

Official Transcript of Proceedings

NUCLEAR REGULATORY COMMISSION

Title: Advisory Committee on Reactor Safeguards
 Reliability and PRA Subcommittee Meeting

Docket Number: (n/a)

Location: Rockville, Maryland

Date: Wednesday, April 6, 2016

Work Order No.: NRC-2301

Pages 1-209

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

DISCLAIMER

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

UNITED STATES OF AMERICA
 NUCLEAR REGULATORY COMMISSION

+ + + + +

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

(ACRS)

+ + + + +

RELIABILITY AND PRA SUBCOMMITTEE

+ + + + +

WEDNESDAY

APRIL 6, 2016

+ + + + +

ROCKVILLE, MARYLAND

+ + + + +

The Subcommittee met at the Nuclear
 Regulatory Commission, Two White Flint North, Room
 T2B1, 11545 Rockville Pike, at 8:31 a.m., Dennis C.
 Bley, Chairman, presiding.

COMMITTEE MEMBERS:

DENNIS C. BLEY, Chairman

CHARLES H. BROWN, JR. Member

MICHAEL L. CORRADINI, Member

HAROLD B. RAY , Member

PETER RICCARDELLA, Member

GORDON R. SKILLMAN, Member

JOHN W. STETKAR, Member

NEAL R. GROSS

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

DESIGNATED FEDERAL OFFICIAL:

CHRISTIANA LUI

ALSO PRESENT:

MATT BUNN, Harvard Kennedy School of
Government*

STEVE FOGARTY, ARES Corporation

MELANIE GALLOWAY, NSIR/DSP

MARVIN LEWIS, Public Participant*

MARC NICHOL, NEI

JOE RIVERS, NSIR/DSP

*Present via telephone

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

Opening Remarks

by Dennis Bley4

NRC Management Introductory Remarks

by Melanie Galloway10

Overview of the Physical Security Regulatory
Framework, Vulnerability Assessment Approach and
Safety/Security Interface

by Joe Rivers13

Proposed Consequence-Based Approach for SMR
Security Regulations

by Marc Nichol54

The Role of Modeling and Simulation in Risk-
Informed Security Decision Making

by Steve Fogarty83

Coping with Complexities of Vulnerability
Assessment

by Matt Bunn122

Public Comment144

Adjourn 147

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

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

(8:31 a.m.)

MEMBER BLEY: Good morning. The meeting will now come to order. This is a meeting of the Advisory Committee on Reactor Safeguards, Subcommittee on Reliability and PRA.

I am Dennis Bley, Chairman of this meeting. Members in attendance are Mike Corradini, Dick Skillman, Harold Ray, and John Stetkar. We may be joined later by Charlie Brown and Pete Riccardella. Christiana Lui of the ACR staff is the designated federal official for this meeting.

The purpose of the meeting is to receive an information briefing on the security regulatory framework of nuclear power plants, and planned activities to more explicitly incorporate vulnerability assessments into the NRC's physical security regulatory approach to improve safety/security interface.

The subcommittee will hear presentations by, and hold discussions with representatives from NRC's Office of Nuclear Security and Incident Response, the Nuclear Energy Institute, ARES Corporation, and the Kennedy School of Government at Harvard University.

NEAL R. GROSS

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

(202) 234-4433

(202) 234-4433

1 The subcommittee will gather
2 information, analyze relevant issues and facts, and
3 formulate proposed positions and actions as
4 appropriate for deliberation by the full committee.

5 I think we'll begin with a little
6 history. Vulnerability assessment has been in
7 development and use for applications in the
8 physical security area since the 1970s. Over the
9 last several decades the methods, data, and
10 subsequent computer based modeling and simulation
11 tools have continued to evolve based on the needs,
12 operating experience, and technology advancement.

13 Other federal agencies, such as the
14 Department of Defense and the Department of Energy
15 have sponsored the development of vulnerability
16 assessment software tools, and used the results in
17 the design and evaluation of protection strategies
18 for sites, facilities, or materials under their
19 jurisdictions.

20 As the desktop computing power grew,
21 the modeling simulation software that used to
22 require multi-station, multi-analysts, migrated
23 onto portable computing platforms.

24 Within the NRC the Office of Nuclear
25 Security and Incident Response, NSIR, and the

NEAL R. GROSS

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

1 Office of Regulatory Research, have participated in
2 or sponsored workshops that focused on
3 safety/security interface and risk informed
4 decision making, since about 2010.

5 Last year I had the opportunity to
6 attend the Joint Institute of Nuclear Materials
7 Management, and the American Nuclear Society
8 Workshop at Sun Valley. And the Committee
9 sponsored me to attend a subsequent workshop in
10 Boston.

11 Based on my observations both the
12 vulnerability assessment and PRA in the safety area
13 use the Tripwood approach. I'm going to go off
14 script for a minute.

15 I spent, before I got on this committee
16 I spent several years working with a group under
17 the Gen 4 Program, looking at proliferation
18 resistance and physical protection, trying to
19 develop methods in that area.

20 And it took us over two years to just
21 get past the language barriers between safety
22 people, risk people, physical protection people,
23 and proliferation resistance people. In the end,
24 pretty much everybody agreed that the problems we
25 were solving were very related.

NEAL R. GROSS

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

1 And they really had to deal with the
2 fact that barriers and protection systems, and the
3 like, don't have intrinsic value. They have value
4 that's very much scenario based. And for one
5 scenario a particular barrier might be very good,
6 for another not so good.

7 And that this idea of a scenario based
8 kind of analysis, and we even had to change the
9 words a little bit so everybody could be
10 comfortable, the pathways approach, really seemed
11 to anchor where we were headed. The same things
12 we're seeing here a bit.

13 Although the quantification processes
14 and certain modeling aspects are different among
15 these analyses, there are many opportunities to
16 leverage the similarities between a vulnerability
17 assessment and say a PRA to improve the
18 safety/security interface, and better facilitate
19 efficiency and effectiveness.

20 Additionally, I understand several
21 operating nuclear power plant fleets, Xcel Energy,
22 PSEG, and Exelon are using the commercially
23 available modeling simulation software to model,
24 assess, and adjust their site protective strategy.

25 In fact, two sites have submitted

NEAL R. GROSS

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

1 proposed changes to their physical security plans
2 to the NRC for review, using the modeling
3 simulation results as part of the support for the
4 proposed changes.

5 On the advanced designs and small
6 modular reactors front, in November 2015 Nuclear
7 Energy Institute submitted to the NRC a White
8 Paper, "Proposed Consequence Based Physical
9 Security Framework for Small Modular Reactors and
10 Other New Technologies", which advocates a more
11 explicit security regulatory framework that uses
12 risk insights for SMRs. We will hear more about
13 that this morning.

14 I think, to put a little perspective
15 here, I'd also mention several SRMs that have been
16 issued over the past many years. There have been I
17 think at least three or four that I remember, that
18 has urged the staff to integrate safety/security to
19 the extent possible.

20 Back in 2003 an SRM on, following a
21 meeting with this committee, our parent committee,
22 the Commission said on the security area, ACRS
23 should continue to focus its attention and
24 expertise on technical issues associated with the
25 progression and potential consequences of

NEAL R. GROSS

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

(202) 234-4433

(202) 234-4433

1 postulated terrorist actions, and the assessment of
2 mitigation strategies.

3 And later, in 2008, in an SRM on SECY-
4 08-0099, Final Rule, Power Reactor Security
5 Requirements, they said the staff should have the
6 Advisory Committee on Reactor Safeguards review the
7 implementation guidance for portions of the
8 rulemaking with the committee's scope.

9 The rules for participation in today's
10 meeting has been announced as part of the notice of
11 this meeting previously published in the Federal
12 Register on March 23rd, 2016. A transcript of the
13 meeting is being kept, and will be made available
14 as stated in the Federal Register notice.

15 Therefore, we request that participants
16 in this meeting use the microphones located
17 throughout the meeting room when addressing the
18 subcommittee. Participants should first identify
19 themselves, and speak with sufficient clarity
20 volume so that they may be readily heard.

21 Also, for all of the folks at the
22 tables, the desk microphones have a little button
23 on the front. Please push that when you're going
24 to talk, and turn it off when you're finished.
25 Having them on all the time interferes with, it

NEAL R. GROSS

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

(202) 234-4433

(202) 234-4433

1 creates noise for the people on the phone listening
2 in.

3 It's requested that presenters first
4 identify themselves. Also, given the nature of
5 today's topic, the presenters should stop the
6 discussion if the content can no longer be
7 discussed in a public forum. And we'll have to
8 leave that up to you to be careful.

9 We will adjourn this morning's sessions
10 promptly at noon. We have another meeting
11 scheduled then. So we'll have to finish the full
12 agenda for this morning by noontime. And we'll
13 return for a closed session with the committee
14 after lunch.

15 We ask at this time that you silence
16 your phones and other electronic devices. Although
17 we have a bridge line open to preclude interruption
18 of the meeting, the phone bridge will be placed in
19 the listen in mode only during the, it will be in
20 the listen in mode only during all presentations
21 and committee discussion.

22 We'll open the phone line late in this
23 open meeting to allow public comment. Prior to
24 today's meeting we have received no written
25 comments or requests for time to make oral

NEAL R. GROSS

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

1 statement from members of the public regarding
2 today's meeting.

3 We will now proceed with the meeting.
4 And I call upon Melanie Galloway, Director of the
5 Division of Security Policy, in the Office of
6 Nuclear Security and Incident Response, to begin.
7 Melanie, please.

8 MS. GALLOWAY: Okay. Thank you very
9 much, Chairman Bley. First of all from a personal
10 standpoint I'd like to say how pleased I am to be
11 back before the ACRS. It's been some time since my
12 ACRS interactions on license renewal. And it's
13 good to see you all again.

14 I'm pleased to be here to introduce
15 this topic, and particularly to give a little bit
16 more information regarding the NSIR work in this
17 area, and to introduce Joe Rivers.

18 As Chairman Bley has mentioned, the
19 idea of risk informed security has been gaining
20 momentum over the last several years, in particular
21 the last four or five.

22 This is part of an overall activity
23 that NSIR is involved in to risk inform. We're
24 taking a leadership role in that regard, both
25 domestically, and doing some international

NEAL R. GROSS

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

1 leadership work as well.

2 It goes without saying that when we
3 talk about risk informing anything we need to
4 reflect on the fact that there is a Commission
5 policy statement that has to do with the use of PRA
6 methods in regulatory activities.

7 And in that policy statement it
8 explicitly points out that all regulatory matters
9 should be further risk informed. And while
10 certainly the risk informing activity by the VA
11 tools is not a PRA, per se, the use of such tools
12 is certainly within the spirit of that Commission
13 policy statement.

14 As Chairman Bley mentioned, we have
15 conducted a number of workshops. In particular,
16 last year we conducted two with the ANS, and with
17 the Institute of Nuclear Materials Management, in
18 which Joe Rivers did provide a leadership in those
19 workshops, and provided discussion in order to get
20 a dialogue going about what are the various ways
21 that can be risk informing in the security realm,
22 and also to talk about the safety/security
23 interface, and what information we can gain and
24 apply to our work, both on the part of licensees,
25 as well as the NRC.

NEAL R. GROSS

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

1 In these workshops we have noted an
2 increased attention and attendance by industry
3 folks, as they are seeing the value in risk
4 informing their security activities.

5 The use of modeling and simulation, we
6 call it Mod Sim, should support better decision
7 making. And that's clearly what everyone is
8 looking for.

9 You know, the industry has its
10 priorities in terms of the decision making that can
11 make more effective use of their resources. And we
12 too have perspectives, in terms of how the values
13 of these tools can better inform our regulatory
14 activities.

15 And they're not always aligned, but
16 they do come at it from the same perspective of,
17 what can we gain, and how can we best use this
18 material? And certainly we're here to talk to you
19 today about the safety/security interface, which is
20 very much fitting in with your safety focus.

21 And that's an area as well that we're
22 doing a lot of work in. Right now it's a little
23 bit of an extension of what we do, because we're
24 focusing primarily on the security piece. But
25 understand that the safety/security piece is

NEAL R. GROSS

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

1 important to us as well.

2 Joe Rivers is going to provide a little
3 bit of a regulatory framework about how the VA
4 tools fit in with our security licensing process,
5 as well as talk about the tools themselves, and
6 then get into some safety/security interface. So
7 with that, I'll turn it over to Joe.

8 MR. RIVERS: Okay. So, Chris asked me
9 to sort of lead into the discussion today, so that
10 the members of the subcommittee would have a better
11 understanding as the later presentation is rolled
12 out. So how it all fits into this framework.

13 How do I make this thing go down? Page
14 down. I hit page down. It doesn't work.

15 PARTICIPANT: Try hitting the space
16 bar.

17 MR. RIVERS: Space bar? No.

18 (Off microphone comments)

19 MR. RIVERS: I tried page down. That
20 doesn't work. Now it does. Okay.

21 (Off microphone comments)

22 MEMBER STETKAR: It's good you could
23 learn something here this morning. This is, you
24 know, a fallout of Project Aim. You are now
25 trained --

NEAL R. GROSS

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

1 MR. RIVERS: I just had to make sure
2 that my --

3 MEMBER STETKAR: -- to do this in any
4 medium.

5 MR. RIVERS: My former boss is here to
6 get things started. So, okay, we're going to cover
7 a number of topics in the next hour. And feel free
8 to interrupt at any time if you've got questions on
9 any specific issues there.

10 We'll talk about the physical security
11 regulatory framework, a little bit about
12 safety/security interface. I'll give you some
13 background on some of the activities we've had on
14 risk informing security that Dennis mentioned
15 earlier, and also Melanie.

16 And then I'll talk a little bit about
17 what vulnerability analysis is, and what some of
18 the different tools are, to lead into later
19 discussion today.

20 So, NRC's power reactor security
21 program, it's really there to provide high
22 assurance of adequate protection to prevent
23 significant core damage with spent fuel, and spent
24 fuel sabotage. So it's designed to protect against
25 the design basis threat, in order to prevent

NEAL R. GROSS

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

1 radiological sabotage.

2 And the process is for NRC to develop
3 licensing and inspection programs, as well as
4 industry initiatives that implement and verify the
5 level of protection described. So the real focus
6 is to protect against radiological sabotage as
7 defined in the design basis threat.

8 There's a lot of individual
9 requirements, both prescriptive and performance
10 based throughout the regulations. But in the end
11 the idea is to protect against radiological
12 sabotage.

13 If we look at how we get moving, we
14 have licensing for operating nuclear power
15 reactors. And 10 CFR 50 and 73 regulations apply.
16 And there's also a formalized process to make
17 changes.

18 For new reactors we have 10 CFR 52 and
19 73. There's also a final safety analysis report
20 which must describe the engineered physical
21 security programs, and implement security
22 requirements before fuel is allowed inside the
23 protected area. So, before the fuel actually
24 arrives onsite, the security measures have to be in
25 place.

NEAL R. GROSS

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

1 The NRC also uses NUREG-0800, the
2 Standard Review Plan, and various regulatory guides
3 to conduct security plan reviews and approvals.
4 Security plans tend to be sort of the foundation of
5 how security operates at the facilities, and also
6 with our regulatory oversight and responsibilities.

7 They provide a physical protection
8 against the design basis threat. They establish
9 and maintain a physical protection system and
10 security organization. They establish and maintain
11 at all times properly trained, qualified, and
12 equipped personnel that are required to interdict
13 and neutralize the threats.

14 The requirements can be found in 10 CFR
15 73.55 and 73.54. There are four basic types of
16 security plans, the safeguard contingency plan,
17 which is, if something happens, what are the, what
18 is the protective force supposed to do?

19 Training and qualification plan. What
20 makes a security protective force officer actually
21 qualified. Physical security plan that sort of
22 covers the spectrum of all the requirements and
23 documents, how the program operates. And then in
24 the recent years, cyber security plan.

25 MEMBER SKILLMAN: And, Joe, if you can,

NEAL R. GROSS

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

1 is there a unique and specific definition of design
2 basis threat in the context of the vulnerability
3 assessment?

4 MR. RIVERS: Essentially what you have
5 in the vulnerability assessments is the NRC
6 proscribes the design basis threat. There's a sort
7 of a general statement that you'll find in the
8 regulations. And then the reg guide, I believe the
9 one that applies for nuclear power plants at the
10 radiological sabotage, which is --

11 MS. GALLOWAY: 5.69.

12 MR. RIVERS: -- 5.69. Actually, it's
13 currently under revision right now. But that
14 provides all of the adversary characteristics.

15 And so, when the utilities are in the
16 process of conducting these vulnerability
17 assessments, they will essentially populate the
18 modeling program with all of the characteristics of
19 the adversaries. And essentially allow the
20 adversaries to attack the facility in the Mod Sim
21 programs.

22 MEMBER CORRADINI: So, can I ask, since
23 I don't know anything about this, but I'm curious.
24 Is the DB, is the group of DBTs determined by just
25 engineering judgment? Or is there a process?

NEAL R. GROSS

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

1 MR. RIVERS: There's a distinct
2 process. Essentially our office has the
3 Intelligence Liaison and Threat Assessment Branch,
4 which is our linkage to the intel community which
5 brings information in, evaluates it.

6 Our office provides recommendations to
7 the Commission when we believe the design basis
8 threat should be changed. So, a lot of it's based
9 on, you know, threat information we receive from
10 the intel community.

11 There are decisions that have to be
12 made as to whether or not something happening in
13 Iraq could migrate itself to the United States. We
14 will make recommendations to the Commission, and
15 the Commission in the end is the one that decides
16 whether something is added to the design basis
17 threat or not.

18 MEMBER CORRADINI: But you make the
19 recommendation?

20 MR. RIVERS: We make the recommendation
21 in our office.

22 MEMBER CORRADINI: So maybe this isn't
23 the right place to --

24 MEMBER BLEY: I think that's right.

25 MEMBER CORRADINI: Okay.

NEAL R. GROSS

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

1 MEMBER BLEY: We shouldn't pursue this
2 one much further.

3 MEMBER CORRADINI: Okay. I figured
4 he'd stop me.

5 MR. RIVERS: Okay.

6 MEMBER CORRADINI: Thank you.

7 MR. RIVERS: So, our process of
8 oversight of course is through an inspection
9 program. We have two basic types of inspection.
10 One is the baseline inspection, which covers a
11 broad variety of topics.

12 And then one that tends to have a lot
13 more visibility is the force-on-force inspection
14 programs. The force-on-force actual graded
15 inspections are once every three years at each of
16 the nuclear power plants.

17 The actual operators of the facilities
18 conduct training versions of these force-on-force
19 four times, generally four times a year. NRC
20 observes at least one of those, in addition to the
21 once every three year graded exercise.

22 Special inspections are done based on
23 things that may have happened at the plant, and the
24 determination that we need to have a special
25 inspection.

NEAL R. GROSS

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

1 Safety/security interface, there is a
2 requirement that's codified in 10 CFR 73.58, that
3 safety/security interface requirements for nuclear
4 power reactors. It applies to all operating
5 nuclear power plants.

6 It requires a pre-assessment and
7 management of all planned and emergent activities
8 involving changes to plant configurations, facility
9 conditions, and/or security programs. It requires
10 to communicate potential conflicts to appropriate
11 personnel, and take necessary actions to maintain
12 safety and security, in accordance with NRC
13 requirements and license conditions.

14 So this is the regulatory discussion.
15 The next two slides I'll talk about sort of the
16 value of it, and some of the things that I think
17 are useful in that area.

18 One of the things to keep in mind, if
19 we look at what are the target sets that are used
20 in vulnerability assessments, and also in force-on-
21 force inspections, they're actually derived from
22 the cut sets from PRAs to inform the target sets.

23 So we use the PRA analysis to actually
24 identify what targets might the adversaries
25 actually hit to actually cause the core damage and

NEAL R. GROSS

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

1 radiological sabotage.

2 Security vulnerabilities and associated
3 consequences are needed by safety organizations to
4 inform safety programs. So if the safety
5 organizations don't know what might happen as a
6 result of an adversary attack on a facility, they
7 are not necessarily going to be able into place the
8 proper safety and mitigation systems to protect
9 that facility.

10 We also need to understand the
11 relationship between safety and security risk. One
12 of the things that, when we look at risk and we
13 look at PRAs, PRAs we have all of these engineering
14 values that say that there's a certain ten to the
15 minus six probability that something is going to
16 happen. And all of these numbers are based on
17 engineering calculations. And some of it's based
18 on judgment calls by experts.

19 In the security world you have a,
20 fairly commonly you hear that we assume the
21 adversary's going to attack. And so, the
22 probability of attack is one. I tend to, as a
23 statistician I tend to not like to look at it that
24 way.

25 Although the safety community is

NEAL R. GROSS

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

1 looking at the risk if something happened, in the
2 security world what we tend to look at is what I
3 would call the conditional risk. If an attack
4 happens, how well do the security systems actually
5 work? So, it's just a different perspective.

6 MEMBER CORRADINI: So, in the range of,
7 so just back to other terminology. So, I don't
8 remember the words you used. But the initiating
9 event is assumed to be one?

10 MR. RIVERS: Well, that's what people
11 talk about. But essentially, in reality what
12 you're doing is, I'm taking a conditional risk. If
13 that attack happens, what is the likelihood that
14 the security systems are going to work?

15 MEMBER CORRADINI: And then all of the,
16 as you had said, given that conditional --

17 MR. RIVERS: Given the --

18 MEMBER CORRADINI: Given that
19 conditional starting point --

20 MR. RIVERS: Right.

21 MEMBER CORRADINI: -- you used PRAs to
22 determine what might be --

23 MR. RIVERS: It's something very
24 similar to PRAs. If you go back into, you know,
25 the earliest days, the security vulnerability

NEAL R. GROSS

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

1 assessments were probably some of the first
2 modeling and simulation that was actually developed
3 at the National Laboratories. And those same
4 statisticians were the ones that actually developed
5 the initial PRA models as well.

6 MEMBER CORRADINI: Okay.

7 MR. RIVERS: So given that it was the
8 same people developing both tools initially, you're
9 going to have a lot of similarities in the
10 software.

11 MEMBER CORRADINI: Okay. Thank you.

12 MR. RIVERS: So, essentially we assume
13 that, we basically say that our analysis in
14 security is a conditional risk. That if an attack
15 happens, what is the effectiveness of the security
16 system?

17 Your sort of have to do that, because
18 it's much, harder to identify the likelihood that
19 an adversary is going to attack. If not random --
20 We really haven't had too many of them, none of
21 them at nuclear facilities.

22 And a lot of it is based on adversary
23 seeing that something is deficient at a plant, so I
24 have an opportunity to do a much better job to
25 attack. So they just don't randomly roll dice and

NEAL R. GROSS

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

1 say, I'm going to hit this facility. They're
2 actually assessing the facilities, and making
3 determinations as when it's best to go.

