

**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**

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23

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.

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25

UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

+ + + + +

644<sup>TH</sup> 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

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25

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

1 ALSO PRESENT:  
2 SUZANNE ANI, NMSS  
3 MATT BARTLETT, NMSS  
4 MEKONEN BAYSSIE, RES  
5 JIM BEARDSLEY, NSIR  
6 SAMANTHA CRANE, NMSS  
7 JOE DEUCHER, ASLBP  
8 JAMES DOWNS, NMSS  
9 ALAN FRAZIER, NMSS  
10 KAYLA GAMIN, OGC  
11 ADAM GENDELMAN, OGC  
12 WILLIAM GROSS, NEI  
13 JIM MALTESE, OGC  
14 CARDELIA MAUPIN, NMSS  
15 CASEY PRIESTER, NRC Contractor  
16 JANET SCHLUETER, NEI  
17 GREG TRUSSELL, NMSS  
18 JAKE ZIMMERMAN, NMSS  
19  
20  
21  
22  
23  
24

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24

CONTENTS

Opening Remarks . . . . . 5

Proposed Rule Draft Regulatory Guide DG-5062 on  
Cyber Security for Fuel Cycle Facilities . . . . . 7

Adjourn . . . . . 113

## 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.

**NEAL R. GROSS**

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

1                   Written comments are also welcome.

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

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

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

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

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

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

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



1 going to be doing the Fuel Cycle Facility Rulemaking.

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

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

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

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

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

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

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

25 The documents under your review provide

**NEAL R. GROSS**

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

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

4 Next slide, please?

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

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

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

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

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

**NEAL R. GROSS**

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

1           Are there any questions on the agenda or  
2           schedule forward?

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

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

13          Next slide, please?

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

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

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

**NEAL R. GROSS**

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

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

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

9           Any questions on that?

10          Okay, next slide?

11          Slide five shows the specific applicants  
12 and licensees that are proposed to be within the scope  
13 of this rulemaking. The proposed rule would apply to  
14 the applicants or licensees subject to the integrated  
15 safety analysis requirements of 10 CFR 70.60 and to  
16 applicants or licensees subject to the requirements of  
17 10 CFR Part 40 for the operation of the uranium  
18 hexafluoride conversion or deconversion facility.

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

25          This corresponds to the different types of

**NEAL R. GROSS**

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

1 licensed material at various enrichment levels of  
2 these facilities.

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

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

11 Category III are those authorized under  
12 Part 70 to possess or use special nuclear material of  
13 low strategic significance.

14 And conversion or deconversion facilities  
15 are those source material licensees authorized under  
16 10 CFR Part 40 to perform uranium hexafluoride  
17 conversion or deconversion.

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

23 MEMBER BROWN: James?

24 MR. DOWNS: Sir?

25 MEMBER BROWN: Could you just highlight as

**NEAL R. GROSS**

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

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

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

5 MEMBER BROWN: Anybody who knows.

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

7 MR. GENDELMAN: It's 20 percent.

8 MR. DOWNS: Twenty percent is the --

9 MEMBER BROWN: With Category I?

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

11 MEMBER BROWN: That's Category I?

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

13 Adam.

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

16 MEMBER BROWN: What's your name?

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

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

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

**NEAL R. GROSS**

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

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

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

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

7 MR. GENDELMAN: Yes.

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

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

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

22 MEMBER MARCH-LEUBA: Why?

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

25 MEMBER MARCH-LEUBA: So, they're licensed

**NEAL R. GROSS**

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

1 by DOE? That does the --

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

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

10 MR. DOWNS: That's right.

11 MEMBER MARCH-LEUBA: Okay.

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

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

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

**NEAL R. GROSS**

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



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

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

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

13 MEMBER KIRCHNER: Thank you.

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

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

23 MEMBER BROWN: Okay. All right, thank  
24 you.

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

**NEAL R. GROSS**

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

1 no overlap between the categories.

