

**Official Transcript of Proceedings**  
**NUCLEAR REGULATORY COMMISSION**

Title: Public Workshop to Discuss  
Instrumentation and Controls

Docket Number: (N/A)

Location: Rockville, Maryland

Date: August 18, 2015

Work Order No.: NRC-1813

Pages 1-79

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

U.S. NUCLEAR REGULATORY COMMISSION

+ + + + +

OFFICE OF NEW REACTORS

+ + + + +

PUBLIC WORKSHOP TO DISCUSS INSTRUMENTATION

AND CONTROLS

CYBER SECURITY-BY-DESIGN AND

ASSOCIATED POTENTIAL REGULATORY IMPACTS

+ + + + +

TUESDAY

AUGUST 18, 2015

+ + + + +

The Public Workshop met in the Commission Hearing Room, Rooms 1F16 and 1G16, NRC Headquarters, One White Flint North, 11555 Rockville Pike, Rockville, Maryland, at 1:01 p.m.

NRC STAFF PRESENT

CATHERINE ALLEN, NSIR/CSD

STEVEN ARNDT, NRR/DE

SUSHIL BIRLA, RES/DE

BERNARD DITTMAN, RES/DE/ICEEB

TERRY JACKSON, NRO/DE/ICE

**NEAL R. GROSS**

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

25 KIM LAWSON-JENKINS, NSIR/CSD

26 ERICK MARTINEZ, RES/DE/ICEEB

27 JAN MAZZA, NRO/DARR/ARPB

28 DAVID McINTYRE, PA

29 JONAH PEZESHKI, NSIR/CSD \*

30 DAVID RAHN, NRR/DE/EICB

31 LANCE RAKOVAN, EDO/AO/CPM

32 PAUL REBSTOCK, RES/DE/ICEEB

33 JOHN RYCINA, NSIR/CSD

34 RICHARD STATTEL, NRR/DE/EICB

35 RUSSELL SYDNOR, RES/DE/ICEEB

36 TUNG TRUONG, NRO/DE/ICE

37 BARRY WESTREICH, NSIR/CSD

38 DEANNA ZHANG, NRO/DE/ICE

39

40 \* Present via telephone

41

42

43

44

45

46

47

48

49

50

51

CONTENTS

52

Page

53

Welcome and Meeting Logistics

4

54

Introduction of Participants

6

55

NRC Staff Topical Presentation

8

56

Facilitated Open Discussion

23

57

Opportunity for Public Comment

43

58

Closing Remarks/Adjourn

78

**NEAL R. GROSS**

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

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

1:01 p.m.

59  
60  
61 MR. RAKOVAN: Thank you, Emily. Again, my name is  
62 Lance Rakovan. I'm a Communications Specialist here at the  
63 Agency. I'm going to try to help keep things on track, facilitate  
64 a little bit, and basically just help out with this meeting today.  
65 The purpose of today's workshop is to discuss current NRC thinking  
66 on incorporating cyber security design reviews into the NRC's  
67 licensing reviews, including scenarios of these reviews and obtain  
68 industry stakeholder feedback for staff consideration. This is a  
69 Category 2 public meeting by NRC's definition, which means that  
70 the primary discussions are expected to occur between NRC and  
71 industry representatives.

72 There is a time scheduled towards the end of the  
73 meeting, I believe around 4:00 or a little after 4:00 by the Agenda  
74 for public questioning of NRC staff at that time, but until then,  
75 we look for the discussions to, again, primarily be between NRC  
76 staff and industry. The Agenda is pretty simple today. We have  
77 a presentation by NRC staff and nuclear industry representatives,  
78 some open discussion between the two, and then, again, we'll have  
79 a short time for public questions. If you're participating by  
80 phone today, we do have Emily who's going to be assisting us.  
81 She'll let you know how to weigh in once we do open the floor to  
82 questions and comments.

**NEAL R. GROSS**

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

83           We are taking a transcription of today's meeting, so  
84 if anything's happening in the room where it's disruptive, side  
85 noise, et cetera, I'll probably take some steps to remedy that  
86 situation. If you can, please use a microphone when you speak.  
87 Again, that'll help, not only those on the phone hear us, but also  
88 make sure that we get a clear transcript. The other thing that I  
89 will ask, especially of those in the room, please identify yourself  
90 when you speak. That not only will help the transcriptionist  
91 follow who is talking, but, again, will also help those on the  
92 phone follow as well.

93           For those of you here in the room, emergency exits can  
94 be found pretty much at the four corners of the room. Restrooms  
95 are out the door here to my right and then to the left. We do  
96 have public meeting feedback forms, copies of the NRC presentation,  
97 and, I believe, the Agenda as well at the door, again, to my right.  
98 I believe that the presentation was shared and posted on ADAMS and  
99 can be linked to on the public meeting schedule as well, so those  
100 of you following on the phone lines, you should be able to find  
101 the NRC presentation there if you go to our public meeting schedule  
102 page on our public website.

103           Before I go ahead and turn things over to our first  
104 speaker, I'd like at least those folks around the room to introduce  
105 themselves. If we could go ahead and start here to my right.

106           MR. STATTEL: Hello, I'm Richard Stattel. I'm

**NEAL R. GROSS**

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

107 representing the INC Branch and NRR.

108 MR. JACKSON: Terry Jackson, Chief of INC Branch in  
109 Office of New Reactors.

110 MS. ZHANG: Deanna Zhang, INC Technical Reviewer,  
111 Office of New Reactors.

112 MS. LAWSON-JENKINS: Kim Lawson-Jenkins, I work in the  
113 Cyber Security Directorate at the NRC.

114 MR. GEIER: I'm Steve Geier. I'm with the Nuclear  
115 Energy Institute and I'm a Senior Project Manager with NEI.

116 MR. CLIFTON: Gordon Clifton with NEI.

117 MR. RAKOVAN: Okay. That's those of us at the table.  
118 I'll ask folks that when we get to the open question and answer  
119 part that folks identify themselves as they go ahead and make a  
120 comment, including those on the phone, so we can make sure that we  
121 have an understanding. There's also a sign-in sheet for those of  
122 you who are here in the room. If you wouldn't mind signing in  
123 there to give us a good indication as to who attended in person  
124 today and for those of you on the phone, you were asked to provide  
125 your name and any organization you are with, so that will give us  
126 a good indication as to who called in one way or another. With  
127 that, I believe I'm going to turn things over to Terry, correct?  
128 Excellent.

129 MR. JACKSON: Okay. Terry Jackson with Office of New  
130 Reactors. And I just wanted to make a few opening remarks. One

**NEAL R. GROSS**

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

131 is I want to thank everyone for joining in on this public workshop  
132 today addressing cyber security and design. And as Deanna will  
133 later go on and she will talk about the purpose for why we were  
134 developing a SECY paper to address this particular topic, but this  
135 is actually the second public workshop that we've had and as a  
136 result of the first one, one of the requests from the industry was  
137 to provide some examples of how the NRC would see the different  
138 options that would be going into the SECY paper work out. So  
139 that's our intent today is to provide some examples. And also to  
140 entertain any questions or comments that you may have with regards  
141 to this effort.

142           Then we also realize that there are several other  
143 efforts within the Agency and the industry with regards to both  
144 instrumentation and controls and with cyber security. We're not  
145 prepared to address those topics today in this meeting. There are  
146 some other meetings in the future that will address those topics  
147 as well. But today we just wanted to focus on this topic of cyber  
148 security and design.

149           MS. ZHANG: Thank you, Terry. So my name is Deanna  
150 Zhang. And today I want to present to you some of the scenarios  
151 that we came up with as requested based on the feedback we received  
152 at the last public meeting. Before I go into these scenarios, I  
153 just want to recap a little bit on our last meeting. So during  
154 our last meeting, we presented on our proposed SECY paper that we

**NEAL R. GROSS**

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

155 plan on sending up to the Commission, where we want to seek the  
156 Commission's direction in allowing the staff to proceed with  
157 reviewing cyber security design information as part of licensing.  
158 This would be to complement what's currently in -- what's required  
159 by 10 CFR 73.54.

160           And as we said last time, we're not seeking to extend  
161 any cyber security technical requirements. This is more of a  
162 change in the licensing process. So we will be doing licensing  
163 reviews of design information submitted by the applicants and  
164 licensees and then we will be writing a safety evaluation report  
165 based on our review. And some of that information will then be  
166 able to be referenced as part of the cyber security inspections.  
167 And, therefore, reduce the level of information that will need to  
168 be provided during inspections and that will be inspected.

169           So let me proceed with the slides. So next slide. So  
170 this is just the list of acronyms that I'll be using. Next slide.  
171 So, again, the NRC's in the process of developing a draft SECY  
172 paper seeking the Commission's direction on evaluating cyber  
173 security related design features as part of licensing. And the  
174 scope is only for safety and important-to-safety digital assets.  
175 So this does not include the entire scope of 10 CFR 73.54. In  
176 addition, again, we do not seek to expand any of the cyber security  
177 technical controls and requirements specified in 10 CFR 73.54 and  
178 the accompanying Reg Guide 5.71.

**NEAL R. GROSS**

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

179           So in the SECY paper, two of the options will modify  
180 the licensing process to enable the review of cyber security design  
181 features. One is very tailored to the boundary controls between  
182 the cyber security defensive levels. The other one is broader,  
183 which includes more cyber security controls specified in Reg Guide  
184 5.71. So, again, during the last meeting, we got the feedback  
185 that industry would like to see us go over a few scenarios as far  
186 as what kind of information do we expect to see from a licensing  
187 submittal and how will we conduct our reviews and then how would  
188 that information be credited or referenced during the cyber  
189 security inspection. Next slide.

190           So we came up with three scenarios. For Scenario 1,  
191 this one is described in Reg Guide 5.71, Section B.1.4. And this  
192 is on the one-way boundary device between Level 4 and Level 3 and  
193 between Level 3 and lower Levels. And the specific item we'd be  
194 reviewing within this Section is the implementation of a one-way  
195 data flow using hardware mechanisms. So, next slide. So we've  
196 kind of broken this up into what we expect from a Design  
197 Certification applicant under the Part 52 process and then what we  
198 would expect to see from a licensee submitting a License Amendment  
199 Request pertaining to a digital upgrade of a safety system or some  
200 important-to-safety system through the 10 CFR 50.59 review.

201           So for Design Certification applicants, we would  
202 expect to see some design descriptions of this device on how it

**NEAL R. GROSS**

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

203 physically enforces one-way communication between Level 4 and  
204 Level 3 and between Level 3 and lower Levels. So some example  
205 would be that an applicant would state that the device uses optical  
206 isolation, that only has a fiber optical transmitter on the higher  
207 security level and a fiber optical receiver on the lower security  
208 level. And there would be no fiber optic receiver on the higher  
209 security level. Therefore, information could only be transmitted  
210 one way physically from the higher security level to the lower  
211 security level. Next slide.

