

OPENING REMARKS BY ROY ZIMMERMAN
DIRECTOR, OFFICE OF NUCLEAR SECURITY AND INCIDENT RESPONSE

Roy Zimmerman, Director, NSIR.

Good morning. I'd hear you a lot better if you were closer, but I think I've made that point already.

I want to welcome you to today's public meeting on nuclear security issues. I extend my welcome to all of you here in the auditorium, as well as individuals that have joined us by phone, and appreciate them dialing in at this early hour.

Commissioner Jaczko will be joining us momentarily, and we extend a special welcome to the Commissioner to share his thoughts with us as we begin our meeting today.

I'm Roy Zimmerman; I'm the Director of the Office of Nuclear Security and Incident Response here in the NRC. In recent years, since 9-11, we have conducted this type of meeting, basically twice a year, in a public setting such as this.

We have used the Regulatory Information Conference, as one venue that allows us to be able to share the initiatives that we have underway, and a status of a variety of security-related activities.

The March time frame was the last reg info conference and then this time of year we hold a session, similar to what we are doing today. The benefit of this type of meeting is we are not pressed for time the way we are during the Reg Info Conference.

There is much more opportunity for discussion and that is what we look forward to doing today. One of the things that I did, prior to this meeting, is I read through the meeting minutes from the last couple of meetings that we held.

And I was pleased to see that in last year minutes that it recalled the fact that many of the members of the public were pleased with the amount of information that we were able to share, recognizing the sensitivity of the topic, and trying to work our way so that we are not discussing safeguards information but, yet, share information with the public about our initiatives and, again, respond to questions and concerns. And that, again, is our intent today.

For me success for this meeting is that we are able to share quite a bit of information with you today and, then, to be able to engage in dialogue, be able to address your questions and also your areas of concern.

What I would like to do now is go around and introduce ourselves, starting with...I asked Ralph Way to begin, we will go around the table, and then around the room, then to the individuals that are on by phone. Thank you.

INTRODUCTIONS:

Ralph Way, Deputy Director for Security Programs, Division of Security Operations.

Rich Correia, Deputy Director for Security Oversight, Division of Security Operations.

Roy Zimmerman (Director (NSIR). Let me just stop for a second and remind you that there is an organization chart that is in your package. So for a number of the individuals that will be speaking today, and around the table, you will be able to identify them and their responsibilities in the organization chart. Thanks.

John Tomlinson, I'm an advisor within the Office of Nuclear Security and Incident Response.

Eric Leeds, Director of the Division of Emergency Preparedness and Incident Response.

Bill Dean, Deputy Office Director for the Office of Nuclear Security and Incident Response.

Glenn Tracy, Director of the Division of Security Policy.

Dan Dorman, Director of the Division of Security Operations.

Rick Rasmussen, Chief of the Security Rulemaking Branch within the Division of Security Policy.

Mark Shaffer, Deputy Director for Material Security in the Division of Security Policy.

Pedro Salas with Areva.

Lance Rakovan , Facilitator. Let's use the cordless; we can pass this around so that people can introduce themselves.

Patricia Holahan, Deputy Director of the Division of Industrial and Medical Nuclear Safety.

Jim York with Bechtel SAIC Company.

Eric Osterley, Division of New Reactor Licensing.

Vince Williams, Reactor Security Branch.

Phil Brochman, Senior Program Manager, Rulemaking Branch.

Terry Reis, Office of Commissioner Jaczko.

John Vandenberg, a Team Lead in the Security Performance Evaluation Branch.

Rocky Foster, Material Transportation Waste Security Branch.

Oleg Bukharin, Fuel Cycle Security Branch.

Jamie Heisserer, Security Performance Evaluation Branch.

Brooks Ameo, DLA.

Andy Rayland, a Team Leader with the Security Performance Evaluation Branch.

Doug Huyck, Team Leader, New Reactor Security Team, Reactor Security Branch of NSIR.

Bonnie Schnetzler, Security Rulemaking Branch.

Rhett Pyree, Security Rulemaking Branch.

Bob Kendling, Director of Quality Assurance, Wackenhut Nuclear Services.

Jack Goldberg, Office of the General Counsel.

Ralph Costello, Team Lead, Reactor Security Oversight Branch.

Jane Marshall, NRC.

Bill Jones, NRC.

Brenda Reed, Constellation Energy.

Joe Willis, Reactor Security Oversight Branch.

Dave Furst, Reactor Security Oversight Branch.

Paul Peduzzi, Team Lead in the Reactor Security Oversight Branch.

Mike Burrell, Office of Enforcement.

Brad Baxter, Access Authorization Program Manager, Licensing Personnel Security Branch.

Holly Harrington, NRC Office of Public Affairs.

Bob Dexter, Fuel Cycle Safeguards and Security Branch.

Larry Harris, Security Rulemaking Branch.

Drew Pretzello, Security Rulemaking Branch.

Susan Bagley, Materials Transportation and Waste Security Branch.

Jim Beardsley, Team Leader Security Performance Evaluation Branch.

Nader Mamish, Deputy Director for Emergency Preparedness.

Jim Riccio with Greenpeace.

Diane Curran, I'm here representing the San Luis Obispo Mothers for Peace.

Dave Lochbaum, Union of Concerned Scientists.

Paul Gunther, Nuclear Information and Resource Service.

Jeff Cruz, Chief, Materials Oversight Branch.

Alan Frazier, Team Lead, in the Reactor Security Branch.

Joe Rivers, Senior Level Advisor, Division of Security Policy.

Alan Madison, Chief of the Security Policy Liaison Branch.

Bob Caldwell, Chief of the Fuel Cycle Safeguards and Security Branch.

Lance Rakovan, I'm in the Office of the Executive Director of Operations here at the NRC, and I will be facilitating today's meeting.

Eric Scarpac, Licensee Personnel Security Branch.

Al Bione, I work with Paralex (phonetic) I'm here supporting DOE and the MP-20.

Dennis Gordon, Security Rulemaking Branch.

Eric Thornsby, Advisory Committee on Reactors Safeguards Staff.

May Ma, NSIR, Financial Management Team.

Sheldon Stuchell, Technical Assistant, Division of Security Operations.

Peter Lee, Reactor Security Branch.

Lynn Silvius, Chief of Information Security Branch.

Roberta Warren, Chief of the Intelligence Liaison and Threat Assessment Branch.

Donna Marie-Perez, NRC Office of Research.

Elliot Pagan, New York State Office of Homeland Security.

Steve Pope, I'm with ISL.

Doug Walters, NEI.

Tony Cualantone, NEI.

Richard Turtill, NSIR.

Susan Abrahams, NSIR.

Kelly Riner, Division of Material Security.

INTRODUCTION OF COMMISSIONER JACZKO

By Roy Zimmerman, Director, NSIR

Roy Zimmerman, Director, NSIR.

Thank you all very much. It may appear as though we have the entire NSIR organization in the auditorium. But, trust me; we do have some folks that are still upstairs working on other things.

The large turnout is because this is an important meeting to us, as it is to you. And, again, we look forward to the opportunity to discuss a variety of issues over the next few hours.

But now, it is my pleasure to introduce Commissioner Jaczko. Dr. Jaczko was sworn in as an NRC commissioner on January 21st, 2005.

Immediately prior to joining the Commission he served as appropriations director for Senator Harry Reid. He also served as the Senator's Science Policy advisor.

Dr. Jaczko also worked in the office of Representative Edward Markey and later advised members of the Senate Committee on Environment and Public Works on Nuclear Security Policy and other scientific matters.

The Commissioner earned his undergraduate degree from Cornell University, and his PHD in particle physics from the University of Wisconsin, Madison.

Commissioner Jaczko is a strong advocate of public participation in the regulatory process and an equally strong proponent of maximizing transparency in how the NRC conducts its business, making him a very appropriate opening speaker.

Please join me in welcoming Commissioner Jaczko.

REMARKS BY COMMISSIONER JACZKO:

I appreciate that introduction. I don't intend to speak very long because this is a meeting for you all. I probably will take a few minutes to just sit in and listen in on some of the discussions you have.

I certainly would encourage all those people who are not NRC, I think Roy did this already, but I will give it my best shot. People who aren't with the Commission, you are more than welcome to sit at the table. I think the idea here is to get some discussion among the staff and members of the public, so I encourage you to take a seat. I know I used to feel like I'm teaching a class, because people are always reluctant to want to come and sit in the front row. And it is probably the equivalent of the front row. So, like I said, don't be shy, and feel free to come sit at the table. I will give you a few moments to think about that. If there are any takers.