2 MEMBER BROWN: All right.

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

6 MR. MALTESE: That's correct.

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

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

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

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

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

**NEAL R. GROSS**

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

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

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

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

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

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

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

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

**NEAL R. GROSS**

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

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

3           MEMBER SKILLMAN: I do.

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

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

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

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

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

25          MEMBER SKILLMAN: Thank you.

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

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

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

14 Are there any questions on the structure  
15 of the FRN?

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

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

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

**NEAL R. GROSS**

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

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

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

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

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

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

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

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

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

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

**NEAL R. GROSS**

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

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

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

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

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

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

21 MEMBER KIRCHNER: Thank you.

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

**NEAL R. GROSS**

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

1 active safety and a latent safety and security.

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

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

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

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

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

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

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

**NEAL R. GROSS**

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



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

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

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

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

16           MR. DOWNS: There is --

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

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

**NEAL R. GROSS**

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

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

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

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

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

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

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

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

**NEAL R. GROSS**

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

1 MEMBER BROWN: That was my --

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

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

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

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

16 MR. DOWNS: That's --

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

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

**NEAL R. GROSS**

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

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

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

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

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

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

16                   MEMBER BROWN: Okay, thank you.

17                   Anything else? Go ahead.

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

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

**NEAL R. GROSS**

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

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

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

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

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

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

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

**NEAL R. GROSS**

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

1 assets.

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

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

10 Are there any questions on the proposed  
11 cyber security program?

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

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

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

**NEAL R. GROSS**

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

1 Analysis consistent with applicable NRC guidance.

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

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

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

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

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

25 Appendix B of the draft regulatory

**NEAL R. GROSS**

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

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

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

9 Are there any questions on the Draft Reg  
10 Analysis?

11 Next slide?

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

17 The exception being future applicants and  
18 current Part 40 licensees.

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

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

**NEAL R. GROSS**

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



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

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

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

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

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

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

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

**NEAL R. GROSS**

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

1 threshold exposure to a single individual to numerous  
2 individuals.

3 Are there any questions on the Draft  
4 Backfit Analysis?

5 MEMBER SKILLMAN: Yes. Why are the Part  
6 40 license holders excluded from backfit provision?

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

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

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

15 (LAUGHTER)

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

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

25 MEMBER SKILLMAN: Is there dialogue from

**NEAL R. GROSS**

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

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

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

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

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

13 MR. DOWNS: That's correct.

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

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

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

22 MEMBER SKILLMAN: Okay.

23 MR. DOWNS: But it is discussed.

24 MEMBER SKILLMAN: I understand, thank you.

25 MR. DOWNS: Okay?

**NEAL R. GROSS**

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

1 Next slide, please?

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

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

10 Okay.

11 So, now, we'll get into the Draft  
12 Regulatory Guide which can also be referred to as DG  
13 5062.

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

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

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

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

25 The staff looks forward to further public

**NEAL R. GROSS**

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

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

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

5 Slide 15 provides the --

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

10 MR. DOWNS: Provides a method.

11 MEMBER BROWN: A method.

12 MR. DOWNS: Correct.

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

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

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

**NEAL R. GROSS**

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

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

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

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

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

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

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

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

**NEAL R. GROSS**

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

1 consequence of concern.

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

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

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

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

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

17 MEMBER BROWN: Be careful.

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

21 MEMBER BROWN: Yes.

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

25 Let me try an example. If I went to my

**NEAL R. GROSS**

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

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

5 MR. DOWNS: Absolutely.

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

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

13 MR. DOWNS: That is 100 --

14 CHAIRMAN BLEY: -- what you're doing.

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

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

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

**NEAL R. GROSS**

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



1 special nuclear material. It was a low level.