212           So for a licensee who's submitting a LAR, if -- as  
213 part of this LAR, the design changes the existing communications  
214 between Level 4 and Level 3 and between Level 3 and lower Levels.  
215 The licensee would be submitting design descriptions of the device,  
216 again, showing how it physically enforces one-way communication.  
217 And similarly with the information provided for the Design  
218 Certification applicant, descriptions of how that one-way  
219 communication would be enforced. Next slide.

220           So for NRC review, we would look at the boundary device  
221 as well as review the diagram schematics to verify that the design  
222 incorporates the use of the fiber optic receiver and fiber optic  
223 transmitter, that they're in the appropriate locations based on  
224 the schematics. For Design Certification applications, we do  
225 expect to see an ITAAC provided that will be used to verify that  
226 the as-built system employs this design and that the as-built

**NEAL R. GROSS**

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

227 boundary device meets the design commitments provided in the Design  
228 Certification application. For LAR submittals, the staff will  
229 audit the development process for the device and may witness the  
230 after-acceptance testing on this device as well as review the FAT  
231 results during the audit. And, Rich, feel free to chime in for  
232 some of the --

233 MR. STATTEL: No, you're doing fine.

234 MS. ZHANG: Okay. Don't want to speak for you guys.  
235 So in this scenario, for the inspection of the one-way boundary  
236 device between Level 4 and Level 3 and the other Levels, so we  
237 expect to conduct the inspection to verify that the device is  
238 installed and documentation exists that identifies the boundary  
239 device as a Critical Digital Asset. The CDA will be controlled  
240 under the plant cyber security program. And, oh, next slide,  
241 sorry. And we do not see a need to reconfirm that the device  
242 performs its intended function during the inspection. So that  
243 part will be what's going to be credited from the licensing review.  
244 Next slide.

245 So for Scenario 2, we will -- this one reviews the  
246 means used to protect the time-stamps utilized in Layer 4 of the  
247 cyber security defensive architecture. So Reg Guide 5.71, Section  
248 B.2.8 discusses the technical controls regarding the time-stamp  
249 source utilized for Critical Digital Assets. In this Section, it  
250 states that Critical Digital Assets should use a time source

**NEAL R. GROSS**

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

251 protected at an equal or greater Level than the CDAs. This time-  
252 stamp synchronizes the time of all CDAs from a dedicated source  
253 protected at an equal or greater Level than the CDAs existing on  
254 the security network. Next slide.

255           So in this case, the Design Certification applicant  
256 provides design information on how time-stamps are generated for  
257 important data from both safety systems and important-to-safety  
258 systems that are likely to be in Level 4. They will provide  
259 information on how the time-stamp is acquired from a protected  
260 source. So, for example, we've seen applicants provide a --  
261 propose to use GPS as a time-stamp source. And as we all know,  
262 GPS can be easily spoofed in that case.

263           So for this particular design, if a COL applicant  
264 inherits that particular design, they would either have to make  
265 design changes or come up with some other means to protect -- to  
266 time-stamp their Critical Digital Asset data. So, they would also  
267 need to discuss some security features that could be used to  
268 protect the source of the time-stamp signal. For licensees,  
269 similarly as discussed, they would provide information on how the  
270 time-stamping source is protected if that time-stamping is on a  
271 system that's included as part of the -- that's modified and  
272 included as part of the LAR. Next slide.

273           So for the NRC review, we would look at the design  
274 descriptions to determine whether the security features that

**NEAL R. GROSS**

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

275 protect the time-stamp is acceptable and that the time-stamp source  
276 is securable. For Design Certification applicants, we would  
277 expect to see an ITAAC that will verify the time-stamp source for  
278 the as-built system and that security features for the time-stamp  
279 source meets the design commitments. For the LAR submittals, the  
280 staff may perform an audit regarding how the time-stamp source is  
281 generated and review the security features for the time-stamp  
282 sources, probably as part of the audit during the FAT and the FAT  
283 results summary. Next slide.

284 So as far as the inspection, we will be conducting the  
285 cyber security programming inspection to ensure that security  
286 features were protecting the time-stamp source, that it is  
287 implemented as described, installed as described in the Design  
288 Certification, and that documentation exists that identify these  
289 features. And they will verify that the time-stamp source is  
290 protecting the same cyber security defensive Level as the system  
291 that will be receiving the time-stamp. So they will have to make  
292 sure that the time-stamp source is part of the overall cyber  
293 security program and that it is protected at the same Level as the  
294 Critical Digital Assets that it is responsible for generating the  
295 time-stamp for. Next slide.

296 So, this next scenario, it's actually from Section  
297 C.12.5 of Reg Guide 5.71. This is actually one of the management  
298 controls, it's not actually a technical control specified in Reg

**NEAL R. GROSS**

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

299 Guide 5.71. In this one, this Section specifies that the licensee  
300 or applicant needs to ensure that the acquired products meet  
301 specified security requirements and, specifically, that the  
302 products are free from known, testable vulnerabilities and  
303 malicious code by identifying and eliminating these following  
304 vulnerabilities. And they go through a list of known  
305 vulnerabilities, such as overflow code or other types of code  
306 vulnerabilities. Next slide.

307           So, for the Design Certification applicants, we expect  
308 that the Design Certification applicant will submit a test plan  
309 that documents how known testable vulnerabilities and malicious  
310 code will be identified. So, again, because the system hasn't  
311 been implemented, we don't expect to see that the code has been  
312 identified, the malicious code has been identified, that would be  
313 a future activity that will be done. But this plan should document  
314 what are some of the methods that the applicant plans to employ to  
315 identify these vulnerabilities and malicious code. And, of  
316 course, provide an ITAAC that would implement this test plan.

317           And we do recognize that vulnerabilities may change  
318 over time, so some of the information that's captured in the test  
319 plan may not be applicable, but we don't -- so this will have to  
320 be a much more higher level plan that we would have to verify as  
321 part of the ITAAC closure. The inspection activities would verify  
322 that this plan has been up-to-date with new vulnerabilities that

**NEAL R. GROSS**

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

323 may have developed. Next slide.

324           So, similarly for the licensee, they'll probably  
325 similarly submit a test plan. But because of the fact that there's  
326 not so much a time difference between when the test plan is  
327 generated and when the activity performed for the test plan will  
328 be implemented, we do expect to see more details here as far as  
329 how testable vulnerabilities and malicious code would be  
330 identified. And then there will be plans for documenting how any  
331 of the identified testable vulnerabilities can be controlled.

332           For some of these items, we don't expect that they can  
333 be eliminated, particularly if it's embedded in a safety system  
334 software and the code can't be removed, so then we'll talk about  
335 some of the other means that could be used to control such  
336 vulnerabilities and malicious code. And because this is a LAR,  
337 we would expect that the summary of the test results be provided.  
338 So, next slide.

339           MR. STATTEL: So, this is Rich Stattel. Just a couple  
340 words. If Deanna's given you the impression that we have this all  
341 figured out, that really wasn't our intent here. Really the  
342 development of these scenarios was really an exercise to try to  
343 provoke some thoughts on how we could coordinate our efforts in  
344 the licensing review area with what NSIR would performing in the  
345 inspection area and the programmatic aspects of cyber security.  
346 So, we're really trying to solicit some feedback from the industry

**NEAL R. GROSS**

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

347 and get some ideas.

348           One of the areas I will mention in the operating  
349 reactors area is the scoping of this and whether these reviews  
350 would become mandatory in the future. It's very uncertain in my  
351 mind how this would play out because the scopes of our reviews are  
352 generally determined by the scopes of the modifications being done  
353 at those plants. And a lot of times or very often, they would not  
354 include things such as the one-way devices that Deanna had  
355 mentioned in the first scenario.

356           So the question comes, do we still rely on the  
357 programmatic aspects or is there some additional activity that we  
358 would have to implement during our license review and basically  
359 extend the scope of our review to include those aspects of the  
360 design. But at the same time, we do recognize that as our  
361 technical reviewers are performing these evaluations, we become  
362 familiar with the designs of the system, it's really an opportune  
363 time to evaluate the cyber security system attributes.

364           So, it's really -- I feel that there's some benefit to  
365 doing these activities during the licensing reviews as opposed to  
366 deferring them to the inspection activities where we may not  
367 necessarily have the experts there that are capable of performing  
368 those evaluations effectively. And it becomes less, everything  
369 becomes a lot less efficient when we defer that to the inspection  
370 space. So really we'd just like to hear back from the public and

**NEAL R. GROSS**

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

371 from the industry on these ideas and see if we can kind of expand  
372 on these concepts.

373 MR. CLIFTON: This is Gordon Clifton from NEI. We  
374 appreciate your looking for subject matter expert input on it  
375 because the industry's got some passionate people on this and I'm  
376 sure we won't have any trouble bringing forth some of their good  
377 ideas. Before we get into the details, I agree with what you're  
378 saying completely there, Rich, that the scoping and whether this  
379 is mandatory all will affect the resource consumption in putting  
380 designs in and there's an appropriate time. As we found in pilot  
381 projects for other industry items is that there's an appropriate  
382 time for each document to come forth in a final format and what  
383 you could end up doing with these audits and early visits is be  
384 seeing something in a very preliminary standpoint.

385 But on the other hand, if you look at it, the time we  
386 become liable for it is when core is loaded, or as the regulations  
387 call for now, is late in the game to get started on a cyber  
388 security. So we appreciate the interest in the NRC and the  
389 industry and the vendors to start this process of being aware of  
390 cyber security considerations very early. And they aren't  
391 necessarily, as you identified, part of a design. Because it's  
392 more in the interface of the digital widget than it is of the  
393 actual component itself. Although you can have with code, you can  
394 have your problems in the code, so we need to keep quality control.

**NEAL R. GROSS**

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

395           What comes to mind in a big picture is these scenarios  
396 are great and I appreciate you bringing them forth on that, the  
397 question I was going to ask is, do we have a driver that caused  
398 these type of responses or, let's say, do we have demonstrated  
399 problems and examples where we have shortcomings in the existing  
400 Part 50 process, Part 52 process or in the QA programs or on the  
401 SER process now? Because from my standpoint, I don't think we  
402 have shortcomings on it. That I'm thinking what we can bring  
403 forth is perhaps an enhancement of what we have. And I'm not sure  
404 we need regulatory assistance for that enhancement if we can put  
405 into guidance or something that's not hard driven as rule as you  
406 put in your comments.

407           MR. RAKOVAN: Well, hold on. Let me step in a second.  
408 I thought the intent was for the NRC to get through their  
409 presentation --

410           MR. CLIFTON: Okay.

411           MR. RAKOVAN: -- before we started discussion. If that  
412 -- if we want to go off-script, that's fine. But I just -- I want  
413 to step in to see what the intent here is, if I may?