Well, let me just say, I think as Roy said, I think it is really important that, as an agency, we really do everything we can to reach out to the public. And I think the public is often a very nebulous concept.

In general, the way I like to think of it is really all those people who aren't employees of the NRC. That includes a large number of people, most of the nation, in fact. And from the specific perspective of the NRC there are a lot of specific groups, I think, that often have an important contribution to make to the work that we do. That involves members of Congress, it involves the licensees, it involves other public interest groups, and a wide variety of different people. So these meetings, I think, are extremely important. One of the biggest dangers, I think, that we can face at the Commission is when we try and make decisions within a very narrow framework.

I think it is important that we do everything we can to reach out to get diverse views. Even views often that may be clearly in alignment with what we are doing, or clearly in opposition. I think it is important for us to hear where those end points are. And also to hear everything that is in the middle. I think we make better decisions, as an agency, when we have a diverse spectrum of views.

So I think today's meeting is a very important meeting, because it is a good chance for the staff to reach out and to hear from people in a way that really puts the focus on what people have to say rather than necessarily what the Staff is thinking, and where the staff is coming from.

Now, having said that, I think it is doubly important, given the topic of today's meeting. We are only three days from the fifth anniversary of September 11th. I think this agency, in many ways, prior to September 11th, was more prepared than any other Federal agency to deal with terrorist kinds of threats at commercial facilities of any kind, whether those be energy generation, or other kinds of financial institutions.

I think that security still plays a fundamental role in the day to day work of the NRC. We have, right now, three very important rulemakings that are ongoing. Rulemakings that really require the public to give us input in the direction we are going, and the thinking that we are doing.

I'm sure many of you are aware of what those are. We have a rulemaking that is, has currently gone out for public comment, on the design basis threat.

We have a rulemaking that is prepared to go out for public comment. It is the rulemaking dealing with 73.55, some of the major security sections in our regulations.

We then have a rulemaking that is really a new concept. And that, in my view, is probably the most important rulemaking that we will have going this Fall. *And that is to deal with how we are going to bring new reactors into the fold for security issues.

And so that third rulemaking, which is projected to come to the Commission sometime this Fall, and then be out for public comment fairly shortly thereafter, really will address the issue of security assessments for new reactors.

The motivation, I think, for that rulemaking is really to take a look at all the things that we know and we've learned from today's environment, and today's reactors, and the experience we have with those, and take lessons from that, so we can design in good security from the beginning.

We talk about the new generation of reactors relying on passive safety features. Well, I would like to see a new generation of reactors that is more secure than today's reactors, relying as much as we can on passive safety features, on good design that eliminates the need for all the operational security programs as much as possible.

I think this new rulemaking is designed to get us there. So there is really a tremendous amount of work that the agency has, before it, on security. And a tremendous amount of work that is going to involve our very public processes of rulemakings and other areas.

So meetings like these are very important, I think, for the staff to get a sense of what kind of views are out there as they begin to tailor those activities and present them to the Commission for a Commission decision.

So, as I said, this is your meeting, so I won't spend any more time on my thoughts. And, again I just encourage you to be active participants, and to make this a valuable exchange for the staff, and for yourselves as well.

Again, I want to thank Roy. I think Roy has really been pushing very hard for these kinds of meetings and has been working to set them up, and to conduct them, and I think that they are valuable.

So, again, I hope you find the meetings as valuable, and I look forward to hearing how the meeting went. Thank you.

Roy Zimmerman, Director, NSIR.

Thank you, Commissioner. Okay, maybe the coffee hasn't kicked in yet, but the chairs are staring at you. I don't feel as bad now, that if the Commissioner didn't entice you to get up there, any more than I did, we will see, maybe our facilitator, Lance Rakovan can accomplish that for us.

We have had good success in the past with the process that has worked through the meeting for us, and maintained what we call the parking lot for items, questions that we may not feel comfortable that we have a full answer at the table, we will take them away, we will respond on the website. And, again, I don't want to steal Lance's thunder. But let me turn it over to Lance to go over the format for this meeting. Thank you.

RULES OF ENGAGEMENT

Lance Rakovan, Facilitator

Thanks, Roy. For those of you who weren't here, or weren't paying attention as we were going around in introductions, I'm Lance Rakovan. I work in our Office of the Executive Director of Operations here at the NRC, and I will be facilitating today's meeting.

I just wanted to go through a little bit of how the meeting is going to be laid out, and go through a few ground rules before we get started.

If you take a look at the agenda, essentially we have three presentations today, with question and answer periods following. If you would like to make a comment, or ask a question, once the presentation is over, just raise your hand or signal me in one form or another.

If you are not sitting at the table where there are conveniently placed microphones, I will bring over the mike, here. It does make it a lot easier to hear you, if you are using a microphone. So I ask that we try to keep one person talking at a time, that way people don't talk over each other and that way I have a chance for everyone who needs it, to use the cordless mike.

If you could, try to keep your comments concise, down to a couple of minutes. We have a lot of people here, and I assume that the presentation, after the presentations there might be a lot of questions, or comments that need to be made.

It would be nice if we could give everybody a chance to make the comments and still try to keep somewhat to schedule. We are going to try to be somewhat flexible on that, given that we are not sure how much feedback we are going to get.

If you ask a question I'm going to turn to the people seated at the table, or the other NRC people seated at the audience, to see who the best person is to answer the question. If it is on topic we will do our best to answer it. If it is off-topic we will consider it. If it is really off-topic we might go ahead and put it in the parking lot, to deal with it later.

We are going to try to have a question and answer session, or a comment session, at the end of the meeting that takes care of all the issues that we have in the parking lot, or any other issues that don't fall into the categories of the presentations.

If you are going to make a comment, or ask a question, I ask that even if you have done it before, please introduce yourself, let us know what organization you are with, if that is appropriate. And that way we can make sure we know who is making the comments.

I know we have Susan Abrahams over here, who is going to be trying to keep track of the meeting, and write everything down. I think Rich Turtill is going to be doing the same thing, specifically in terms of action items. So if you could just let us know, again, who you are and who you are with, before you make your comment, or ask your question, we would really appreciate that.

In terms of questions, if you don't necessarily want to ask them yourselves, we have some index cards and I believe there is going to be a couple of NRC employees who are going to be collecting them. Those are going to be given to Roy and I think he is going to try to address those questions at some point during the meeting. So, if you want to do them anonymously, so to speak, this is your opportunity to do that. I see a gentleman there that has some. So if you need an index card you can let me know, as I'm walking by, or just go ahead and try to get one from the gentleman there.

In terms of what level of discussions we want to have, we don't want to get into safeguards information, secret information, and sensitive information at this meeting. We want to keep it strictly public information.

I know the NRC staff is going to try to stick to that and we ask that everyone try to stick to that as well. If you ask a question that goes into that realm then chances are you are going to get the answer, we can't answer that question or go into that here.

I believe we have some public meeting feedback forms on the table that you came in. Please use them, you can fill them out and leave them here, or you should be able to drop them in the mail and we will get them.

In terms of feedback, we take feedback forms from all the public meetings we have, and we do look at the responses that we get, and make decisions on how to change, or what to do with them. So please take a moment to fill those out.

Anything that we don't get to, in terms of follow-up questions, or that kind of material, I believe the policy is that we will place them on the website at some date after the meeting.

If something like that happens there will be a time where those will be posted. I'm going to go to the phone in a second and ask for the people who have called into the phone to identify themselves.

If you are calling on the phone I will go to you during each Q&A session to see if you have any comments, or questions. I ask that you mute your phone if you are not going to make a statement, and that you go ahead and wait until I prompt you, just because it is difficult to make sure that you are not going to talk over someone else, or if we have someone in the room who is going to make a comment, that you don't speak over them.

Do we know who is on the phone?

We are going to go ahead and do that as soon as I'm done. Thanks, Dave.

In terms of logistics, the rest rooms are right across the atrium. There is a cafeteria and a snack shop upstairs, in case you want to grab something during the break.

If you have any other questions about that just grab one of the NRC employees, we should be able to give you directions on where you need to go, to get stuff done.

If you haven't turned your cell phones off yet, or pagers, please do so, so we don't have them going off and distracting during the meeting. I'm hoping to keep this as on schedule as possible but, like I said, we are going to be flexible.

If there are no other questions, I'd like to go and do a quick roll call on the phone. If anyone on the phone line would like to identify themselves, please do so now.

Brian Miller, Progress Energy identifies himself.

Lance Rakovan, Facilitator

Welcome, gentlemen. Anyone else on the line? (No other response noted.)