4 And if we go, the other part, to
5 understand the relationship between safety and
6 security. I know talking to some of the security
7 managers in facilities, one of the things that you
8 find is that when they're trying to decide how
9 much, how to spend their money to make sure that
10 their reactor operates safely and securely, it
11 becomes quite a challenge when we measure risk
12 differently in the safety world and the security
13 world.

14 And it would be much better if in the
15 end we could achieve an understanding of how that
16 safety risk relates to the security risk, so that
17 the owners of these reactors can actually better
18 risk inform their decisions on how to spend the
19 money they have to protect that facility.

20 MEMBER BLEY: And you just hinted at it
21 though, but didn't go in some. Some things you
22 might do to improve security could actually hamper
23 safety.

24 MR. RIVERS: That's right.

25 MEMBER BLEY: And vice versa.

NEAL R. GROSS

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

1 MR. RIVERS: That's correct.

2 MEMBER BLEY: Yes. And that's the
3 things we really would like to keep an eye on if we
4 can.

5 MR. RIVERS: That's right.

6 MEMBER CORRADINI: And that currently
7 is, just to make sure I understand. That currently
8 is looked at by the licensees?

9 MR. RIVERS: Well, the licensee,
10 because we don't really understand what that
11 relationship is. And I know that a couple of the
12 initiatives that have been briefed to this
13 subcommittee and the full committee, like the risk
14 prioritization initiative, and some other things,
15 have talked to the fact that, yes, we're, you know,
16 industry and NRC staff are trying to understand how
17 those risks may be related.

18 We really don't have the answer yet.
19 And I think it's something that in the end it
20 probably would be of value to both the NRC and
21 industry to have that understanding.

22 MEMBER CORRADINI: I'm sure that John
23 and Dennis know this. But I just, I'm still
24 struggling. So, since as a conditional situation
25 where you're assuming that this whatever chooses to

NEAL R. GROSS

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

1 be the thing that happens, happens, can you really
2 ever do a comparison?

3 MR. RIVERS: Well, I think, you know,
4 there have been, there are a lot of activity going
5 on in the DoD world, and also, probably more so the
6 DoD world, trying to understand the terrorist
7 likelihood of attacks, the intel community.

8 And I think probably initially you
9 probably want to do some sort of a semi
10 qualitative, where I put it in some sort of a
11 range.

12 MEMBER CORRADINI: So, in other words,
13 there is some thought to essentially binning these
14 assumed things into very large bins of likely, less
15 likely, not so likely.

16 MR. RIVERS: I think there's been a lot
17 of work in that area. I think that in the end
18 that's where you have to start. Hopefully we never
19 see an attack at a facility. And then we never
20 have any empirical data. But I think initially you
21 have to look at some sort of a binning process.

22 MEMBER CORRADINI: So, last question.
23 Is there philosophically resistance by other parts
24 of the Government to even think like this?

25 MR. RIVERS: I don't think there's any

NEAL R. GROSS

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

1 resistance. I think people look at it as such a
2 challenge to solve that not a substantial amount of
3 work has been done in this area.

4 MEMBER BLEY: There's another side to
5 it that, at least that has struck me whenever I've
6 played with this concern. For the most part, from
7 the safety side and the PRA side, the likelihood of
8 a challenge is kind of constant thing.

9 In this area the likelihood of a
10 challenge may not be, and may be changing. There
11 are Government agencies that, Jeff said, that
12 interact with NRC, that talk about threat level is
13 changing day by day, week to week, or whatever.
14 But it's probably not a constant.

15 MEMBER CORRADINI: So the risk is a
16 dynamic concern? The risk is dynamic?

17 MR. RIVERS: The risk is very dynamic.
18 You know, other things to keep in mind is there are
19 other factors that are also hard to quantify. For
20 example, what is deterrent scale?

21 If we look at our nuclear power plants
22 in the U.S., we probably have some of the best,
23 well guarded facilities in the world. If they were
24 less well guarded, it might be adversary want to be
25 attacking them more frequently. And so, even the

NEAL R. GROSS

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

1 level of deterrence factors into the likelihood of
2 an attack.

3 MEMBER BLEY: Because it's a choice,
4 rather than a roll of the dice.

5 MR. RIVERS: Right. So --

6 MEMBER SKILLMAN: Joe, you made a
7 comment that speaks loudly to me, several minutes
8 ago. And that had to do with, when there's been a
9 change that presents a vulnerability in the plant.

10 MR. RIVERS: Right.

11 MEMBER SKILLMAN: Let me back up. I've
12 watched force-on-force for years. I've got a
13 pretty good appreciation for how effective that
14 security force anticipates and responds.

15 At the same time, the greater risk, at
16 least in my judgment from being around these plants
17 for decades, is the inside threat. The disgruntled
18 employee, or the individual who can connect the
19 dots and say, since we have that diesel down and
20 that transformer out, or whatever that might be,
21 this I the time.

22 What consideration is given to that
23 more subtle, and perhaps deeper infection that's so
24 difficult to dig out?

25 MR. RIVERS: We have, you know, a lot

NEAL R. GROSS

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

1 of requirements for insider mitigation programs, to
2 include behavioral observation programs. And then
3 when we're considering, for example, in the force-
4 on-force exercises, essentially you have an insider
5 adversary that participates and provides complete
6 information.

7 So, we do test the fact that, okay, if
8 you do have an insider, what's going to happen?
9 You know, insiders can also do more things. They
10 can damage parts of the facility. They can, you
11 know, make it easier for an adversary to get in.

12 There's a lot of things they can do.
13 We may not test all of those. But those are things
14 that the facility has to protect against. And
15 insider activities are definitely real.

16 If we look at the Doel Reactor in
17 Belgium, where they drained fluid from some system
18 that ended up costing millions of dollars to
19 repair, and lost revenue of millions of dollars as
20 well, the insider adversary is something to be
21 concerned about.

22 MEMBER SKILLMAN: Thank you, Joe.

23 MR. RIVERS: Sure.

24 MEMBER CORRADINI: If the Chairman will
25 allow me? So, who are the peers that reviews what

NEAL R. GROSS

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

1 you choose to do?

2 MR. RIVERS: What do you mean the peers
3 that review?

4 MEMBER CORRADINI: Well, I mean, so to
5 put it a different way. So, we're listening to
6 this now. But all the front end of all of this is
7 not our expertise. So somebody has that expertise
8 that must peer review what you do, or what the
9 group does.

10 Is there other parts of the
11 intelligence community that says, yes, that sounds
12 reasonable, or this seems unreasonable, or this is
13 too much, this is too little?

14 MR. RIVERS: Well, we have a lot of
15 interaction with our, the other agencies that
16 protect this type of material, for example, the
17 Defense Department and Department of Energy.

18 We have a lot of engagement with you
19 all here this afternoon from the Director of the
20 Office of Security at Department of Energy. And
21 his organization is one of the ones that we engage
22 with frequently.

23 MEMBER CORRADINI: But if I switch over
24 to chemical or biological is there, I still have
25 associated safety consequences.

NEAL R. GROSS

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

1 MR. RIVERS: That's correct.

2 MEMBER CORRADINI: Or a consequence, I
3 should say, due to the assumed whatever.

4 MR. RIVERS: Yes. And we, you know, we
5 do look at chemical hazards at these facilities as
6 well, both from a safety and security stance side
7 as well.

8 MEMBER CORRADINI: Okay.

9 MEMBER BLEY: I'll just remind all the
10 members, today is an information brief. And we
11 have tons of topics. So I don't want to stifle
12 questions. But we don't want the introductory one
13 to get into the meat of the rest of the program.

14 MR. RIVERS: Yes. So one of the
15 fundamental reasons for safety/security interface
16 is one that Dennis mentioned as well. Is the need
17 to evaluate impacts on each discipline as changes
18 in the plant configurations or operations are
19 planned.

20 So you don't, if I'm a security
21 organization, you know, we go to the fundamental
22 principles. In the security organization I try to
23 lock all the doors. In the safety organization
24 they try to unlock all the doors.

25 And so, the two disciplines have to

NEAL R. GROSS

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

1 work together to achieve a balance between safety
2 and security. And that's one of the real
3 fundamental reasons for safety/security interface.

4 MEMBER BLEY: And that simple example
5 we actually had happen early on.

6 MR. RIVERS: Right, yes.

7 MEMBER BLEY: Doors were locked, and
8 safety guys couldn't get to the rooms they needed
9 to.

10 MR. RIVERS: Yes. I'll give you an
11 example. At one of the Category 1 facilities, when
12 they were building the Great Wall of Erwin, which
13 was a large wall around the facility, the
14 preference by the security organization was to have
15 one opening.

16 And safety said there had to be two.
17 And so, those discussion go on. And essentially,
18 in the end we're much better off when both safety
19 and security both work.

20 So we also need to understand how
21 information from each discipline can better inform
22 the other discipline. And I think that's a lot of
23 what we want to understand as well.

24 When, you know, we, the security world
25 uses the information from the PRAs to support, you

NEAL R. GROSS

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

1 know, identifying target sets, the safety world
2 needs to understand what can happen if an adversary
3 actually attacks, to make sure the proper safety
4 and mitigation systems are in place. So, in the
5 end the two disciplines have to work very closely
6 together.

7 Risk informing security. Dennis
8 mentioned and Melanie mentioned the fact that we've
9 worked on a number of workshops. We had an initial
10 workshop in 2010, hosted by Sandia National
11 Laboratories.

12 Due to budget cuts I shifted the focus
13 to getting professional societies to organize them.
14 We ended up only having to pay registration fees,
15 which makes it a lot more cost effective for NRC.

16 With, the INMM Stone Mountain workshop
17 was actually a follow-on to the Sandia workshop.
18 Both of those workshops were focused on trying to
19 identify what some people might call low hanging
20 fruit, as to, you know, what are the best areas to
21 focus our attention on early on.

22 I also hijacked an INMM reducing risk
23 workshop in March of 2015 to try to get better
24 insights into risk informing security. And then in
25 the spring and fall of 2015 the two workshops that

NEAL R. GROSS

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

1 Dennis mentioned earlier started focusing on some
2 of the things that had been identified in the
3 earlier workshops.

4 Sun Valley workshop was focused on the
5 safety/security interface. We actually took
6 advantage of a meeting that ANS was hosting in Sun
7 Valley on probabilistic risk assessments. And then
8 set the meeting up on the Sunday prior to that
9 meeting. And got security folks through the INMM
10 to actually participate. So we actually had a
11 pretty good engagement, about 30 to 35 individuals.

12 Then in the fall we had a workshop in
13 Boston hosted by the Institute of Nuclear Materials
14 Management. And it was really focused on VA tools.
15 That it talked about the history of them, what some
16 of the basic aspects of it.

17 We brought in an actual project I'd
18 shared at the IEA on nuclear security assessment
19 methodologies, where they developed a case study.
20 And that case study was evaluated by each of the
21 three vendors to give people an indication of what
22 each of the tools actually does on a similar
23 facility, essentially.

24 If we look at some of the things that,
25 activity we have ongoing in risk informing

NEAL R. GROSS

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

1 activities for nuclear power plants, we're all,
2 we're looking at the use of modeling and simulation
3 tools.

4 So that aspect we're, you know, trying
5 to host workshops. We're trying to, or the staff
6 is trying to understand how that can be
7 incorporated in the regulatory framework.

8 Most of the staff doesn't have a lot of
9 experience in this area. So I've been doing some
10 internal workshops, trying to help the staff
11 understand what this concept is, and how it can be
12 used and incorporated in the regulatory framework.

13 Safety and security risk. I know that
14 several of the participants at the Sun Valley
15 workshop were NRC staff. And there's been a lot of
16 discussion amongst the senior level advisors of
17 trying to get some working group established to try
18 to sort of come up with ideas of how to better do
19 safety and security interface, and take advantage
20 of that within the agency itself.

21 Cyber security. As that program was
22 implemented when we got to the balance of plant
23 area, we're interfacing with a grid. A lot of
24 those critical digital assets, and those, that area
25 are not heavy into the safety impacts.

NEAL R. GROSS

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

1 And so, that concept of looking at
2 potential consequence, which is risk informing,
3 helped to better define what the requirements ought
4 to be in a more graded program.

5 And then I mentioned earlier the IEA
6 coordinated research project on nuclear security
7 assessment methodologies. It's been ongoing for
8 about three years.

9 The concept is to essentially develop a
10 methodology for assessing the effectiveness of a
11 security program at a wide range of facilities, to
12 include things like a nuclear power plant, an
13 irradiator facility, and independent spent fuel
14 storage installations.

15 So, looking at the broad spectrum of
16 facilities, and how do I actually determine the
17 effectiveness of security. And as I said, the case
18 study for the nuclear power plants was actually
19 used at the Boston workshop.

20 Then we can look at a couple of
21 industry initiatives. We mentioned earlier the
22 risk prioritization initiative, which was both an
23 NRC and an industry initiative.

24 But we also, in the last roughly half
25 year, we've received a couple of submissions on

NEAL R. GROSS

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

1 security plan changes that are 50/50/4P changes,
2 which basically state that we're making a change in
3 the security program. However, there's no change
4 or reduction in the effectiveness of the security
5 program.

6 Those submissions were supported by
7 modeling and simulation, the VA tools. And we as a
8 staff now are trying to determine how to use that
9 analysis that was submitted to essentially validate
10 the submissions of the industry. And so, that's
11 sort of the initial steps of the process.

12 We'll have to, in end, between industry
13 and NRC probably issue a number of guidance
14 documents to better understand how that process
15 needs to work.

16 Also, something you'll hear from the
17 next speaker is the consequence based approach for
18 SMR security regulations. And I won't talk too
19 much of this.

20 But the NRC received their White Paper,
21 industry's White Paper. And are, currently have it
22 under evaluation. But you'll hear more about that
23 White Paper from the next speaker. Yes.

24 MEMBER CORRADINI: So, is there
25 stakeholder feedback on a lot of this as this

NEAL R. GROSS

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

1 proceeds? Or are these workshops that you were
2 speaking about, the first, wherever they were, on
3 Slide number 10.

4 MR. RIVERS: Yes.

5 MEMBER CORRADINI: Are they the first
6 ones where you get stakeholder, from the fleet, and
7 how they're dealing with -- Given --

8 MR. RIVERS: We used to have to sort of
9 open up the discussion. I think that I've tended
10 to find that if we get on a neutral ground that
11 sometimes that allows people to be more frank and
12 open in their discussions.

13 Also, at these workshops it also had
14 value that we had external stakeholders that are
15 not industry and not NRC, to include the National
16 Laboratories, and some of the university types that
17 don't necessarily have a vested interest in what
18 we're doing, that can talk about their experiences
19 and their ideas on how to do things better.

20 MEMBER CORRADINI: Okay. Thank you.

21 MR. RIVERS: So, I've tried to take
22 advantage of those outside organizations, to try to
23 foster a better dialogue between industry and NRC.
24 So, the question is, what is a vulnerability
25 analysis?

NEAL R. GROSS

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

1 It's a systematic performance based
2 process that is used to evaluate the ability of a
3 physical security system to meet its performance
4 requirements. So, how well does that system work?

5 You know, if we look at what VA tools
6 are, you know, there tends to be a focus that, if
7 I'm using a VA tool it's that modeling and
8 simulation program, that computer simulation.

9 In reality, there are a number of types
10 of VA tools. If we look at tabletop analysis,
11 that's probably the most simple and straightforward
12 one that's probably used. And has historically
13 been used by this industry, the nuclear power plant
14 industry.

15 A lot of them have very interesting
16 tabletops. I know if I went to the Lynchburg
17 facility, they actually have, had a former model
18 railroader that actually built his model of the
19 facility. Very impressive. Some of them are just
20 made out of cardboard.

21 But tabletops have been around for a
22 long time in this industry. And I think we miss
23 the point when we don't consider those
24 vulnerability assessment tools, because they very
25 much are vulnerability assessment tools.

NEAL R. GROSS

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

1 Then the one that you'll hear more
2 about today is the computer simulations. Dennis
3 talked about the fact that these have, really were
4 started probably in the 1970s, and have developed
5 ever since.

6 And then we have some more labor
7 intensive type ones. The limited scope performance
8 test, where we want to test an element, or a system
9 or subsystem of a protection system. We'll run an
10 exercise on a portion of the actual overall
11 physical protection system.

12 And then we have the ones that are
13 force-on-force exercises. And those are also
14 vulnerability assessment tools. They're probably
15 the most expensive to get a single run. But they
16 all are part of the vulnerability assessment
17 process.

18 MEMBER BLEY: Joe.

19 MR. RIVERS: Yes.

20 MEMBER BLEY: I might be jumping the
21 gun, but I want to ask a couple of related
22 questions about this group of things. And when you
23 look at a tabletop I think you can understand the
24 model, what's going on and what you're doing.

25 When you get into computer simulations

NEAL R. GROSS

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

1 you see what comes out. How do you as a regulator,
2 if you look at these, understand the validity of
3 what's coming out of the models? I'm not, I guess
4 I'll get more familiar with limited scope
5 performance tests. You might mention something
6 about that.

7 And then the thing that kind of struck
8 me at these workshops I went to is, you know, and
9 this is true for safety too. We don't have very
10 many core damage events, so that we can look at
11 those and learn from them. And we don't have many
12 attacks. And certainly none on our nuclear plants
13 that we can look at.

14 But I heard a lot from the people doing
15 computer simulations, and the people who might use
16 them, that the way we confirm that these models are
17 accurate is by looking at force-on-force exercises
18 as data, which really struck me as uncomfortable.

19 Because they are at least to some
20 extent stylized, with a set of rules. And they
21 aren't, it might be the only data you have. But
22 it's not completely applicable to the real world.

23 MR. RIVERS: Well, I think that the
24 reason that people talk about the fact that force-
25 on-force exercises gave them comfort, and what

NEAL R. GROSS

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

1 they're saying are the results of the performance,
2 you know, the results from the VA tools about the
3 computer simulations is that that's what they're
4 comfortable with. That's what they're familiar
5 with.

6 And so, I think that you're going to
7 see when that's their experience base, that's the
8 thing that they try to relate to. I think that --

9 MEMBER BLEY: Which brings in some
10 dangers.

11 MR. RIVERS: It brings in some danger.
12 But I think if you talk to them a little bit more
13 you find out that they also look at portions of the
14 analysis, and tie them back to their limited scope
15 performance tests. That what they're seeing there
16 also, you know, rings a bell as well.

17 And then, you know, if I'm the one
18 that's actually looking at these results from model
19 and simulation, and trying to get some confidence
20 they're working well, I probably would want to
21 know, you know, where the data came from.

22 A lot of them come from data libraries
23 that have been used and developed in the Department
24 of Energy and the Department of Defense. I'd
25 probably ask questions about how robust is that

NEAL R. GROSS

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

1 data?

2 Some of it I think we find it turns out
3 to be fairly robust is we look at the PH/PK, which
4 is Probability Hit/Probability Kill, with the
5 battle simulation part of it.

6 What, it appears that even if I
7 decrease the effectiveness of my protective force,
8 that the likelihood of winning the battle and still
9 killing the adversaries still stays pretty high.
10 And probably a good explanation of that is that
11 there's so much lead flying that some of it's going
12 to hit somebody. So I think that --

13 And some of the utilities have actually
14 done that analysis. And we have to degrade their
15 protective force very significantly before we see
16 any change in those results.

17 I think if we look at the part of the
18 data that looks at the detection systems, you know,
19 those are fairly, you know, common detection
20 systems throughout both the whole nuclear complex
21 deemed defense, you know, at NRC regulated
22 facilities.

23 That if they're installed right, if
24 they're calibrated, if all of that stuff is done
25 properly we could probably have some level of

NEAL R. GROSS

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

1 confidence that the numbers that are associated
2 with those detection systems are probably
3 reasonable.

4 What I have a tendency to be more
5 concerned about is some of the traversal times, and
6 response times, and things like that. Because
7 really what you're trying to do is make sure that
8 the protective force can actually engage the
9 adversary before they get to the target.

10 And so the, you want to have a little,
11 understand really the uncertainties in some of
12 those traversal times of the adversaries, and the
13 response times of the protective force. Or, how
14 long does it take them to get through a barrier or
15 through a fence, things like that.

16 Because that's probably the one area of
17 these modeling and simulation that if you're off,
18 you could significantly impact the results. You
19 know, that's my professional opinion. You know,
20 we, you know, other people may have other opinions.
21 But that appears to be probably the weakest link in
22 the thing, in my opinion.

23 MEMBER BLEY: Thanks. That helps.
24 But, I'll ask the folks who actually talk about
25 some of these computer based tools. To your

NEAL R. GROSS

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

1 knowledge, do they do much in the way of V&V, QA on
2 the actual code development?

3 MR. RIVERS: Well, you know, the
4 vendors will put it through all of the, you know,
5 international guidelines for quality code, and all
6 of that.

7 DOE and DTRA did do some V&V work on
8 multiple codes, two that you'll hear about this
9 afternoon, the AVERT from ARES Security, and
10 SIMAGINE from RinoCorps. In that they will
11 periodically, in fact, they're getting ready to do
12 some of that.

13 It won't be a complete V&V. But part
14 of the problem is that it's, things constantly
15 change. As the computer technology change, the
16 softwares are constantly being changed. So some of
17 what you have to do is really look at the results.

18 And do they make sense? Are they
19 consistent? If I make this little change, does it
20 really adversely impact things? Or does it make
21 what I would expect generally?

22 So, it's not probably the V&V you might
23 expect from a widely used, you know, software
24 program like you have on your cell phones, because
25 of the, you know, billions of people that use them.

NEAL R. GROSS

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

1 You know, this is used by a very
2 limited set. And, you know, you have to be doing
3 V&Vs almost constantly. And the Government can't
4 afford that.

5 MEMBER BLEY: Okay. Thank you.

6 MR. RIVERS: Okay. So these are the
7 four general types of tools. If you look at
8 tabletop exercises, it's a method to simulate an
9 adversary attack on a site's existing or proposed
10 physical protection system, similar to a board
11 game.

12 It analyzes the most common things we
13 look at in security, the detection, the delay, and
14 the response. It also provides insight into a
15 physical protection that can stand alone, or be
16 used in other analysis tools.

17 You tend to find that a lot of these
18 tools feed information, and receive information
19 from other tools of that type.

20 Computer simulations, if we look at,
21 you know, how some of them are actually, what they
22 actually do, some of them are pathway analysis that
23 look at how does the adversary actually move
24 through the facility, generates what is the optimal
25 path, or the various paths they might use.