414           MR. CLIFTON: Thanks for keeping us on track.

415           MS. ZHANG: Thank you. So let me go through -- I'm  
416 almost done with these slides. So --

417           MR. RAKOVAN: Okay.

418           MS. ZHANG: -- we can --

**NEAL R. GROSS**

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

419 MR. RAKOVAN: Okay. Thank you.

420 MS. ZHANG: -- move then into answering Gordon's  
421 question. So let me just finish these last few slides. For this  
422 slide, the -- which discusses what the NRC license review would  
423 look like for Scenario 3. So the staff will review the test plan  
424 to determine whether the test activities are sufficient to identify  
425 testable vulnerabilities and malicious code. And for Design  
426 Certifications, we will look at the ITAAC to make sure that's it's  
427 sufficient to capture what would be verified as part of the ITAAC  
428 closure process. And for LARs, the staff will review the summary  
429 of the test results and may conduct audit during the development  
430 process.

431 So for the NRC inspection, next slide. For Design  
432 Certification applicants, during ITAAC closure, we will be  
433 conducting an inspection to ensure that the test plan was  
434 accurately implemented and any identified vulnerabilities and  
435 malicious code will be adequately controlled. We'll be looking  
436 at the documentation as part of this verification, as part of the  
437 inspection. And for the cyber security program inspection, the  
438 NRC will inspect the documentation provided as supplemented by the  
439 staff's previous review. We would also look at that this Critical  
440 Digital Asset has been incorporated into the overall planned cyber  
441 security program to ensure that as vulnerabilities change that the  
442 effectiveness of the controls are still adequate. Next slide.

**NEAL R. GROSS**

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

443           So, again, for this proposed SECY paper, we are seeking  
444 the Commission's direction on evaluating cyber security related  
445 design features as part of licensing. We do not intend to expand  
446 the scope of what's currently stated in 10 CFR 73.54, just what  
447 will be reviewed as part of licensing. And for Design  
448 Certification applicants, we feel that this proposal will provide  
449 added assurance that certified designs can be secured upon  
450 implementation.

451           And for NRC licensing review of cyber security design  
452 controls, we hope it could support subsequent cyber security  
453 program inspections and thereby reducing the information that  
454 needs to be reviewed as part of cyber security inspections. So  
455 this concludes my presentation and we'll move into the question  
456 and discussion portion. So with that, let me go ahead and turn  
457 back to Gordon, I think, with his question. If --

458           MR. RAKOVAN: Please. If you would, could you just  
459 give a -- rephrase if you could, briefly?

460           MR. CLIFTON: Sure. I guess what I was bringing to the  
461 table is these are great scenarios of what's out there. But I was  
462 wondering if we have examples that you've seen that perhaps we're  
463 not aware of where we've had a shortcoming in cyber security that  
464 -- where something was broken and we're trying to fix? Or are we  
465 just looking to enhance the process so we all have a greater  
466 comfort zone that when we implement the systems as you pointed out

**NEAL R. GROSS**

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

467 here, that upon implementation that's when we're most liable with  
468 it?

469 MS. ZHANG: Okay. So I do have a couple examples. But  
470 I don't want to call it shortcomings. Because we don't want to  
471 say that our current cyber security regulatory framework is broken  
472 or anything like that. Just as we said before, this is to  
473 facilitate implementation of the cyber security program. And this  
474 is to compliment it, not that there needs to be anything -- but  
475 this is to help support it. So, for Design Certification, and you  
476 can probably see, there's a little bit of a difference between new  
477 reactor applicants and a current licensee seeking a License  
478 Amendment Request.

479 And what we've seen in the two examples I'm going to  
480 talk about, they're Design Certification applicants. So in one  
481 case, an applicant picked a time-stamp, a GPS as their time-stamp  
482 for both their safety and important-to-safety, all their Level 4  
483 systems. And when we looked at this, obviously that source is not  
484 securable. However, because there wasn't an active COL that maybe  
485 would drive that design at the -- feature at the time, that part  
486 was specified in the certified design. So if an applicant were  
487 to come back and say, well, that can't be secure, well, we can't  
488 use that source. They would need to make certain design changes  
489 and probably much later in the development process, maybe much  
490 later in the development process.

**NEAL R. GROSS**

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

491           So that's one thing we would like to help prevent is  
492 that when we have Design Certifications proposing designs that are  
493 not securable, that we can get it ahead of time and help drive it  
494 to something that is securable. Something similar was another  
495 applicant proposed a firewall between Level 4 and Level 3 systems.  
496 And, again, this is something similar. We noticed that, that it  
497 was a firewall. And although there was a COL applicant, we  
498 informed of this, there wasn't a proposed design change.

499           They said they would have to do something after the  
500 fact, after Design Certification, after it gets into the plant,  
501 they may have to add another device on top of the firewall. So,  
502 as you can see, these two examples shows how the securable aspects  
503 of the designs were not really thought out during the Design  
504 Certification.

505           MR. CLIFTON: Early on?

506           MR. JACKSON: I think one of the other things we saw  
507 too was that, especially on the new plants, when they're developing  
508 a new INC system, that they're not really separating out cyber  
509 security and the INC safety aspects either. They're developing  
510 them simultaneously. So they're part of the requirements if they  
511 need be. So, therefore, when they come in to the NRC for license  
512 approval and so forth, they're separating out cyber security from  
513 the safety aspect because, at this time, we're not reviewing the  
514 cyber security aspects in the INC safety review. So it takes a

**NEAL R. GROSS**

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

515 little bit of work and a little bit of coordination on their end  
516 to separate back out, even though it really is done concurrently.

517 MR. STATTEL: I'd like to point out, clearly the  
518 scenarios weren't developed in a vacuum and clearly our experiences  
519 kind of factored into the development of these. But they are  
520 hypothetical. So don't read too much into these scenarios.  
521 Really the idea was just to get the thought process going. We  
522 also have experience in the operating realm in our applications  
523 and in our safety evaluations. We've evaluated one-way devices  
524 that are credited in cyber security programs and we've done, to a  
525 certain degree in the early applications for Ocone for example,  
526 we did some cyber security evaluation portion of that application.

527 So -- but please don't read too much into these. We're  
528 really not pointing at any shortcomings of past projects or  
529 current, ongoing projects. Really what we tried to do is we  
530 developed the scenarios based on our experience and we tried to  
531 jot down some notes here on how -- what would be the best way that  
532 we could approach these things in the future. And really, that's  
533 kind of the direction we're kind of seeking from the Commission as  
534 far as policy and how we address these cyber security issues going  
535 forward and doing it as efficiently as we can. And it is a  
536 challenge, I will say that.

537 MR. CLIFTON: The challenge for you is drafting the  
538 SECY with the words that you prefer, a direction to take in the

**NEAL R. GROSS**

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

539 future and then looking for approval of that. And we appreciate  
540 it on the industry side for you opening up the dialogue, if you  
541 will, so that we can discuss it in public formats and come back to  
542 optimize it as what we have. Have you got an implementation  
543 schedule for your SECY? Are you looking in 2015, early 2016 or  
544 anything like that?

545 MS. ZHANG: Yes. So currently, we're scheduled to  
546 provide the SECY paper to the Commission at the -- sometime this  
547 calendar year. So, it is an aggressive schedule.

548 MR. STATTEL: Yes, it is. But --

549 MR. RAKOVAN: I'm going to step in real quick and just  
550 remind folks if you could introduce yourselves when you speak so  
551 those on the phone can follow. Thank you.

552 MR. STATTEL: Sorry.

553 MR. JACKSON: This is Terry Jackson. And so I think  
554 our next step is after incorporating feedback from this public  
555 meeting, we would try to finalize the SECY and get it to the  
556 Commission. Gordon, I think you asked another question earlier  
557 as well. You were asking if we needed really like a rule making  
558 to do this or could it be done in guidance. And I think where  
559 we're at right now is we're kind of leaving that up to the  
560 Commission. And that's part of what we're seeking direction on,  
561 all the way up to rule making.

562 We kind of see right now the point where we would need

**NEAL R. GROSS**

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

563 at least some kind of policy decision with regards to that because  
564 the policy was basically set to implement 73.54 as a programmatic  
565 rule. So that wouldn't necessarily force anyone to bring any kind  
566 of design information in. So it really is up to the Commission  
567 to decide if they want to go all the way to rule making or if they  
568 want to stay with guidance. Or there's also the third option we  
569 have in SECY, which is basically stay with what we have right now.

570 MR. CLIFTON: And so, do nothing and use -- this is  
571 Gordon Clifton with NEI. Doing nothing and using existing  
572 processes, as Deanna pointed out, is we're pretty pleased that  
573 it's working and we have confidence that when you're looking at  
574 enhancement here, a step forward. I'd be concerned if we put rule  
575 making in that got into too much details of how to do something.  
576 We want to keep rule making up at level where it tells what's  
577 required, what criteria are expected to be met. And then we'll  
578 use Reg Guides and lower level guidance material to say how to do  
579 things or provide an approved path to do something. Reg Guides  
580 are best purposed for that.

581 But we don't want to get into an order or rule,  
582 something that is trying to design components and enforce  
583 inspection intervals that are perhaps unnecessary. And if we get  
584 into, like you and I have talked and projects have graded  
585 approaches, some of these things would be foolish use of resources  
586 to go with a full auditor inspection if you have a very small

**NEAL R. GROSS**

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

587 modification.

588 MR. STATTEL: Right. This is Rich Stattel. One of the  
589 things that occurred to me when we were developing these scenarios  
590 and writing down what our proposed actions would be, is that a lot  
591 of these actions, I would say the majority of actions that you see  
592 listed in these slides here are things that we already do. So,  
593 for example, if a cyber security requirement was going to be  
594 implemented within the design of a system, that would become part  
595 of the design requirements. And we already review those and we  
596 already review how they're implemented and how traceability is  
597 established.

598 So, you really can't separate the cyber security  
599 aspects from the design elements of a system or the design  
600 processes because they are part and parcel. So, currently -- in  
601 our recent experience, we don't see a lot of 73.54 criteria being  
602 implemented within the design of safety systems, for example. A  
603 lot of it falls outside of that into the important-to-safety  
604 classifications or they're being foregone for other reasons. So  
605 their programmatic approach is more on the lines of protecting the  
606 crown jewels, rather than imposing the protections within them.

607 So, we don't have a lot of experience with reviewing  
608 the implementation of those aspects. And our current SDOE  
609 approach to performing our licensing reviews really concentrates  
610 on protecting the safety functions and not really looking at the

**NEAL R. GROSS**

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

611 malicious aspects of that. So that's one of the things that could  
612 potentially change as a result of the direction we receive from  
613 the Commission.