Okay, I thought we had one more person call in but maybe not. Again, gentlemen, I just ask that you keep your phone on mute and I will go to you during each Q&A session, specifically, to see if you have any comments or questions.

Having said that, I believe I will turn it back over to Roy.

Roy Zimmerman, Director, NSIR.

I've got high expectations for this meeting. And those high expectations are built on our past meetings where, I think, we have found ways to be able to share information, share concerns, work our way around safeguards information, and other sensitive information concerns.

It sounds a little ominous, that there is not much left to talk about but there really is. We have a lot of information that we are going to share shortly and I don't see the constraints holding us back.

One approach that we have also put into effect in past meetings, that I don't think has held us back, and you will let me know otherwise, is we tend not to drill down on a particular plant issue and get into excruciating detail about an issue at a plant. We tend to take the issue and look at it from a generic standpoint. I think collectively we have been able to do that fairly well, and try not to dominate the discussion focused on a particular facility.

This is a good opportunity to talk policy issues, to talk generic concerns that may have spun from an individual plant. We don't want to focus on any one particular facility for extended periods of time.

There are a few comments that I want to make and then we are going to get right into the presentations. We handed out the organization chart for multiple reasons. One, so that you can identify some of the faces and names of individuals that will be speaking today. There are some new faces that weren't around the table last year. But also to remind you of a significant change that occurred within our office, again, that stood up, in April of 2002 with about 80 people, and now we are just over 200 individuals. And we saw the need, because of the large influx of good folk that we brought in the security area, to split the security division in two. Glenn Tracy now has the lead in the policy issues.

This is oversimplifying but it will convey the thought. Glenn Tracy has the lead for the policy issues and Dan Dorman has the other new division. Dan's division has the lead for those items that are in the operations side of security, including the implementation phase, such as the force-on-force, and the inspection program, and threat intelligence area, and so forth.

Again, we will get into that, and you will hear more about it in the presentations. But that is, simply, the breakout that we have. The NRC budget for nuclear security has increased more than ten-fold since 9-11, so it has been a very dynamic area.

Since the last time that we spoke at this time of year, and, again I don't want to steal folks' thunder in the presentation, but we have made considerable progress in moving into the implementation phase, out of the pilot phases, and the inspection baseline program, and the force-on-force aspect of the inspection program.

There are still areas for improvement in those. We continue to work on those areas. But we clearly view ourselves in the implementation phase. I think our connections to the intelligence community, to other agencies, that we liaison with continue to get stronger.

Our relations with the FBI, with the others in the intelligence agencies, DOE, Department of Defense, NORAD, NORTHCOM, all continue to get stronger and stronger.

Clearly, we have daily interactions with the Department of Homeland Security. As you know, following 9/11, we issued a large number of orders that we felt were appropriate due to the urgency of getting new requirements in place.

There are still some orders planned. You will hear about that today. But the majority of those orders are out and we are, as Commissioner Jaczko indicated, heavily working on rulemaking activities to be able to add stability to the process, and to be able to include the public comments in that rulemaking process.

You will also hear today about the controls that have gone into effect on radiological sources, and how we have approached that, both for fixed facilities and in-transit materials.

I wanted to hit one other area before turning to Glenn Tracy. Commissioner Jaczko spoke about the policy issues on new reactors. That, clearly, is an area that this office is directly involved. We are actively working them now, but the point that I want to punctuate is that our primary focus is on the existing fleet, and making sure that the existing fleet is safe and secure. We are not going to turn attention to the new reactors if we have concerns about the existing plants. That is our primary mission, and our primary focus. So with that let me turn to Glenn Tracy.

Glenn Tracy, NSIR - DSP

Good morning. Again, I'm Glenn Tracy, Director of the Division of Security Policy. Quickly, if you will allow me a little leeway, it has been publicly announced that I will be moving to a different division, the Construction Inspection and Operational Program Division in the New Reactor Office.

And my relief, and the individual who is going to take the reins is Dr. Trish Holahan, who is right here, and the continuity is important, in terms of your insights, and your comments today, and that is exactly why Dr. Holahan is here, to hear those views on the phone, and those views publicly.

And since it is, probably, my last public meeting in this venue, I wanted to publicly thank my staff that has worked tirelessly for that period of time. But, also, the public stakeholders.

And many of you can remember prior to 9-11 when we were working biweekly on the rewrite of 73.55, many of you in the front row. And also working the DBT before that, it also became a more closed project.

And, shall I say, that although I get to see it from my venue, many of the comments that have been raised by those meetings, in terms of that rewrite of 73.55 linger, and you will get to see aspects of that in the proposed rule that I will speak of shortly.

But, I wanted to thank those of you in the public that have had an impact in developing the DBT or in the rewrites of our rules, and we hope to continue that despite the balance that we are trying to achieve with public access.

My next slide is about our topics. Post-9-11 orders I will quickly give the re-brief of those orders, access the foundation of where we are heading in our rulemakings, which is the exact next topic. Then I will go into nuclear materials security initiatives. And we have quite a list of folks in the room that can help in those discussions and can provide feedback to you in any responses to questions that you may have.

We are going to go over the Department of Homeland Security initiatives and, as Roy said, daily interactions with that agency, and also new reactor security which is, obviously, an important discussion.

The next slide, the security orders, you have seen many at this time. And, again, but I want to reiterate, that as Commissioner Jaczko said, we had a fairly strong security program, a robust security program certainly, the finest of the critical infrastructure in America, in the commercial sector, prior to 9-11. However, things had to be done after 9-11, that was clear. And so the February 25th, 2002, Orders were implemented. Those, of course, increased the security officers, and the armed responders, made greater stand-off distances, and larger vehicle barriers, improved the insider mitigation aspects of our programs, and background checks, and included aspects of coordination, response forces and, of course, consequence analysis and consequence requirements for large scale attacks.

On January 7th, the following year, we improved our access authority further by removing any thought of temporary unescorted access to the sites. And also enhancing the consistency across the sites with access to those facilities. And then in April of that particular year we had three elements, sets of orders. We improved our design basis threat. We substantially enhanced the training and qualification to include day, nighttime, tactical, and various written examinations of these officers.

Then, thanks much to the project and government oversight, and other stakeholders, we

became aware of and improved the fatigue requirements, and the overtime, and the work hour requirements of the security officers across the fleet.

On March 20th of 2006, we then enhanced one specific adversary characteristic this year, of the design basis threat.

On our next slide, we basically want to talk a little bit about the materials security orders. And in that realm you are aware that the large or greater than 10,000 curie panoramic irradiators, we issued orders in 2003.

This was the first time that we actually implemented for non-special nuclear material licensees safeguards information. These were 61 orders. We have developed a temporary instruction for those.

And we have, in fact, completed those inspections. We also applied to manufacturing and distributing licensees and those are the individuals who make and distribute the sealed radioactive sources for medical and industrial uses.

Again, these were safeguards information. It covered approximately 58 facilities across the country. And we conducted a temporary instruction and completed the inspections in those facilities.

We also issued orders on the radioactive materials quantities of concern, by Order, in 2005. These measures were safeguards information as well. Ninety materials licensees. And the bottom line on that is these measures were made to address the quantities of materials above what we call category one byproduct limits for the isotopes identified in the Atomic Energy Agency's code of conducts documents, but below the highway route control quantities regulated by the Department of Transportation.

These were fully coordinated with the Department of Transportation, as well as the Transportation Security Agency. And they represent the interim measures that will be superseded once Federal regulatory requirements become effective. And we have, we are in the midst of inspector training on this particular topic.

The next item we did was increased controls for the development of the higher risk, radioactive materials licensees, authorized for the IAEA category one and two (inaudible) material. These particular measures are the groups of the medical and research licensees, the radiography and well logging licensees, broad scope licensees, calibration sources, waste brokers, and remote service, and service licensees.

There are thousands of Orders that belong to the NRC, as well as other multiple of thousands that we handle through the agreement state process have been issued by the agreement states. These discuss access controls, intrusion detection and response, transportation security, advance notification to the NRC, and the physical control for the portable mobile devices, as well as the protection of the licensee's security information in these particular areas.

And then, lastly, there has been fingerprinting orders. As you may know we were allowed significant enhancements as a result of the Energy Policy Act of 2005 which you, as public

stakeholders, had a role of shaping in Congress. And, as a result of that, these orders were developed in compliance with the Energy Policy Act of 2005 to grant access to safeguards information, an important role, and an important act because prior to then we only had the ability to fingerprint individuals who actually had access to a reactor or to spent fuel. Therefore the Energy Policy Act states that a person must be subject to fingerprinting, and criminal history checks, prior to receiving access to safeguards information.