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

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

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

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

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

**NEAL R. GROSS**

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

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

7           MR. DOWNS: So, the --

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

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

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

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

**NEAL R. GROSS**

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

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

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

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

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

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

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

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

**NEAL R. GROSS**

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

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

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

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

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

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

21 MEMBER BROWN: Hold it, hold it.

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

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

**NEAL R. GROSS**

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

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

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

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

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

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

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

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

**NEAL R. GROSS**

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

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

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

6 Latent safeguards, that's Category II.

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

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

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

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

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

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

**NEAL R. GROSS**

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

1       overly burdensome.

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

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

12                   MEMBER BROWN: Any other discussion?

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

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

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

24                   MEMBER KIRCHNER: Thank you.

25                   MEMBER CHU: I have some comments, yes.

**NEAL R. GROSS**

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

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

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

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

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

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

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

23 MR. DOWNS: That's correct.

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

**NEAL R. GROSS**

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



1 sure what from Subcommittee until now whether stuff  
2 has changed.

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

7 MR. DOWNS: That's correct.

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

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

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

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

**NEAL R. GROSS**

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

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

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

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

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

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

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

**NEAL R. GROSS**

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

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

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

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

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

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

25 MEMBER CHU: Thank you.

1 MR. GENDELMAN: This is Adam Gendelman.

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

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

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

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

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

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

**NEAL R. GROSS**

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

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

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

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

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

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

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

**NEAL R. GROSS**

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

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

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

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

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

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

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

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

**NEAL R. GROSS**

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

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

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

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

13 Go ahead, move on, James.

14 MR. DOWNS: Okay.

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

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

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

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

**NEAL R. GROSS**

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

1 vital digital assets.

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

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

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

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

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

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

**NEAL R. GROSS**

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



1 when we get to the appendices of the guidance.

2 Are there any questions on Section C?

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

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

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

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

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

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

**NEAL R. GROSS**

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

1 adequately protected against cyber attacks.

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

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

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

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

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

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

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

**NEAL R. GROSS**

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

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

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

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

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

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

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

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

25           For example, a vital digital asset

**NEAL R. GROSS**

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

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

4 Basically, that control prohibits any  
5 remote access.

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

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

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

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

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

25 MEMBER BROWN: I don't remember that.

**NEAL R. GROSS**

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

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

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

12 MEMBER BROWN: Okay, thank you.

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

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

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

25 Across the top of the table are 18

**NEAL R. GROSS**

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

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

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

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

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

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

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

**NEAL R. GROSS**

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

1 security vulnerabilities.

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

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

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

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

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

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

24 Are there any questions on the controls?

25 MEMBER STETKAR: Yes. This is a great

**NEAL R. GROSS**

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

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

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

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

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

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

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

25 MEMBER STETKAR: Don't get me started on

**NEAL R. GROSS**

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



1 risk.

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

4 MEMBER STETKAR: Okay.

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

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

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

10 MEMBER STETKAR: Okay, thank you.

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

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

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

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

24 MEMBER STETKAR: By checking off boxes?

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

**NEAL R. GROSS**

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

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

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

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

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

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

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

24 MEMBER STETKAR: Right.

25 MR. DEUCHER: -- you see the program

**NEAL R. GROSS**

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

1 activity and that cross, is what we're hoping that --  
2 and our goal with the rule itself is for the licensees  
3 to be focused on that, that overall, from a  
4 programmatic standpoint, that you're looking across  
5 the entirety of your facility. You're looking at  
6 these consequences, you've identified the areas that  
7 there are issues and you're looking at it from that  
8 10,000-foot view.

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

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

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

**NEAL R. GROSS**

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

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

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

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

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

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

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

**NEAL R. GROSS**

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

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

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

11 MR. DOWNS: And, I think for what you just  
12 --

13 MEMBER STETKAR: That's the concern.

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

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

**NEAL R. GROSS**

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

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

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

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

15 MR. DOWNS: And, in addition --

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

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

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

25 Forty-six years ago, the NRC required

**NEAL R. GROSS**

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

1 licenses to develop a QA program. Before about 1971,  
2 there wasn't one.