614 MR. CLIFTON: All right.

615 MR. STATTEL: So you need to be aware of that as well.

616 MR. CLIFTON: I think that's what --

617 MS. ZHANG: Yes.

618 MR. CLIFTON: This is Gordon Clifton from NEI. That's  
619 what you addressed earlier, right?

620 MS. ZHANG: Yes.

621 MR. CLIFTON: It's a separation between physical  
622 security versus electronic security --

623 MS. ZHANG: So --

624 MR. CLIFTON: -- devices.

625 MS. ZHANG: Yes. So as Terry had mentioned, if we want  
626 to -- this isn't just requiring an applicant to submit some design  
627 information. But even if we want to review voluntarily submitted  
628 cyber security design information, there needs to be probably a  
629 policy decision there as currently we do not do that per policy.  
630 So that's why we are seeking the Commissioners' direction.  
631 Because we have had Design Certification applicants come in and  
632 say, here's our proposal, can you review it? And we did not have  
633 the ability to do that under our current policy.

634 MR. CLIFTON: This is Gordon Clifton. I'm not sure

**NEAL R. GROSS**

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

635 ability is the right word there, but you didn't have, let's say,  
636 a regulatory driven --

637 MS. ZHANG: Yes.

638 MR. CLIFTON: -- requirement to do that. But we had  
639 an example at Diablo Canyon, where NSIR came and audited but as  
640 the project manager of NRC made it clear is that there was no  
641 regulatory need for inspection, inspection findings, and  
642 enforcement because that was outside their purview, their scope at  
643 the moment. So that's where we appreciated that it was brought  
644 up, it was an issue. But it was a volunteer basis from the  
645 industry, utility to encourage the audit, let them come on site,  
646 show them what was going on, develop the confidence that it was  
647 being done, even though it wasn't regulatory driven. And so, I  
648 think that's supporting what all of us are saying is, what's  
649 working now is working. We only need to polish the apple or  
650 enhance what's already working right now.

651 MR. STATTEL: Right. And that -- this is Rich Stattel.  
652 That was a pilot project, so we were kind of just --

653 MR. CLIFTON: Seeing if it would work?

654 MR. STATTEL: -- kind of breaking the ice on this. At  
655 the time that those audits were performed, the design really had  
656 not been complete or implemented in the Diablo Canyon project. I  
657 will say -- now you can read the reports, right? And there's  
658 really no safety conclusions resulting from that. There's some

**NEAL R. GROSS**

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

659 observations. But now that some time has passed, we're nearing  
660 completion of our safety evaluation, but, again, we're not really  
661 addressing the malicious code aspects of that at all. And that's  
662 still really deferred to the programmatic aspect.

663 So how the licensee implements that system within  
664 their cyber security program is really going to be the subject of  
665 future inspections. So there wasn't any concerted cyber security  
666 review effort as part of this application. So, we really haven't  
667 figured it out. Even though we've learned a lot from the pilot,  
668 I will say, but we really haven't figured out exactly how to tackle  
669 this.

670 MR. CLIFTON: This is Gordon Clifton again. Go look  
671 for it at the installations? Or installation testing or something  
672 like that? But then it's so late, if there's a problem that we -  
673 -

674 MR. STATTEL: And that's --

675 MR. CLIFTON: -- didn't catch earlier --

676 MR. STATTEL: And that's the risk that --

677 MR. CLIFTON: -- it stops the calendar and --

678 MR. STATTEL: Yes.

679 MR. CLIFTON: -- hurts us.

680 MR. STATTEL: Yes. We recognize that there's some risk  
681 there. Particularly with the -- in the operating plants as a new  
682 system is being implemented, if no cyber security review or

**NEAL R. GROSS**

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

683 evaluation was done during the licensing review, then the danger  
684 is they get down to the installation and either through the  
685 inspections or through just the process of implementing that system  
686 or putting into their cyber security program, they identify  
687 shortcomings and now they're in a place where they have to make  
688 design changes, create new requirements for that system that had  
689 not been evaluated by the NRC. So they may be handled under a  
690 50.59 process or maybe not. I'm not exactly sure how that would  
691 go. I guess it would depend on the significance of the findings  
692 at that time.

693 MR. CLIFTON: Yes. You'd hope -- this is Gordon  
694 Clifton again. You'd hope it would be in the modification process.  
695 Because the 50.59 is just going to be whether we bring the process  
696 to you for LAR-type processing or we take care of it ourselves.  
697 But the process that would find and incorporate necessary  
698 enhancements to the cyber security plan would be in the  
699 modification process. And we would expect that starting 13 to 15  
700 months beforehand.

701 MR. STATTEL: So --

702 MR. CLIFTON: But that -- there's nothing that you see  
703 as the --

704 MR. STATTEL: Yes.

705 MR. CLIFTON: -- SER author that would identify that,  
706 that had been accomplished.

**NEAL R. GROSS**

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

707 MR. STATTEL: Yes. So, Rich Stattel again. So there's  
708 kind of a dual purpose to the SECY paper that we're writing. One  
709 is to help us as far as defining what is our review process going  
710 to look like and how does this coordinate with the NSIR activities  
711 when the inspections are performed. The second is, it's a little  
712 bit more subtle, but it's really -- under the current process where  
713 we're really only looking at the malicious aspects of cyber  
714 security at the very end or at the implementation stage of design,  
715 we may be inadvertently discouraging addressing them early on in  
716 the design.

717 Which is clearly -- I think the industry knows, that's  
718 the better place to do it. So it's kind of a matter of perception.  
719 I think most people understand that it's better to do the  
720 vulnerability assessments and to address them early in the design  
721 phases. But we're not looking at them then. We're not looking  
722 at them until they're implemented under our current processes. So  
723 there's kind of a gap there, it's kind of a timing gap.

724 MR. CLIFTON: Right. This is Gordon Clifton. When we  
725 look at a milestone for installation, we could identify a milestone  
726 in there to commence involvement with cyber security concerns.  
727 But that's still just a bullet on the milestone calendar. That's  
728 -- where to set it is a choice we all have to discuss.

729 MS. ZHANG: And -- this is Deanna Zhang. And for new  
730 reactors with Design Certification applicants, sometimes there is

**NEAL R. GROSS**

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

731 no COL applicant to work with the Design Certification applicant  
732 at their time of Design Certification --

733 MR. CLIFTON: Right.

734 MS. ZHANG: -- to get the design such that it is  
735 securable once implemented.

736 MR. CLIFTON: So what we need to work together with is  
737 come up with some optimum positioning, if you will, of the start  
738 date for involvement with cyber security. And then looking at the  
739 boots and gun as well as the small wires aspects of it. Okay.

740 MS. LAWSON-JENKINS: Hi, this is Kim Lawson-Jenkins.  
741 I just wanted to add one comment about the example we have about  
742 finding the vulnerabilities early. I appreciate the example for  
743 using test plans. But there's another scenario that could have  
744 been said for doing those kind of vulnerability -- to find those  
745 in, I think you said, in the coding phase. Because now you have  
746 compilers that will eliminate vulnerabilities.

747 They'll say, if they find it, while you generate and  
748 compile the software and pull it into a build. And to find that  
749 there, you're really reducing the attack space that -- much earlier  
750 in the cycle so then you only have to worry about the newer  
751 vulnerabilities. So there's a lot of scenarios here where it's  
752 really advantageous to get things out earlier. And to reduce the  
753 attack space and worry about the newer threats that are coming  
754 along, rather than the same things we've been seeing year after

**NEAL R. GROSS**

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

755 year.

756 MR. CLIFTON: Right. This is Gordon Clifton. Rich,  
757 you could probably bring the example of Oconee, where you had to  
758 go back and look at code and the security that went with the code  
759 development while it was early on stages.

760 MR. STATTEL: And we do. We do that frequently during  
761 our application reviews. What is new here though is the NSIR  
762 involvement. Because even during the inspection activities or the  
763 audit activities that we did with Diablo Canyon, I don't think the  
764 inspectors had a lot of previous experience or opportunities to  
765 get involved in that design implementation or the design  
766 development, the design processes.

767 So it's a little awkward because they're not used to  
768 doing that. They're used to reviewing or doing inspections on a  
769 completed design implementation operating in the plant and we're  
770 on the other end of it, where we're looking at the design processes  
771 and the development of the design. So where do we meet in the  
772 middle? I think that's the crux of the matter here.

773 MR. CLIFTON: This is Gordon Clifton again. We're  
774 counting a lot on the quality control of the vendors who are  
775 creating the code. Because we're getting into a situation where  
776 we're going to have topical reports and packages. And digital  
777 packages are going to come to us pretty much black box. And they  
778 may have 1,200 installations around the world elsewhere working

**NEAL R. GROSS**

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

779 just fine and our opportunity, NRC or current reviewers, would  
780 have a great deal of difficulty getting into the code that's been  
781 in place for years and years and practiced and sealed.

782 MR. STATTEL: Right. Now, I will mention -- this is  
783 Rich Stattel again. I will mention that we do recognize that.  
784 And we recognize that the licensees, the ultimate licensees aren't  
785 always involved in those development processes, particularly in  
786 the platforms. So for that reason, we do perform a, not a cyber  
787 security review, but we perform a secure development and operating  
788 environment review of the platforms themselves. And that does --  
789 that review does involve assessment of how the vendor is  
790 identifying vulnerabilities and hazards that may be present in  
791 that system and how they're addressing them.

792 So that's kind of our effort, that's what we've done  
793 so far in trying to address those early on. But, again, it can  
794 be years, it can be five, ten, 15 years between the time that those  
795 platforms are developed and the time they end up actually going  
796 into a plant and performing safety functions. So there's a long  
797 span of time and a lot of development activities that occur during  
798 that period of time.

799 And it's a little daunting, but that's really what  
800 we're trying to address here to try to, A, encourage early  
801 identification of vulnerabilities and means of addressing them and  
802 also provide basically a two-stage, as part of the licensing

**NEAL R. GROSS**

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

803 process, we would evaluate how those are being assessed, how the  
804 regulations are being met, and then once they're installed, the  
805 inspection would basically be the final coverage of the regulatory  
806 requirements.

807 MR. CLIFTON: Going back to what Kim's saying, the  
808 challenge that we'd have in setting this milestone for starting  
809 the review is the challenge in ownership too. Because at the  
810 early stages when the code is written, especially in a platform  
811 basis, the ownership is with the vendor, which NRC doesn't have  
812 direct hooks on. And the licensee can request and ensure that in  
813 their specification development that they put these type of  
814 requirements in, but when we go back for platforms that were  
815 written, like you said, five, ten, or 15 years earlier, to go back  
816 to assess whether there was a code anomaly in there is a real  
817 challenge if it belongs to somebody else, it isn't to the vendor's  
818 control yet, their ownership, or anything like that. So not an  
819 easy task, no question.

820 MS. LAWSON-JENKINS: No. I've worked in software  
821 development. I agree it's not an easy task. But to, at least,  
822 to start to look at where the flaws are, where the vulnerabilities  
823 are, and to do ongoing updates to keep moving forward. Because,  
824 as you say, these things have been in the field for years, but new  
825 vulnerabilities come every day and they have to be addressed and  
826 there's a process for addressing that, so that whenever you do

**NEAL R. GROSS**

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

827 bring it into a new device, you know you've gotten the latest best  
828 software at that date.