So, there is a flavor of some of the orders that have taken place and they set the background for our next subject, and next slide, rulemaking.

I will quickly discuss reactor rulemaking. And Commissioner Jaczko set the tone, I think, that is the right one. We need your comments, we appreciate your comments. And all these rulemakings are on a very fast pace in terms of what has been the practice of the agency. And, Roy, I would offer you to comment further. But the truth is for many years, three years, it has been a model of what typical rulemaking would be. And I say that rulemaking process has been cut by, at least, in half, in terms of how the agency is to conduct its business.

Roy Zimmerman, Director, NSIR

The only thing that I would add to that is Chairman Klein comes with a new perspective. And he has looked at the way we do business, and there are a few areas that he has focused on. And one of those areas is the area of rulemaking. And he is appropriately challenging us on what we can do to accomplish rulemaking in a more effective and efficient manner.

That is an issue that is not new to our agency. We have tried to define efficiencies, and we will continue to try to wring those out of the process.

Glenn Tracy, NSIR - DSP

So on reactor rulemaking, the design basis threat, 73.1 mentioned by Commissioner Jaczko the final rule is due in October 2006. It will include answers to the 919 public comments, a substantial number of comments, and the final Commission consideration of the Energy Policy Act, which required 12 specific factors to be considered.

We are also working Part 26, along with my partner Dan Dorman, who is the actual lead in this area, for the fitness-for-duty program, the final rule is due in January of 2007. And this rule will, extensively, revise and enhance the fitness-for-duty requirements, both for drug testing and fatigue, for Part 26, 73.21, the protection of safeguards information, we republished this rule, and we received the guidance to do that in June 30th of this year. The proposed rule is due to be published in September, this month. And the final rule is expected to be completed in springtime, March, is what I would call 2007.

This rule revises the requirements for access to safeguards information, consistent with the new requirements of the Energy Policy Act that I previously discussed.

73.62, the one that Commissioner Jaczko mentioned as one of his most prioritized, I would say, rules that he has in mind, is called the security assessment rulemaking. The proposed rule is due September of 2006, as in this month. The final rule is due in September of 2007. This

proposed rule requires that the designers evaluate security at the design phase, with the goal of making the new reactors inherently more secure, thus reducing the reliance on operational security programs.

And then 73.55. I mentioned that, that was the rule that we had constructed with substantial public input, prior to 9-11. And this is, again, the rewrite after 9-11, those horrible events, as well as the substantial orders that have been placed for the reactors.

This * to publish the rule, was received June 30th. The staff is currently publishing, and planning to publish the rule in October of 2006. The final rule is due in the December 2007 time frame.

This rule includes revisions to numerous rules, but I will go through them, because it is important for the public to keep aware; 73.2, 73.55, 73.56, which is access; 73.71, Appendix B, Appendix C, and Appendix G. So if you would pull out your 10CFR, those are the areas, as well as new sections, 18, 19, and 58. And this deals with our new allowance for enhanced weapons, as authorized by the Energy Policy Act of 2005.

Lance Rakovan, Facilitator

I see pens trying to write quickly. Do you want to hear that again, or do you get it?

Glenn Tracy, NSIR - DSP

That is correct, it will, and Jim knows the rules. Bottom line, it will be in the *ANPR (phonetic) and it will delineate every aspect, and every section that Rick Rasmussen's leadership has taken him through this particular rule. The proposed rules and extensive revision of the security regulations, it incorporates all the orders, the thinking prior to 9-11, the SFAQ, or the security frequently asked questions program that we have, where we work to further clarify the guidance that we provided since 9-11, and a substantial number of activities and insights we have gained from 9-11 to the current date, at the fifth anniversary.

The proposed rule includes the provision to allow these enhanced weapons, based on the positions of the Energy Policy Act, and a new requirement for licensees to perform safety security assessment, something that was a public input from the Union of Concerned Scientists.

The next slide. I will talk, a little bit, about the rulemaking in the areas of materials. Secure transfer of nuclear materials, this has to do with the Energy Policy Act, section 656, the comment period closes September 29th of 2006, and the final rule is expected in December of 2006, depending upon the scope of public comments.

This rule implements section 656 of the Energy Policy Act, and establishes the requirements for a system of manifests, and requires security background checks related to the transfer and receipt of nuclear materials, and provides certain exceptions for licensees, where appropriate.

The next rule is radium, and what is known as the NORM, or the naturally occurring and accelerated produced radioactive materials rule. The final rule is due in December of 2006.

This proposed rule establishes the regulatory framework for regulating certain radium sources, accelerated produced radioactive material, and certain discrete sources of naturally occurring radioactive material. And this is required by section 651, subpart E, of the Energy Policy Act. Then there is a very substantial rulemaking in nuclear materials management and safeguards system rule. It is a proposed rule due in December of 2006.

The final rule is due in approximately December of 2007. And it will provide requirements for reporting to that particular data base, I will discuss later.

And that data base, just to give you a quick description, provides the state's system of accounting and the United States government's information system, containing the current and the historical data on the receipt, shipment, and inventory adjustments of certain forms and quantities, and source of special nuclear material, and other materials of interest to the government.

The next rule is the geologic repository operations area, known as the GROA rulemaking. The proposed rule is due July 2007, the final rule is due in July 2008. And this rule establishes the security requirements applicable for Yucca Mountain.

And, lastly, the access authority for non-reactors, EPA 652. The proposed rule is due September of 2007, the final rule is due September of 2008, and this rule establishes the access authorization requirements for the manufacturing, distributors -- access, excuse me, not access authorization, the access requirements for manufacturers, distributors, irradiators, and the quantities of concern.

So that is a very quick and dirty rundown of the rulemakings. And as Commissioner Jaczko said, the purpose is to make sure that you are aware and engaged, at the opportunities and the time frames, and we would appreciate comments from you on how we can further enhance that activity.

The next slide is on materials security. The National Materials Management and Safeguards System, known as NMMSS, I've already described, generally, what that system does. But it basically allows us to keep track and meet our treaty requirements associated with strategic nuclear material. We conducted a major re-baselining of that particular data base, under the leadership of Bob Caldwell who is here in the front row.

The NRC issued bulletin 200304 to facilitate the re-baselining. The bulletin's primary purpose was to confirm the inventories of special nuclear materials, and source materials, and all licensees, were correctly reflected in the data base by September 30th of 2004. And a related TI was developed and completed, and subsequent revisions are incorporated into our inspection manual chapters.

Based upon the lessons learned from that re-baselining, we are developing a rule to revise Parts 40, 72, 74, and 150, to basically require licensees with specific *(inaudible) to report those inventories, require anyone with these types of materials to ensure that the inventories of documented NMSS, and to reconcile all inventory reports with records, and a multitude of other requirements.

It is a basic enhancement to the NMSS data base, and there is a substantial amount of work that has been done in order to verify our knowledge, location, and meeting our requirements in that area.

The next two bullets talk about the source tracking. And that is, obviously, not the special nuclear material, but other radioactive sources dealing with radiological dispersal devices.

A joint NRC-DOE report, and this is a lot of joint work, led by *Dr. Tretollahan (phonetic) as well as members of my staff. The bottom line is the report of this RDD recommended the development of a national source tracking system.

The Energy Policy Act that I have discussed, substantially, in 2005 provided legislative requirements on the rule, and requirements on the specific system. And this has been done in a two-phased approach; well before the Energy Policy Act was, in fact, legislated. An interim inventory now provides a data base on these sources.

This is a short term solution, but it is a means to gather the information, and provide a baseline for the national source tracking system.

The interim inventory began in 2004, and covers NRC and agreement state sources at the IAEA byproduct category one and two material.

The rulemaking for the national source tracking system is under development and, as you well know, it has been out in public and proposed stages, and we are expecting the completion of that rule by the end of the year.

Lastly, I would like to point out that, as Roy stated, we have routine dialogue with representatives of the Department of Homeland Security, not only for the reactors side, but in terms of the domestic nuclear detection office we have staff, full time, working deliberately on these issues and the issues of domestic nuclear detection for both large radioactive sources, as well as special nuclear material.

My next slide, which goes directly into the Department of Homeland Security interface, many of you have heard the term comprehensive reviews, which is an area led by the DHS, and it has chosen the nuclear sector to be the model upon which they are going to conduct these substantial two-week long assessments of the power reactors across the country.