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

6 And, for those who were there before and  
7 after, in the after environment, the organizations  
8 started with two and then four and then ten and then  
9 15 then a 100.

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

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

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

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

**NEAL R. GROSS**

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

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

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

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

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

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

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

**NEAL R. GROSS**

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



1       creditable to prevent that consequence of concern.

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

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

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

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

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

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

**NEAL R. GROSS**

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

1 I'm very perplexed with a chart like this.

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

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

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

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

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

**NEAL R. GROSS**

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

1 to protect.

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

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

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

11 MR. DOWNS: That's correct.

12 MEMBER KIRCHNER: So, basically --

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

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

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

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

24 (LAUGHTER)

25 MR. DOWNS: And, just to be clear on

**NEAL R. GROSS**

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

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

4 MEMBER KIRCHNER: That's right.

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

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

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

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

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

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

**NEAL R. GROSS**

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

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

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

10 MEMBER KIRCHNER: I'm aware of that.

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

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

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

**NEAL R. GROSS**

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

1 that were raised in the Subcommittee meeting.

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

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

14 MEMBER KIRCHNER: Thank you.

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

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

25 So, to answer your question directly, yes,

**NEAL R. GROSS**

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

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

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

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

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

**NEAL R. GROSS**

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

1 MEMBER SKILLMAN: Thank you.

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

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

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

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

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

20 I just wanted to put that on the record.

21 MEMBER SKILLMAN: Thank you.

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

23 MEMBER SKILLMAN: Thank you.

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

**NEAL R. GROSS**

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



1 be a tremendous amount of interaction with the  
2 stakeholders.

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

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

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

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

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

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

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

**NEAL R. GROSS**

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

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

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

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

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

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

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

18 MEMBER STETKAR: James?

19 MR. DOWNS: Go ahead.

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

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

**NEAL R. GROSS**

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

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

2 MR. DOWNS: That's right.

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

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

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

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

18 CHAIRMAN BLEY: And it becomes unworkable.

19 MEMBER STETKAR: It's unworkable.

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

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

**NEAL R. GROSS**

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

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

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

7 Appendix B is applicable to any vital  
8 digital asset.

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

13 MEMBER STETKAR: Okay.

14 MR. DOWNS: -- to. So, but I can't really  
15 --

16 MEMBER STETKAR: Reduces it to 50 or 70 or  
17 80 or something. So, either I have a 133 or I have  
18 127, if I've added -- close enough.

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

25 MEMBER STETKAR: That's the agenda.

**NEAL R. GROSS**

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

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

3 MEMBER SUNSERI: One question over here.

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

6 Go ahead.

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

14 MR. DOWNS: Absolutely, 100 percent.

15 MEMBER SUNSERI: Okay, thank you.

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

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

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

**NEAL R. GROSS**

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

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

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

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

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

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

15          So, does the Reg Guide give examples of  
16          alternatives?

17          MR. DOWNS: Yes.

18          VICE CHAIR CORRADINI: Can you give me  
19          one?

20          MR. DOWNS: Sure.

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

25          So, what are some examples that you would

**NEAL R. GROSS**

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

1 avoid doing this?

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

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

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

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

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

21 VICE CHAIR CORRADINI: Okay.

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

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

**NEAL R. GROSS**

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

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

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

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

13 VICE CHAIR CORRADINI: Okay.

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

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

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

25 VICE CHAIR CORRADINI: Sorry, this is the

**NEAL R. GROSS**

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



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

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

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

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

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

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

17 MEMBER STETKAR: Charlie, before you do  
18 that --

19 MEMBER BROWN: Yes, go ahead.

20 MEMBER STETKAR: Can I ask --

21 MEMBER BROWN: Go ahead.

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

**NEAL R. GROSS**

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

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

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

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

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

13 MEMBER STETKAR: Yes.

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

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

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

**NEAL R. GROSS**

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

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

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

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

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

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

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

**NEAL R. GROSS**

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

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

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

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

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

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

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

25 MEMBER MARCH-LEUBA: Yes, Charlie, I have

**NEAL R. GROSS**

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

1 a --

2 MEMBER BROWN: Let me finish.

3 MEMBER MARCH-LEUBA: -- offering an  
4 opinion.

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

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

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

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

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

**NEAL R. GROSS**

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

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

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

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

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

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

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

**NEAL R. GROSS**

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

1 about in terms of how do you protect those.