NEAL R. GROSS

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

1 Some are based on the types of
2 scenarios that you might want to actually exercise.
3 And then both of the ones you'll hear about this
4 afternoon have a combat simulation element to it.

5 So they all have different elements,
6 and they're constructed differently. But these are
7 probably the three most common things that are
8 involved in these computer simulations.

9 MEMBER CORRADINI: Are these just
10 degrees of the same thing? So, the first one you
11 just kind of wend your way through the maze? And
12 then there's various mazes? And then there's
13 actually stuff happening as you go through the
14 maze?

15 MR. RIVERS: Right, yes.

16 MEMBER CORRADINI: Is it just --

17 MR. RIVERS: Yes. The things will
18 happen. Some of them will have the adversary
19 making decisions based on, you know, what the level
20 of firepower is, how much delay, have I been
21 detected? All of those types of things get
22 factored in.

23 So, as the computers become much more
24 powerful, you know, the complexity of these
25 simulations has gotten much, much more complex.

NEAL R. GROSS

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

1 And you'll hear a lot more about that this
2 afternoon. So I'm probably not the best person to
3 ask those questions to.

4 We go to limited scope performance
5 test. This is where we'll have a manual exercise
6 to assess the effectiveness of a portion of the
7 overall physical protection system. And the
8 results can support other VA tools.

9 So, a lot of times what will happen is,
10 even on the force-on-force exercises they want to
11 figure out how long does it take for somebody to
12 climb over a fence, climb over a wall.

13 They'll run those exercises
14 independently. And then when they get to the
15 force-on-force exercises, they won't run that part.
16 They'll use the values that came up in the limited
17 scope performance tests.

18 Also, these limited scope performance
19 tests also validate information that may be found
20 in the modeling and simulation. Or it may feed
21 information that, you know, that provide the data
22 that actually goes into that.

23 Force-on-force inspection is actually
24 the full scale security exercising, using mock
25 adversary forces. And it does provide essentially

NEAL R. GROSS

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

1 how well a given scenario works. But probably in
2 the end what force-on-force exercise tells you is,
3 does the system work as a whole? Yes.

4 MEMBER RICCARDELLA: Excuse me. This
5 is my first exposure to any of this kind of stuff.
6 So if my questions are naive --

7 MR. RIVERS: That's okay.

8 MEMBER RICCARDELLA: -- please forgive
9 me. These force-on-force drills, are they
10 unannounced? Or does anybody say --

11 MR. RIVERS: No, there's --

12 MEMBER RICCARDELLA: -- show up for
13 work Saturday --

14 MR. RIVERS: No.

15 MEMBER RICCARDELLA: Friday morning
16 we're going to have a force-on-force drill.

17 MR. RIVERS: They're very, very
18 complex, and require a lot of planning. So they
19 are not unannounced. Essentially what you end up
20 having to have is, you have, you actually have a
21 real guard force. And then you have a guard force
22 that plays in the game. And then you have an
23 adversary force.

24 MEMBER RICCARDELLA: Okay.

25 MR. RIVERS: They're typically

NEAL R. GROSS

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

1 performed in the nighttime hours, because there's
2 less impact then of having plant people involved in
3 the exercise. And usually what will happen is,
4 they'll say, we have a window that sometime in this
5 timeframe the attack will take place.

6 And so, you have the onsite force that
7 has to be there to guard the facility. And then
8 you have the other ones that are sitting there
9 waiting for the attack to take place, knowing it's
10 going to take place within this two hour window, or
11 whatever. So, very, very complex, very, very
12 complicated. But definitely staged.

13 MEMBER CORRADINI: So, if you tell us
14 to wait, I'll wait. But to follow-up Pete's
15 question. Is there, are there, if I take it away
16 from the plant is there some importance that it has
17 to be at the plant?

18 MR. RIVERS: There's a --

19 MEMBER CORRADINI: Versus if you're not
20 going to involve the guard force that's already
21 there, that you'd have some sort of facility that
22 is more generic?

23 MR. RIVERS: The facility, this
24 actually has to take place at the plant. Because
25 each plant has a unique set of targets, a uniques

NEAL R. GROSS

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

1 protective posture.

2 MEMBER CORRADINI: The geometry --

3 MR. RIVERS: Right.

4 MEMBER CORRADINI: The geometry matters
5 enough.

6 MR. RIVERS: Right.

7 MEMBER CORRADINI: Okay.

8 MEMBER SKILLMAN: Joe, I'd like to ask
9 this question. Please feel free to say later or
10 no.

11 MR. RIVERS: Okay.

12 MEMBER SKILLMAN: it seems to me that,
13 and I've watched these. In the middle of force-on-
14 force you've got your onsite team doing what
15 they're there to do. They're protecting.

16 Then you have the adversary force. And
17 I've seen these folks. And they are mighty
18 capable. And then there's the responding security
19 force that's responding to the threat.

20 It's always seemed to me that that is
21 among the most vulnerable times for the unit.
22 Because you got to be careful to figure out who's
23 who. Who's really guarding the chicken coop.
24 Who's in and who's out.

25 MR. RIVERS: Well, and you have a lot

NEAL R. GROSS

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

1 of controllers. And it's a very, very active time.

2 MEMBER SKILLMAN: My question is, is
3 that assessed at a level that ensures that the true
4 force guarding is able to do what it needs to do?

5 MR. RIVERS: I'm not an expert in this
6 area, so I can't really respond to that. But I
7 would believe that that's always the number one
8 issue is protecting the plant. So if something
9 happens that could potentially jeopardize it, the
10 exercise would be halted.

11 MEMBER BLEY: I think we're getting
12 close to areas that probably ought to be --

13 MEMBER SKILLMAN: Fair enough.

14 MEMBER BLEY: -- done later.

15 MR. RIVERS: And we talked about target
16 sets and safety/security interface. It's an
17 important element of both computer simulations and
18 force-on-force exercises. And it's the minimum
19 combination of equipment which is, if prevented
20 from performing their intended safety function
21 would like likely result in a significant core
22 damage.

23 So, as I said, these target sets are
24 actually pulled from the PRA cut sets. So, and
25 actually, you've got a large number of these. So

NEAL R. GROSS

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

1 you pretty much have to take a subset of those that
2 make the most sense to actually be evaluated.

3 And that's actually the end of the
4 presentation. So I'm more than happy to take any
5 additional questions.

6 MEMBER BLEY: I'm sorry. I just want
7 to throw one comment, and then I'll give it to you,
8 John. The last thing you talked about. I don't
9 know if any of the rest of you remember when the
10 first PRA was done, WASH-1400, the Rasmussen study.

11 Norm Rasmussen and Saul Levine were
12 asked by people in Congress, and some other places,
13 isn't publishing this study like putting the
14 combination to the safe on the window of the bank
15 vault? And there's been worry about that.

16 MR. RIVERS: I know.

17 MEMBER BLEY: I mean, it is the thing
18 you go to to figure out how you would want to do
19 stuff.

20 MR. RIVERS: But part of what we assume
21 though is that they will have all of that
22 information anyway because of insiders.

23 MEMBER BLEY: That's true too.

24 MR. RIVERS: But we have to protect
25 with the understanding that that information is

NEAL R. GROSS

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

1 available.

2 MEMBER STETKAR: I suspect we'll get --
3 You know better how this day will unfold. But Joe
4 mentioned right at the end that, you know, there's
5 a large number of cut sets from a typical PRA. And
6 that some winnowing process needs to be used to
7 identify the cut sets that are used, I guess to
8 inform these types of activities.

9 There's kind of an interesting concept
10 that you don't necessarily look at the dominant cut
11 sets, if you will, from an internal events PRA,
12 because those things are at the top of the pile
13 because of unique attributes of the numbers that
14 are run through the PRA, that are identifying
15 vulnerabilities for a security assessment.

16 You might need to look down at the
17 bottom of the pile, which is difficult to see,
18 because it might be, because of the numbers that
19 are used in the quantitative analyses there might
20 be combinations of things that could be very, very
21 bad, but are very, very unlikely to occur --

22 MR. RIVERS: Yes. Yes, I would --

23 MEMBER STETKAR: -- that you want to
24 look at. So I'm kind of interested to find out how
25 this vulnerability assessment uses those cut sets

NEAL R. GROSS

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

1 from the PRA to kind of inform this process.

2 MEMBER BLEY: I think you might want to
3 save this.

4 MEMBER STETKAR: Yes.

5 MR. RIVERS: What I would do is say
6 this. You may also get some insights when Steve
7 Fogarty talks --

8 MEMBER STETKAR: Okay.

9 MR. RIVERS: -- after the break.

10 MEMBER STETKAR: Okay.

11 MR. RIVERS: Because Steve has
12 participated on both sides, PRA analyses and VAs.
13 And so, he can help you understand how --

14 MEMBER STETKAR: I thought you'd said
15 that. You just left yourself open.

16 MR. RIVERS: That's okay.

17 MEMBER STETKAR: You have something
18 that says questions, so I wanted to ask.

19 MR. RIVERS: That's fine. I know how
20 to pass the buck to later speakers. So, not a
21 problem. So, any other questions?

22 MEMBER BLEY: Joe, thank you very much.

23 MR. RIVERS: Okay.

24 MEMBER BLEY: And I guess now we go on
25 to Marc Nichol. Thank you. You can help him find

NEAL R. GROSS

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

1 his -- Oh, after asking everybody to make sure we
2 stay on schedule, I didn't mean to stifle comments.
3 And we're actually 15 minutes ahead of schedule.

4 MEMBER STETKAR: You're doing well as
5 Archie Bunker.

6 MEMBER STETKAR: And I could be Edith
7 if you want.

8 MEMBER BLEY: Marc, please go ahead.

9 MR. NICHOL: Okay. Thank you for
10 inviting the Nuclear Energy Institute to come and
11 talk with you today. I'd like to discuss the paper
12 that we submitted in November of last year,
13 focusing on consequence based security for small
14 modular reactors and advanced reactors.

15 We submitted that paper after having
16 put quite a bit of thought into it. If I back up a
17 little bit, and sort of paint the situation, or the
18 stage at the time.

19 The NRC staff had sent up, I believe
20 it's SECY-11-184, that discussed the conclusion
21 that the current regulatory framework was adequate
22 to license and approve small modular reactors and
23 advanced reactor designs.

24 And we don't disagree that small
25 modular reactors and advanced reactors could be

NEAL R. GROSS

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

1 licensed under the current regulations and
2 guidance. That's true. But we don't believe that
3 it's the most effective or efficient way to do so.

4 And so, after putting some thought
5 behind what would be some generic policy issues to
6 be addressed, and how they could be addressed
7 without having design specific information, we came
8 up with the approach that we outlined in the paper.
9 So that's what I'd like to discuss today.

10 I'll cover three main areas. One is
11 why a consequence based security framework is
12 necessary for small and advanced reactors. I'll
13 discuss the approach that we laid out, and more
14 importantly the policy issues that we framed in
15 that paper. And then discuss the path forward.

16 MEMBER STETKAR: Go ahead.

17 MR. NICHOL: Okay.

18 MEMBER BLEY: That will happen
19 occasionally.

20 MR. NICHOL: And then --

21 MEMBER STETKAR: It tends to eventually
22 go away.

23 MR. NICHOL: Okay. I think we're
24 clear. And then discuss the path forward, and why
25 we believe we need to start today to develop this

NEAL R. GROSS

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

1 framework. I'll start off discussing why small and
2 advanced reactors are different from large
3 reactors.

4 It's really the reason that we think
5 things can be done more effective and efficiently
6 for these reactors. It's based on a concept that
7 as technologies evolve and advance, we think the
8 regulations should evolve and advance with them.

9 And so, small and advanced reactors are
10 looking at enhancing safety. That enhanced safety
11 in turn has some enhanced benefits to security.
12 And there's also opportunities, because these are
13 early in their design stage, to incorporate
14 additional enhancements to security, if
15 appropriately incentivized to do so.

16 So, some of the difference is, they're
17 simplified, they're more simple designs. For
18 example, small modular reactors don't have large
19 piping. Small modular reactors have smaller cores,
20 more inherent and passive safety features.

21 Small modular reactors are, all the
22 designs currently being discussed are underground,
23 which provide additional benefits. There's a, all
24 of those translate into reduction in potential
25 accident sequences. And so, there's less scenarios

NEAL R. GROSS

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

1 in which accidents could occur.

2 And also, a slower accident
3 progression, and longer coping time. So even if an
4 accident does occur, then the consequences of such
5 accident would be less, because the accident is
6 slower to progress.

7 All of those together significantly
8 reduce the risk of radiological release, and
9 offsite consequences. And that's true in the
10 safety area. And that would also translate into
11 security considerations as well.

12 And as I mentioned, there's also an
13 opportunity to further enhance the security of the
14 designs early on in the process.

15 So, the paper is recommending that the
16 requirements be a right size for small and advanced
17 reactors. It's looking at having the equivalent
18 level of protection.

19 MEMBER BROWN: Excuse me. Does that
20 mean reduced?

21 MR. NICHOL: It could. When we're
22 talking about the security staff there are options
23 in there that, if you were to provide more security
24 base through the design features, the engineered
25 features, that there would be opportunities to

NEAL R. GROSS

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

1 reduce some security staff, yes. And I'll go
2 through that in more detail.

3 MEMBER BROWN: It just seems to be
4 problematic, that's all. I mean it's --

5 MR. NICHOL: Yes.

6 MEMBER BROWN: I understand your point,
7 since we've done, we've had considerable small
8 modular reactor meetings. But the idea that I even
9 have a 300 megawatt plan sitting there with a bunch
10 stuff somehow has some less radiological long term,
11 you know, consequences.

12 And so as soon as you hear consequence
13 based and right sizing it just seems to me to be, I
14 don't know, problematic. So I just wanted to make
15 sure I understood the thrust of --

16 MR. NICHOL: Okay, yes. And the
17 approach that's outlined in the paper is really
18 looking at what we're terming security by design.
19 So it's trying to achieve security through the
20 design features, the engineered safety features,
21 and the physical barriers.

22 And it's an approach that's consistent
23 with the NRC's policy statement on advanced
24 reactors, which is to reduce the reliance on human
25 actions to achieve safety and security.

NEAL R. GROSS

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

1 And so, the premise of the paper is
2 that in order to further encourage security by
3 design there need to be commensurate benefits for
4 the designers and the potential operators.

5 So, certainly they're going to meet and
6 exceed the current requirements for design
7 features. But there's not much incentive to go
8 beyond, much beyond that, if there's no opportunity
9 for savings.

10 And there's up front costs to include
11 further enhancements and considerations of security
12 in the design early on. There could be additional
13 up front costs in the construction of facilities
14 that are further enhanced through design features
15 for security.

16 And there needs to be an incentive to
17 do so. And that would be to be able to capitalize
18 on the benefits of reduced operator, reliance on
19 operator reactions.

20 MEMBER BROWN: It seems -- I just want
21 to make an observation. I mean, all the security
22 stuff, and I'm not an expert in this, you know.
23 I'm just an electrical guy. I'm someone that feeds
24 comment. I'm not a, hearing some of this for the
25 first time.

NEAL R. GROSS

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

1 But thought, thinking about it is that
2 security, regardless of how you think about it, is
3 really a function of controlling the access to the
4 plant, and those parts of the plant which have
5 consequence, severest consequence results if you
6 get into them.

7 And the large, large plants, where you
8 have a large facility, a wide barrier, fencing,
9 whatever the barriers are, you have, it's more
10 difficult. The control of access has more things
11 to go through.

12 Whereas, with a smaller plant
13 arrangement, and if you look at the size of the
14 sites where these have been going they're smaller
15 in many cases, in most cases.

16 It seems like the easier the access is,
17 or the closer the access, you would seem to have to
18 have an increased physical presence at some sites,
19 in order to minimize the access to the pieces that
20 could give you problems. So I'm just putting that
21 out. And I don't expect a --

22 MR. NICHOL: Yes.

23 MEMBER BROWN: -- large coherent answer
24 to that. But it just seems, I don't think the
25 basic assumption going into it is very good.

NEAL R. GROSS

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

1 That's just my thought process.

2 MR. NICHOL: Well, there's two
3 underlying assumptions in the current requirements
4 that we need to state. And they may not be
5 applicable to small and advanced reactors.

6 The first assumption is that without a
7 security force to interdict and neutralize, the
8 design basis threat would cause radiological
9 sabotage, or risks that are not acceptable. And
10 that may be true for small and advanced reactors.

11 The second is that even if the design
12 basis threat were able to cause, was able to cause
13 core damage or sabotage, that that would actually
14 result in offsite consequences that aren't
15 accepted, and that unacceptable. And that may not
16 also be true for small and advanced reactors. So
17 that --

18 MEMBER BROWN: Are you saying that the
19 consequences may be? You said may not be
20 unacceptable. That means to me they may
21 acceptable. Is that?

22 MR. NICHOL: Correct. Right.

23 MEMBER BROWN: So, it's okay to have
24 the stuff spilling outside the boundaries of the
25 site, of the plant facility?

NEAL R. GROSS

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

1 MR. NICHOL: Well, the --

2 MEMBER BROWN: Just because of the size
3 of the dose --

4 MR. NICHOL: It may not do that at all.

5 MEMBER BROWN: -- of the --

6 MR. NICHOL: So this is one of the
7 central policy issues that need to be addressed.
8 So, one, some designs may be able to achieve a
9 condition where the design basis threat comes in
10 and can't do any damage at all. And so, without
11 considering the activities or human actions of the
12 security force, that's one condition that needs to
13 be addressed.

14 Another condition that needs to be
15 considered is that if the design basis threat
16 causes say core damage, and there's no offsite
17 release of radiological material, that's another
18 condition that needs to be considered, and
19 determined whether that's acceptable or
20 unacceptable.

21 The third is if the design basis threat
22 causes damage that results in offsite release, but
23 the offsite release is very minor, much below say
24 part 100 limits, is that acceptable or not
25 acceptable?

NEAL R. GROSS

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

1 So these, we've tried to frame these as
2 policy issues that need to be addressed form small
3 modular reactors. These policy issues didn't
4 necessarily apply to large reactors, because large
5 reactors may not be able to achieve those types of
6 consequence based results.

7 MEMBER BROWN: It seems to me TMI had
8 no offsite problems at all. And yet, it literally
9 stopped the entire nuclear program of expansion of
10 plants in the country for 30 plus years. So that
11 assumption seems to be not have been born out.

12 Same thing applies with the Japanese
13 experience. Nobody died, that I'm aware of, yet
14 from radiological consequence. And somebody might.
15 But I'm not aware of it, or at least I personally
16 am not from our discussions.

17 Yet, that had massive reverberations
18 also when they shut down their entire, virtually
19 their entire nuclear industry since that occurred.
20 And they're just struggling to get it back. So I
21 just look at that statement relative to how we
22 operate. And so anyway, I'll let you go on.

23 MR. NICHOL: Yes.

24 MEMBER BROWN: I just wanted to make
25 sure I understood the thought process you all were

NEAL R. GROSS

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

1 going through.

2 MR. NICHOL: Right. And those are good

3 --

4 MEMBER BROWN: I'm not saying it's
5 right or wrong.

6 MR. NICHOL: Yes.

7 MEMBER BROWN: I'm just asking
8 questions.

9 MR. NICHOL: And those are --

10 MEMBER BROWN: That's all.

11 MR. NICHOL: Those are good
12 considerations. Because I laid out three or four
13 different types of potential consequences. And
14 what's needed is clarity to the applicant on what
15 is the performance standard that needs to be met.

16 And so it's, that's a wide range. It
17 could be very narrow and conservative, which means
18 that the design basis threat's not capable of any
19 core damage. Or it could be something different
20 from that.

21 So I think a lot of discussion is
22 needed. We didn't put in our paper a specific
23 answer, or our belief on what the answer should be.
24 Because we wanted the paper to be the starting
25 point for a discussion with the NRC and other

NEAL R. GROSS

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

1 stakeholders.

2 We want to get everybody's opinion in
3 the process. And we want to get it started early
4 and up front, so we can bring out all these good
5 insights.

6 MEMBER BROWN: Okay. Well, thank you.

7 MR. NICHOL: Yes. So the other things
8 is that the NRC requirements, there are performance
9 based requirements that are prescriptive
10 requirements. What we would like to see is a more
11 performance based, and a more technology neutral
12 approach to it.

13 So I mentioned some of the assumptions
14 that have gone into the regulations, based on the
15 characteristics of large light water reactors that
16 may not be appropriate or true for small and
17 advanced reactors. So those types of
18 considerations.

19 and I mentioned incentivize reduction
20 and reliance on human actions. I think we have a
21 choice going forward. Do we want to continue the
22 current security paradigm, where there's a heavy
23 reliance on human actions to protect against the
24 design basis threat?

25 Or do we want future designs to achieve

NEAL R. GROSS

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

1 that more through engineered features, and have
2 less reliance on human actions? I think the NRC
3 policy statements on advanced reactors is clear on
4 that.

5 And if we do want to reduce reliance on
6 human actions, then I think we need to begin now.
7 Because designs are in the process of being
8 developed. And if we wait too long then these
9 considerations can't be incorporated into the
10 designs. They'd be too far along.

11 So, I've talked about some of this. So
12 protection by design alone. That's the central
13 policy issue that we framed in our paper. And the
14 question is, if protection of, if protection
15 against the design basis threat can be achieved by
16 the design alone, then what's the appropriate role
17 of the security organization? And what are the
18 performance based requirements for those engineered
19 features?

20 And we talked a little bit about
21 different types of consequence based results in
22 consideration of the performance of engineered
23 features. And so, that's the question of, which is
24 the right level of performance characteristics that
25 need to be achieved to provide that high level

NEAL R. GROSS

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

1 assurance of adequate protection?

2 The other is the security organization.
3 So in, if a design were able to protect against the
4 design basis threat by engineered features along,
5 is the actions to detect, assess, interdict and
6 neutralize appropriate? Or are they unnecessary?

7 We have proposed that if, for security
8 by design the appropriate approach would be detect,
9 assess, and then communicate that threat.
10 Communicate that that threat exists to offsite law
11 enforcement, which would come and support.

12 So that's consistent with what's been
13 done in other areas. That's consistent with fuel
14 site facilities, with used fuel installations,
15 where the risks of, and the consequences that could
16 be a result of the design basis threat's attack are
17 considered, and deemed that that communicate portion
18 is an appropriate response. And that interdict and
19 neutralize is not necessary.

20 And just to make sure we're all clear,
21 the design basis threat would be the same for
22 advanced and small reactors. We're not proposing
23 that the design has an influence, or would change
24 the characteristics of the design basis threat.