829 MR. STATTEL: Right.

830 MS. ZHANG: Yes. So I think what we're trying to say  
831 is that we're trying to set up -- have the licensees set up a  
832 baseline when they take in that platform. So they will evaluate  
833 and test for known vulnerabilities and malicious code. And, as  
834 you have brought up, there probably was some quality assurance  
835 process used. We saw that for the TELEPERM XS for the Oconee  
836 review, back when they were developing the system. They did have  
837 some measures that they did to prevent malicious code from being  
838 injected into the system.

839 But on top of that, you have vulnerable code. That  
840 is something that a quality assurance project would not be able to  
841 capture. And that's why you need to test for known vulnerabilities  
842 at the time that you are adopting this platform for this particular  
843 application.

844 MR. CLIFTON: And that's -- this is Gordon Clifton  
845 again. That's using third party software typically, right?

846 MS. ZHANG: Yes.

847 MR. CLIFTON: Which then we have to validate that as an  
848 appropriate means as well. So it's a cascading sense of  
849 responsibilities that it will be a challenge to direct or to put  
850 it in writing.

**NEAL R. GROSS**

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

851 MS. LAWSON-JENKINS: And the last thing I want to say,  
852 at least on this topic, is that it really forces everyone to  
853 understand what the product does, what's in the product. And a  
854 lot of times, we buy things where the seller is making the  
855 assurance, this product does this function, it does this type of  
856 security feature. And then at the end of the day, how do you know  
857 what software's in there, what software's performing that  
858 function?

859 There have been vulnerabilities, like for example,  
860 with OpenSSL. New vulnerabilities have come up and people don't  
861 know what software's in their product. So you don't even know the  
862 vulnerability's there. So when you start this process of engaging  
863 with the suppliers, understanding really how are they providing  
864 these services, what software it's built on, then you can go  
865 forward and say, okay, we'll have to watch for these advisories on  
866 this type of software, you understand that. And it is a long  
867 process and it's involved, but then you have better assurance that  
868 you are protected and then meeting the rule.

869 MR. STATTEL: Absolutely. Did we want to open to the  
870 floor to -- I guess it would be a good time, I think, to basically  
871 get some feedback on the individual scenarios, if anyone has  
872 questions about what we've written in the slides here?

873 MS. ZHANG: Lance?

874 MR. RAKOVAN: Okay. Sounds good. Emily, if you would,

**NEAL R. GROSS**

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

875 could you go ahead and start taking some questions or comments  
876 from the phone lines and start a queue?

877 OPERATOR: Thank you, sir. At this time, anyone  
878 wishing to ask a question or make a comment, please press Star 1  
879 on your touchtone phone. Please be sure that your telephone is  
880 unmuted and clearly records your name when prompted so that your  
881 question may be introduced. Once again, if you're wishing to ask  
882 a question or make a comment, please press Star 1 at this time.  
883 And it does take just a few moments for the questions to come up.

884 MR. RAKOVAN: Thank you. And for those of you in the  
885 room, obviously you don't have to hit Star 1, you can come over to  
886 the podium that we have here. And if you could just, again,  
887 introduce yourself and any organization that you're with, we'd  
888 appreciate that.

889 OPERATOR: And, sir, we do have a question from the  
890 telephone lines.

891 MR. RAKOVAN: Okay. Please go ahead.

892 OPERATOR: And that question comes from Jay Amin. Sir,  
893 your line is open.

894 MR. AMIN: Okay, hi. Okay, I have a couple of comments.  
895 On the examples, if an LAR is submitted, say for an operating  
896 plant, the key thing to look at is the architecture for the change  
897 and the connectivities and how cyber is addressed. This is what  
898 I would want to see as an NRC. Because if you kind of leave it

**NEAL R. GROSS**

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

899 vague, then it is very difficult to ascertain how the  
900 connectivities are impacting or how cyber security comes into play.  
901 So the connectivity part and the architecture are key elements  
902 that you want to look at up front.

903           And then, also, if one does -- if the architecture  
904 shows and the connectivity shows that everything is behind the  
905 existing diode, then I don't believe there is a reason to even  
906 look at the diode that has already been implemented and bought off  
907 previously. Unless there is a reason to look at it. For example,  
908 if I'm installing a massive platform and I already have a diode  
909 and then I'm sending data outside that diode, that could interest  
910 you because I'm sending data that is going to be quite a bit of  
911 data going through a diode that was installed for, who knows, maybe  
912 a small bandwidth versus a larger bandwidth. But that's one  
913 example.

914           Another comment that I had is, I'd like to have  
915 everything move towards a standard. And that's something trying  
916 to work in the backgrounds to see who IEEE sees this. But when  
917 you look at cyber, it is no more than one element of many digital  
918 design attributes. For example, seismic environment, EMI, RFI.  
919 And I don't think so that every time we address digital, we need  
920 to be too prescriptive.

921           And I believe that the code reviews for malware and  
922 anything else, and I'm talking application codes, unless there is

**NEAL R. GROSS**

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

923 an operating system from Microsoft that was modified by an  
924 integrator, you want the V&V process to address cyber security as  
925 one of the elements. Because that's where you want to do that,  
926 because V&V tests code, they review codes and scripts. So that's  
927 where you want to integrate it. So I think the focus should be  
928 to integrate some of these elements of cyber that touch base with  
929 software and all of that into the V&V process going forward.

930 MR. STATTEL: This is Rich Stattel. Thanks for your  
931 input, Jay. I kind of want to respond to your first question with  
932 a question back to you. Why -- I do agree with you that the  
933 architecture and the interfaces are basically key features of a  
934 system that I always want to review on a system. Why would you  
935 think that would be more or particularly applicable to a license  
936 amendment as opposed to a new reactor design?

937 MR. AMIN: Well, it could -- I don't know. It depends  
938 upon what the application is on an operating plant coming on an  
939 LAR and for a new plant. And the reason why I say that is my  
940 simple mind says that if you want to -- if I'm bringing in a new  
941 application today for Comanche Peak or, say, for example, anything  
942 new, then I got to be smarter based on all the experience levels.

943 So, in other words, you want the architecture because  
944 if you do not address things in either a holistic manner, where  
945 everything inhabits, like somebody used the diamond example, then  
946 that is fine if it's acceptable, but if not, then if you're going

**NEAL R. GROSS**

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

947 to go implement security controls within the platform, then you  
948 have to have an architecture that determines how the  
949 connectivities, how the flows will occur, so that you can then  
950 assure yourself that you can carry that design through the  
951 implementation.

952           Because, remember, there is functional design that  
953 comes into play where a software person may say, hey, functionally  
954 I should allow this widget to talk to this particular non-safety-  
955 related item. And so you want some rules in place up front. You  
956 cannot do that unless you establish some of those up-front  
957 architecture rules. Because I think software, malware, and all  
958 that, I believe IEEE 10-12 should address that for consistency and  
959 standardization.

960           The only thing that will not work is on the operating  
961 system, like I said. Because I'm not sure that Microsoft is going  
962 to provide code to everybody to review. They will provide you out  
963 of the box trusted software and a version number and a  
964 certification that it's free from malware and a list of  
965 vulnerabilities that still may be open, known vulnerabilities. So  
966 that becomes your starting point.

967           And then at the integrator's facility, like you said  
968 before and, I guess, Gordon Clifton had been talked about it, which  
969 is that you have a secure development environment that would then  
970 ensure that any changes made to operating systems were done under

**NEAL R. GROSS**

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

971 a process in a secure environment. Because I think you'd have a  
972 false sense of security if we believe that we are going to go do  
973 a code-by-code review on a Windows operating system. I'm not sure  
974 that's going to happen or it's -- because the vendors would cut us  
975 off.

976 MR. STATTEL: Okay. This is Rich Stattel. Thank you  
977 for that input. I'd like -- there's a couple aspects of this I  
978 would like to speak to. One is the V&V activities. And I agree  
979 with the idea that the V&V activities could be a useful means of  
980 addressing cyber security vulnerabilities. However, it would  
981 require kind of a paradigm shift because 10-12, IEEE 10-12, as  
982 many of you know, is really a serial or sequential process for  
983 developing a system and with an end goal of installing it into the  
984 plant.

985 And the challenge here, when it comes to cyber  
986 security, is that a lot of the vulnerabilities and the vectors can  
987 happen after the fact. So after the system is running, it's  
988 operating the plant, performing safety functions, these  
989 vulnerabilities become apparent or they get developed after the  
990 fact. And the 10-12 processes, the V&V has been completed prior  
991 to installation in the plant. So it's really not set up to  
992 directly address those. Although I think the activities are  
993 wholly appropriate, but you can't -- it's hard to envision a V&V  
994 process that would be ongoing that you're constantly re-performing

**NEAL R. GROSS**

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

995 the V&V activities.

996           So I think that's a challenge. I'm not on the 10-12  
997 Committee, so I don't know exactly where -- how IEEE 10-12, the  
998 membership is trying to address these aspects. But they do include  
999 activities to address the architecture of the system. So you had  
1000 mentioned that in your first question. I believe the architecture  
1001 is very important and it's something that we do concentrate on in  
1002 both the new reactor reviews, design reviews, and the operating  
1003 reviews. It's a little -- I kind of feel that it's a little bit  
1004 easier to do in the new reactor designs because you have the whole  
1005 system, safety, non-safety, out in front of you when you're doing  
1006 the Design Certification reviews.

1007           Whereas, in the operating plants, we're kind of having  
1008 to shift our MO here because we're typically only looking at a  
1009 little piece of the system that's being upgraded. And it's -- to  
1010 get an idea of what the architecture of that is and what the  
1011 overall perspective of that system is, you really have to go beyond  
1012 the scope of the license amendment itself. So that's been  
1013 challenging for us, but we do that on a regular basis.

1014           So, for example, the Diablo Canyon project that's  
1015 currently under review, it's really just a PPS. It's a very  
1016 limited scope upgrade of the reactor protection system and the  
1017 ESFAS system. But we required the applicant to describe all the  
1018 interfaces to all other systems and we -- in their application,

**NEAL R. GROSS**

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

1019 they did include a very detailed description of what those  
1020 interfaces are. So we have a pretty good understanding of that  
1021 architecture. And I think we would carry that forward into any  
1022 future reviews. But it is a little bit more challenging in the  
1023 operating realm because typically we're seeing piecemeal upgrades  
1024 when these license amendments come through.

1025           Now, as far as the standards development, it was your  
1026 second question, I can speak a little bit for the IEEE standards.  
1027 They -- it has been debated at the impact level and we've had a  
1028 lot of discussions in IEEE 7432, of which Deanna and I are members  
1029 of that working group, there's a lot of people who think that the  
1030 IEEE should pursue developing a separate standard just to deal  
1031 with the cyber security aspects of digital systems.