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

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

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

11 (LAUGHTER)

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

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

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

**NEAL R. GROSS**

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

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

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

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

11 Now, Jose, fire away.

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

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

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

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

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

**NEAL R. GROSS**

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



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

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

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

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

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

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

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

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

25 So, I don't see this as a tremendous

**NEAL R. GROSS**

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

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

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

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

8 MEMBER MARCH-LEUBA: And --

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

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

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

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

**NEAL R. GROSS**

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

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

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

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

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

16          MEMBER STETKAR:   That's right.

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

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

**NEAL R. GROSS**

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

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

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

6           MEMBER BROWN: That's my problem, is the  
7 rule specifies addressing digital assets and does not  
8 include some allowance for some other methodologies as  
9 --

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

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

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

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

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

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

**NEAL R. GROSS**

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

1 accretion of what's expected as you go forward.

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

4 CHAIRMAN BLEY: Indeed.

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

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

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

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

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

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

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

**NEAL R. GROSS**

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

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

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

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

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

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

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

**NEAL R. GROSS**

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

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

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

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

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

15 Are there any questions on Appendix G?

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

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

**NEAL R. GROSS**

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

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

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

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

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

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

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

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

**NEAL R. GROSS**

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



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

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

7 MR. DEUCHER: Well, it's not necessarily  
8 --

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

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

16 MEMBER KIRCHNER: I agree with you.

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

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

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

**NEAL R. GROSS**

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

1 without having a separate rule.

2 Thank you.

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

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

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

13 MEMBER BROWN: You want to go on, James?

14 MR. DOWNS: Sure.

15 MEMBER BROWN: Okay, please.

16 MR. DOWNS: Okay, last slide here.

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

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

**NEAL R. GROSS**

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

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

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

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

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

15 With that, I conclude.

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

18 Go to the mic and give your name, please.

19 CHAIRMAN BLEY: Name and affiliation.

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

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

25 MEMBER BROWN: Oh, hold it. Can you tilt

**NEAL R. GROSS**

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

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

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

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

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

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

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

25 These facilities have corporate cyber

**NEAL R. GROSS**

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

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

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

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

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

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

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

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

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

**NEAL R. GROSS**

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

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

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

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

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

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

**NEAL R. GROSS**

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

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

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

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

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

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

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

25           One, that the policy issue of this very,

**NEAL R. GROSS**

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

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

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

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

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

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

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

**NEAL R. GROSS**

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



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

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

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

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

**NEAL R. GROSS**

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

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

5 Thank you.

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

8 (NO RESPONSE)

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

11 THERON: Open.

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

14 (OFF MICROPHONE COMMENTS)

15 THERON: Bridge is open.

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

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

21 (NO RESPONSE)

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

25 (NO RESPONSE)