It is, basically, a cooperative inter-government community and private sector analysis of the critical infrastructure. And it is to prevent and mitigate, and respond to events.

The current status is, we have completed these, jointly, led by DHS with multiple of local, State, Federal agencies, at 34 reactor sites, averaging three per month.

I have two full time employees that attend these meetings and coordinate between licensees, and with licensees and DHS, with an estimated completion date of Fall of 2007.

We are prioritizing and implementing specific enhancements. They write substantial reports associated with enhancements that can be achieved. And, as I have already mentioned, there

are two full time staff dealing with these measures.

The next area we deal with DHS, which leads, and is basically a byproduct of the entire comprehensive review, in my next slide, is integrated response.

The overall national preparedness goal set by our Administration provides the priorities and standards for the assessments, and the strategies, and the system for preparedness across the four mission areas; that are prevention, protection, response, and recovery.

And I will deal, primarily, with response. But the bottom line here is you have to implement the national incident management system known as NESS, and you have to follow the guidelines and the concept in the national response plan. And the whole point of this is the expansion of regional collaboration.

Implementation of national infrastructure protection plan, and the capability of specific priorities, the capabilities, interoperable constraints, and basically detection response. And it is all coordinated through these multitudes of different plans that we have located in this slide. I would like to point out that the national infrastructure protection plan, which is finalized, and we had a significant role of ensuring that the nuclear sector's responsibilities, and our responsibilities, those of the Federal government were, in fact, deliberated in this particular overview of a plan. And the national response plan, are complimentary plans. Just to explain, the national infrastructure protection plan establishes the overall risk based approach that defines the nation's critical infrastructure steady-state protective posture.

And then the NRP, or the national response plan, provides the approach for domestic incident management. We have two other plans that are very important, and we are finalizing them, and will be likely to be the first sector completed, and that is the sector-specific plan. And what the sector-specific plan does is it provides the actual resources and the protective strategies for those entities that I have already mentioned, both our facilities and material licensees, and then our power reactors, of course.

What those coordination efforts are, what the concept of the baseline levels of protective strategy should be, and how we should interface in a contingency under the national response plan. I would like to point out that as you are well aware, this particular sector is fairly practiced with the national response plan, because we have something called the nuke rad annex, the nuclear radiological annex, a very specific supplement to the national response plan, that Eric Leeds, in his leadership of emergency preparedness response uses routinely as the main overview and methodology upon which we would handle a nuclear radiological event, and the coordination of the Federal and State assets.

So the bottom line is there has been tremendous effort, since 9/11, on many global plans through the coordination of Department of Homeland Security.

We have been heavily engaged in these particular overriding strategic level plans which get very specific when you are talking about what you will soon see on some plan, the sector-specific plan. And the Nssp then provides our ability to further enhance the nuclear sector, through DHS's efforts of the comprehensive reviews, which I have discussed in the previous slide.

The last point I wanted to make was the fact that there is a routine dialogue, Roy said daily, but on a higher strategic level Roy, myself, and several executives from the varying agencies, such as FBI, DHS, and all the entities which DHS deal with, have quarterly meetings. And this is called the Government Coordinating Council for the Nuclear Sector, which discusses not only power reactors, but radio isotopes, research test reactors, other elements of the sector, and issues are raised, or discussed.

And then jointly, the industry itself, as do all of the sectors, have what is called a nuclear sector, chemical sector, you could go with any sector, banking, coordinating council. And those councils then meet jointly, on a quarterly basis, to discuss these issues and further enhance the interoperability, communications, and the coordination of the strategic resource oriented issues.

The one that is of most interest to us now is known as those enhancements that have been identified through those 34 sites that have had the comprehensive reviews. And we have enhancements that have been identified. Roy's entire efforts, right now, is to ensure that the agencies are prioritizing those, and using the grant process, within the Department of Homeland Security, to address those measures, and get the tactical assets to the tactical responders that could assist in the response, should we ever have an event at a nuclear power plant.

My last slide talks about new reactor security. And I will just quickly touch on three aspects of it. The scopes of rulemaking, licensing, policy development, oversight and, of course, stakeholder interaction, the purpose of today's meeting.

We have standard review plans revisions that are ongoing. We, obviously, you already knew it was a substantial effort, but some 202 plans were made consistent across this particular sector.

We are talking about power reactor, and the cat one facilities. First time ever, that was done via templates that we personally approved, and the industry then utilized those templates in order to ensure that there was a consistent approach that met our requirements post-9/11. We are revising and updating those generic security plans with the industry in order to validate that it addresses the expectations that we have had in the guidance, and the clarifying issues that we have had from 9/11 to today.

We are developing, and you are aware of varying public venues of the inspection test analysis and acceptance criteria. And there will be public access to those particular ITAACs.

Of course they are in the details of the specific requirements associated, for example, for a vehicle, and the mass and the type bomb will never be made public. But the aspects of what is in the ITAAC are exactly what Mr. Huyck, who introduced himself earlier is, in fact, dealing with today. And you will have access to those particular aspects of the new reactors. For new reactors security licensing, we have been required, by the Energy Policy Act, to consult with the Department of Homeland Security. And I, and Roy, have had several meetings at the senior levels of the Department of Homeland Security to, in fact, define consultation. Ms. Ordaz, who is in the audience, deals directly on that, and we are clarifying the consultation, how the consultation, and the timing of that consultation, and to ensure that, basically, a site is appropriate and considers the post 9/11 threat.

We have ongoing design certification, and early site permit reviews that Mr. Morris, who is in the audience, is leading in those efforts. And then we have some policy issues to deal with. And we are not shy about those policy issues. They are important, and you have heard some of these through a meeting that Ms. Ordaz and Mr. Morris had recently. But the access authorization, the physical security around these new sites, is not news to you, that is post-9/11 thinking, in terms of the requirements that we currently do not have. And that is the security upon and around the construction of these sites, and the timing, and the technical basis, the scopes of those programs, and the regulatory scheme upon which one uses, when one is actually developing the construction of a site before it is a protected area, before there is fuel on-site, etcetera, are policy issues that we are currently deliberating within the Commission.

And, lastly, there is the development of the overall inspection construction oversight program. It deals, primarily, with ITAAC initially but, ultimately, there is going to be licensed operators, and all the other aspects should one ever get licensed, and the development of those concepts, and those inspection programs have to be developed, in terms of security.

So on that note I close with that is a taste of some of the policy matters since the last time I saw you, a substantial amount of rulemaking, which was the thrust of the Commissioner, and I open it up to you, and go back to you, Lance.

Lance Rakovan, Facilitator

Are there are any questions or comments?

Paul Gunther, Nuclear Information and Resource Service.

Before I actually make a comment, how much time do we have? I mean, there is a lot of material here. I note that there is, you know, not anybody sitting here, but I would like a few minutes to respond. And I can do that now, or I can do that at the public comment period.

Lance Rakovan, Facilitator

This would be a good time to do it.

Paul Gunther, Nuclear Information and Resource Service.

My name is Paul Gunter; I'm Director of the Reactor Watchdog Project for Nuclear Information and Resource Service. Ladies and gentlemen, there is a crisis of confidence. It has been the subject all along here, particularly from the public. It is a problem that does not go away.

It is a problem that has combined 9/11 and post-Katrina. It is a crisis of confidence that includes both the Department of Homeland Security, FEMA, and the NRC.

The problem is that we cannot restore public confidence while the agency maintains vulnerability at the current sites, and proposed to transfer that vulnerability to new reactor sites.

It is our concern that this vulnerability is being maintained by constrained and unrealistic rulemakings. For example, the fact that we cannot raise, through rulemaking, the issue that 19

attackers, in four coordinated teams, have already successfully attacked the United States.

Yet, the DBT is designed to go under that bar. We cannot restore public confidence by maintaining a lack of meaningful enforcement. For example, the fact that the current fire protection in the industry maintains an unrealistic level of protection for an integral part of the security infrastructure for nuclear power stations.

We cannot restore that confidence if we continue to prioritize the financial interests of the regulated over public health and safety security, as documented by the GAO report in April of this year, *Touche's (phonetic) subcommittee.

We cannot restore that public confidence by denying the independent oversight through public intervention and its experts. And that, of course, is now under challenge as well. But the fact that we find the agency as an adversary in that process, does not lend to building public confidence. We also can't restore public confidence by ignoring other independent scientific bodies, such as the National Academy of Sciences and their report on the safety and security of commercial spent fuel, which was given to Congress.

The continued denial, by this Commission, to address the vulnerabilities, particularly posed by elevated storage ponds in the nation's boiling water reactor force.

