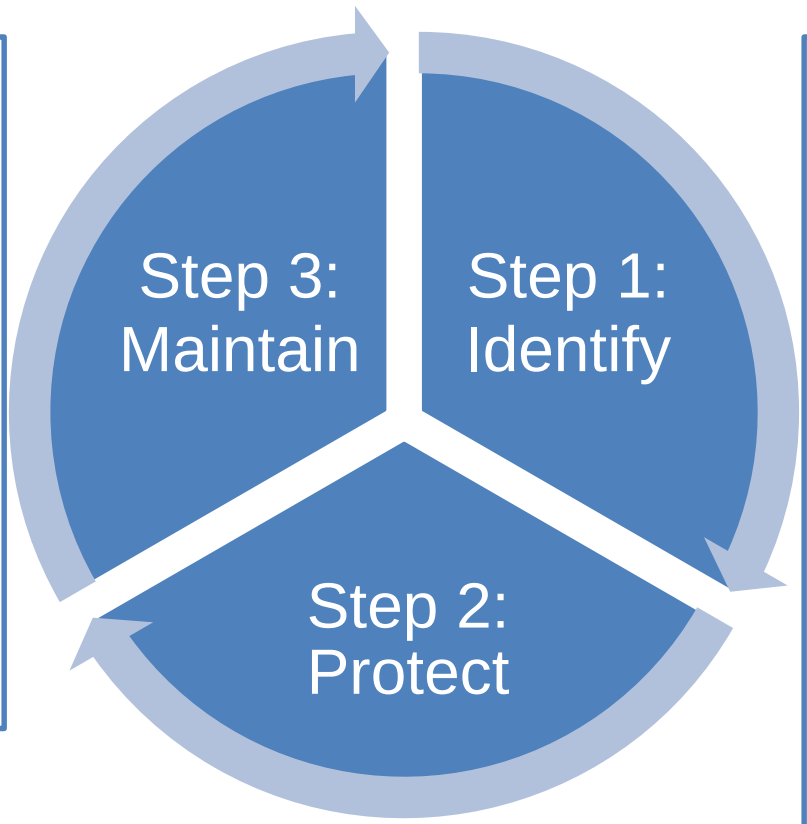
Overview of FRN – consequences of concern

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; • Theft or diversion of formula quantities of strategic special nuclear material; or • Loss of nuclear material control and accounting for strategic special nuclear material.	10 CFR 73.1(a) 10 CFR 73.20 10 CFR 73.46 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 • Loss of nuclear material control and accounting for special nuclear material of moderate strategic significance.	10 CFR 73.67 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; • 30 mg or greater intake of uranium in soluble form for any individual outside the controlled area; or • An acute chemical exposure that could lead to irreversible or other serious, long lasting health effects for any individual.	10 CFR 70.61 10 CFR 70.62
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; • 30 mg or greater intake of uranium in soluble form for any individual outside the controlled area; • An acute chemical exposure that could lead to irreversible or other serious, long lasting health effects for any individual; or	10 CFR 70.61 10 CFR 70.62
• Loss or unauthorized disclosure of classified information or classified matter.	10 CFR Part 95

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

Overview of FRN – proposed cyber security program

- Maintain protection, detection, and response
- Utilize configuration management system
  - evaluate facility changes prior to implementation
  - ensure changes do not adversely impact ability to meet program performance objectives
- Perform periodic review
  - annually for Category I
  - triennially for all others
- Report and track events



- Establish site-specific cyber security plan
  - methodology for meeting program performance objectives
  - commitment to maintain program
  - graded cyber security controls specific to consequences of concern
  - template provided in draft regulatory guide
  - NRC review and approval
- Establish cyber security team
- Identify digital assets that could result in consequence of concern
- Determine VDAs (consider alternate means)

- Ensure each VDA is protected using applicable controls
- Document measures taken to address controls in implementing procedure

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

Overview of draft regulatory analysis

- Provides background, states the problem, clarifies objectives for rulemaking, and identifies alternative approaches considered.
- Estimates and evaluates benefits and costs:
  - Considers various affected attributes;
  - Includes impact on both industry and NRC;
  - Quantitative costs; and
  - Qualitative benefits.
- Appendix B provides a discussion of vulnerability of fuel cycle facilities to a cyber threat.