25 MEMBER BLEY: I feel moved to make a

NEAL R. GROSS

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

1 few comments. In your paper you very often in your
2 talk about security by design. And I think I wish
3 your paper were titled that for several reasons.

4 I don't think anybody can argue with
5 the idea that we can design in better features to
6 protect either individual targets, or sets that
7 would affect whole processes, that sort of thing.
8 Two areas trouble me. And I know it's a
9 prospective paper. So I appreciate you bringing it
10 and sharing it with us.

11 The first aspect that troubles me is
12 the title, Consequence Based Physical Security.
13 Once you decouple likelihood from consequence, and
14 I think this consequence based rather than risk
15 based, risk informed, you challenge someone to come
16 up with an unacceptable consequence that would
17 undermine your whole house.

18 And I've yet to see any systematic
19 approach that involves our reactors, and many other
20 hazards, that can survive on a consequence based
21 approach alone. Because somebody can invent some
22 approach that will make the consequences worse than
23 you thought of.

24 Once that become very unlikely, we can
25 live with that. But if we have a system that locks

NEAL R. GROSS

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

1 in on consequence based, we have a system that I
2 don't think can be stable and work.

3 The other piece of this that bothers me
4 is kind of where Charlie was coming from, 300
5 megawatts isn't tiny. And sets of several hundred
6 megawatt facilities all hooked together on some
7 common systems need to be thought of very carefully
8 in this area.

9 Your argument that the design basis
10 threat ought to be the same for everybody is one I
11 can understand. But if we design to a design basis
12 threat, and protect against it, we're very
13 vulnerable to something akin to imagine a line.

14 Somebody will come up with a new threat
15 you haven't thought of. And it may be a very
16 reasonable one. I mentioned I was involved in this
17 Gen 4 project that was looking at perforation
18 resistance of physical security.

19 And one of the things we hung up on
20 quite a bit was, you know, a single design basis
21 threat might not be the right way to go. You might
22 need a threat space, or a threat set.

23 And if we're going to try something
24 like you're proposing, I think we need to be very,
25 very careful about what that space of threats might

NEAL R. GROSS

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

1 be. Because it's very easy to game a particular
2 EBT, and build your system to it's in, you know,
3 pretty well invulnerable to that.

4 And maybe there's a slight modification
5 in the threat for which you're now vulnerable. So
6 I think this whole approach requires a lot of
7 thought and careful consideration.

8 MR. NICHOL: Okay.

9 MEMBER SKILLMAN: I'd like to support
10 Charlie's gut instinct. What I'm interpreting from
11 what you're saying, Marc, is that particularly for
12 the SMRs, NIE would think a small guard force or a
13 small security force would be adequate.

14 And with sufficient design features
15 almost a Mayberry RFD with one policeman who has a
16 .32, and is, on his hip that's empty, and he has
17 one bullet in his pocket. And I certainly don't
18 share that point of view.

19 I think there are two threats that need
20 to be considered. One is the perceived threat, and
21 the other is the real threat. My own view is the
22 public would have extreme negative reaction to the
23 idea that you could have an SMR that really isn't
24 strongly protected.

25 But I also have another point of view.

NEAL R. GROSS

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

1 And this came after years of TMI. I remember our
2 security force at the time of the accident was
3 generally men and women, each carrying a revolver,
4 uniformed. And they spent most of their time
5 telling people to go down the road, that they
6 weren't allowed to drive onto the island.

7 And I watched that security force go
8 from being a small handful of men and women, to
9 being a force that was greater than ops or
10 maintenance. And I understand why those changes
11 came.

12 But in the middle of that metamorphosis
13 to more and more security, I think what those of us
14 at the plant realized was that the guard force was
15 there, the security force was there to protect us.

16 Clearly they were there to protect the
17 fuel, the spent fuel pool, and the facility. But
18 at the end of the day we realized they were
19 teammates. And they were there to defend us so we
20 could do our jobs operating that facility.

21 And it seems that that part of the
22 discussion isn't being clearly communicated. That
23 force does two things. It protects the facility,
24 and the vulnerabilities in the facility. But that
25 force also protects the people who are licensed to

NEAL R. GROSS

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

1 operate that facility.

2 I watched that happen when Pierce Ne
3 drove through the gate in 1997. And that was the
4 event that brought the industry its security
5 barriers, it's Jersey barriers. I was the EDESD
6 for that Sunday morning.

7 We were less concerned about the
8 facility, and more concerned about whether that
9 person was a shooter, and whether that person would
10 take out our staff. Let me make that point again.
11 We were concerned whether that person was a
12 shooter, and that shooter was going to take out men
13 and women on our staff.

14 And I would just offer, if you use that
15 lens to think about what you're proposing here, you
16 may come up with a different point of view. We can
17 talk about protecting pumps, pipes, and heat
18 exchangers all day long. We can talk about
19 protecting buildings.

20 But that security force protects men
21 and women who are able to drive that plant to a
22 safe shutdown, and to protect it. Those people are
23 important.

24 MR. NICHOL: Right. And I agree with
25 that.

NEAL R. GROSS

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

1 MEMBER SKILLMAN: Thank you.

2 MR. NICHOL: I agree with that. And I,
3 hopefully I haven't given the perception that we're
4 advocating for no security force, or even, you
5 know, just a single guard with a side pistol.

6 There still would be a security
7 organization that needs to perform other functions,
8 like search and seizure, and access checkpoints,
9 and all those things.

10 There would certainly be people there
11 to guard, and make sure the facility is safe, is
12 secure. And I do agree that protection of the
13 people is important as well.

14 What, where we're coming from in terms
15 of what would be required by the regulations,
16 stemming from the protection of the radiological
17 material, that's what we're talking about here, in
18 terms of what we think the regulations should say.

19 I think the plants will go above and
20 beyond that to protect their people. But that's,
21 you know, up to the companies to protect their
22 people. It not necessarily needs to be dictated in
23 the regulations to protect people. So, but I agree
24 it's important.

25 So, and to go back to the other point,

NEAL R. GROSS

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

1 in terms of the size, and not being small. The
2 definition of small is certainly less than 300.
3 And it's up to the design to actually be able to
4 demonstrate they can achieve these performance
5 criteria that would need to be established.

6 Not all small reactors would be able to
7 do that. Would a 300 megawatt reactor be able to
8 do that? Maybe, maybe not. But a lot of the
9 designs are much smaller than that. So some are
10 even down in the 20 to 50 megawatt size. So
11 they're much smaller.

12 What, to translate security by design
13 into other terms. One performance based criteria
14 would be the elimination of target sets. So if you
15 had no target sets to begin with, what's the
16 correct security posture to protect the plant at
17 that point? That's what we're asking.

18 And the regulations are very
19 prescriptive that you need to have ten armed
20 security guards with the sole duty of responding to
21 the design basis threat. Are those ten guards
22 still necessary if there are no target sets? That
23 would be one extreme.

24 And then the other would be, if you did
25 have target sets, maybe it's a target set with a

NEAL R. GROSS

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

1 large number of pieces of equipment that are
2 protected very well with physical barriers, that
3 the design basis threat does not have the resources
4 and capabilities to actually do harm and damage
5 that target set.

6 So those are the considerations. And
7 of course, the designs have to prove that they can
8 achieve those design criteria.

9 It's, we're not proposing that all
10 small and advanced reactors get a pass on this just
11 because they call themselves so. They would
12 actually have to demonstrate that to the NRC, that
13 they could achieve whatever performance standard
14 that's set.

15 And looking at the major policy issues,
16 we talked quite a bit about the security
17 organization response, that the performance
18 standard. I highlight there unreasonable risk to
19 the public. And so that's a major question. What
20 is reasonable, unreasonable risk to the public?

21 I appreciate your comment about if we
22 focus only on the consequence, we're ignoring the
23 probability side of the risk equation. And I think
24 that's true.

25 In our paper we didn't attempt to

NEAL R. GROSS

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

1 explore the use of PRA or probability on the, or
2 the likelihood of the types of attacks that would
3 occur. We took it very much as Joe talked about
4 earlier, as a probability of one, or a conditional,
5 if this occurs, what happens next?

6 If that were to change in the future, I
7 think it could certainly be applicable in this
8 area. But we didn't see a trending to change that
9 approach, at this time anyway.

10 But there may be other uses of PRA that
11 aren't in place today. So Joe also talked about
12 the --

13 MEMBER BLEY: I'm sorry. Even if you
14 don't put in a probability of attack, when you do
15 the kind of analyses that Joe was talking about,
16 you get out a probability distribution of
17 consequences. So they're not, even in a
18 conditional analysis, probability is part of the
19 answer.

20 MR. NICHOL: Right, right. Yes. And
21 we'd certainly like to talk about how that could be
22 introduced. We don't have a strong position on it
23 right now. We'd like that conversation to occur
24 though.

25 And other uses of the PRA. So, it's

NEAL R. GROSS

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

1 used to identify the target sets. That's based on
2 significant core damage, or spent fuel sabotage.
3 If that's still the performance metric for small
4 and advanced reactors, then maybe the use of PRA
5 may not be much different.

6 But if the performance metric were
7 instead the possibility of releasing radiological
8 material from the site, or a dose based standard
9 offsite, then perhaps the use of PRA could be
10 expanded.

11 And then there are other areas of the
12 requirements that, depending on how the major
13 policy issue is answered, may need to be looked at.
14 So, what are the requirements for the use of
15 firearms, or the armaments that are needed at the
16 site? What about the use of deadly force, and the
17 applicability of the NRC's policy on that.

18 And is there a need for force-on-force
19 exercises? Or do they, could they be something
20 different than what's done today? And all that
21 depends on how the major policy issues are
22 addressed.

23 I think what you may be getting a sense
24 of is that our paper posed more questions than
25 answers. And certainly that was the intent of the

NEAL R. GROSS

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

1 paper. We wanted it to be a point of discussion
2 with the staff and other stakeholders.

3 We recognize very much, as you pointed
4 out, that the public will have their own
5 perceptions of what we're proposing here. And will
6 have their own perspectives and questions to be
7 answered. And we want to make sure that they're
8 engaged in this process as well.

9 That's why we're, that's why we believe
10 that the discussion needs to start now. I know
11 that the NRC SECY, part of the justification on why
12 the current regulations are adequate is because
13 there's a process for alternative measures and
14 exemption requests.

15 And certainly we could go that route.
16 I don't think that that's the most efficient or
17 clear. If we draw the parallel, there's many
18 parallels with what we're proposing on security,
19 and what's being done in the emergency preparedness
20 space for small and advanced reactors, in terms of
21 the basis and the consequence based approach that
22 we're trying to achieve.

23 The NRC Commissioners approved to go
24 forward with rulemaking with that. And part of the
25 decision, or part of the basis for approving moving

NEAL R. GROSS

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

1 forward on rulemaking with that was that doing that
2 now, rather than waiting for exemption requests
3 was, provided one more clarity to the applicants,
4 more regulatory stability.

5 But it also provided an early
6 opportunity for stakeholder involvement. And I
7 think that's what's needed on this topic as well.
8 In terms of the clarity to the application,
9 business decisions are being made.

10 And decisions on the design are being
11 made today. So, if a designer is looking at how
12 they can enhance this for safety and security, the
13 framework itself has an influence on what they
14 consider, and what they try to achieve with that
15 design.

16 The current framework is very
17 prescriptive in what's needed for the security
18 organization. I don't believe there's incentive to
19 go very far in enhancing the design for security.

20 If there were opportunities to gain
21 benefits on the security organization side, then
22 there may be more incentives to further enhance the
23 design. And I think that's something that we
24 should pursue.

25 MEMBER CORRADINI: So, can I ask a

NEAL R. GROSS

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

1 question at this point? So I think I see your,
2 where you sit. So, how much have the current
3 owner/operators looked at this, given that they are
4 on the front lines of doing it now, compared to
5 what might be done?

6 MR. NICHOL: They, so security is one
7 of three of the major business, major regulatory
8 issues that are going into the business decisions.

9 MEMBER CORRADINI: No. But I'm asking
10 something different.

11 MR. NICHOL: Yes.

12 MEMBER CORRADINI: Maybe I asked it --
13 So, if I went to Exelon, which is running 25
14 plants, and they have a security plan that meets
15 current regulations, and they look at this, what
16 would their reaction be?

17 MR. NICHOL: In respect to their
18 operating --

19 MEMBER CORRADINI: In other words, do
20 they agree with the general feeling that improved
21 security by design, whatever Dennis called it. I
22 like the way he said it.

23 MEMBER BLEY: And it was their words.

24 MEMBER CORRADINI: Would essentially,
25 they would at least see the attributes that you're

NEAL R. GROSS

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

1 after. My only point is that it seems to me, where
2 I would go are the people that actually have to
3 make this happen now.

4 MR. NICHOL: Yes, yes. Yes, the --

5 MEMBER CORRADINI: And their reaction
6 to it. Kind of what is being asked.

7 MR. NICHOL: Yes. The owner/operators
8 had input into the NEI paper. And they see that as
9 a, you know, a good way to move forward as well.
10 So, now, we don't, we didn't propose that this be
11 applied to the operating reactors. Not that it
12 couldn't. But we didn't propose it to be.

13 One, because it may require extensive
14 modifications to the plant, which would be cost
15 prohibitive. And the other is, we're looking at
16 this as a going forward. But --

17 MEMBER CORRADINI: Right. But the
18 reason I asked the question the way I did is I'm
19 kind of reflecting on Charlie's reaction and Dick's
20 reaction, as a Navy reaction and a former
21 operator's reaction to it.

22 So I'm trying to get a feeling for what
23 the reaction was of those that are actually now
24 having to make this work, given current
25 regulations. That's what I guess I'm getting at.

NEAL R. GROSS

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

1 MR. NICHOL: Yes, yes.

2 MEMBER CORRADINI: Okay. Yes, and I,
3 if I wasn't clear before. The reaction was
4 positive. So, the regulatory framework in this
5 area can be developed without the design details.

6 Certainly design information helps give
7 confidence. But a lot of what we're talking about
8 are the more general high level policy questions
9 that we discussed earlier in establishing the
10 performance based criteria, which doesn't
11 necessarily need design details.

12 We have seen, from what we know about
13 small modular reactor designs, and advanced reactor
14 designs, we do believe that they are capable of
15 this. Not all of them will meet whatever
16 performance standard is established, or would be
17 established. But some certainly could.

18 Talked to, starting now would also
19 develop a regulatory basis that would support near
20 term exemptions and rulemaking, if those are
21 necessary. Certainly we're not going to be timely
22 enough for near term SMR applications. Probably
23 can be timely enough for advanced reactor
24 applications.

25 But nonetheless, developing the

NEAL R. GROSS

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

1 regulatory basis would support that. And I already
2 talked about how it's, about similar concepts with
3 what's being done in EP and advanced reactors.

4 So, given the time, just to reiterate.
5 So, we think the existing requirements aren't
6 appropriate for small advanced reactors, a
7 consequence based approach, or even something that
8 incorporates more of the risk insights could be, is
9 needed, and should start now.

10 Our paper's just a point for starting
11 that discussion. And we look forward to that
12 discussion. What we would hope to see is a meeting
13 in the relatively near term with NRC staff, to
14 discuss the paper, their considerations or
15 questions, get other stakeholder input into that.

16 We hope that the Commission would like
17 to move forward on this, and would make a decision
18 to do so in this year, and establish a regulatory
19 basis next year that, if needed, would support
20 exemptions that we're making. Thank you.

21 MEMBER BLEY: Marc, thank you very
22 much. Any comments from members of the committee?
23 Some good food for thought. And we appreciate you
24 coming --

25 MR. NICHOL: Thank you.

NEAL R. GROSS

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

1 MEMBER BLEY: -- and joining us. We're
2 going to take a break at this time. Try to be back
3 by about 10:25 a.m., and we'll start up again.
4 Thank you.

5 (Whereupon, the above-entitled matter
6 went off the record at 10:11 a.m. and resumed at
7 10:30 a.m.)

8 MEMBER BLEY: This meeting is almost
9 back to order. And we're going to move forward
10 with the presentation by Steve Fogarty of ARES
11 Corporation. On the Role of Modeling and
12 Simulation in Risk-Informed Security Decision
13 Making.

14 And this is kind of a break from the
15 overview and philosophy that we've done so far and
16 we're going to get into some of what the meat of
17 today's session is about. At this point I'll turn
18 it over to Steve. Thank you for joining us.

19 MR. FOGARTY: Yes, thanks for the
20 opportunity. I appreciate it, Dennis.

21 So what I want to talk about today, a
22 little bit of the history, if you will. Because
23 this is as much a perspective, as anything, on
24 modeling and simulation and its role in risk-
25 informing security.

NEAL R. GROSS

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

1 So back in the mid '90's, when I was at
2 PLG, I had an opportunity to apply some PRA
3 technics to DoD weapon systems. And specifically,
4 that involved taking some deterministic components
5 and probabilistic components and combining them
6 together into what the time was a pretty novel
7 application of PRA. But it was still very much
8 accident focused.

9 So DoD, in an effort to understand
10 their security risks, took that and funded an
11 effort, which I lead, starting with RND all the way
12 through to commercialization of a software tool
13 set. And then later we implemented that tool set
14 at DoD facilities, nuclear facilities DOE
15 facilities and commercial nuclear power facilities
16 more recently.

17 So then about a year ago I left the
18 vendor community and returned to being a risk
19 practitioner. But in the intervening time, and
20 since that time, there's still some unanswered
21 questions.

22 I did sort of, with these unanswered
23 question, in and around how best to risk-inform
24 security using some of these methods and tools. So
25 that's what I want to talk about.

NEAL R. GROSS

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

1 So before I talk about how this is done
2 generally, and this is a very general treatment of
3 modeling and simulation. No tool specific,
4 anything.

5 I want to talk about why we might do
6 it. So that being the benefits of modeling and
7 simulation for security.

8 So first of all, to get at that,
9 there's these figures for merit that you'll hear.
10 I call these here listed on the bullet there,
11 meaning the system effectiveness metric, defense-
12 in-depth and critical system elements that you get
13 at maybe through a sensitivity analysis as sort of
14 primary figures of merit.

15 There are many other statistics that
16 you can get at through these processes. It's a
17 data rich process so you're going to get a lot of
18 ability to do that. And understand the program
19 strengths and weaknesses, if you will, through
20 those metrics.

21 The ability to convey visual
22 information, I think, is pretty unique and uniquely
23 impactful in our ability to do risk communication
24 to leadership. So I consider that to be a
25 significant benefit of these tools. And methods.

NEAL R. GROSS

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

1 The ability to discovery and identify
2 emergent behaviors sort of manifest itself through
3 these unique, and maybe new vulnerabilities, that
4 hadn't been identified earlier. Or an ability to
5 characterize an emergent threat.

6 So there's a litany of secondary
7 benefits as well. First off, the safety security
8 interface and enabling that. I'll try and touch on
9 that where I can.

10 Just sort of warning you, I have a
11 pretty expansive definition of risk. I like to
12 include frequency, consequence, all components of
13 it in my, whether or not I can quantify all the
14 pieces as a secondary effort. But I'm going to
15 focus on the compatibility, where it exists, and
16 contrasts. And some cases, with safety, throughout
17 here.

18 I think it can be applied in various
19 phases of the design. We just heard a talk on
20 SMRs, as one application, when I've got a paper
21 design and can't very well do an OFF. Exercise
22 against that.

23 So tools like this really provide a
24 unique, I think benefit.

25 One of the things that's maybe often

NEAL R. GROSS

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

1 overlooked is these tools, although complex and
2 whatnot, the data input is done in a very natural
3 way for those that build these models.

4 I can talk to a security professional
5 about the time for a responder to get from one post
6 to a response location, where they may be in be
7 interdict and are up, neutralize the adversary.
8 And they have access to that timeline, okay. They
9 already test to that.

10 If I start talking in maybe more
11 abstract terms, especially with our security
12 professionals, security organizations, such as
13 there are today, about probability of interruption,
14 it's just a little more abstract for them, okay?

15 And then lastly, the bullets there on
16 their safety benefits. Obviously to over live
17 exercise. I'm not suggesting that we get real live
18 exercises, but more about, in cases where there's
19 an option.

20 And for example, I am a first
21 responder, I might be able to, I don't get in that
22 facility very often, I can use some of these models
23 that are secondary benefits. Get in through an
24 orient myself, to these facilities, through these
25 models.

NEAL R. GROSS

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

1 All right, so how we might go about it
2 and specifically, you know, how do we do it
3 successfully in implementing this? So first thing
4 is a terminology, and I'll hit more on terminology
5 in a minute.

6 The term there, PSMS, physical security
7 modeling and simulation, is just the way I
8 characterize, if you will, the security application
9 of risk, or PRA. Okay?

10 Here. So you we'll see that
11 throughout. The statement there is just one in a
12 paper that I wrote on this subject and more of a
13 thesis statement.

14 But what I want to focus on are the two
15 items there. To be successful I think there's an
16 effort that needs to be put forth to get the data
17 in such a way that we can build these models.
18 Okay? And I'll talk a little bit about what's
19 required there.

20 And then also the methods. A little on
21 the methods that are used generally in the tools
22 that are there, and by the analysis.

23 And then secondarily, how we use them
24 and what's the context for using these to risk-
25 inform a decision?

NEAL R. GROSS

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

1 So you'll see there's been a few papers
2 and presentations I have given. There was one at
3 the RIC last month, in this area.

4 Okay, so on creating input. So
5 regardless of the tool I'd like of think that this
6 is, this is how I see it anyway, are the inputs
7 necessarily to build these models. Three tasks, if
8 you will.

9 So we have to characterize the facility
10 into something that I term as a security virtual
11 environment. So think, starting with, there on the
12 chart there, virtual environment.

13 This is our facility, as we recognize
14 it, but in the computer. Right? So this is our 2-
15 3D model. All the terrain elevation, whatnot.

16 And so that's our representation, our
17 virtual environment, if you will, the facility, and
18 we're going to lay over top of that the security
19 that goes with it.

20 So fundament to security. And you've
21 seen already, I think in Joe River's presentation,
22 detection, delay and response. Our fundamental
23 concepts, not only required, but in that order, to
24 protect a facility. Of any kind.

25 So here we're just laying down those

NEAL R. GROSS

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

1 things that exist. Where detectors are, where the
2 delay systems exist on that. And collectively we
3 create this security virtual environment. Okay?

4 So that's Step 1 in the process. Step
5 2 then is, well how do the components perform?
6 These are the speeds that are, and whatnot, say
7 over a barrier using certain equipment, say by an
8 adversary. The performance of our weapon systems
9 that if they're utilized, by either in the hands of
10 the security force or the adversary.

11 And there's just a lot of data that
12 goes into that. But we have to understand the
13 performance piece, or what I call PDL there.
14 Performance data library.