We also can't restore public confidence by continuing to trivialize the consequences of a successful attack in the radiological releases on our communities and biological regions which impact on the lack of public confidence in maintaining unrealistic and impractical emergency plans that won't protect public health and safety.

So this is the crisis that we come here to you today as we have in times past, and I'm afraid we will continue to have to approach the staff and the Commission in order to address this vulnerability. And that's my statement, and I'm happy to take questions --now or later.

Roy Zimmerman, Director, NSIR

Thanks, Paul.

Dave Lochbaum, Union of Concerned Scientists

Good morning. My name's still Dave Lochbaum. I'm still with the Union of Concerned Scientists.

Roy Zimmerman, Director, NSIR

Good morning, Dave.

Dave Lochbaum, Union of Concerned Scientists

Good morning. I wanted to talk today about new reactor security, or actually to explain why we're not going to be talking about new reactor security in the upcoming months, basically because, with all due respect to Glenn and Scott and Vonna, it's all a joke. Nothing's going to

happen on new reactor security. So there's no use in us commenting on things that aren't going to happen.

Since we've acquired a local public document room and been able to get access to documents like new reg CR1345 and the new reg that *Bob Budnitz (phonetic) wrote on relay chatter. I forget the exact number. But it had a seven in it somewhere.

We've been able to see that, back about 20 years ago that this agency did a lot of work at looking at existing reactor designs and determining ways it could be implemented in new designs to make it more secure.

The whole focus of most of those efforts was to look at how to make more secure reactor designs. Then when we looked at the advanced reactor designs that this agency certified, the AP100, etcetera, none of those recommendations that came from those many efforts 20 years ago were incorporated in any of the reactor designs. So, it's unlikely -- and by the way, some of those recommendations were better protected control rooms so they weren't so easy to get in to, hardened spent fuel pools from 20 years ago, segregated diesel generator rooms, making it harder for a ground or air adversary to cause harm to both divisions of diesel generators, and a bunch of other recommendations.

There were even cost estimates of what it would cost relative to the existing designs. And they were relatively modest. Of course, doing nothing is cheaper still.

And that's what happened, which reinforces Paul's comment about cheapness rather than success. Also, it was at the Senate Hearing earlier this year where your Commissioners were asked by the Senate how they were going to ensure that these things, these new reactor designs get approved or get built quickly. So, it isn't to get it right, it's to get it fast. That was the message you received from the Senate in June. And the majority of your commissioners were vying to see who could turn it out the fastest, not the best, the fastest.

So, all this talk about making the security assessment rule making, you might as well save some FTEs and just skip that, because nothing is going to come out of that. We know that. You know that. Why don't we just call it a day? So, with that, you know, I've got to apologize, because we're not going to be commenting on rule making that we know is not going to go anywhere. We're going to save the postage and spend it on perhaps sending concerns to people who do care about security issues. And at this moment on this issue that's not this agency. Thanks.

Roy Zimmerman, Director, NSIR

Thank you. We'll come back and address the comments all of you raised and Dave, yours as well. Other comments at this point? Any other comments or questions?

No verbal response.

Lance Rakovan, Facilitator

I will go to the people on the phone to see if you have any comments or questions.

Mr. Miller, Progress Energy.

No comments.

Lance Rakovan, Facilitator

Okay. All right. Do we want to go ahead and take a break then?

Roy Zimmerman, Director, NSIR

Yes, I think we'll take a short break. And I think what we'll continue to do, we'll go through our presentations, just part of success from our standpoint, from my standpoint, is getting the information in your hands.

And then I want to make sure that we come back and address the points that both Paul and Dave already made. So that will come a little later in the program, plus any other comments as we go through our presentations. So, why don't we take a few minutes?

Lance Rakovan, Facilitator

All right, let's take a 20 minute break. I believe we had one set. So, by that clock, it puts us at about five after.

(Whereupon, the above-entitled matter took a 20 minute recess.)

Lance Rakovan, Facilitator

If everyone will take your seats, we're going to get started again. Before we go to the next section, one of our lawyers from the Office of General Counsel wanted to make a clarification on a comment that Glenn Tracy had made, but I don't see her.

Glenn Tracy, NSIR - DSP

She wants me to say when I said the words "due" -- and I appreciate this -- I mean due to the Commission, due to the Commission. So the dates that I was stating, I was saying due to the Commission. Okay? It's a good clarity, and that would mean that in most cases the Commissioners, you know, placed those things in the public realm. In a lot of cases, I should say, but not always, and so those due dates were due to the Commission. Thank you for that comment, by the way. I do appreciate it.

Marjorie Rothschild, Office of the General Counsel

Thank you.

Lance Rakovan, Facilitator

Thanks, Glenn. Our next presentation is on status of NRC security operations by Dan Dorman.

Dan Dorman, NSIR, Director of Security Operations

Thank you, Lance.

This morning I'll be sharing key activities over the past year in the NRC's programs for the oversight of security, particularly reactor security in many cases, and including the implementation of the force-on-force exercise program for the performance based evaluation of licensee security performance.

I'll also address the staff's activities in the areas of information management and information sharing. Go to the next slide, please.

Following the events of 9/11 and as we developed and implemented the enhanced security provisions that Glenn already talked about, we also revamped the baseline security inspection program. The revised program increased the inspection effort fivefold and broadened the focus areas for inspection of security at power reactors from four areas to nine areas. And as the licensees revised their protective strategies and security plans in 2004, the NRC's inspections during that period focused on the access authorization attributes of the orders of January 2003 and on the security force work hour limits.

In 2005, the focus of the inspection efforts shifted to the implementation of the approved protective strategies, and those focused inspections were completed in December of 2005 and we are now in 2006 implementing the full scope of the revised baseline security inspection program at all of the power reactors.

Over the past several years, we have established and operated an interoffice management

review panel. We call it the Security Findings Review Panel. This panel consists of management representatives from several headquarters offices: NSIR, NRR, NMSS, Office of Enforcement, OGC, as well as regional representation, to review all security inspection findings and ensure that the requirements are being consistently interpreted and applied by the inspectors and that the significance of the findings that come through from the regions are being consistently assessed.

Through this process and with the full implementation of the baseline inspection program, we believe that the oversight of nuclear power plant security has reached a period of relative stability, but as you know, in 2004, the Commission determined that the security inspection findings contain sensitive information that could be useful to the persons who wish us harm. And accordingly, the Commission at that time directed the staff to remove from the public domain all information related to security findings.

I hope you have also recognized that the Commission revisited that decision earlier this year and starting in May of 2006, the staff has been providing some but still limited information on inspection findings in the publicly available cover letter that forwards the inspection reports to the licensee.

So, now the public will have visibility of the fact that there was an inspection conducted, whether or not there were findings. If the findings were green, that will be identified. If the findings are potentially greater than green, that will be identified in the cover letter that forwards the inspection report to the licensee.

Concurrent with the removal of the information in the inspection program in 2004, the staff made conforming changes in other areas, such as the communication of allegation results back to the individuals that had raised the concerns.

We recognize that those changes created difficulty in communicating how the staff has resolved the concerns that individuals have brought forward and has made that program challenging over the last several years. We are currently working with the Office of Enforcement which owns the allegation policy to make similar conforming changes to open that up again a little bit, consistent with the Commission's policy.

We believe this will help improve communication with key stakeholders while continuing to protect information that would be useful to those who wish us harm, and I would expect that as we implement the current policy that we will continue to revisit that as we continue to try and find the right balance on sharing information.

Also, when the Commission restricted the inspection information two years ago we recognized that the sensitivity of information on inspections would be reduced with the implementation of the licensee's corrective actions and with the passage of time, and accordingly, they directed the staff at that time to provide in 2006 a publicly available report to Congress reporting on the inspection results for 2005.

In addition, in the Energy Policy Act of 2005, the Congress directed the Commission to provide an annual report of the results of force-on-force exercises. The first such annual report was provided to Congress on June 30th, and is available to the public on our Website at

www.nrc.gov under the nuclear security link.

Another area of focus in the oversight program over the past year has been the implementation of strategies to mitigate the effects of large explosions and fires, including ones that significantly exceed the capabilities of the design basis threats.

In February of 2005, the staff provided guidance to the industry on mitigation strategies that considered insights from research activities, from industry best practices, and from lessons learned from the responders at the World Trade Center and the Pentagon in 2001.

All of the licensees have committed to procedures and training for diverse and redundant mitigation capabilities and some of the more significant measures have been incorporated in licensing basis through orders.