1032           And that's -- it sounds like a good concept and a good  
1033 path to go down, but it's very challenging because a lot of those  
1034 same people who you would need to develop that type of standard  
1035 are also on these other committees and developing the standards  
1036 for 7432, which deal with all the multitude of other aspects of  
1037 digital systems that have to be addressed. So I will admit, we  
1038 haven't really addressed it very thoroughly within IEEE 7432.

1039           MS. ZHANG: Well, we actually took an effort to remove  
1040 it because we felt that it's a broader subject that's beyond the  
1041 scope of IEEE 7432. And, in addition, one of the things that we  
1042 have to recognize is that anything that would be related to cyber

**NEAL R. GROSS**

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

1043 security that would be developed would -- it's going to be a long  
1044 development process. So we're not going to get a standard that's  
1045 going to come out any time soon from the IEEE group regarding cyber  
1046 security.

1047 MR. STATTEL: No. The other thing I'm very adverse to  
1048 is the development of duplicative standards. And since we have  
1049 guidance on cyber security implementation in Reg Guide 5.71, I  
1050 believe it might not be too beneficial to try to duplicate those  
1051 type or modify that set of guidance --

1052 MS. ZHANG: Unless it's --

1053 MR. STATTEL: -- inside of IEEE space.

1054 MS. ZHANG: -- at implementation. Yes. More of an  
1055 implementation type of guidance of Reg Guide 5.71.

1056 MR. CLIFTON: This is Gordon Clifton. That's what I  
1057 was just leading to is implementation. Because Kim's talking  
1058 about code writing, you're talking about involvement in the  
1059 development of the process and approach. You're looking at  
1060 implementation in the site. We're looking at in an inspection  
1061 process, audit process, a review from milestone, from soup to nuts.  
1062 We're looking at when it gets started to actually when it's in  
1063 plant and you have a very, let's say, code fault and you get a  
1064 trigger long after installation, that's the way we get a fault in  
1065 digital. It's a two step process, you have the error in the code  
1066 and then you get a trigger later on.

**NEAL R. GROSS**

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

1067 But we're looking at something that goes from soup to  
1068 nuts. We're not in a single point that's going to work acceptably.  
1069 And we saw that when we were at the audit that occurred at Diablo  
1070 Canyon. They came out and they looked at it and stuff wasn't  
1071 ready for their perusal at the moment. But it was way past the  
1072 code writing. So multiple stages in here and, like you said,  
1073 that's going to be a challenge of implementation of how to look  
1074 for cyber from start to finish without slowing down the process  
1075 unnecessarily or duplicating other process that's already in  
1076 place. And we've got 5.71 and 1.152 are both in place that are  
1077 working pretty well right now for their own respective parts.

1078 MR. STATTEL: I do agree and I believe they have been  
1079 effective. And we have been using them for a number of years now.  
1080 Now, it hasn't been that many years so --

1081 MR. CLIFTON: Or that many examples.

1082 MR. STATTEL: -- and it only takes one incident to prove  
1083 me wrong, right?

1084 MR. CLIFTON: Right.

1085 MR. STATTEL: But I do believe a lot of the measures  
1086 that have been implemented will be effective in maintaining the  
1087 security of these systems. Now, we have learned a lot and the  
1088 industry has matured and over the last ten years, I got to say,  
1089 the discussions even five years ago were much different. Because  
1090 what we were really discussing then is, do we do these reviews as

**NEAL R. GROSS**

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

1091 part of the licensing application or do we do them just simply by  
1092 programmatic and inspection activities? And it was just an  
1093 either/or type discussion.

1094 And it may seem to you that we're having the same  
1095 discussion today, but in truth, I think we've all learned that  
1096 neither approach really covers the whole range of cyber security  
1097 issues. So it's a complicated matter and I think it does deserve  
1098 a multi-prong approach. So I think approaching it basically from  
1099 the top down, from the inspection perspective, as well as from the  
1100 bottom up, where we do some review of cyber security at the license  
1101 review stage, I think that's appropriate. And that's really what  
1102 we're suggesting in the SECY paper. And that's what we will be  
1103 recommending to the Commission as a policy going forward. So I  
1104 think there's benefits to both sides.

1105 MR. CLIFTON: We cover everything Jay brought forth?

1106 MR. STATTEL: Probably not. But I'm sure Jay will  
1107 point out the aspects --

1108 MR. CLIFTON: Omissions.

1109 MR. STATTEL: -- we missed of his questions there.

1110 MR. AMIN: No, you haven't. I mean, that's good. But  
1111 I'd just like to point only one thing on the V&V. The V&V is for  
1112 a large-scale system, whether it's in an operating unit or whether  
1113 it's a new build application. But the baseline V&V software  
1114 doesn't change. If you put it under configuration management and

**NEAL R. GROSS**

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

1115 all the tight controls, then it's not going to change. The key  
1116 thing is the -- after installation, during the operations and  
1117 maintenance phase, how are those systems managed, maintained, and  
1118 reviewed and evaluated for cyber security? And that is where we  
1119 as licensees, when you look at Reg Guide 5.71 controls, are  
1120 implementing some of those elements into our processes.

1121           Because that's what's going to drive change, right?  
1122 If I'm going to make a change to an operating system, I'm going to  
1123 change a safety alert screen with another screen that has an  
1124 updated software or identical software, the process because of  
1125 cyber security as we march towards Milestone 8 will be address all  
1126 those elements.

1127           MR. STATTEL: Okay. So there was two things I heard  
1128 in that discussion. One was the graded approach aspect. And  
1129 that's something we're trying to address in the ISG6 process. So  
1130 we do have some ideas for how to scale based on a full reactor  
1131 protection system versus single components. And I think there's  
1132 some progress to be made there. And the second part of that --

1133           MR. CLIFTON: Configuration management and then  
1134 maintaining it once it's going.

1135           MR. STATTEL: Yes, right. Basically it refers back to  
1136 the process or the cyber security plan, implementation of the plan  
1137 or the --

1138           MR. AMIN: Correct.

**NEAL R. GROSS**

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

1139 MR. STATTEL: -- the programmatic aspects of that. And  
1140 I think that's just as important. The plants need to be diligent.  
1141 They need to be constantly looking out for new threats and  
1142 identifying different vectors. And that's where your programs  
1143 come into play. Our inspections kind of go out and make sure that  
1144 you're meeting the regulations, but the real defense we have  
1145 against cyber security attack is really going to come down to how  
1146 well those programs are implemented on an ongoing basis at the  
1147 plants.

1148 MS. ZHANG: This is Deanna. And as we said before,  
1149 we're just trying to set a baseline so that when you install the  
1150 system into the plant, we know at that point that there was a good  
1151 look to make sure that it is a secure design such that when you do  
1152 put it into the plant, you can let the cyber security program then  
1153 take over. So it would be additional on top of what was done as  
1154 the baseline, not -- you wouldn't have to look at all  
1155 vulnerabilities that weren't identified prior to that.

1156 MR. AMIN: And, no, I agree. You have to understand,  
1157 up until now configuration management was for digital attributes.  
1158 Now, with cyber security nuances, there is also configuration  
1159 management that pertains to cyber security. We never went into  
1160 vertical depth of version numbers for like equipment and software  
1161 and all that. Now, every change coming in is challenged to make  
1162 sure it's identical, if so, how is it proven it's identical?

**NEAL R. GROSS**

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

1163 Because a vendor may call everything, oh, it's identical. When  
1164 you look at it, it's not. So licensees are getting a lot smarter  
1165 in that area and that will significantly help cyber security.

1166           And then the -- several initiatives in the industry is  
1167 looking at to address the threat and vulnerability, how do we  
1168 become smart in addressing vulnerabilities? Because you can't  
1169 just go poll the internet every day looking for vulnerabilities.  
1170 So we have to be smart about what we have and what are the  
1171 vulnerabilities associated with it. And many times many  
1172 vulnerabilities do not apply because most of the vulnerabilities  
1173 I see many times are network related. If your systems are not  
1174 even network connected behind diodes, you still have to assess  
1175 that, but there is no threat vector that makes it in. And, of  
1176 course, I worry more about the portable media.

1177           MR. STATTEL: There was -- I just remembered. There  
1178 was one other question you had asked about is the review of the  
1179 data diode and the repeat reviews on subsequent applications. We  
1180 have, like for instance, the Oconee -- the data diode that was  
1181 used for the Oconee, that device was evaluated by the NRC and it  
1182 was a fairly extensive evaluation. That same device is being used  
1183 at Diablo Canyon and we did not repeat that evaluation. So we do  
1184 credit the precedent that we set and we try to be efficient and  
1185 not repeat our evaluations when we get those results.

1186           MR. AMIN: Well, that's good.

**NEAL R. GROSS**

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

1187 MR. STATTEL: So, I'll just mention that.

1188 MR. AMIN: Okay.

1189 MR. RAKOVAN: Just a quick question before we continue  
1190 on. We were scheduled to take a break around 2:10. Do we want  
1191 to go ahead and keep going at this point or do we want to take a  
1192 break? Just looking at the table to get a general thought. Keep  
1193 going? Keep going? Okay. We do have a comment or question from  
1194 the room. If we could go ahead and -- that was my understanding.  
1195 Go ahead and then we'll go back to the phones, please.

1196 MR. NEFF: Hello. Dave Neff, Exelon Nuclear. My  
1197 perspective is licensing, so it's not so much implementation and  
1198 INC kind of work, but from a process standpoint. So back on Slide  
1199 15, you talked about revising safety or important-to-safety  
1200 systems and equipment. And the cyber security rule applies to  
1201 security, safety-related NEP functions. And it also brings in the  
1202 important-to-safety equipment as well. But your scenarios would  
1203 include security, doesn't -- you're intending to exclude security,  
1204 is that correct?

1205 MS. ZHANG: No. We actually -- we are only -- for this  
1206 SECY paper, the scope is only safety related and important-to-  
1207 safety systems. So, for licensing, that's what we'll only focus  
1208 on now. For the cyber security program, we do recognize that the  
1209 scope is broader than that.

1210 MR. NEFF: The elements of the cyber security plan

**NEAL R. GROSS**

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

1211 related to safety and safety-related or important-to-safety are  
1212 covered under 50.54(p), because it's part of the cyber security  
1213 plan. So you may get changes from 50.90 submittals for license  
1214 amendments coming out of reduction and effectiveness of the  
1215 security plan, not your 50.59 questions. Right? So from a  
1216 licensing perspective, just remember that you might getting  
1217 questions on effectiveness of the security plan, not effect on the  
1218 core from a 50.59 perspective. Okay.