15 And then lastly we've talked a lot
16 already, I think there's been some discussion on
17 the threat. And this isn't the DBT so much, as the
18 implementation locally in the DBT, into the
19 scenarios that we're going to run to understand the
20 securities. So those are the three inputs.

21 And now I want to maybe talk, a little
22 bit, of the departure, but directly, hopefully in
23 line with the meeting, some of my thoughts on the
24 safety security interface, through the terminology
25 that we commonly use.

NEAL R. GROSS

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

1 So for, at least for this presentation,
2 I'd to think of that first column there, PSMS
3 column, as the security application of PRA or risk.
4 And the PSA columns as the safety side. Okay?

5 Meaning, I'm just trying to use it as a
6 way to compare some terminology.

7 So you've got the security virtual
8 environment, that I just talked about in the last
9 chart. And we really don't, I can tell, we really
10 don't have something there on the PSA. Not that we
11 can't create our system models of the facility but
12 we don't use them, at least as a general approach
13 in PSAs, to actually quantify the risk. Okay?
14 That's abstracted.

15 And so if you go to the next row there,
16 the fault tree/event tree logic, for example, is
17 our abstraction and represents the failure logic
18 for the power plant. But there is analogy to that.
19 And I'll talk about this on the next chart or two.

20 But for now we'll call it the
21 adversary/traversal graph, if you will. That is if
22 you think of the adversary as your agent to
23 failure, maybe that's your comparison to safety
24 there. And mathematically there's also a
25 correlation, I mean direct relationship, a tree

NEAL R. GROSS

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

1 just being a subset of a graph structure.

2 So the next piece of comparison, the
3 PDL that I called on the prior chart, performance
4 data library, is directly comparable to the
5 terminology we use in safety for failure rate
6 databases and whatnot.

7 Target sets and, and it should,
8 probably here in this case, say we either begin
9 with minimal cutsets or just say cutsets. But
10 there's a relationship.

11 We've already heard about it. And
12 unfortunately I'm not going to be the expert, I
13 don't think, on experience in building those target
14 sets from cutsets, but generally you've got to
15 account for more than just the minimal sets, right?

16 You got to look at co-location of
17 equipment when looking at cutsets for failure.
18 What's co-located? Maybe a piece of equipment is
19 in a less protected location.

20 Those all go into selecting from the
21 family of cutsets. Which ones then build up the
22 target sets. So it's a special information
23 combined with the cutsets, from the PSA.

24 MEMBER STETKAR: Steve, you said you're
25 probably not the person to talk about that, are we

NEAL R. GROSS

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

1 going to here today from anybody who is?

2 PARTICIPANT: No.

3 MEMBER STETKAR: I think that's --
4 okay, thanks.

5 MR. FOGARTY: Okay, so then on the
6 threat scenarios and initiating event piece, I
7 think there's, I think we all understand we need a
8 driver for this analysis to go forward. So those
9 are, in that way, they're the same.

10 But it's also a clear and significant
11 difference between the random components of failure
12 in the initiating events and the actions of an
13 intentional adversary. Our adaptive adversary.

14 So it's bolded there and I'll treat it
15 on a subsequent slide.

16 So here's my, back to my comment, that
17 expansive definition of risk, if you will. Whether
18 it's conditional or not, I put that frequency in my
19 formulation because I believe it's important to
20 recognize it. And in the consequences as well.

21 But what I really want to drill down to
22 here, because this is where PSMS is focused, is the
23 likelihood estimate. Okay?

24 Conditional likelihood given an attack
25 that the adversary is successful, okay? So I'm

NEAL R. GROSS

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

1 going to touch on those. So both of those bolded
2 items I'm going to touch on, here in the next
3 charter.

4 MEMBER CORRADINI: So can I just say it
5 back to you so I understand?

6 So you do assign something to the --

7 MR. FOGARTY: The frequency?

8 MEMBER CORRADINI: Oh, I was going to
9 say, I guess the threat scenario is what you call
10 it. The initiating event, you do assign something?

11 MR. FOGARTY: Well the typical
12 approach, whether it's guaranteed or not, right,
13 you assign something. So yes, if you're saying
14 it's guaranteed or once per whatever unit of time
15 you want to look at --

16 MEMBER CORRADINI: I understand. I
17 just wanted to make sure I understood what you're
18 saying.

19 MR. FOGARTY: Right. And really the
20 purpose of this here is not to get into how we
21 might do better at that, but I believe it's
22 important to recognize --

23 MEMBER CORRADINI: But your point is,
24 it's included in the calculations?

25 MR. FOGARTY: Yes.

NEAL R. GROSS

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

1 MEMBER CORRADINI: Okay.

2 MR. FOGARTY: I think so. All right,
3 so the adaptive adversary -- go ahead.

4 (Off microphone comment.)

5 MEMBER BROWN: Sorry about that. Go
6 back to the Slide 5.

7 MR. FOGARTY: Sure.

8 MEMBER BROWN: Your line that says,
9 adversary agent traversal graph. And it says, the
10 adversary graph can be determined, automatically,
11 from the SVE, the security environment, virtual
12 environment, while the FT/ET logic is developed by
13 a risk analysis.

14 I guess it puzzles me that, yes, you
15 may know what the pathways are, but you've got a,
16 this is not like a normal cut set in a PRA where
17 you've blacksmith technology. You know, pipe
18 breaks, water goes out, valve opens, blah, blah.
19 You can predict what goes in some circumstance.
20 Most circumstances.

21 These are humans. And they don't
22 necessarily conform to a path. They get smart as
23 they go through.

24 How do you factor in, at least the
25 experience I've got from people, like seals guy

NEAL R. GROSS

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

1 that you know, says that they go in and they never
2 know what they're going to encounter. If they have
3 a path and they, most often never use the path.
4 They alternate, they improvise and they have to as
5 they go through.

6 How can you say or how do you say you
7 have any validity to the predictions when now, when
8 you've got a human involved in making decisions and
9 changing what they may do, even as they start
10 initially?

11 MR. FOGARTY: Well I guess first of
12 all, I'm going to agree with you --

13 MEMBER BROWN: Oh.

14 MR. FOGARTY: -- that if you don't do
15 that, then you've got a problem. And it is sort of
16 fundamental and foundational to the difference
17 between safety and security that we address that.

18 MEMBER BROWN: Yes.

19 MR. FOGARTY: And it's actually on my
20 next two charts.

21 MEMBER BROWN: Oh, okay. I just --

22 (Simultaneously speaking.)

23 MEMBER BROWN: -- automatically and --

24 MR. FOGARTY: No, and I did that
25 intentionally to identify it as it sort of

NEAL R. GROSS

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

1 distinct.

2 MEMBER BROWN: Okay.

3 MEMBER BLEY: I think I'm right. I
4 think this afternoon you'll see some actual
5 simulations where we'll actually see that happen.

6 MEMBER BROWN: That's fine. I just
7 wanted to make, I hadn't heard that in all the
8 previous discussions and this was the first time I
9 saw the line item that implied. It's automatically
10 determined from the environment that's the traverse
11 path and I suspect that they won't use the traverse
12 path that they initially planned on. More than
13 likely.

14 MR. FOGARTY: Yes, I can agree with
15 that. I'm not -- I'd be interested in your
16 comments on whether you think the approaches that
17 are out there are valid, but definitely there's an
18 effort to --

19 MEMBER BROWN: Okay. No. Okay, just
20 wanted to make sure I understood. Thank you.

21 MEMBER RICCARDELLA: Charlie, I'd just
22 like to say I object to the term blacksmith
23 technology.

24 (Laughter.)

25 MEMBER BROWN: On a comparable basis,

NEAL R. GROSS

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

1 okay, pipes and iron and steel and valves and wire
2 and insulation have been around since, well the
3 iron and steel --

4 MEMBER BLEY: Thanks, Mr. Brown, I
5 think we got that.

6 MEMBER BROWN: What? And the
7 insulation and the electricity have been around for
8 150 years. So the basics, fundamentals, are as
9 they are. But the new technology is far more
10 sophisticated. So it is blacksmith technology. So
11 we'll have to agree to disagree.

12 MEMBER BLEY: Steve, please go ahead.

13 MEMBER BROWN: Okay, thank you. Got to
14 have some humor here.

15 MR. FOGARTY: So the first statement
16 there at the top is really, how do we got out
17 these? I want to identify the steps or what will
18 start to introduce this term pathways, a given
19 threat could use to defeat the system, okay?

20 And we're going to start out here, I'm
21 going to try to generalize in just four steps, the
22 way these tools compute that likelihood estimate
23 that you saw on the prior chart. And we'll see how
24 well they do.

25 So the security virtual environment

NEAL R. GROSS

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

1 that I mentioned, okay, it needs to be broken down
2 into some component parts or data structure. One
3 of those is termed navigational mesh.

4 I don't know how well you can see it,
5 but in the notional figure there, the little
6 triangular pieces that are in there, and breakup
7 the model that's there on the right, are what you
8 might term that navigational mesh.

9 So we're going to breakdown that data
10 structure, into this navigational mesh.
11 Historically, if you look back, back to even to the
12 mid to late '70's, Sandia created ways to do this
13 using a much more even closer analog to PSAs.

14 If you take, they're called adversary
15 sequence diagrams, you take an event tree and you
16 like rotate it 90 degrees, it looks kind of like
17 that. So there's a lot of history there.

18 There's just be more automation, and
19 that's maybe the navigation mesh is where that
20 comes in. So I have to break into pieces first,
21 okay.

22 MEMBER RICCARDELLA: I'm sorry, you
23 talked about triangular pieces. I don't --

24 MR. FOGARTY: Yes, I don't know if you
25 can see them well on there. Yes, they're probably

NEAL R. GROSS

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

1 a little hard to see in the figure. I don't know
2 if you've got a hard copy. It may be a little
3 easier to see in the hard copy, but --

4 MEMBER CORRADINI: Can you point?

5 MR. FOGARTY: Sure.

6 MEMBER BROWN: There's some
7 quadrilaterals in there.

8 MR. FOGARTY: Yes. So the triangular
9 pieces here and here, everything is broken into, in
10 some form, into triangular pieces of concave
11 pieces. And it's really just a mesh --

12 MEMBER STETKAR: Steve, make sure
13 you're close to the, you can use the mouse --

14 MR. FOGARTY: Oh, sorry.

15 MEMBER STETKAR: -- make sure you kept
16 close to the --

17 MEMBER BROWN: No, you can use the
18 screen right here.

19 MR. FOGARTY: Oh, there we go.

20 MEMBER STETKAR: Yes, there you go.

21 MR. FOGARTY: There we go. Now I can
22 see --

23 MEMBER STETKAR: And you can see.

24 MR. FOGARTY: Now I can see it too. I
25 don't have to look behind me.

NEAL R. GROSS

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

1 MEMBER BROWN: No you don't, you can
2 look right up here.

3 MR. FOGARTY: Yes, be trained on this.
4 So here's one of the triangles, for example. It
5 goes from here and then there's another one here.

6 Okay, so what we're really doing is
7 we're trying to say if you go from a start point to
8 an endpoint, I have to traverse through these
9 paths. And I do so by this, breaking this side
10 into little pieces. If you will, triangular pieces
11 in one way or another.

12 So that tree structure that I
13 mentioned, that is created historically using those
14 sequence diagrams, adversary sequence diagrams, is
15 sort of automated in the sense that the edges of
16 the triangle become maybe nodes, if you will, in
17 the tree structure. Okay?

18 So I'm basically creating this tree
19 structure, or graph as we call it mathematically,
20 somewhat in an automated sense. By my ability to
21 break the site down into pieces. Nodes and edges
22 if you will, overall.

23 MEMBER RICCARDELLA: Okay, now that you
24 pointed them out I can see the triangles.

25 MR. FOGARTY: Can you see it better?

NEAL R. GROSS

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

1 Okay.

2 MEMBER RICCARDELLA: On the --

3 MR. FOGARTY: Sorry, I should have done
4 a better job on the figure there. So now I have
5 this and I want to find the path. You can see one
6 of the paths here.

7 So for any given structure, if you
8 think of entries, fault trees having split
9 fractions or weights, as we'll call them here, we
10 need a weight along the penalty, or cost if you
11 will, to get from one place or another. Okay?

12 MEMBER CORRADINI: Just so I got it,
13 when I entry a point, I have three choices, you
14 just give me a weight as to, at least a dynamic
15 weight, as to where I might go?

16 MR. FOGARTY: Yes. And we'll talk
17 about the weights on the next chart. But let's for
18 minute just say, if I have the weights and I have
19 the graph, I can actually solve for the minimum
20 cost to target. Okay? Okay.

21 And there's a lot to that. But I want
22 to get to the point that was brought up early, on
23 Step 3 here.

24 So I'm going to virtually, now I've got
25 this model, if you will, and I've got an attack

NEAL R. GROSS

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

1 plan, if you will, for the adversary. Meaning he's
2 going to look at this most vulnerable condition and
3 understand how we perform under this attack like
4 this.

5 That virtual attack, or simulation,
6 some would say combat simulation. But I like to be
7 expansive and we need to simulation all actions, if
8 you will. Including the combat component of it.

9 They perceive down the path as planned.
10 But they need and ability to adapt to conditions,
11 especially the stochastic nature of things, as
12 things evolve. Okay?

13 So they need both an initial plan to
14 sort of look at the greatest vulnerability and try
15 to attack along that and be able to adapt as they
16 go.

17 And then simply speaking, that
18 likelihood estimate, is very simply the number of
19 times the adversary was successful over the number
20 of times we simulated his attack. And that's how
21 we get at that estimate. Sort of an objective
22 probability estimate, if you will.

23 Okay, so that's just the steps. Now
24 I'll talk about the weight, if you will. How this,
25 because it gets to the behavior part of this, for a

NEAL R. GROSS

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

1 minute.

2 So try to classify the way these
3 behaviors work. There are, in my mind, a couple of
4 ways, nowadays, that this is done.

5 The first classification I want to use
6 is what I call task-based models, okay? So
7 adversaries are going along and they are through
8 interactions with our subject matter experts. They
9 have a defined set of mission tasks they need to
10 accomplish. From that start location to the end
11 being the target sets, if you will. So they have
12 this defined.

13 But between them, think of it maybe as
14 the route between the tasks they have to do. If
15 they're breaching one barrier and then another,
16 they have a route between those two, they can
17 adapt.

18 So they have an adaptation, okay, in a
19 task-based model. They do adapt. They just don't
20 do it in the same way that this other one is, which
21 is the preference-based models.

22 And those preference-based models look
23 more, if you will, globally at vulnerability for
24 the facilities. Finding the best route and task.
25 Not just the route to get there. And they do it on

NEAL R. GROSS

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

1 these preferences.

2 Their preference being, how much do I
3 want to minimize detection. How much do I value
4 that versus minimizing delay, versus minimizing
5 being neutralized by the protective force.

6 In this case, the modeling is very
7 global and expansive, but it requires more data.
8 And is more computationally expensive.

9 So back to the application quickly, for
10 a minute. DOE will, for example, will use these
11 task-based models. They use them on a fairly
12 regular basis at their facilities. Their nuclear
13 facilities.

14 And they do so because they fully
15 believe they already understand what some of these
16 tasks are. And they feel like they already have a
17 very good handle on their vulnerabilities, okay?

18 So, it doesn't mean they don't use the
19 preference-based models, but they gravitate a lot
20 to task-based models because of that. It's also
21 the only one that's in NUREG-7145 on security risk
22 assessment. At least as I see it mentioned there.

23 Preference-based models are very good
24 at searching for new vulnerabilities. So if you
25 had a new design, you're trying to evaluate it for

NEAL R. GROSS

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

1 the security system, they kind of tend to be good
2 at that.

3 They can also do the whole picture and
4 the whole security effectiveness performance
5 measure. But that's just a strength up there.

6 By way of example, there's a
7 preference-based model that's kind of listed on
8 the, now that I know how to use the mouse here,
9 that's listed on the chart here. And to give you
10 more, just an example how some of this stuff may
11 work.

12 So this is a phase one. So early on
13 they attack, the adversary minimizes their chance
14 of being detected. They transition at some point
15 to a delay focused minimizing their time to target,
16 if you will.

17 And then they transition at the next
18 threshold to a balance between, and this is
19 probably they're in some combat kind of simulation
20 or combat kind of environment, and they're
21 realizing, not that they don't care about, you
22 know, they're certainly willing to die for their
23 end goal maybe, but they understand that they're
24 neutralized, they can't achieve their objective
25 either. So they have to balance their ability to

NEAL R. GROSS

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

1 be neutralized with the time target.

2 So that's just one example that's
3 referenced there.

4 Okay, so one of the other key factors
5 in doing this is, what uncertainties are we facing?
6 And this is by no means an exhausted list or even a
7 list of all the things we ought to treat. But
8 these are things that I, from experience, believe
9 are not just important, but maybe commonly
10 overlooked uncertainties, when doing this.

11 So decision making. This decision
12 making focused on deployment of officers, shift
13 tactical commanders, such as they are.

14 A lot of our sites, they all have this
15 concept, even if there's preassigned response
16 locations. If an adversary makes it through, maybe
17 outer layers of security, there's always a concept
18 of flex to redeploy forces on the fly.

19 And all I'm recognizing is that we need
20 to account for that. And I'm not trying to
21 exhausted interview every one of these guys, but
22 appreciate the uncertainty and the effect on
23 performance.

24 The second one is, failure of the
25 security system. Not due to the adversary failure,

NEAL R. GROSS

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

1 but failure due to the latent failure, much like
2 PSA kind of thing.

3 So I'm going to give an example if that
4 because I think it's kind of telling and there's
5 some lessons in there, on the next chart. And
6 that's why it's bolded.

7 The others I think you can kind of get.
8 Operating modes, target sets for example. If I'm
9 in a detention in the reactor head I'm probably in
10 a more vulnerable condition than I am in full power
11 operations, for example.

12 So these are just things that I believe
13 need to be looked at. And I thought, if I could,
14 I'd give you an example of one. To kind of tell a
15 little bit of a story.

16 So this is the event. I'm guessing
17 many of you at least heard about this at some
18 level. But back in 2012, we had three protestors
19 at a DOE facility that penetrated the exterior
20 layers of the security system. Okay?

21 And I guess I want to talk about, is
22 there anything to learn from this? And we better
23 learn something, in my opinion.

24 And I think there's some stuff specific
25 to PSMS. Or Mod Sim for security that can be

NEAL R. GROSS

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

1 learned as well.

2 So I separated it in the way I see it.
3 The equipment and human performance side into two
4 separate pieces.

5 So first of all, I'm not here to say
6 that the material in the facility was ever at
7 direct risk, but I don't think it can be argued
8 that the system functioned as designed. I think it
9 clearly did not.

10 So it's a question of, where was the
11 failures? So first of all, there on the equipment
12 side, there was a critical assessment camera at
13 this facility.

14 So as the protestors made their way
15 through the outer layers, they couldn't slue the
16 camera to assess. So detection requires sensing
17 and assessment. We didn't have assessment and we
18 really didn't have detection, fully.

19 And they had a lot of history of high
20 nuisance alarm alerts at the facility. Just
21 exasperates the problem.

22 Next was human performance. On that
23 side, our primary assessment patrol didn't respond
24 fast enough.

25 It wasn't just slow response, it was

NEAL R. GROSS

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

1 outside of the timeline that they had for that
2 individual, in total, including uncertainty to
3 respond, okay? So that is another failure.

4 And then the last is, the alarm station
5 operator didn't declare a high priority soon
6 enough, if you will, as expected. Okay, so those
7 are just two areas.

8 And then I state the statement, well
9 okay, so PSMS, it reinforces the benefit of that
10 for this. But that's not the whole story.

11 PSMS was actually used at this
12 facility. And so you might say, well great, so why
13 didn't it find this problem?

14 This gets down to the fielded system
15 and the analyzed system. The system as fielded,
16 had these issues in it. The system as analyzed,
17 assumed these things were functional, okay.

18 There's nothing I'm telling you
19 probably that you've not seen before in other
20 situations. But I think it's a critical part of
21 the connectivity between this and the fielded
22 systems, if you will.

23 So we were basically analyzing an
24 idealized system and we weren't going to find
25 anything. And in fact maybe made it, us, maybe a

NEAL R. GROSS

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

1 little more confident than we should have been
2 because we had these results.

3 All right, so back to risk, down to
4 risk informing decisions here. I want to talk a
5 little bit about how that process might work.

6 And I'm going to do it in the framework
7 of Reg Guide 1.174. I just think it's a good
8 framework for risk informing decisions and I don't,
9 but I'm going to use terminology from security.

10 So defining a proposed change is how we
11 start the process. So this doesn't necessarily
12 mean I'm looking at it in the, I'm trying to be
13 expansive in the way I look at decisions too.

14 It could be an NRC decision that gets
15 advanced through a 5054 popup change like you've
16 heard about already today. Or it could just be any
17 decision. I'm sort of advocating for where
18 security fits into the decision process, regardless
19 of who the decision maker is.

20 So first off, if we can use it in early
21 in the process, we know where we're sensitive,
22 where system is sensitive, we can optimize a good,
23 we can come up with a good change. Is one area.

24 But regardless of what kind of change
25 we have, we need to perform some form of analysis,

NEAL R. GROSS

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

1 okay?

2 And I guess I'm just mentioning, and
3 Joe Rivers mentioned earlier, it's really a
4 combined effort, right? It's PSMS and Mod Sim and
5 it's limited in full scope performance testing,
6 it's force on force, tabletops, all that kind of
7 thing. So it's a full picture of performing
8 analysis, okay.

9 But once we have that analysis, the
10 other aspect of the decision process is, okay, if
11 we're going to implement that and maybe post
12 implement, how are we going to monitor it? How are
13 we going to ensure that we were actually right and
14 the assumptions were protected that we, as we field
15 them? So we have to come up with a way to define a
16 monitoring program.

17 So what I've done there, in the figure
18 below, is really just to speak to things that I
19 think are, can kind of tell somebody how to put a
20 model like this together.

21 It is one of the biggest problems in
22 modeling and simulation, is not having a scale for
23 how big your model needs to be to support the
24 decision at hand. And you end up spending a lot of
25 resources building these models sometimes. And

NEAL R. GROSS

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

(202) 234-4433

(202) 234-4433

1 sometimes in the wrong area.

2 So these are just areas for physical
3 security that I think are important to look at.

4 So the system layers. So, I don't
5 know, generally we have the owner controlled area
6 outside the plant, we have the protected area and
7 then maybe the vital area inside that. So just
8 generally, those layers is what I'm talking about.

9 As I get through those layers of the
10 security system, the more of them I get through, I
11 would qualitatively expect higher levels of detail
12 in my analysis to support that change. Because
13 it's affecting multiple layers of the security
14 system.