In the area of accounting for spent nuclear fuel, especially pieces of rods that have been removed from assemblies in the spent fuel pools, the NRC has continued the program of inspections through a temporary instruction to assess the effectiveness of licensee spent fuel inventories and record keeping.

Eighteen sites have been inspected to date, and based on the results of those inspections; the NRC is developing plans to accelerate the pace of those inspections such that all sites will have been inspected by this time next year.

Concurrently, we are working with stakeholders to enhance the inventory and record keeping requirements in the applicable ANSI standard, and once that standard has been revised and the endorsement in a subsequent reg. guide, the staff will return the spent fuel inventory inspections to the baseline inspection program.

During the past year, the staff also completed inspections of security enhancements post-9/11 at a number of other facilities, including independent spent fuel storage installations that are not collocated with power reactors and at certain fuel facilities.

Next slide, please.

During 2005, we completed the first full year of the new, more realistic force-on-force program. This program provides a performance based evaluation of each licensee's ability to protect against the design basis threat.

Before 9/11, these exercises were conducted at each site about once every eight years. The new program incorporates significant enhancements in the conduct and realism of the exercises and is conducted at each site once every three years.

One of the major enhancements to the program over the last several years has been the use of the multiple integrated laser engagement system, or MILES. The MILES system, with additional enhancements in recent years, records hits and near misses, enabling the exercise evaluators to more accurately score the combat results and provide a clearer picture of the effectiveness of the licensee's protective strategy. Another significant enhancement is the use of a dedicated adversary force subject to stringent physical and tactical qualification

requirements established by the NRC and trained specifically in offensive tactics. This force has been used in all of the force-on-force exercises at power reactors under the implemented program. Their speed and tactical ability have been consistently demonstrated and have significantly enhanced the realism of the exercises.

We have completed these exercises at 37 sites to date. These inspections have resulted in four green findings, several related to security performance, and one related to controller performance in aspects of the exercise simulation.

In all of these cases, corrective actions are implemented prior to the NRC inspectors leaving the site to provide assurance that the site remains well protected.

The results of these inspections in 2005 were also addressed in the June 30 report to Congress. The force-on-force program has now been fully integrated into the baseline security inspection program. It has got a separate significance determination process specifically designed for assessing the exercise results.

Force-on-force findings, like all of the other security inspection findings are reviewed by the Security Findings Review Panel to ensure consistency in the implementation of the program and in the assessment of the results.

Next slide, please.

Throughout the past year we have continued our efforts to ensure that key security information is adequately protected and to provide clarity to stakeholders regarding what categories of information are protected. Last fall the NRC completed a first of its kind designation guide to better enable users of safeguards information to recognize and properly designate safeguards information.

In addition, we have developed and deployed for the NRC staff a Web-based training program on the safeguards information program.

The proposed revisions of 73.21 Glenn touched on in his remarks regarding control of safeguards information, was issued for public comment. We had public comments on the incorporation of changes, the addition of the modified handling program post-9/11. That was on its way to a final rule. The Energy Policy Act of 2005 added some fingerprinting requirements and background checks for access to safeguards information. So that rule is going to be going out soon for another brief comment period addressing those Energy Policy Act requirements.

As the rule is finalized the staff will update the guidance on handling safeguards information in NUREG 0794.

Next slide please.

The staff has also been active in working with other Federal agencies to enhance information sharing among agencies and to clarify the myriad categories of sensitive, unclassified information. There are well over 50 different categories of sensitive unclassified information in use throughout the Federal government. This information is not classified. It's unclassified. It's

not under any law or executive order, subject to diverse handling requirements established by the various departments and agencies that have established these programs.

This creates a system that is at best confusing and is at least a burden on the ability to share information with key stakeholders across agencies. The NRC staff is actively participating in a presidential task force to identify the scope of the problem and to attempt to standardize and minimize the categories and the handling requirements with an objective of enhancing information sharing.

In the area of classified information, the administration is proposing changes in longstanding principles in the control and handling of classified information. For example, narrow interpretation of the need to know principle and the originator control of information are concepts that enhance information protection, but it can also tend to constrain information sharing among stakeholders who have use for the information in their official capacity.

The staff will continue to work closely with the other departments and agencies as the Federal family strives to strike the right balance between information protection and information sharing.

Next slide, please.

While we have implemented the security enhancements for the last five years and arrived at relative stability in the oversight program, we continue to learn from program implementation, and we will need to address the effects of the various rulemaking activities that Glenn described earlier.

These lessons learned and the revisions in the rules need to be properly incorporated in our baseline inspection procedures, and in addition, we are working to update the construction inspection procedures in the security area to ensure that we're ready for the anticipated construction activities.

In addition, with the limitations on sharing information, there is a challenge to identify, compile, and disseminate operating experience among licensees in the security program. During the past year we have issued a variety of advisories and information notices to ensure that the licensees are kept informed of key operating experience and have the opportunity to learn from mistakes of their peers.

Unfortunately, due to the fact that most of these issues involve safeguards information, these advisories and information notices are largely not visible to the public. Nonetheless, these tools are resource intensive and rely on the staff to compile and distribute the information so that we continue to seek means of sharing information that will enhance the licensee's ability to learn from each other's lessons as they are able to do on the safety side.

Next slide, please.

As we work to maintain the stability in the oversight program, we will also seek continuous improvement through incremental incorporation of lessons learned in the inspection procedures.

In addition, as we complete the spent fuel accounting inspections at all sites next year and complete the ANSI standard revision in that area, we will incorporate that area as an additional element of the security cornerstone and the baseline inspections and ultimately transfer the implementation of that inspection program to the regional offices. And as we pass the halfway point of the first triennial cycle of force-on-force exercises, we are already beginning to look for ways to enhance the exercise realism in the second cycle and to gain effectiveness and efficiency throughout the baseline inspection program, including the force-on-force.

Next slide, please.

Within the NRC, the staff has established several working groups to enhance our own organizational effectiveness and to bring closure to some of the challenges that we have borne as a new office over the last few years. We continue to formalize our internal processes and are turning more to information technology solutions to enhance our own efficiency.

In addition, over the last several years, we have steadily recruited and hired a robust security staff with strong and diverse backgrounds. As our program stabilizes, so is our staffing. We are committed to the continued development of our outstanding people, and as we transition away from aggressive hiring and growth, we are committed to capturing, retaining, and building on the exceptional experience and knowledge base that we've gained.

Next slide, please.

Over the past year, the NRC has continued to enhance the oversight of nuclear security and to increase its information sharing capabilities, and with more than half of the power reactor sites having completed an NRC evaluated force-on-force exercise, the effectiveness of the security enhancements of the last five years is being routinely demonstrated.

As we look to the future, we are focused on protecting the public as we continue to enhance the effectiveness of our oversight activities. While we have achieved a measure of stability and consistency in the implementation of the program, we continue to learn from our ongoing activities and operating experience and feed that back into improving the program.

In addition, we are applying appropriate efforts to prepare for the anticipated construction proposals while we strive to enhance our effectiveness in overseeing the security implementation in the existing fleet.

I appreciate your attention and look forward to the continuing dialogue. I'll turn it back to Lance.

Lance Rakovan, Facilitator

Thank you, Dan.

Roy Zimmerman, Director, NSIR

Let me make one comment in listening to Dan related to licensee performance and force-on-force, separate them for a minute. As you can expect, the logistics of setting up a force-on-force exercise are relatively significant. One of the things that we try to do and have done on

occasion is if we have a concern about a particular plant based on some other aspects of their security performance, we will evaluate and look to try to move up their force-on-force date to be able to do a performance based test to see how that helps inform the overall picture that we gain on how that licensee is performing. So we try to maintain as challenging as it is and logistically we look for opportunities to be able to do that as well.

Dan Dorman, NSIR - DSO

Thanks. Roy.

Lance Rakovan, Facilitator

Any questions? Any comments?

Okay. Please state your name and your organization.

Jim Riccio, Greenpeace.

Just a quick question. In your understanding of how the ROP will work on security, will the industry be allowed to argue that they can use emergency planning to downgrade the consequences of a possible attack on a nuclear power plant? And will you accept that as a way to keep a reactor performance indicator from changing color?

Dan Dorman, NSIR - DSO

The SDP for the baseline security, my recollection is there's no EP component to that. In the force-on-force, the criteria and the exercise is getting to equipment that would lead to core damage, which is independent of whether it actually gets to the point of causing the release.