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

3                   CHAIRMAN BLEY: Thank you, Charlie.

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

10                  CHAIRMAN BLEY: Thank you.

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

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

16

17

18

19

20

21

22

23

24

25

# **Fuel Cycle Cyber Security Rulemaking**

**ACRS Full Committee Meeting**

June 8, 2017

---

# Agenda

---

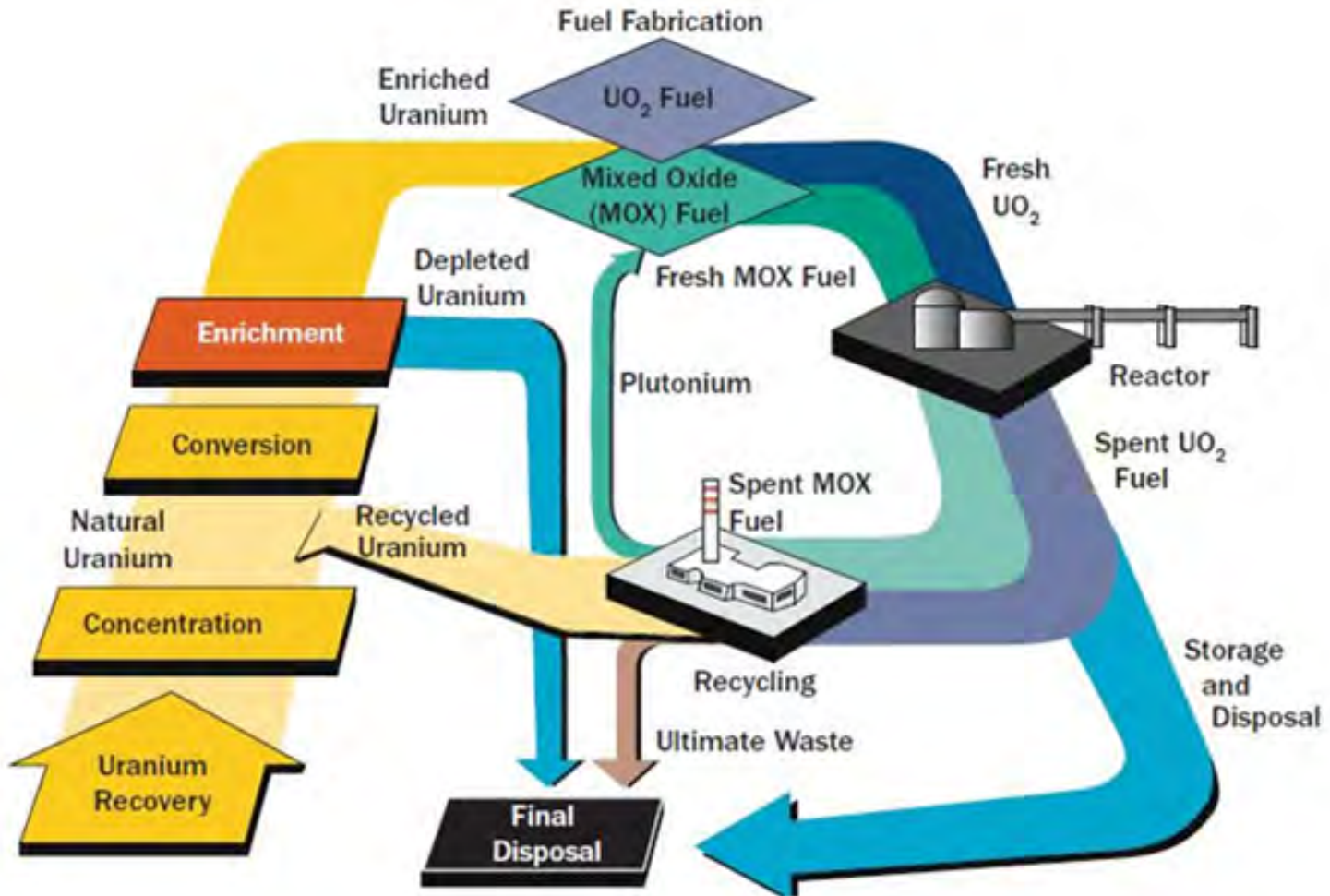
- Overview of the proposed rule and associated documents:
  - SECY paper;
  - *Federal Register* notice (FRN);
  - Draft regulatory analysis;
  - Draft backfit analysis;
  - Draft environmental assessment; and
  - Draft regulatory guide.
- SECY ticket for sending the proposed rule to the Commission was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