15 Similarly, on the other axis there, if
16 the critical elements in my system, that previously
17 identified were critical to the performance, I need
18 to protect those. More of those impacted, more
19 detail expected.

20 And lastly, thinking of those design
21 areas are fundamental concepts to security,
22 detection, delay and response. If I'm going to
23 affect my ability to detect, delay and respond,
24 yes, I'm going to need more details.

25 This is not anything quantitative here,

NEAL R. GROSS

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

1 but just an idea to help those that build these
2 models, kind of look at how much detail to put into
3 them. In their analysis and also in their
4 monitoring, I believe it could apply equally well
5 to both of those.

6 So lastly I need to document these
7 changes. So I'm going to document them in two
8 forms, right?

9 I need a decision document that the
10 decision maker is going to sue to understand their
11 performance and what decision is being advanced.
12 And it's supported by technically basis documents,
13 depending on the analysis that was done, okay?

14 I'll come back to that because I think
15 it's kind of a critical difference between safety
16 and security.

17 So as I wrap here, the next two charts
18 as I wrap up, before I conclude, I guess I wanted
19 to point out who's doing this currently and what
20 their nuclear experience is with this.

21 And I want to point out what DOE does,
22 as I see it. Having worked with them, sort of when
23 this was emerging, if you will, with them and their
24 interest in Mod Sim.

25 So they have more of what I call a hub-

NEAL R. GROSS

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

1 and-spoke configuration in their use of these
2 tools. They have a center with DTRA, Defense
3 Threat Detection Agency, is just one of them.

4 But as a good example, that the
5 services and bases and units in the field can
6 access to get Mod Sim done for them. But they
7 don't typically have that capability in the field,
8 okay. With trained expertise, okay.

9 They also, so I would say use it
10 intermittently, as needed. However, you want to
11 describe that, on the DoD side, for physical
12 security.

13 And then lastly, it was mentioned,
14 verification and validation. There's a whole topic
15 for discussion on how that's done.

16 I'd be happy to talk to that, but DoD,
17 for example, has done formal tool verification
18 validation and accreditation activities. Of course
19 you have to verify the implementation of the tools
20 and whatnot. But they've done some of that.

21 On the DOE side, they have more
22 organic, as I said, their risk assessment teams.
23 They're trained up in the fundamentals of this,
24 they've been leading the community, I think in this
25 area, in terms of implementation of some of these

NEAL R. GROSS

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

1 tools.

2 They'll typically apply more than one
3 tool set in-house, and do sort of this best to
4 breed kind of decision making on which tool to use
5 at a particular time.

6 Problem there is that can be pretty
7 cost, I don't know if it's cost prohibited, but
8 certainly costly, depending on who you are. At
9 least getting them spun-up and trained-up and kept
10 current.

11 I mentioned their existing policy can
12 be difficult when adopting new approaches. I think
13 that's sort of expected.

14 They have a regulatory framework for
15 using these, they require them, DoD does not.
16 Okay, so that's kind of a big difference.

17 So they're going to have polices. And
18 I will say you'll hear from Sam Callahan, I think,
19 this afternoon. He's really the expert in this
20 area and has been working hard for policy change,
21 including a new design basis threat that they're
22 about to come out with in DOE.

23 So my last sort of summary here talking
24 about, I guess I want to focus on the decision
25 maker's expectations when it comes to this. In

NEAL R. GROSS

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

1 terms of moving forward if we're going to use
2 these, what are the decision maker's expectations?

3 With respect to, and let's just maybe
4 focus it maybe on an NRC for example. What are the
5 reviewers of submittals that come in and when
6 they're reviewing a change to a design, what are
7 their expectations with respect to modeling
8 uncertainties, treatment of those? Do they need to
9 be treated, how to treat, qualitative,
10 quantitative, sensitivity analysis and that kind of
11 thing.

12 Okay, so that one thing I think that's
13 important to move forward with, we need to
14 understand those expectations.

15 One reason why, right, is, well for
16 quality purposes, but also those that implement
17 these, licensees or whatnot, if they don't
18 understand what their deliverable is, that is to
19 say what there is expected of them, they're less
20 likely to dip their toe into doing this, if it's
21 seen as a benefit. And the benefits of the whole
22 process get advanced the more that participate. I
23 think.

24 So I think that's one of the reasons.

25 Referenceable performance data is on

NEAL R. GROSS

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

1 there. Mainly to focus, not on the data itself or
2 data quality, but the fact that we really need to
3 keep an eye on, in my opinion, on how referenceable
4 that data is.

5 But that gets back to the decision
6 makers expectations. What are they going to
7 except?

8 I mean we sometimes will see it say,
9 subject matter expert, as the whole reference
10 behind where that data came from. And I'm not out
11 to say that expert elicitation and subject matter
12 experts aren't ideal candidates in some cases for
13 certain types of data, because we can't get at them
14 another way.

15 But I would say that's an insufficient
16 generally and insufficient answer, without a basis
17 for their logic. And it gets us in a situation, at
18 least, that we might reuse it in an inappropriate
19 way.

20 Peer review. What are their
21 expectations, prior to decision makers seeing the
22 decision document, what peer review has been done
23 on this work?

24 So, and then the last pieces here,
25 there isn't a common data library. So think

NEAL R. GROSS

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

1 generic failure rate data basis. There isn't such
2 a thing, okay.

3 Currently there's a lot of data. Okay.
4 DOE and DoD have shared a lot of data through these
5 initial analyses with NRC. And I think that's a
6 very powerful thing.

7 But there hasn't been anything capture
8 with respect to having a common library that can be
9 used. And I think that goes a little to quality,
10 in my opinion.

11 There's a limited quantitative
12 experience in this community. Doing quantitative
13 analysis in general and documenting it.

14 That's just a sub-bullet there, it's
15 just a suggestion that I think the PRA analyst
16 community might be able to, at the licensee merit,
17 help them understand what a technical basis
18 document really typically looks like kind of thing.

19 And then I think, because there's just
20 out, the applications today, in my opinion, can be
21 very tool-centric and not focused on the decisions.
22 I mentioned the 3D models.

23 You can overdo that, right? You can go
24 into a situation where the tool is really good at
25 building these cool looking models. And they're

NEAL R. GROSS

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

1 great. But you can overdo that. And it takes a
2 lot of resource into doing that.

3 And when you do that, that resource
4 gets expended, there's no going back and recovering
5 it. And it wasn't necessary to support the
6 decision in the end, probably. So that throttling
7 of that I think is largely just to do with the fact
8 that there hasn't been a lot of tools implemented.

9 And then this last one is a little more
10 policy level, which isn't my strength, I'm an
11 analyst. But it's just my feeling on the subject.

12 I think as we do more, there's going to
13 be more of a tension, a natural tendency to compare
14 safety and security risks. If we quantify risks
15 and security, we have quantified risks and safety,
16 we at least need to understand that people are
17 going to want to put them down next to each other
18 and say, wait, why is this one so different than
19 that or are they comparable.

20 And I think there needs to be an effort
21 to at least explain it, if not drive it all the way
22 down to normalizing some of the assumptions that
23 exist, where it makes sense, between them. So
24 that's what I wanted to cover and take questions.

25 MEMBER BLEY: Steve, thank you very

NEAL R. GROSS

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

1 much. Anything from the Members? Charlie, just a
2 short one, we're running out of time. No
3 soliloquies, Charlie.

4 MEMBER BROWN: Okay, Slide 10. You
5 talked about levels, systems layers impacted. And
6 that you had less detail in the outer layers and
7 more detail as you walked your way into the inner
8 layers. At least that's the way I read in critical
9 systems elements type thing.

10 And I'm just trying to think, why in
11 the world would I want my out layer to be breached
12 in the first place? I mean if you look at the
13 classic defense setups that you do in almost all
14 installations, you build one heck of an outer wall.
15 And you don't want to have to be scurrying around
16 inside the inner walls, inside those, to try to
17 stop a threat.

18 And so to me that would imply that you
19 would want to apply more detail to the ability of
20 an adversary to break through that outer wall
21 first.

22 I mean the kings in the old days didn't
23 build castles because they didn't want to have to
24 fight it in the villages.

25 MR. FOGARTY: Yes.

NEAL R. GROSS

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

1 MEMBER BROWN: And so it just seemed to
2 be counterintuitive to me.

3 MR. FOGARTY: Yes, I wasn't, it's
4 probably just a clarity issue on my part. I wasn't
5 trying to suggest that there wasn't detail in the
6 outer layers of the security, but that the entirety
7 and breath of the analysis that's performed, needs
8 to expand if the adversary, if the change I'm
9 making affects my perimeter fence, like you just
10 said, or my perimeter, as well as my vital area
11 inside the plant.

12 Okay, so for example, if I have
13 response forces that respond to both locations,
14 right, I've now affected the inner layers of the
15 security system and the outer layers
16 simultaneously.

17 So I'm suggesting that the breath of my
18 analysis needs to be, it needs to be broader and
19 detailed in such a way to address that. I'm not
20 saying that we don't need security at the perimeter
21 by any means.

22 MEMBER BLEY: I think we're going to
23 have to stop on that at this point.

24 MR. FOGARTY: That's fine.

25 MEMBER BLEY: Steve, thanks very much.

NEAL R. GROSS

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

1 MR. FOGARTY: Yes.

2 MEMBER BLEY: And again, thanks for
3 joining us. Our next speaker won't be in the room
4 with us, but he'll be on the phone. We have to get
5 the phone line open, which I think you'll have to
6 do.

7 MR. BUNN: The phone line is open. I'm
8 here.

9 MEMBER BLEY: Oh, you're here. Oh,
10 very good. If will give us just a minute, we'll
11 get your slides up.

12 MR. BUNN: Okay.

13 MEMBER BLEY: Yes, if can speak a
14 little softer or back away just a little bit it
15 will work better. It's coming in very loud.

16 MR. BUNN: Okay. How's that, is that
17 better?

18 MEMBER BLEY: That's perfect.

19 MR. BUNN: Okay.

20 MEMBER BLEY: Our next speaker, who was
21 just speaking, is Professor Matt Bunn of Harvard
22 Kennedy School of Business, Government.

23 We've had an introduction and an
24 overview this morning of kind of why we're doing
25 all of this, what's going on and where it can be

NEAL R. GROSS

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

1 useful. And a little bit of what some of the tools
2 are beginning to look like.

3 And I think Professor Bunn will maybe
4 give us some things to ponder about where we need
5 to be careful as we go forward. I thank you very
6 much for joining us this morning, Matt, and at this
7 point we'll turn it over to you.

8 I have to say we do have to end
9 promptly at noon because there is another meeting
10 that's challenging us as well. So I'll turn it
11 over to you at this time and some of the members
12 may ask you questions as we go along.

13 MR. BUNN: Okay, that's fine. So thank
14 you very much for the opportunity. I apologize for
15 not being able to be there. I wish I was there.

16 It was in the 20's when I was last
17 outside. We've got two or three inches of snow on
18 the ground here.

19 MEMBER BLEY: Matt, if I can interrupt
20 you, if you can back your sound off just a little
21 more.

22 MR. BUNN: Okay.

23 MEMBER BLEY: It's too loud here.

24 MR. BUNN: How's that?

25 MEMBER BLEY: That's better.

NEAL R. GROSS

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

1 MR. BUNN: So I apologize both for not
2 being there and for, unfortunately, I was in
3 another meeting and wasn't able to take part in the
4 earlier discussion. So it's at least conceivably I
5 may be repeating some things that have already been
6 said.

7 Next slide please. So I would argue
8 that computer tools for vulnerability assessment
9 are extremely helpful. This is the computer tools
10 as what the staff asked me to mainly talk about.
11 I'll talk about another point toward the end of the
12 talk.

13 If they're properly developed, then
14 you've had a lot of discussion this morning about
15 the strengths and weaknesses of where we are, so
16 far, on these tools.

17 They can give you higher fidelity in
18 simulating possible adversary scenarios then just
19 doing, for example, a tabletop exercise.

20 They can allow you to look at different
21 security options more easily. Which may help you
22 identify cheaper ones or more efficient ones to
23 accomplish the same objectives.

24 They can help the regulators try to
25 confirm if somebody's asking for an exemption and a

NEAL R. GROSS

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

1 change in what would normally be required. They
2 can help you confirm that, yes, that will actually
3 achieve the objective reasonably well.

4 They can help give you greater easy in
5 looking at a new adversary scenario that somebody
6 just thought of. And so that helps you have more
7 complete coverage of possible vulnerabilities.

8 And they can also help you look at what
9 if we did include something else in the DBT or what
10 if there was an adversary that went beyond what's
11 in our DBT right now?

12 How much would it cost to have an
13 effective system against that, modify its threat or
14 how much can our existing system do to deal with
15 that modified threat? So they can help you model
16 things like that.

17 Next slide please. But at the same
18 time, it's very important to understand the limits.
19 Nothing is perfect.

20 And in particular, there's the
21 fundamental issue of, garbage in, garbage out.
22 Models are only as good as the assumptions that go
23 into them.

24 So I have this famous quote, "all
25 models are wrong, some are useful." And my variant

NEAL R. GROSS

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

1 of that is also that some can be dangerous.
2 Because people tend to believe the output of a
3 computer model.

4 There's this sort of feeling, oh, it
5 got printed out by a computer, it's got to be true.
6 And I think often we get a little bit deluded by
7 thinking that the real world looks more like our
8 model than it actually does.

9 So I would say the models are very
10 useful for identifying factors that need to be
11 addressed and approaches for dealing with them.
12 But they're not likely to be very good at giving us
13 an absolute estimate of risk.

14 Particularly in security where we don't
15 really know what the probabilities of various
16 adversary actions might be. And there are large
17 uncertainties and complexities.

18 So I'm going to talk about five
19 different particular complexities. One, the
20 overall modeling of complex systems. The
21 complexity of the system itself and the difficulty
22 of modeling it.

23 You're limited by just the user of the
24 models ability to think of all the defeat
25 strategies adversaries might think of.

NEAL R. GROSS

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

1 There are human and organizational
2 factors that are more difficult to model than the
3 technical factors in the system.

4 The insider threats are more difficult
5 and the cyber threats make things difficult.

6 Next slide please. So there are a
7 number of key assumptions that even the best
8 vulnerability assessment tools, they're sort of
9 baked in to the idea of these tools.

10 One is that the technological elements
11 will perform according to the estimates that are
12 built into the model. Another is that the human
13 parts will perform according to the estimates built
14 into the model.

15 Another is that the adversary
16 capabilities and tactics will be within what's
17 imagined in the design basis threat.

18 And finally, the adversaries won't use
19 any strategies we haven't thought of. And that's,
20 you know, of course the number of strategies the
21 adversaries might come up with is pretty broad so
22 we need to think of defenses that will cover a wide
23 range of possibilities.

24 But still, there may be some defeat
25 strategy that gets at a vulnerability we haven't

NEAL R. GROSS

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

1 noticed or thought about. So any of those
2 assumptions can turn out to be wrong.

3 Next slide please. So let me talk
4 about these that I mentioned in turn. So one is
5 the difficulty in modeling complex systems.

6 When a system is complex and you have
7 somewhat uncertain system interactions, when you
8 pull on one side it may cause something to happen
9 someplace else in the system that you weren't
10 expecting. So there's emergent behavior.

11 And this is a situation where the
12 interactions among the elements, and especially the
13 how the human and organizational elements react to
14 changes in the technical elements, how they react
15 to just the passage of time going by as complacency
16 builds up and so on, is really not well understood.
17 Apologies for the misspelling of understood there.
18 I was doing this quickly yesterday.

19 So the 2012 incident at Y-12 gives you
20 a good example. They had just installed a new
21 intrusion detection system called ARGUS, that was
22 intended to improve security. But with the
23 installation they had, which may not have been
24 exactly correct, it was leading to many unexpected
25 false alarms. About ten times as many false alarms

NEAL R. GROSS

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

1 as previously.

2 So normally you'd check out the false
3 alarms with cameras, but the cameras had been
4 broken for months and nobody had bothered, yet, to
5 fix them. And so the guards were getting sent out
6 to check out the false alarms, but if there's ten
7 times as many false alarms, at a certain point you
8 get sick of it.

9 So these protestors went through four
10 layers of fencing, three of them alarmed. Set off
11 countless alarms, were at the very wall of the
12 building with thousands of bombs worth of highly
13 Uranium, spent a substantial period there singing
14 protest songs, pounding on the building with
15 sledgehammers and were finally accosted by a single
16 guard.

17 There were very heavily armed guards
18 inside the building who heard the pounding and
19 thought, huh, must be construction, even though we
20 haven't been told there is going to be any
21 construction and even though it's before dawn,
22 guess I won't bother to check.

23 So there was a pretty profound
24 breakdown in security culture. But if you're just
25 on a vulnerability assessment computer model, you

NEAL R. GROSS

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

1 would have seen all this good equipment and
2 intrusion detection and so on and you wouldn't have
3 realized that those problems were going to come up.

4 Next slide please. So a second
5 complexity is that it's just hard to imagine all
6 the things the adversary might do. And the tools
7 are only as good as the people who use them.

8 And so the personal solution to that is
9 to get people with our creative hacker kind of
10 mentality to use these tools and think of potential
11 adversary tactics.

12 One of my colleagues, Roger Johnston,
13 has a saying. He says, any real system has an
14 infinite number of potential vulnerabilities. Most
15 of which will never be discovered by either the
16 good guys or the bad guys.

17 And he says, we think that because
18 every time our team looks at something we looked at
19 before, we find new vulnerabilities we didn't
20 notice before. Every time somebody else looks at
21 something we looked at before, they find new
22 vulnerabilities we didn't see before. Every time
23 we look at a system that somebody else already
24 looked at, we find vulnerabilities they didn't find
25 and so on.

NEAL R. GROSS

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

1 So I think one, one thing is, I think
2 it would be very important to establish red teams
3 that are incentivized. Not only assigned to, but
4 reward for finding vulnerabilities. And of course
5 proposing fixes to them.

6 Next slide please. So this is a
7 fundamental one that gets back to the Y-12 case
8 that I mentioned. Which is, that it's difficult to
9 model how human and organizational behavior is
10 going to change over the years, and even decades,
11 that these systems are operating and in play.

12 You have to remember that for the
13 average nuclear guard, there will never be a real
14 event in his entire career. So every alarm he ever
15 responds to in his whole life will either be a
16 false alarm or a test.

17 And so trying to avoid complacency in
18 that situation is actually very difficult. So that
19 complacency in human behavior ends up affecting the
20 various assumptions made about how well the humans
21 in the system do their job.

22 This is particularly an issue for
23 various aspects of the insider threat. And the
24 degree to which people are willing to report
25 behaviors that might suggest that there is an

NEAL R. GROSS

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

1 insider problem.

2 My colleagues Scott Sagan and I, at
3 Stanford University, have put out a little pamphlet
4 called A Worst Practices Guide to Dealing with
5 Insider Threats, where we have a number of lessons
6 from real incidents in the past.

7 Not only in the nuclear industry but in
8 other context. About the difficulties that
9 organizations have in dealing with the insider
10 threat. Which I'll talk about more in a moment.

11 But this whole question of, how does
12 the organization and the human factor, factor in to
13 the performance of the overall system, is not well
14 modeled in a lot of these computer tools so far.

15 Next slide please.

16 MEMBER BLEY: Hey, Matt?

17 MR. BUNN: Yes.

18 MEMBER BLEY: Excuse me. This is
19 Dennis Bley. Can you make that guide you just
20 talked about available to us?

21 MR. BUNN: Absolutely.

22 MEMBER BLEY: Yes, I think --

23 MR. BUNN: I'd be happy to --

24 MEMBER BLEY: I'd personally be
25 interested in it. It sounds pretty good.

NEAL R. GROSS

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

1 MR. BUNN: I will drop a link to the
2 staff. And I should mention, just as advertising,
3 that we are, we've done a more elaborate version
4 with other authors going into cases in more detail.
5 And also a lot of interesting data on what Jihadis
6 have looked at in this broad category.

7 MEMBER BLEY: Okay.

8 MR. BUNN: That will be coming out as a
9 book from Cornell University of Press later this
10 year.

11 MEMBER BLEY: Oh, good, we'll try to
12 keep track of that and --

13 MR. BUNN: All right. So I will
14 certainly send a link to the staff for the Worst
15 Practices Guide that's already out.

16 MEMBER BLEY: Okay, thanks very much.
17 And I just wanted to back up to your previous slide
18 since I interrupted you. And just mention one
19 thing, in pretty much agreement with you.

20 One thing we found in doing analyses,
21 more for safety than in this area, but it works the
22 same in both, is just the mind shift, I think, of
23 instead of trying to figure out what somebody else
24 will do, saying, I really know the system inside
25 and out, how would I attack it for developing

NEAL R. GROSS

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

1 scenarios really makes a difference and helps.

2 MR. BUNN: Right. Absolutely. And so
3 I think having that kind of red team sort of
4 assigned to think that way, is quite important.

5 And that's one thing actually that
6 tabletop exercises are good for. Because you can
7 get a bunch of staff people together, at a site, to
8 just brainstorm about things like that.

9 All right, so I wanted to talk about
10 Slide 8. The one that says security culture
11 matters. So this is just a demonstration of the
12 point.

13 I love this picture because this is a
14 propped open security door at a Russian site that
15 had been upgraded with U.S. assistance. And what's
16 great about this photo is it's propped open on the
17 day that the general accounting office is there to
18 take a picture of it being propped open. Which
19 means that the people at the site really didn't get
20 the concept that it was a bad thing that it was
21 propped open.

22 So security culture can make a big
23 difference on your system. And I can talk about
24 that at lengths, if people are interested.

25 Next slide please. So this gets back

NEAL R. GROSS

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

1 to the insider point I was making a moment ago.
2 That those threats are more difficult to model.

3 A lot of the computer tools are really
4 much better on the outsider threat. They're
5 traditional methods based on sort of the detection
6 probability as the outsiders go through various
7 layers of the system, the task time that it takes
8 them to get from one layer to another and then to
9 do the things they need to do to either carry out a
10 theft or conduct a sabotage, the response for
11 survival time and so on.

12 All of that is more complicated and
13 tricky when you're talking about an insider who's
14 inside the system for months and years at a time.
15 And you may detect things, but you may not realize
16 that what you've detected is something you need to
17 deeply worry about.

18 One of the things that's been most
19 remarkable to me, in our work on insiders, is the
20 redness of the red flags that people will ignore.
21 So the guy who almost certainly carried out the
22 anthrax attacks in 2011, for example, Bruce Ivan,
23 had written an email to his own staff complaining
24 about his own dangerous paranoia and speculating
25 about ending up in the newspaper under a headline,

NEAL R. GROSS

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

1 mad scientist in control of deadly germs. And
2 nobody reported that.