1219           The other thing I want to bring -- a couple other  
1220 points. NEI 13-10 initiative, are you familiar with the work  
1221 that's going on with NEI and the NRC team? Probably not. You  
1222 are? Okay. So a lot of the work right now on this revision is  
1223 going after balance-of-plan equipment and trying to reduce the  
1224 controls that are required for that equipment. So -- direct and  
1225 indirect. So, when you're talking about important-to-safety  
1226 equipment here in this scope, if we apply where we're headed with  
1227 NEI 13-10, with balance-of-plan the amount of controls that would  
1228 be necessary for BOP equipment is really reduced. So having a  
1229 reduction in effectiveness of the security plan for BOP probably  
1230 won't reach the level for a submittal.

1231           So, let me encourage you to take a look at the NEI 13-  
1232 10, the current revision, as we're looking to go into pilot phase  
1233 next month with NRC concurrence, should be coming in here shortly  
1234 for, not full endorsement, but at least our comments. So, that's

**NEAL R. GROSS**

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

1235 coming at us pretty quickly and we're looking pretty encouraging  
1236 to implement that. So I think that will have some bearing on the  
1237 scope of what you think might be applicable to this SECY, at least  
1238 for operating power plants.

1239 MR. STATTEL: This is Rich Stattel. Just for my  
1240 benefit, because I'm not familiar with exactly where that  
1241 initiative is going, is it intended to change the criteria for  
1242 identification of Critical Digital Assets or changing the controls  
1243 --

1244 MR. NEFF: Controls.

1245 MR. STATTEL: -- based on the safety significance of  
1246 the --

1247 MR. NEFF: The second part of it. We're not looking  
1248 to revise what the definition of a CDA is, but rather what controls  
1249 are appropriate for that based on its emergency preparedness  
1250 function or its balance-of-plan function.

1251 MR. STATTEL: I see.

1252 MR. NEFF: And what the vulnerability is and how it  
1253 could result in an attack. So Bill Gross and the NEI team can  
1254 probably better feed you what exactly is going on with 13-10. I'm  
1255 a little bit on the periphery. But I think that has a lot of  
1256 value in reducing the scope of what you think this SECY might need  
1257 to cover for an operating power plant.

1258 MR. STATTEL: Thank you.

**NEAL R. GROSS**

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

1259 MR. NEFF: During the July Nuclear Information  
1260 Technology Strategic Leadership, NITSL, conference in July, EPRI  
1261 made a presentation around standards. So let me encourage you to  
1262 go talk to your EPRI contacts. Because they're looking to really  
1263 gear up and it sounded rather encouraging. It won't be this 2015  
1264 time period to get your answers, but I think there's -- and Bill  
1265 Gross can get you that contact who made the presentation at the  
1266 NITSL conference from EPRI. But I think there's some value coming  
1267 to the industry and to the NRC as well from a standards  
1268 perspective, even though, like you said Deanna, IEEE is going to  
1269 take us a while. I think EPRI will as well, but there is work  
1270 coming out that will be beneficial for future reactors and for  
1271 design changes.

1272 The last comment I had, suggestion, was have you looked  
1273 at, and I don't know if it's applicable, but the standard review  
1274 plan, NUREG-0800? So in my days of starting up from Limerick, we  
1275 relied on the NUREG-0800 as to how you design a power plant. So  
1276 I don't know if there's a modification to 0800 that would work  
1277 here for you and maybe you need the Commission to tell you that's  
1278 an okay way to go. But from my previous days, NUREG-0800 was like  
1279 the bible to how to design a power plant. And if we met that  
1280 design, then it went through the NRC review period process pretty  
1281 easily at that point in time. So I don't know if you've already  
1282 thought about that as an option, but if you're looking for an easy

**NEAL R. GROSS**

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

1283 standard, NUREG-0800 sounded like a good spot for me where I'd go  
1284 to take a look at. That's all I had then.

1285 MR. JACKSON: Terry Jackson. To address your last  
1286 point there, I'm not quite sure we're at that point as to where we  
1287 might modify aspects and so forth. We're mainly first looking for  
1288 the Commission to determine, one, if they want us to make any  
1289 change and then, two, if they do want us to make a change, what  
1290 extent would that need to be done? Primarily looking for a policy  
1291 direction, which would then either direct us towards rule making  
1292 or something smaller scope, which may be like a regulatory guide  
1293 or maybe standard review plan.

1294 MR. NEFF: Okay, good. Thank you.

1295 MS. ZHANG: And -- yes. And as far as with your other  
1296 suggestions, again, right now, as Terry said, we're looking for  
1297 the permission to do something from the -- their direction. So  
1298 as far as the implementation later on, I think that's when we'll  
1299 be engaging in the other groups more.

1300 MR. NEFF: From an informed -- when you go to make,  
1301 provide them an informed information, help them making an informed  
1302 decision, I think some of these other inputs may help in your  
1303 recommendation and some of the dialogue you might have with the  
1304 Commission later on. Good, thanks.

1305 MR. RAKOVAN: Okay. Emily, do we have any other  
1306 speakers in the queue at this point?

**NEAL R. GROSS**

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

1307 OPERATOR: Yes, sir, we do. Our next question comes  
1308 from --

1309 MR. PEZESHKI: Jonah Pezeshki.

1310 OPERATOR: Sir, your line is open.

1311 MR. PEZESHKI: Hello. I don't necessarily have a  
1312 question, I just have a few comments based on what I've heard.  
1313 Oh, before I continue, this is Jonah Pezeshki, Nuclear Regulatory  
1314 Commission, Cyber Security Directorate. So first, I just wanted  
1315 to warn against getting too caught up in the prescriptive elements.  
1316 I've heard a lot of comments about code review, whether or not  
1317 that's possible based on the type of product that we're talking  
1318 about, et cetera. I just want to remind that we're trying to  
1319 maintain the same scoping that currently exists in both 73.54 as  
1320 well as 5.71 and other applicable guidance. And so we need to  
1321 avoid getting too deep in the weeds on this. I mean, right now  
1322 we're talking about a very high level perspective.

1323 At the same time, there were some comments about  
1324 additional regulatory burden, additional audits, et cetera. I  
1325 think it was mentioned earlier, but it's my understanding that our  
1326 overall intent is to dovetail with current safety review processes  
1327 in order to avoid any additional regulatory burden. I'm correct  
1328 in saying this?

1329 MR. STATTEL: That is our intent, Jonah.

1330 MR. PEZESHKI: Okay. And I just want to make it

**NEAL R. GROSS**

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

1331 abundantly clear, because I know that there is definitely fear  
1332 from the industry that there's going to be additional regulatory  
1333 burden and additional processes that they have to adhere to and I  
1334 don't believe that's our intent in the slightest. And so, really,  
1335 this is just, as we said before, to give industry an earlier bite  
1336 at the apple.

1337           As many would tell you, cyber security is generally  
1338 considered throughout the entire design, implementation, and  
1339 eventual retirement of a system. We know that the licensees being,  
1340 well, quite frankly, incredibly confident people, are already  
1341 considering cyber security throughout the design process. This  
1342 is really just to help ensure that there are no hiccups along the  
1343 way that will eventually bite them during the implementation phase  
1344 or post-implementation. Yes. If there's any questions or  
1345 comments, but that's pretty much it.

1346           MR. RAKOVAN: Okay. Thank you.

1347           MR. PEZESHKI: Yes. Thank you.

1348           MR. RAKOVAN: Emily, can we go to the next person,  
1349 please?

1350           OPERATOR: At this time, I'm showing no additional  
1351 questions.

1352           MR. RAKOVAN: Okay. I guess I'll go back to the table  
1353 and see how you guys want to proceed.

1354           MS. ZHANG: Gordon, did you have any of the questions

**NEAL R. GROSS**

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

1355 that Bill wanted to ask? Do you have that available?

1356 MR. CLIFTON: This is Gordon Clifton. I think we've  
1357 covered that ones that Bill had identified earlier. He was looking  
1358 for confirmation that you didn't perceive we had problems out there  
1359 we were trying to fix. We've clarified that, that's the situation,  
1360 we're confident in what's out here. We're moving to allow or  
1361 encourage or create an NRC involvement early enough in the stage  
1362 that we don't have problems later on. And I think that's a common  
1363 goal for both sides, for the industry and the NRC, is we don't  
1364 want findings or failures or problems that stops production of  
1365 power or safe operations.

1366 And we can do that by being prepared earlier. And  
1367 that's -- whether it's at code level or all the way at  
1368 implementation, it's still a theme that's going through. One of  
1369 the key aspects that we look at cyber security is it's sort of  
1370 grout between the bricks. It's always out there, but it's not a  
1371 stand alone item by itself. So it's difficult for us to write  
1372 guidance on something that's addressing so many different aspects.  
1373 For whether it's code writing or turning wrenches later on, boots  
1374 and guns for the security people coming in, whether it's physical.  
1375 I think we did a great job of separating those two a couple years  
1376 ago. We were doing a good job of maintaining boots and guns from  
1377 fine wire, electronic aspects. And now, as somebody mentioned,  
1378 we've got portable aspects and wireless aspects as new challenges.

**NEAL R. GROSS**

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

1379           And we've identified in here we're going to be  
1380 addressing vulnerabilities in the future. We don't know all of  
1381 the ones that are coming out there, so we have to have some  
1382 flexibility to change with what's going out. And Bill's concern  
1383 was we don't want to try and fix something that's not broken, we  
1384 don't want to make life -- consume resources that both sides, the  
1385 industry and the vendors and the NRC, have unnecessarily. Because  
1386 we can get good products now, we just want to make sure we maintain  
1387 the quality that we have and then continue the same aspect.

1388           And I think we're on the right path. It's a tough  
1389 challenge. My guess is we'll come back with the Commissioners --  
1390 with direction to set a policy to be involved, but not to stop the  
1391 process. But that's speculation in the future. And that's I  
1392 think one that the whole industry can support. Terry's shaking  
1393 his head, yes, here.

1394           MR. JACKSON: Well, I was going to maybe -- because I  
1395 think you started addressing the question I was going to ask. At  
1396 the last public meeting, the industry more or less gave us their  
1397 position on the SECY was basically take Option 3, which is not do  
1398 anything. I think today what I hear is, is that there is caution  
1399 about maybe making things too prescriptive or increasing  
1400 regulatory burden where it may not necessarily be necessary because  
1401 the current process works well

1402           But if there is opportunity to enhance the process so

**NEAL R. GROSS**

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

1403 that there is some efficiencies gained, particularly one advantage  
1404 I think I hear from you all is the ability to be able to start  
1405 address cyber security earlier in the process versus later on.  
1406 Then if we have those opportunities then that would be something  
1407 I think the industry would want to support.

1408 MR. STATTEL: This is Rich again. There were two  
1409 messages that I got from the last meeting. And they were kind of  
1410 conflicting. So, one of them was, there was a concern that any  
1411 new guidance or regulation that comes out of this effort would  
1412 basically do the double whammy on the applicant. So, in other  
1413 words, we would have a shot at your systems during the license  
1414 review and then the second shot when the inspectors get out to the  
1415 plants and it would basically make things more difficult for them.  
1416 That was the one aspect. Now, I think Deanna and I agree that,  
1417 that's not our intent here, right? We're really just trying to  
1418 do a more holistic approach to addressing cyber security with  
1419 regard to regulations.