# 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

# Overview of impacted fuel cycle licensees – facility types



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

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

Licensee/ License Applicant	Material Present and Operation
<b>Category III (10 CFR Part 70)</b>	
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)



# 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*.

# 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.

# 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).

# 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; 10 CFR 73.1(a)
- Theft or diversion of formula quantities of strategic special nuclear material; or 10 CFR 73.20
- Loss of nuclear material control and accounting for strategic special nuclear material. 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 10 CFR 73.67
- Loss of nuclear material control and accounting for special nuclear material of moderate strategic significance. 10 CFR 74.41

## ACTIVE – SAFETY

One or more of the following that directly results from a cyber attack:

- Radiological exposure of 25 rem or greater for any individual; 10 CFR 70.61
- 30 mg or greater intake of uranium in soluble form for any individual outside the controlled area; or 10 CFR 70.62
- An acute chemical exposure that could lead to irreversible or other serious, long lasting health effects for any individual.

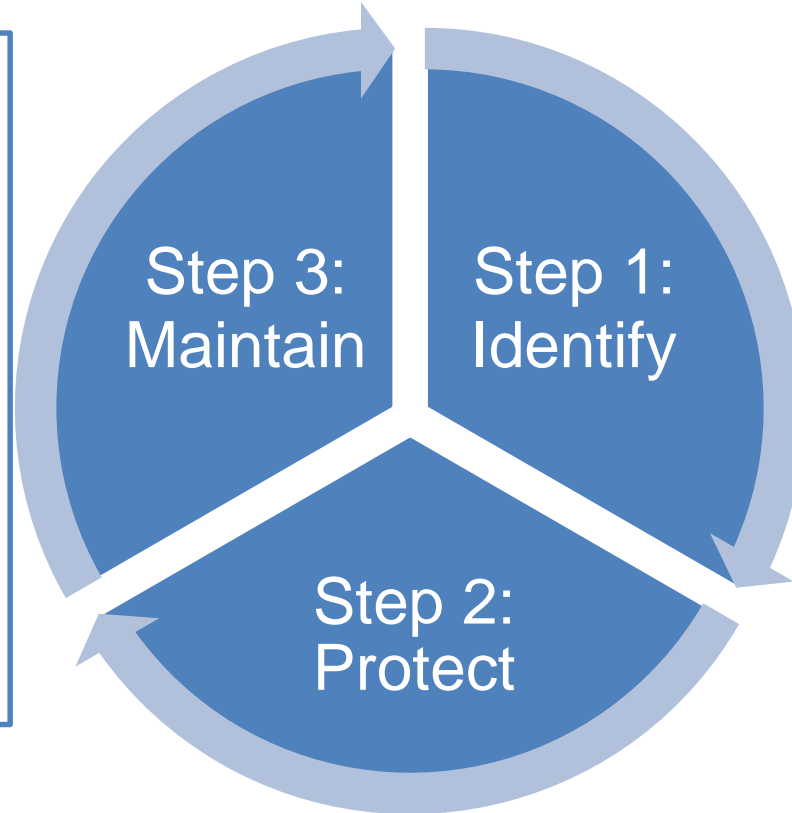
## LATENT – SAFETY AND SECURITY

The compromise, as a result of a cyber attack, of a function needed to prevent:

- Radiological exposure of 25 rem or greater for any individual; 10 CFR 70.61
- 30 mg or greater intake of uranium in soluble form for any individual outside the controlled area; 10 CFR 70.62
- An acute chemical exposure that could lead to irreversible or other serious, long lasting health effects for any individual; or
- Loss or unauthorized disclosure of classified information or classified matter. 10 CFR Part 95

# 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



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

- 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)

# 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.

# 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.

# 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.



# Overview of draft regulatory guide – content

---

A. Introduction

B. Discussion

C. Staff regulatory guidance

D. Implementation

Supporting glossary, references, and appendices

# 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

# 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.

# 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.

# 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						•		•										

# 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.

# 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.