3 That was, by the way, one piece of
4 many, many things that if anybody had really been
5 reporting properly, would have led to that incident
6 not occurring. In any case.

7 So insiders also aren't deeply familiar
8 with the security system and its weaknesses. Or
9 they may be.

10 Some of them may be the people who
11 designs the security system. And they have a lot
12 of opportunities for social engineering. For
13 convincing other staff to do seemingly harmless
14 things that facilitates a plot.

15 You see that in amazing detail in the
16 case of the escape from the Clinton Correctional
17 Facility this past year. Where the inmates really
18 succeeded in social engineering with a lot of, with
19 a number of the guards. In addition to the woman
20 who was actually in a romance with one of the
21 inmates. Or sort of in a romance.

22 And insiders may recruit other
23 insiders. And very few of our DBTs include a
24 multiple insider scenario. But if you look at
25 major thefts in the non-nuclear world, multiple

NEAL R. GROSS

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

1 insiders are at least as common as alone insiders.

2 Next slide please.

3 MEMBER BLEY: I want to interrupt you
4 for another time, Matt.

5 MR. BUNN: Okay.

6 MEMBER BLEY: In the area of risk
7 assessment, I've often found that the more even
8 antidotal stories one can find, it really helps
9 when you're doing modeling to keep your thinking
10 very broad. Are there good sources in this area
11 for the kinds of stories you just went through?

12 Are you going to have these in your
13 book or can you send us to some other sources?

14 MR. BUNN: So I think that is a very
15 important point. I have been advocating for years,
16 so far unsuccessfully, that the U.S. Government
17 ought to put such a thing together. And in
18 particular, that we ought to create a shared global
19 database of incidents and lessons-learned.

20 You know, in the safety space, if
21 you're a U.S. Nuclear Power Reactor, as you know,
22 and you have some kind of near-miss incident,
23 there's a root causes analysis, lessons-learned
24 that get sent to INPO. INPO does trend analysis
25 based on what's happening in other reactors, that

NEAL R. GROSS

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

1 may be similar.

2 Those lessons-learned get distributed
3 to the other reactors. INPO even inspects to see
4 how well you're implementing the lessons-learned.

5 None of that exists in the security
6 world. And I think there are restraints created by
7 security issues, but I think there's a lot that
8 could be done.

9 If you look in the cyber security
10 world, there is a lot of this sort of data
11 compilation that gets done.

12 There's a group at Carnegie Mellon, for
13 example, that collects anatomized data so that
14 companies are willing to hit it over on insider
15 cyber cases in many different industries. And they
16 have a database of over 300 particular incidents
17 that you can go through and learn from these
18 different incidents.

19 And it's a big enough database now that
20 they can do statistics about, well, how many
21 insiders have this characteristic and that
22 characteristic and so on.

23 One thing I would point you to is a
24 very nice piece, which again, I can send the link
25 to the staff, that was done in Sandia National Labs

NEAL R. GROSS

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

1 a couple years ago called the Perfect Heist.

2 Which goes through, oh, 15 or so major
3 sort of multi-million dollar non-nuclear threats
4 from garden facilities in recent years and just
5 looks in detail at what was the security
6 arrangement, how was the security arrangement
7 defeated, what kinds of tactics and capabilities
8 did the adversaries have. I think that's the kind
9 of thing that we definitely need.

10 I'll just give you an example of, in
11 2003, there was a court case in Russia that
12 revealed that a business man from Nizhny, Novgorod
13 had been offering \$750,000 for stolen weapon grade
14 plutonium for sale to a foreign client. And at
15 that time in Russia, that was about a century of
16 the average person's salary.

17 And he made contact with people who
18 lived in one of the closed nuclear cities in
19 Russia, who promised to steal plutonium for him.
20 Fortunately for the world, the people he made
21 contact with were scam artists who tried to pass
22 off a canister full of mercury on him.

23 But I have yet to meet a Russian
24 security manager who was aware of that case. And
25 it seems to me if, people are offering \$750,000 for

NEAL R. GROSS

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

1 stolen weapon grade plutonium, your security
2 managers ought to be aware of that.

3 So sorry to go off on a rant on that
4 subject, but --

5 MEMBER BLEY: I'm sorry, there was some
6 chuckles here thinking, I hope he's well -- he's
7 the right guy. Thanks, we'd appreciate that.

8 Is the Carnegie Mellon data publically
9 available or is there a contact there that --

10 MR. BUNN: Well, it's certainly the
11 case that NRC could get access to it. I don't
12 believe it's available to the public.

13 There is a book that they've published
14 based on it. A guy named Randall Trzeciak is one
15 of the key people there, but I can send relevant
16 contact info to the staff.

17 MEMBER BLEY: We would appreciate that
18 a lot. Thanks, Matt.

19 MR. BUNN: Okay. All right, so I'm now
20 on Slide 10, cyber threats.

21 So these, as you know, I'm sure you've
22 talked about those in the Panel before, they're
23 very difficult to model in part because the
24 adversary capabilities are mutating and evolving at
25 fairly frightening speed.

NEAL R. GROSS

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

1 And also the vulnerabilities that we
2 have in cyber, you know, the zero day is called
3 that because you're vulnerable when somebody
4 discovers that on that zero day. And so you don't
5 necessarily know you have that vulnerability until
6 all of a sudden it's discovered.

7 And then there's the interactions
8 between cyber threats and physical threats.

9 I gave a similar talk at a workshop
10 here in Boston, that the staff organized with the
11 Institute for Nuclear Materials Management. And
12 the key thing that the audience objected to in my
13 talk was when I asserted that of course we're all
14 thinking about the interaction between the physical
15 attacks and cyber-attacks. And various people in
16 the audience said, no, nobody is really thinking
17 about that effectively yet.

18 And people at Pacific Northwest said,
19 but we are, but we're in the early stages. So I
20 think there's a lot more work on thinking about
21 exactly how could what different levels of
22 adversary use cyber to interfere with the physical
23 security systems and contribute to their physical
24 assault. Whether it's a sabotage or a theft
25 scenario.

NEAL R. GROSS

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

1 A lot of the physical security systems
2 are becoming more and more and more digital. And
3 therefore potentially vulnerable.

4 Next slide please. So I would say we
5 should use these computer tools, but we should be
6 aware of their limitations.

7 Department of Energy and Department of
8 Defense, as you've probably been hearing this
9 morning, have used these kinds of tools for a long
10 time. To good effect.

11 I do think that overall, the use of
12 these tools has greatly contributed to improved
13 security and improved efficiency of security.
14 Although nobody will claim, in either Department of
15 Defense or Department of Energy, that efficiency of
16 security is where it needs to be, yet.

17 We're spending, especially in the
18 Department of Energy, an amazing amount of money on
19 security these days.

20 As you may or may not know, the annual
21 Department of Energy budget for security, which
22 isn't all nuclear facilities but is mostly nuclear
23 facilities, is in the range of \$1.8 billion. So
24 that's a lot of money for not a huge number of
25 facilities that the Department of Energy has.

NEAL R. GROSS

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

1 But we do need to avoid putting more
2 reliance than they deserve on these models. As I
3 said, they're no better than the assumptions.

4 I think when you're thinking about,
5 should we reduce a requirement or make an exemption
6 based on the results of a model, you need to put in
7 some expert judgment as to how important that
8 change is. As well as only relying on the results
9 of a model.

10 So it should be informed by the models,
11 but not entirely based on the models just as in
12 safety.

13 And I think as you shift towards more
14 performance based approaches, the realistic
15 testing, including a really good force-on-force
16 program, is going to be critically important, I
17 think. To make sure that the security systems
18 really do perform as well as we think they do, in
19 the face of adversaries who are intelligent in
20 trying to think of ways to beat them.

21 Next slide please. So I just wanted to
22 talk for a moment about material attractiveness. I
23 think it absolutely does make sense, as the staff
24 is proposing, to have less security for material
25 that would be much harder to make into a nuclear

NEAL R. GROSS

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

1 bomb.

2 But I think the current staff proposal,
3 in my view, goes much too far. And I know the
4 staff doesn't agree with me and we've been back and
5 forth about this on quite a number of times now.

6 The current staff proposal says, if you
7 got less than ten percent by weight Plutonium-239
8 or Uranium-235, you can drastically reduce security
9 to the point that the security plan can be based on
10 the adversaries steal the material and then local
11 law enforcement is in hot pursuit.

12 I just think that goes way too far. We
13 have very modest reason for confidence that hot
14 pursuit will always work. NRC doesn't get to
15 regulate the local law enforcement and the hot
16 pursuit because it's local law enforcement. It's
17 not the licensee.

18 I think there's been many past U.S.
19 Government studies, including NRC studies, that
20 have concluded that it's not a good idea to rely so
21 much on dilution. So this is a change from past
22 NRC policy. And it would lead to us having the
23 weakest rules in the world for security for that
24 kind of material.

25 Which I think is the wrong direction

NEAL R. GROSS

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

1 for the United States to be leading. And I've put
2 up there a link to a more detailed public comment
3 that I made on that subject.

4 So that's the end of the slides I
5 wanted to do. So I am totally open for questions.
6 And I apologize for going on so long.

7 MEMBER BLEY: No, that was wonderful.
8 Thanks, Matt, we really appreciate your time. I'd
9 ask if any of the members have any questions for
10 Matt at this time?

11 I think we're running too close to
12 lunch, Matt. We're out of questions. But we
13 really appreciate your presentation and the links
14 you've given us to new information. And we will
15 make use of that in the future, and we hope to see
16 you one of these days.

17 MR. BUNN: Okay. I hope to be there
18 one of these days.

19 MEMBER BLEY: Thank you. At this time,
20 I think we're going to go off the record and end
21 this public meeting. Oh, but I have to look for
22 comments first.

23 Can we get the regular phone line open
24 so the public can make comments? And I will ask at
25 this time, is there anybody in the room who would

NEAL R. GROSS

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

1 like to make a comment on today's session?

2 We'll wait a few minutes to get some
3 indication that the phone lines open.

4 MR. BUNN: I'm going to stay on just in
5 case somebody has a question for me.

6 MEMBER BLEY: Okay.

7 PARTICIPANT: The lines open.

8 MEMBER BLEY: I've been told the line
9 is open. Is there anybody on the public line who
10 would like to make a comment at this time? If so,
11 please identify yourself and make your comment.

12 MR. LEWIS: My name is Marvin Lewis.
13 And I don't know if it's a question, I don't know
14 if it's a comment.

15 MEMBER BLEY: Oh, okay. Well go ahead,
16 Marvin. Thank you for joining us.

17 MR. LEWIS: Okay. I'm just wondering,
18 if these defenses, if this security isn't setup for
19 an atomic bomb, nuclear bomb, that was designed
20 back in the '40's?

21 Right now, this 76-year-old name Sam
22 Kohen, K-O-H-E-N, who worked for the Clinton
23 Administration and says we have the ability now to
24 make a 25 pound bomb with very different
25 characteristics then the new bombs nowadays.

NEAL R. GROSS

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

1 And I'm not saying it's right, he's
2 right, I'm not saying he's wrong. But I
3 respectfully respect, suggest you look at 615, 7,
4 by Christopher Ruddy, R-U-D-D-Y, he's a reporter.

5 And he says, this bomb inventor is
6 speaking the truth. And he's in the Tribune
7 Review. I don't know where they are.

8 MEMBER BLEY: Okay. Well, we would --

9 MR. LEWIS: But I'd really like to
10 raise a question. Are these security measures for
11 a time in the '40's and not a time in this century?
12 Thank you.

13 MEMBER BLEY: Marvin, thank you very
14 much. I've been advised to say that the Nuclear
15 Regulatory Commission, the Advisory Committee,
16 don't have anything to do directly with weapons and
17 that's true.

18 But thanks, Marvin, for you comment.
19 We will make use.

20 Is anybody else on the line who would
21 like to make a comment? All right, at this time
22 we'll close the public phone line. And I go around
23 the table and ask the Members to make any comments
24 they'd like to.

25 And today's meeting is an information

NEAL R. GROSS

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

1 brief, essentially, but any thoughts you have are
2 welcome. Why don't we start with you, Pete?

3 MEMBER RICCARDELLA: No comment.

4 MEMBER SKILLMAN: No comments, thank
5 you.

6 MEMBER STETKAR: Nothing at all. I'm
7 interested, learning.

8 MEMBER BROWN: Fascinating briefs.
9 Thank you.

10 MEMBER CORRADINI: Okay. Well, at this
11 time I would like to thank the members of the
12 public for their comments and I'd like to thank all
13 of our speakers for a very informative day. We've
14 learned a lot.

15 I'd particularly like to thank Joe
16 Rivers and his staff for helping us put this
17 together and for organizing those IM/MM workshops,
18 which were really helpful and really opened our
19 eyes a bit to lead to this session today.

20 And I want to thank Christian Lui,
21 because she's really put this whole thing together
22 today and made it work. There's been a lot of
23 coordination to get the various groups here.

24 For the Members, we're going to break
25 now and we'll have a PMP meeting at noon. The

NEAL R. GROSS

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

1 session back this afternoon is closed.

2 And part of it will be absolutely
3 closed with no electronics here. No cell phones,
4 no computer, no watches that talk, none of that.
5 So when you come back, you may as well not bring
6 any of that back here with you.

7 At this time, we'll go off the record
8 for today and we will end this meeting. It's
9 adjourned. We'll start up with the other one at
10 1:00.

11 (Whereupon, the above-entitled matter
12 went off the record at 11:47 a.m.)
13
14
15
16
17
18
19
20
21
22
23
24
25

NEAL R. GROSS

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

1

2

Overview of the Physical Security Regulatory Framework, Vulnerability Assessment Approach and Safety/Security Interface

Joe Rivers

Office of Nuclear Security and Incident Response

April 6, 2016

Outline

- Physical Security Regulatory Framework
- Safety/Security Interface
- Risk-Informing Security
- Vulnerability Analysis

NRC's Power Reactor Security Program

- **Purpose:** To provide HIGH assurance of adequate protection to prevent significant core damage and spent fuel sabotage.
- **Objective:** To ensure security programs are established such that licensees can protect against adversaries up to and including attributes described by the Design Basis Threat (DBT) in order to prevent radiological sabotage.
- **Process:** Develop NRC licensing and inspection programs, as well as, industry initiatives that implement and verify the level of protection described.

Licensing

- For Operating Nuclear Power Reactors;
 - 10 CFR 50 and 73 Security Regulations apply
 - Formalized process to make changes
- For New Reactors:
 - 10 CFR 52 and 73 Security Regulations apply
 - Final Safety Analysis Report (FSAR) must describe the engineered physical security programs
 - Implement security requirements before fuel is allowed inside the protected area
- The NRC utilizes NUREG-0800, “Standard Review Plan,” and various Regulatory Guides to conduct security plan reviews and approvals

Security Plans

- **Regulatory Basis:**
 - Provide physical protection against the design basis threat (DBT) of radiological sabotage
 - Establish and maintain a physical protection system and security organization
 - Establish and maintain, at all times, properly trained, qualified and equipped personnel required to interdict and neutralize threats
- General requirements for the content of each security plan are found in 10 CFR 73.55(c) and 10 CFR 73.54
- **Required Security Plans:**
 - Safeguards Contingency Plan
 - Training and Qualification Plan
 - Physical Security Plan
 - Cyber Security Plan

Inspection Program



- Process: The commercial nuclear power reactor inspection activities for physical protection programs include:
 - Baseline Inspections, including Force-on-Force Inspections
 - Special Inspections



Safety/Security Interface

- Requirement codified in Title 10 CFR 73.58
“Safety/security interface requirements for nuclear power reactors”
- Applies to operating nuclear power reactors
- Requires a pre-assessment and management of all planned and emergent activities involving changes to plant configurations, facility conditions, and/or security programs
- Communicate potential conflicts to appropriate personnel and take necessary actions to maintain safety and security in accordance with NRC requirements and license conditions

Safety/Security Interface

- Security uses the cut sets from the PRAs to inform the target sets used in vulnerability assessments
- Security vulnerabilities and associated consequences are needed by safety organizations to inform safety programs
- Need to understand the relationship between safety and security risk

Safety/Security Interface

- Need to evaluate impacts on each discipline as changes in plant configuration/operations are planned
- Need to understand how information from each discipline better informs the other discipline

- Numerous workshops over the past six years
 - Sandia Workshop – 2010
 - INMM Stone Mountain Workshop - 2014
 - INMM Reducing Risk Workshop - March 2015
 - INMM/ANS Sun Valley Workshop - April 2015
 - INMM Boston Workshop - September 2015

Risk-Informing Security Activities for NPPs

- Use of modelling and simulation tools
- Safety/Security risk
- Cyber Security
- IAEA Coordinated Research Project on Nuclear Security Assessment Models

Industry Initiatives

- Submission of security plan changes supported by modelling and simulation
- Consequence-based approach for SMR security regulations

Vulnerability Analysis (VA)

- A systematic, performance-based process that is used to evaluate the ability of a physical security system to meet performance requirements

VA Tools

- Types of Simulations
 - Tabletop analysis
 - Computer simulations
 - Limited scope performance tests (LSPT)
 - Force-on-force exercises

Tabletop Exercise

A method to simulate an adversary attack on a site's existing or proposed physical protection system (PPS), similar to a board game

- Analyzes PPS elements:
 - Detection, delay, response
- Provides insight into a PPS that can stand alone or be used in other analysis tools

Computer Simulations

- Pathway analysis
- Scenario Analysis
- Combat simulation

Limited Scope Performance Tests

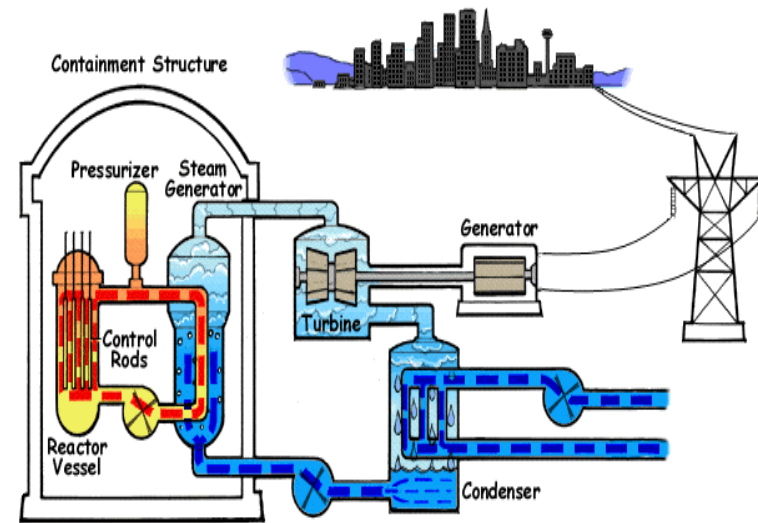
- A manual exercise to assess the effectiveness of a portion of the overall physical protection system
- Results can support other VA tools

Force-on-Force

- Full-scale security exercise, using mock adversary forces

Target Sets

- Important element of computer simulations and force-on-force exercises
- Minimum combination of equipment, which if prevented from performing their intended safety function would likely result in significant core damage (e.g., non-incipient, non-localized fuel melting, and/or core destruction) or a loss of coolant and exposure of spent fuel



Questions?

Consequence Based Security for Small and Advanced Reactors

Generic policy issues and industry's proposed approach

April 6, 2016

Meeting of the
**Advisory Committee on Reactor Safeguards,
Subcommittee on Reliability and PRA**



NUCLEAR ENERGY INSTITUTE

nuclear. clean air energy.

Areas of Discussion

- Need for consequence-based security
- Industry proposed approach
- Path forward

Small and advanced reactors differ from current designs

- Simplified designs (e.g., no large piping)
- Reduction in potential accident sequences
- Slower accident progression/longer coping times
- Significantly reduced risk of radiological release and offsite consequences
- Opportunity to incorporate security early in design

NRC requirements need to be right-sized for small and advanced reactors

- Protection of public health and safety equivalent to existing reactors
- Portions of current requirements unnecessarily burdensome for SMRs and ARs
- Should be technology-neutral and consequence-oriented
- Incentivize designs to reduce reliance on human actions

Industry Proposed Approach

Security Element	Existing Framework	Options for Small and Advanced Reactors
Protection by design-alone	Not contemplated	Performance-based
Engineered features	Prescriptive physical barriers	Enhanced safety and security features
Security Organization	Prescriptive (e.g., detect, assess, interdict and neutralize)	Graded based on ability of design alone to protect against radiological sabotage
Design Basis Threat	Independent of design	

Major Policy Issues to be Addressed

Topical Area	NRC Policy Decision Needed
Security Organization Response	Detect, assess and communicate is appropriate if design basis threat cannot cause unreasonable risk to public.
Performance standard for “unreasonable risk to public”	Should be based on potential for off-site consequences
Use of Probabilistic Risk Assessment	Expand role of PRA (e.g., risk informed assessment of off-site dose consequences)
Others (e.g., firearms, use of deadly force, FOF exercises)	To be addressed depending on resolution of other policy issues

Need to start developing framework now

- Security enhancements need to be incorporated early in the design process
- Potential owner/operator business decisions need to be made well in advance of submitting applications
- Can be developed without design details
- Clarity on regulatory basis will support near term exemptions and longer term rulemaking
- Concepts for consequence-based security parallel basis for planned rulemaking for emergency preparedness
- Consistent with NRC Advanced Reactor Policy Statement

Conclusions and Path Forward

- Existing requirements are not appropriate for small and advanced reactors
- A consequence-based approach is needed, and development should begin now
- NEI paper is starting point for discussion
- Proposed next steps
 - Meet with NRC to discuss steps to develop details
 - Commission decision to move forward in 2016
 - Regulatory basis in 2017
 - Near-term exemptions and future rulemaking, if necessary



The Role of Modeling and Simulation in Risk Informed Security Decision Making



ARES
CORPORATION

TRANSFORMING CHALLENGE INTO SUCCESS

 www.arescorporation.com

**Advisory Committee on Reactor Safeguards
Reliability and PRA Subcommittee**

April 2016

Steve Fogarty, VP Special Projects



Benefits of Modeling and Simulation for Security

- The primary benefit is a clearer understanding of the security programs' strengths & weaknesses.
 - Measures of system performance such as System Effectiveness (Pe), Defense-in-Depth, and identification of Critical System Elements (CSEs)
 - Conveying “visual information” to leaders on all aspects of the site security posture (i.e., successful risk communication)
 - Ability to capture emergent behaviors such as previously unidentified vulnerabilities as well as emerging threats (e.g., UAS)
- Secondary benefits:
 - Compatibility with existing PSA processes particularly in the area of risk-informed decision making (i.e., enables a strong safety-security interface).
 - Can be applied prior to implementing a design change at an existing facility as well as in new facility design (e.g., SMRs)
 - Model construction and population is done in a “natural” way for the security professional
 - Virtual environment provides safety benefits over live exercises
 - 3D models for virtual tabletop exercises and walkthroughs





Successful PSMS Implementation

*“When operated within their design specifications, Physical Security Modeling and Simulation (PSMS) tools have progressed to a point that they can be counted on to produce a high-quality measurement of the facility’s security posture and risk profile.”**

Successful tool implementation requires a focus on:

- 1. Transforming the current data and facility knowledge into the input needed for PSMS analysis.**
 - Addressed in recent papers and in presentations on *Facility Characterization, PSMS Applications, Model Robustness, VV&A, Risk Drivers*
- 2. Providing a context for how the PSMS analysis results will fit into existing decision processes, regulatory requirements, and security design requirements of the organization.**
 - Addressed in a recent paper and a RIC 2016 presentation regarding current industry challenges with balancing analysis scope and expected quality

*Fogarty, S. P., “The Role of Modeling and Simulation in Risk-Informed Decision Making”, Proceedings of the 56th Annual Meeting of the Institute of Nuclear Materials Management, July 2015.