1420 And then, on the other side, the other feedback we got  
1421 was more from the new reactors vendors, where they really want us  
1422 to do the reviews more during the Design Certification stage to  
1423 eliminate the risk that would be posed later on during  
1424 implementation. So, as we were developing these slides and as we  
1425 were developing these scenarios and talking about this, I think we  
1426 kind of were trying to keep both of those perspectives in mind.

**NEAL R. GROSS**

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

1427 And I don't know how successful we were. But our objective here  
1428 is not really create any new requirements, is we just want to be  
1429 more efficient at how we address cyber security throughout the  
1430 process.

1431 MR. CLIFTON: One of the things, lessons learned from  
1432 the Diablo Canyon, was identifying what you're looking for and  
1433 when you're looking for it. And if we can come up with a scenario  
1434 where the NRC involvement isn't, as you called it, a double  
1435 involvement, that while the book's open, somebody's looking over  
1436 the shoulder to confirm, yes, that does cyber security as well as  
1437 the interface with the plant that we expected or the performance  
1438 we expected.

1439 And part of that maybe is an inspection plan or  
1440 guidance for your inspectors and/or auditors as the case may be,  
1441 because we're looking at audits before implementation, that they  
1442 have something specific that they're looking for. And if we have  
1443 clarity of what you're coming in to validate or inspect or audit,  
1444 and it's a short-term many times over, that's probably quite  
1445 understandable and acceptable to put in to the modification plan.  
1446 That you put a milestone that you're checking for code, you're  
1447 looking for physical/digital characteristics, you're looking for  
1448 implementation, you're looking for interface between the system  
1449 and that digital widget.

1450 Those are all -- could be ten years apart, but they

**NEAL R. GROSS**

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

1451 have to be an administrative check that we have all confidence  
1452 that we've gotten involved early to make sure cyber security is  
1453 progressing acceptably, that we're identifying hurdles that would  
1454 be out there by the NRC inspector's experience or the site's  
1455 development of answers to questions, and then we can get them  
1456 resolved while they're small --

1457 MR. STATTEL: Okay.

1458 MR. CLIFTON: -- rather than while they're large.

1459 MR. STATTEL: This is Rich again, Rich Stattel. With  
1460 all that said, I do acknowledge, there's some danger there that -  
1461 -

1462 MR. CLIFTON: Absolutely.

1463 MR. STATTEL: -- there could be an increased burden.  
1464 And it kind of all depends on how this plays out and how well we  
1465 communicate with NSIR and the inspectors going forward. Now we  
1466 have some experience with this, not only in the cyber security  
1467 area, but in the licensing review area. So, in our past reviews  
1468 at Oconee, for example, we did the license review of the license  
1469 amendment and that was a pretty significant effort that went over  
1470 the course of two years.

1471 But it was also followed up by inspection activities  
1472 that occurred on site when the site acceptance testing was  
1473 performed and when the installation and during startup as well.  
1474 And in those cases, there were several aspects of the design that

**NEAL R. GROSS**

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

1475 could not be reviewed at the time we were doing our safety  
1476 evaluation. So we kind of had to defer those, right? And the way  
1477 we did that is we made a list of recommended inspection items,  
1478 that's part of the safety evaluation, and those were used to  
1479 develop the inspection plans.

1480           So we were communicating regularly with the inspectors  
1481 and I actually -- several members of our group actually  
1482 participated in those inspections. We went down to the plant and  
1483 performed -- were part of the inspection team. So, I think that's  
1484 key here too. If you don't have that communication, if you don't  
1485 have some hand shaking going on with the inspectors, I think the  
1486 danger becomes a lot greater that there's an increased burden and  
1487 you have -- you're being attacked from two different sides here.

1488           So, it's important and I'm not sure how to make sure  
1489 that happens in the future. But I think that's an important  
1490 aspect, maintaining the communications. In fact, we have an  
1491 inspector from Region IV that's currently participating in our  
1492 evaluation of the Diablo Canyon safety evaluation. So we do have  
1493 overlap, we do have some experience with coordinating these  
1494 efforts. And I would expect the same thing to occur for the cyber  
1495 security.

1496           MR. CLIFTON: This is Gordon Clifton again. One of the  
1497 lessons learned we've had is in these processes we've done is Phase  
1498 Zero Meetings, is what we're calling them. And these are before

**NEAL R. GROSS**

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

1499 the submittals, where we have open dialogue between the applicants  
1500 and the NRC that identifies low hurdles, high hurdles, solid walls  
1501 that we need to get around. And if you find yourself in a position  
1502 that the policy is such that you don't have inspection and finding  
1503 capabilities until implementation, as it is now, you could identify  
1504 these earlier interfaces as Phase Zero Meetings with the applicant,  
1505 the utility, whoever's building this modification.

1506           And those Phase Zero Meetings we had at Diablo Canyon,  
1507 what, four, six of them, something in that respect, over a series  
1508 of months. And the communications affected the design  
1509 significantly while it was on the paper and before it was being  
1510 built. And it encouraged the flow of the modification very well.

1511           With that success applied to cyber security, if you  
1512 come in and have a Phase Zero Meeting to talk about, what did you  
1513 do about code, what did you do about malware, what did you do about  
1514 what your plans here, without a penalty, then the communication  
1515 aspect is the part that we're trying to encourage between the NRC  
1516 and the utility rather than the enforcement of something that's  
1517 wrong or violating a rule or something. And then it's really  
1518 received as an assist, if you will, rather than a penalty or  
1519 something to fear while you're in the early stages of planning.

1520           MS. ZHANG: Yes. And we've been -- this is Deanna  
1521 Zhang. And we've been doing this on the new reactor side for both  
1522 Vogtle and Summer participating and supporting regional staff in

**NEAL R. GROSS**

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

1523 doing the different milestone implementations for the cyber  
1524 security program as these systems are getting developed. But,  
1525 again, I think what Rich said before was, there is a bit of a  
1526 dichotomy here between new reactors, and I wouldn't say new  
1527 reactors, I would say between Design Certification applicants and  
1528 a licensee COL applicant.

1529           And that's where we see there may be a potential gap  
1530 is that Design Certification applicants, they don't -- 73.54 does  
1531 not apply to them. And, therefore, some of these design controls  
1532 that should be considered early on in the overall INC architecture  
1533 and the system design, were not done as part of the Design  
1534 Certification. And, therefore, a COL applicant may have to  
1535 inherit a unsecurable design and then would need to do design  
1536 modifications after the fact.

1537           MR. CLIFTON: And that's pricey and neither one of us  
1538 want to do that.

1539           MS. ZHANG: No.

1540           MR. CLIFTON: Have we developed any more questions on  
1541 the phone?

1542           MR. RAKOVAN: All right. Let's go ahead and check in  
1543 one more time. Emily, by any chance do we have anyone who is  
1544 wanting to make a question or comment at this time?

1545           OPERATOR: I'm showing no questions at this time.  
1546 However, as a reminder, it is Star 1 if you're wishing to ask a

**NEAL R. GROSS**

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

1547 question.

1548 MR. STATTEL: I guess we can go on to discuss the next  
1549 steps.

1550 MR. RAKOVAN: Sure.

1551 MR. STATTEL: I think we're at that point.

1552 MS. ZHANG: So at this point, we're hoping to finalize  
1553 this draft SECY paper and present it, send it up to our EDO's  
1554 office for review prior to sending it up to the Commission. We  
1555 do expect that we will be making a Commission or probably  
1556 Commissioner TA briefing at some point. And that some of the  
1557 things we discussed at these last couple public meetings would  
1558 also be raised at that briefing too.

1559 MR. CLIFTON: I guess I -- this is Gordon Clifton. I'd  
1560 ask, do we get the public involved again in the --

1561 MR. STATTEL: Well, you don't --

1562 MR. CLIFTON: -- future that you see?

1563 MR. STATTEL: You don't get to see the SECY paper until  
1564 --

1565 MS. ZHANG: It becomes public, I guess. Until --

1566 MR. STATTEL: I guess it has to go through the EDO's  
1567 office and then it would become public.

1568 MR. CLIFTON: When it goes --

1569 MR. STATTEL: Sometime after that.

1570 MR. CLIFTON: -- to your TA -- the Commissioner --

**NEAL R. GROSS**

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

1571 MR. STATTEL: But I don't think --

1572 MR. CLIFTON: -- TA reps?

1573 MR. STATTEL: -- there would be any -- I don't think  
1574 there's going to be any surprises. The subject matter is really  
1575 what we're talking about here.

1576 MR. CLIFTON: Good.

1577 MR. STATTEL: So, I don't think you're going to see  
1578 this as blindsiding you or anything like that. We're not proposing  
1579 anything to the -- any concepts or ideas to the Commission that we  
1580 haven't already discussed in these meetings.

1581 MR. CLIFTON: That's good. And then following, the  
1582 Commissioners will have a COMSECY, right?

1583 MS. ZHANG: Yes. So we would expect to see an SRM that  
1584 would reflect their decision.

1585 MR. CLIFTON: And optimistically, we think Santa Claus  
1586 is bringing that by the end of the year, right?

1587 MR. STATTEL: Though I think the public would have an  
1588 opportunity to chime in between the SECY paper and when the  
1589 Commission makes its decision. Is that not correct? I'm not --

1590 MR. CLIFTON: I don't think so.

1591 MR. STATTEL: Okay.

1592 MR. CLIFTON: I don't think I've seen it yet.

1593 MR. STATTEL: Okay. So the first time the public would  
1594 have access to this would be when the COMSECY paper goes out.

**NEAL R. GROSS**

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

1595 Okay.

1596 MR. CLIFTON: Your work's cut out for you.

1597 MR. JACKSON: But that's why we wanted to engage the  
1598 industry in the past two public workshops is to get your feedback.

1599 MR. CLIFTON: Yes.

1600 MS. ZHANG: Okay. So with that, if we don't have any  
1601 more questions, I would like to thank everyone for participating  
1602 again. Taking this opportunity to get the feedback from industry  
1603 and the public has been very important to us and we hope that it  
1604 would better inform our SECY paper development. So, thank you.  
1605 And hopefully you will see the SECY paper, the COMSECY paper at  
1606 the end of this year.

1607 (Applause.)

1608 MR. RAKOVAN: All right. With that, we're closed.

1609 (Whereupon, the above-entitled matter went off the  
1610 record at 2:43 p.m.)

1611

1612

1613

1614

1615

1616

1617

1618

1619

1620

1621

1622

1623

1624

1625

1626

1627

1628

1629

1630

1631

1632

**NEAL R. GROSS**

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