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

Overview of draft backfit analysis

- Determines the portions of the proposed rulemaking that constitute backfitting in accordance with the requirements in 10 CFR 70.76.
- Specific entities impacted by the proposed rule are not afforded backfit protection (e.g., 10 CFR Part 40 licensees and future license applicants).
- Applies the adequate protection exception to specific provisions of the proposed rule (e.g., protecting against the design basis threats and safeguarding of classified information).
- Demonstrates a cost justified substantial increase in protection for the remaining provisions using a threshold (i.e., break even) analysis.
- Commission makes final determination.

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

Overview of draft environmental assessment

- Examines the environmental impact of developing a performance-based regulatory framework for protecting against cyber attacks at fuel cycle facilities.
- Discusses:
  - Identification of the proposed action;
  - Need for the action;
  - Alternative approaches considered; and
  - Environmental impacts of the proposed action and alternatives.
- Concludes with finding of no significant impact for the proposed rule.

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

Overview of draft regulatory guide – content

A. Introduction

B. Discussion

C. Staff regulatory guidance

D. Implementation

Supporting glossary, references, and appendices

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

Overview of draft regulatory guide – Section 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 temporary compensatory measures
9. Configuration management
10. Review of the cyber security program
11. Event reporting and tracking
12. Recordkeeping

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

Overview of draft regulatory guide – 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 submission of the plan and Appendices B – F provide guidance on an acceptable methodology.
- Should a 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.

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

Overview of draft regulatory guide – Appendices B – F: Controls for VDAs

- Provide cyber security controls that NRC considers adequate to effectively address cyber security for VDAs.
  - Appendix B contains controls applicable to all consequences of concern.
  - Appendices C – F contain additional controls applicable to a specific consequence of concern.
- A licensee can choose to adopt the controls in 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.

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

Overview of draft regulatory guide – Appendices B – F: Controls for VDAs (continued)

Objective	Category	Control Families																	
		Access Control (AC)	Awareness & Training (AT)	Audit & Accountability (AU)	Security Assessment & Authorization (CA)	Configuration Management (CM)	Contingency Planning (CP)	Identification & Authentication (IA)	Incident Response (IR)	Maintenance (MA)	Media Protection (MP)	Physical & Environmental Protection (PE)	Planning (PL)	Program Management (PM)	Personnel Security (PS)	Risk Assessment (RA)	System & Services Acquisition (SA)	System & Communications Protection (SC)	System & Information Integrity (SI)
Identify	Asset Management	●			●	●	●						●	●	●		●		
	Business Environment						●					●		●			●		
	Governance	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
	Risk Assessment				●									●		●	●		●
	Risk Management Strategy													●		●	●		
Protect	Access Control	●						●				●		●				●	
	Awareness & Training		●						●					●	●		●		
	Data Security	●		●		●	●				●	●			●			●	●
	Information Protection Processes & Procedures	●			●	●	●		●	●		●	●	●	●	●	●		●
	Maintenance									●									
	Protective Technology	●		●		●	●				●							●	
Detect	Anomalies and Events	●		●	●	●	●		●							●			●
	Security Continuous Monitoring	●		●	●	●						●		●	●	●	●	●	●
	Detection Processes			●	●							●	●	●		●			●
Respond	Response Planning						●		●										
	Communications			●	●		●		●			●		●		●			●
	Analysis			●	●		●		●			●							●
	Mitigation				●		●		●							●			
	Improvements								●										
Recover	Recovery Planning						●		●										
	Improvements						●		●										
	Communications						●		●										

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

Overview of draft regulatory guide – Appendix G: Example of implementation

- Example can be used by a licensee to assist with developing site-specific identification process, alternate means analysis, implementing procedures, and additional considerations.

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

Conclusion

- NRC currently lacks a comprehensive regulatory framework for addressing cyber security at fuel cycle facilities.
- Methodology in proposed rule and draft regulatory guide would:
  - Identify digital assets whose compromise by a cyber attack would result in specific consequences of concern to public health and safety and the common defense and security;
  - Protect vital digital assets through a graded approach consistent with industry accepted standards; and
  - Maintain a cyber security program that ensures fuel cycle facilities remain adequately protected against cyber attacks.
- Staff recommends ACRS endorsement of publishing the proposed rule and draft regulatory guide for formal public comment.