Creating the Input for PSMS

PSMS Requires Completion of the Following Three Tasks:

1. Characterize the Facility Into a Security Virtual Environment

Virtual Environment

- Infrastructure
- SSCs
- Elevation / Terrain

Detection Systems

- Cameras
- BMS
- Vibration Sensor

Delay Systems

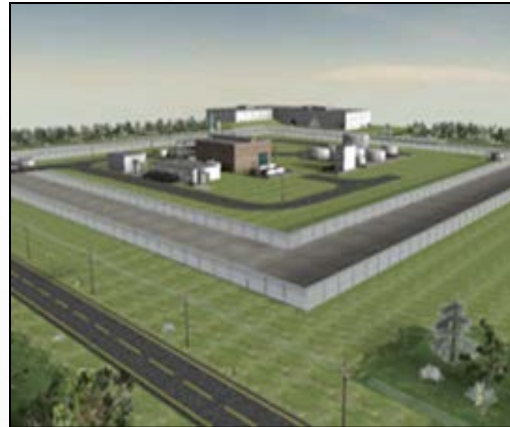
- Perimeter Fencing
- Vehicle Barriers
- Doors

Response Force

- Posting/Patrol
- Response Locations
- Vehicles and Tools



Security Virtual Environment



2. Develop the Performance Data Library for the Physical Protection System

Performance Data Library

- Detection Probabilities
- Defeat Times for Barriers
- Speeds Over Barriers and Terrain
- Weapon Hit/Kill Probability

3. Characterize the Threat into a Set of Threat Scenarios

Threat Characterization

- Threat Structure (i.e., teams)
- Threat Size
- Starting Locations
- Target Type (e.g., sabotage, theft)
- Target Sets





Terminology Comparison: The Safety-Security Interface

PSMS	PSA	Comments
Security Virtual Environment (SVE)	N/A	PSA has attempted some automation of P&IDs to system FTs, but with limited utility.
Adversary/Agent Traversal Graph	Fault Tree/Event Tree Logic	The adversary graph can be determined automatically from the SVE while the FT/ET logic is developed by a risk analyst.
Performance Data Library	Failure Rate Database	PSMS can directly adapt PSA analysis techniques for using historical data (generic and site-specific) to estimate performance.
Target Sets	Minimal Cutsets	Minimal cutsets along with spatial information are used to generate target sets.
Threat Scenarios	Initiating Events (IEs)	The most significant difference between PSA and PSMS approaches are in the treatment of the random IEs vs. the intentional acts of an adversary.
Risk $R_k = f_k \sum_{j=1}^{m_k} l_j * c_j$	Same as PSMS	Definition of risk is the same for a given threat scenario/initiator, but with PSMS conditional likelihood l_j , coming from simulation, and with f_k and c_j , commonly set to unity.



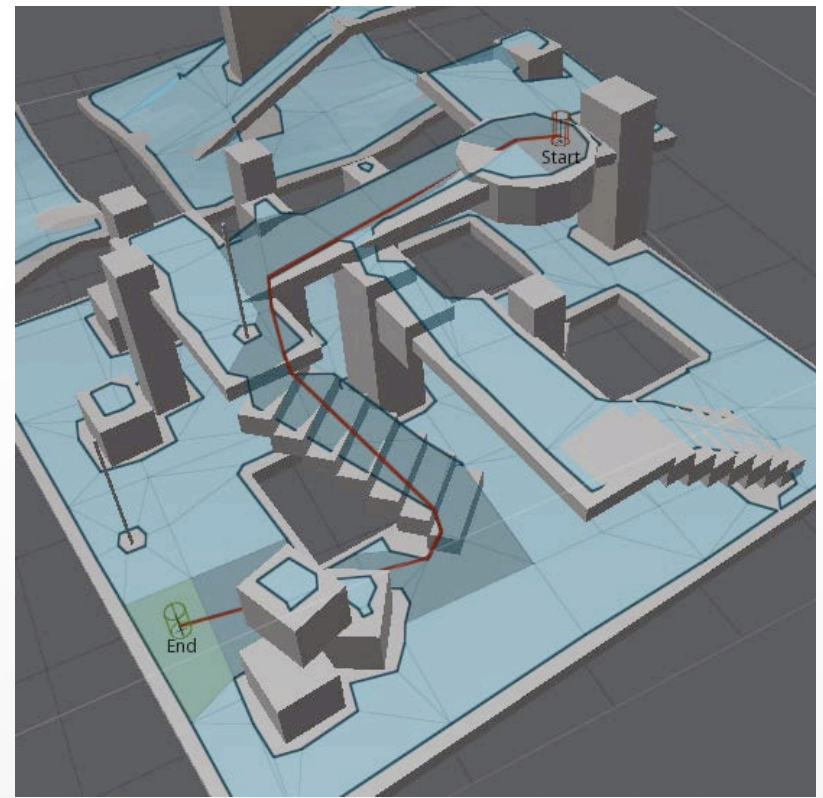


The Adaptive Adversary

Goal: Identify and prioritize the possible steps (i.e., paths) a given threat could use to defeat the security system and determine the corresponding likelihood of adversary success

General Steps:

1. Break Security Virtual Environment into a data structure (e.g., navigational mesh, ASD) that a behavior model can use for adversary pathfinding
 - Possible pathways represented by mathematical graphs (nodes and edges) analogous to event trees (events and split fractions) in PSAs.
2. Solve graph to find the adversary pathways of greatest vulnerability to the facility
 - These vulnerabilities become the adversaries' "attack plans."
3. Virtually attack (i.e., simulate) the facility using this attack plan, but allow adversary to **adapt** to conditions on the ground that could not have been known during planning
4. Divide the number of successful attacks by the total attacks simulated to give the likelihood of adversary success



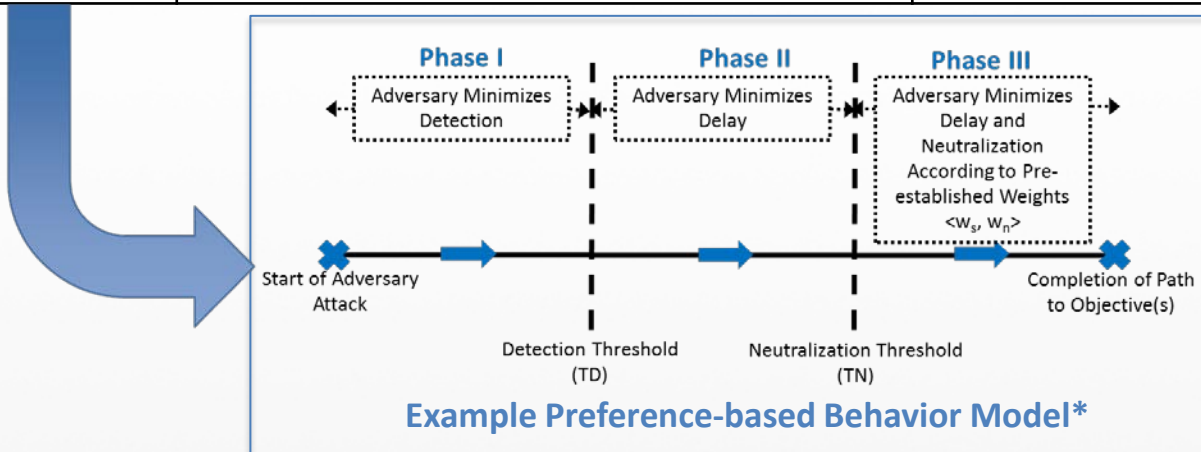
Example Navigational Mesh and Pathway





Behavior Model Determines Whether Adaptations Are Believable

Model	Description	Application
Task-based Models	Adversaries must accomplish pre-determined mission tasks, as defined by Subject Matter Experts (SMEs), but are free to determine how these tasks are accomplished and to locally adapt routes between these tasks.	Used throughout DOE's existing nuclear facilities where vulnerabilities are well understood and required adversary tasks are well defined. Only PSMS approach addressed in NUREG/CR 7145.
Preference-based Models	Adversaries are free to search globally for the "best" routes and tasks (i.e., paths) based upon their defined preferences (e.g., detection, delay, neutralization), but modeling requires more data and searches can be computationally expensive.	Can be used for searching for "new" vulnerabilities and "unanticipated" adaptations. Especially useful for less "hardened" facilities and during initial facility design.



*Fogarty, S. P., "An Improved Model for Adversary Decision-making through Modeling and Simulation", Proceedings of the 57th Annual Meeting of the Institute of Nuclear Materials Management, forthcoming.





Sources of Modeling Uncertainty

PSMS analysis provides a means to address these key uncertainty contributors that are present in the security systems of today.

Source	Description
Decision-making on officer deployment	Details of how officers are deployed can be left to shift tactical commanders (STCs) and these commanders can make different decisions all within a given response plan.
Failure of security system components to function as designed	Random failure of any system components (including officers). The failure modes for equipment components are generally knowable. This is not failure due to the adversary defeating the components (that failure is integral to the simulation), but rather an unrepaired/latent failure prior to attack. Common use of compensatory measures exacerbates this issue.
Operating Modes and Target Sets	This is the uncertainty in the modeling of the defined operating modes (e.g., full power, refueling) of the facility. Some operating modes may occur only infrequently, but may represent increased vulnerability due to target set exposure or security design configuration.
Environmental Conditions	This is uncertainty in the modeling of environmental conditions. Only choosing to model daytime operations in the summer are examples of this insufficient modeling uncertainty.





Example: Failures in the Security System

July 2012 incident at DOE's Y-12 facility: Three protestors were able to breach the perimeter of the high security facility and deface the building prior to being interdicted by the protective force.

- Equipment side: A critical assessment camera had been inoperable for an extended period of time.
 - In addition a historically high nuisance alarm rate (caused by animals, winds, etc.) contributed to desensitizing the central alarm systems operators.
- Human performance side:
 - Slow response by the primary assessment patrol
 - Failure of the alarm station operator to declare a high priority (immediate) response based on the activation of three separate alarm sensors

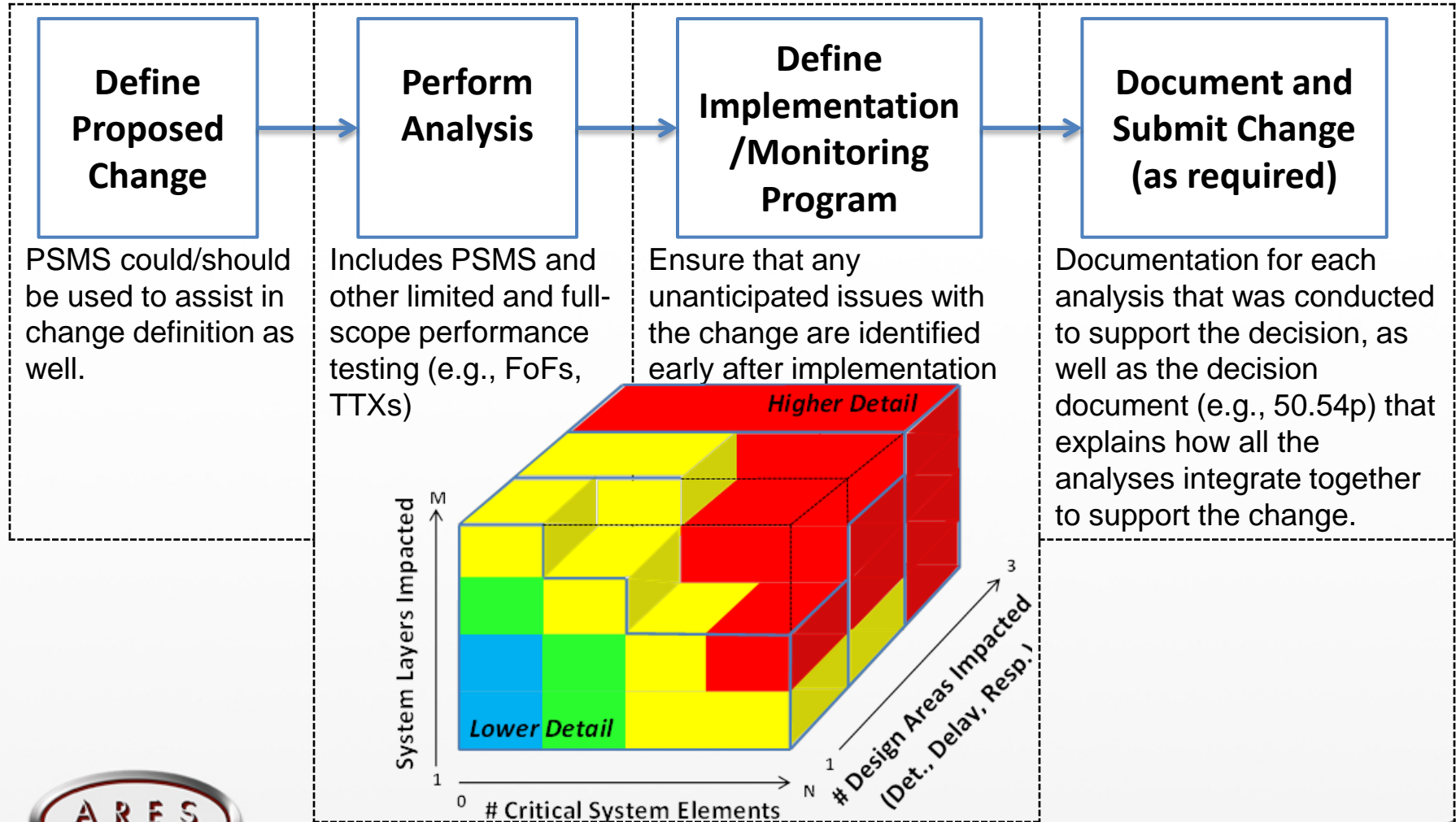
Reinforces the benefit of PSMS for addressing this risk contributor





Risk Informing Security Decisions with PSMS

Given the similarities between PSA and PSMS analyses it is natural to look at the current risk informed decision process (RG 1.174) as a template for risk-informing security.





Nuclear Experience with PSMS

DoD

- Approach is generally centralized – hub-and-spoke model (e.g., DTRA as “hub”)
- Individual military bases and security force units typically don’t have in-house expertise or local access to PSMS software tools
- Services generally use PSMS intermittently compared to DOE
- Selected efforts at using PSMS internationally with NATO
- Have conducted PSMS tool Verification, Validation, and Accreditation

DOE/NNSA

- In-house “organic” risk assessment teams with expertise in PSMS fundamentals and the use of tools
- DOE/NNSA was an early adopter of PSMS and leads the community in the use of PSMS tools
- DOE sites typically employ more than a single PSMS tool
 - Allows sites to compare the results between software tools as well as performance tests
 - Effective but expensive approach (at least initially)
- Existing policies can make it difficult to adopt new approaches





Going Forward

- Limited guidance on implementation process and quality expectations for modern PSMS, resulting in uncertainty on how to address:
 - Modeling uncertainties (e.g., operating modes, system failure)
 - Sensitivity analysis (e.g., Critical System Elements, Defense-in-Depth)
 - Referenceable performance data
 - Peer review
- No common library of security performance data
- Limited quantitative analysis skills resident in the licensees' security organizations
 - PRA analysts might be trained for these efforts including providing the associated technical basis documentation
- Applications to date are tool-centric rather than deliverable/decision-centric
- Natural tendency to compare safety risks (i.e., PSA) to those from security (i.e., PSMS)
 - Some normalization of assumptions is needed
 - Cannot continue to set consequences and attack frequency to unity





HARVARD Kennedy School

BELFER CENTER

FOR SCIENCE AND INTERNATIONAL AFFAIRS

Complexities of Vulnerability Assessment

Matthew Bunn

Professor of Practice, Harvard Kennedy School

Advisory Committee on Reactor Safeguards, NRC

6 April 2016

belfercenter.org/managingtheatom

Computer tools for vulnerability assessment are extremely helpful

- ❑ Computer tools, if properly developed and used, allow:
 - Higher fidelity in simulation
 - Greater ease in considering different security options (can identify cheaper, more efficient solutions)
 - Greater ease for regulators seeking to confirm effectiveness of proposed exemption approaches
 - Greater ease in exploring new adversary pathway scenarios (can lead to more complete coverage of potential vulnerabilities)
 - Greater ease in considering impact of changes in adversary capabilities, tactics (can make it possible to assess impact of potential changes to the DBT, design systems to offer some protection against threats beyond the DBT)

But it is crucial to understand the limits of these tools



- ❑ “All models are wrong. Some are useful.” Some can also be dangerous – they can create false impressions that all key factors are included
- ❑ Vulnerability assessment models are useful for identifying factors to be addressed, approaches to address them
 - NOT likely to provide reliable absolute estimates of risk, because of large uncertainties and complexities
- ❑ Key complexities and uncertainties include:
 - Complexity of overall security system
 - Limited by assessor’s ability to think of complete set of defeat strategies adversaries could use effectively
 - Human and organizational factors usually poorly modeled
 - Insider threats more difficult to model
 - Cyber threats (and integrated cyber-physical threats) more difficult to model

Key assumptions built into vulnerability assessment tools

- ❑ Technological elements will perform as estimated
- ❑ Humans and organizations will perform as estimated
- ❑ Adversary capabilities and tactics will be within the DBT
- ❑ Adversaries will not use defeat strategies the defense has not thought of
- ❑ Any of these assumptions could turn out to be wrong
 - Technology may be improperly installed, operated, maintained
 - Humans may become complacent, organizations may put priorities elsewhere
 - Adversaries may be beyond the DBT
 - Adversaries may defeat the system with unimagined strategies


1: Difficult to model complex systems

- ❑ Security systems include many elements
 - Technical elements (e.g., barriers, cameras, alarms)
 - Human and organizational elements
 - Interactions among elements are complex and poorly understood
 - e.g., under what circumstances will employees report concerning behavior? What factors lead to complacent behaviors that undermine system performance?
- ❑ Y-12 example:
 - Installation of ARGUS system intended to improve security – but led to many unexpected false alarms
 - Cameras to check alarms had been broken for months
 - Guards had gotten sick of checking out false alarms
 - Result: protestors penetrated to HEU building, spent substantial period there, before being accosted by a single guard
 - Vulnerability assessment tools would not have shown problems

2: Difficult to imagine adversary tactics

- ❑ Tools are only as good as the people who use them
- ❑ Need creative, “hacker” mentality to envision approaches adversaries may use to defeat security systems
 - Real systems have many potential vulnerabilities – most of which will never be discovered, either by defenders or by adversaries
 - Partial solution: operators should establish “red teams” assigned to find vulnerabilities – and rewarded for doing so

3: Difficult to model human, organizational behavior over time



- ❑ Tools typically include simple assumptions on human performance based on past data
 - E.g., probability of detection for a guard in a guard tower
- ❑ Changes in security culture, organizational priorities change performance in hard-to-predict ways
 - How well will guards assess, respond to alarms?
 - How likely is it that staff will report behaviors that might reveal an insider threat?
 - What fraction of security rules will be followed, and implemented correctly?
 - What corners will be cut as production or budget pressures increase?
 - How will staff training, experience, security awareness change over time?

Security culture matters: Propped-open security door

8



Source: GAO, Nuclear Nonproliferation: Security of Russia's Nuclear Material Improving, Enhancements Needed (GAO, 2001)

4: Insider threats are difficult to model

- ❑ Computer tools typically do better modeling protection against outsiders
 - Traditional methods based on detection probability, task time, response force arrival time work better for outsider scenarios
- ❑ Insiders start off past many layers of defense – and may pursue hard-to-predict strategies
 - Insiders may be deeply familiar with the security system and its weaknesses – may have months or years to think, plan, experiment
 - Insiders have many opportunities for “social engineering” – convincing other staff to do seemingly harmless things that facilitate the plot
 - Insiders may recruit or coerce other insiders (few DBTs include multiple insiders, but in major non-nuclear thefts, multiple insiders are common)

5: Cyber threats are difficult to model



- ❑ Cyber threat environment evolving at frightening speed
- ❑ Cyber vulnerabilities are often unknown until exploited by an adversary
- ❑ Interactions between cyber threats and physical threats are complex and difficult to model
 - Systematic assessment of cyber-physical threat interactions is in its infancy, requires further development

Use computer tools – while being aware of their limitations

- ❑ DOE and DOD have used computer vulnerability assessment tools for many years to good effect
 - Have helped strengthen effectiveness and efficiency
- ❑ But need to avoid undue reliance
 - Results are no better than the assumptions that went into the model – some of which may be wrong
 - NRC should use expert judgment to decide whether to grant an exemption based on a computer analysis
 - As NRC shifts toward more performance-based approaches, realistic testing of security performance – including an effective force-on-force exercise program – will be critically important

Similarly, be careful in relying too much on material attractiveness

- ❑ Absolutely makes sense to adjust security requirements for material that would be very difficult to use for a nuclear bomb
- ❑ But current NRC staff proposal goes much too far
 - If material was less than 10% by weight Pu-239 or U-235, licensees could have a security plan based on adversaries stealing the material and local law enforcement recovering it
 - This degree of reliance on material dilution is contrary to decades of U.S. studies (including by NRC) that concluded recovery of pure material was straightforward enough that moderate dilution alone did not justify major security reductions
 - Would likely result in the United States having the weakest rules in the world for security for MOX fuel – wrong direction to lead
 - Public comment available:
<http://pbadupws.nrc.gov/docs/ML1429/ML14293A636.pdf>