If it gets to the point of causing a significant release, then that escalates the significance of it. At that point, planned and exercised activities that mitigate that release, it would potentially be of consideration, but in terms of the off-site EP, the criteria for that escalation of significance is looking more at the dose at the site boundary. So off-site EP activities that would evacuate or shelter or would not be related to that criterion.

So I think the off-site EP would not impact the security finding.

Jim Riccio, Greenpeace.

Okay. So my understanding would be that -- because I know you guys are working with emergency planning now and doing the joint EP, and so you do at some point posit that you do have a release to the public. Yes or --

Roy Zimmerman, Director, NSIR

Yes. Eric can jump in here, too, on the EP side. We are looking at integration from both directions. So when we do the force-on-force exercises, there's an EP component to the force-on-force exercises in terms of the communications between security and operations and the EP organization and ensuring that the determinations that need to be made on the EP side are

being adequately informed in a timely manner, and those determinations are being made appropriately.

Then from the EP side, incorporating a security component into the exercises so that the exercises consider the full range of possible initiators of events that will then cycle both the site and the off-site response organizations.

Eric Leeds, NSIR - DPR.

If I could chime in for a minute, Jim. Yes, I think you asked a pretty specific question for the reactor oversight process. If there is a release, can licensees take credit for their emergency preparedness from the security aspect, from the security cornerstone?

I mean, I thought the answer to that was no.

Dan Dorman, NSIR - DSO

Right.

Eric Leeds, NSIR - DPR.

No, they cannot.

Jim Riccio, Greenpeace.

I'm just trying to insure that the agency doesn't use emergency planning to mask performance problems at reactors, whether they be in the security realm or in the realm of, you know, nuclear reactor regulations. And I would like to hear from you guys if the answer is no.

Dan Dorman, NSIR - DSO

No.

Jim Riccio, Greenpeace.

Is that answer the same from other parts of the agency?

Eric Leeds, NSIR - DPR.

I also want to take an opportunity, since you raised emergency preparedness. You know, I want to put a plug in because I think it's a great initiative that we have ongoing with states, with locals, with the industry where we're having every plan.

We're in Phase 3 of our emergency preparedness exercise program where every plant, every nuclear power plant, over the next three years will practice an emergency preparedness scenario with a security initiator, and we've already done the pilot program. We did four tabletops at four different sites, at Diablo Canyon, Duane Arnold, North Anna and Vermont Yankee, and we got very, very positive feedback and participation by the various state, local

and first responders. Then we did an actual -- well, more than a tabletop, we did an emergency preparedness exercise at Calloway where everyone played the actual roles, another case of a security initiator, and now every plant will do one over the next three years. Then we'll incorporate it into the regular biannual graded exercises that we inspect and DHS grades, and I think we've made a lot of progress on that and are looking forward to running through those exercises.

Roy Zimmerman, Director, NSIR

Just a couple of comments to add on. One, on the point of the exercises that Eric is going over, I give credit to the industry that they have been arm in arm on this topic; that they believe it needs to get done, and the industry has embraced this, these exercises. So I do credit the industry.

Going back to the role of EP and force-on-force, very candidly, when we first started coming out of 911 and starting with tabletops when we restarted force-on-force and raised the questions about, okay, you've got bad guys here; you know, they're firing from the OCA; they're doing this, they're doing that; where are you in your classification scheme? Who are you going to call?

It left a little something to be desired at that point in time, which led to more practice, which led to more clarity in licensee procedures, which led to the bulletin going out that has made the kind of improvement that we would expect; that the action levels based on security initiators is something that the industry is quite good at now. But subsequent to 911, before having as much emphasis in security as we do now, that's one of the things that has led us to keeping an EP component in force-on-force, to make sure those classifications are done accurately and quickly and the right individuals are notified.

Okay. Question on the floor.

Steven Dolley, Inside NRC Platts.

The updated final safety analysis reports that constitute the licensing basis for each power reactor, prior to 911, they were available in the public domain. Subsequent to the attack, they were removed from the public domain.

Very limited sections of the FSARs have been returned to the public domain specifically, I think, on the aspect of waste management in the context of the liquid radioactive effluent task force, but are there plans to return the updated FSARs or at least significant portions thereof to the public domain? And if not, what is a viable basis for the public and other stakeholders to assess, you know, very specific regulatory activities related to the plans because this is pretty much the font of detailed plant specific information?

PARTICIPANT

(Inaudible.)

Lance Rakovan, Facilitator
Anyone want to?

Roy Zimmerman, Director, NSIR
We'll address it.

Lance Rakovan, Facilitator
Okay.

Roy Zimmerman, Director, NSIR
I'll address it.

Lance Rakovan, Facilitator
All right.

Roy Zimmerman, Director, NSIR

The issue of information including the FSAR has been one that starts with a background that we have always prided ourselves with being an open agency and making as much information available as possible, and I tend to think we have stood out in that category pre-911.

Following 911, we removed a lot of information only for the reason of the information not being available to the adversary and having it turned around and used against the United States. We have relooked at that. We have put some information back. We've had more than one task force that has evaluated where that break point ought to be, and we continue to learn.

On one hand, we want to go back to where we were, where we are able to make more and more information available, but we balance it with is somebody going to turn this on its ear and use this information against this country.

So periodically we'll reevaluate, reassess as time goes by as we learn from other aspects of what's occurring domestically or internationally. You're asking specifically about the FSAR, and I'm being more general currently, but that's what led to our inspection reports being something that we were not sharing and now we are sharing some information.

Later on will the staff put something in front of the Commission that perhaps there's even more we can share? We'll have to see. We'll have to see how that develops.

So we try to seek the right level on this, and that concept to me applies to the FSAR as well. So I personally can't be specific about if there are other specific sections of the FSAR that are currently in consideration, but there is nothing that I see that precludes us over time to weigh the pros and cons and make those decisions as we learn from ourselves and we learn from others.

Lance Rakovan, Facilitator

Anyone else wants to comment on that?

Steven Dolley, Inside NRC Platts.

I'll just follow up really quickly. What I got is there's nothing that stops you from considering it in the future. Am I to take that to mean that it's not currently under consideration to return the FSARs to the public domain?

Roy Zimmerman, Director, NSIR

I'm not aware of an initiative in that area. If there's somebody else with the NRC here that may know of something, they should speak up, but I personally am not aware of any activity currently underway.

But, again, I'm looking at it in that broader context that a decision can get revisited over time, if there's new information that can modify a decision, and I'm not trying to lead to say that's, you know, going to occur in this case, but we did it in the inspection reports, and nothing precludes us from reviewing other areas of information that we have taken down from public disclosure.

Lance Rakovan, Facilitator

Anyone else want to comment on that?

Vonna Ordaz, NSIR, DNS

I would just offer one other item, which is the --

Lance Rakovan, Facilitator

Could you introduce yourself, please?

Vonna Ordaz, NSIR, DNS

Sure.

Lance Rakovan, Facilitator

I don't know if you were here when we did invitations -- introductions.

Vonna Ordaz, NSIR, Deputy Director for Reactor Security and Rulemaking in the Office of Nuclear Security and Incident Response

I just wanted to also mention that 10 CFR 73.21 rule, proposed rule will be out relatively soon, and that might be another opportunity for the public to comment in terms of the threshold of information that's available to the public, and that should be relatively -- I'm looking at Marjorie. Marjorie, do you have a specific? This fall some time?

Marjorie Rothschild, OGC, GCLR, RFC
(Inaudible.)

Vonna Ordaz, NSIR, DNS
But in the -- very soon?

Marjorie Rothschild, OGC, GCLR, RFC
I cannot say very soon, but certainly I'm told the fall that it will be published.

Vonna Ordaz, NSIR, DNS
Right.

Steven Dolley, Inside NRC Platts
Thank you, (inaudible). Thank you.

Diane Curran, I represent the San Luis Obispo Mothers for Peace
I'll just reiterate some of the comments that I made to Roy during the break.

I think one of the reasons why there's such a concern about the NRC's accountability to the public for security is because of the lack of public information. I came here this morning to listen, just to hear what is the status, especially of the design basis threat rule, which I think is one of the most important items on the NRC security agenda.

The Mothers for Peace filed extensive comments on the rule, and we think the rule has very, very serious shortcomings. The rule happened to result, in my opinion, from a lawsuit that was brought by the Mothers for Peace and Public Citizen against the NRC. We challenged the NRC for upgrading the design basis threat in 2002 and 2003 in secret enforcement orders. They were identical orders that were issued to each licensee for nuclear power plants, and we said the NRC should be conducting a rulemaking in which the contents of these orders in general form are provided to the public so that the public can comment.

That's one of the cornerstones of our public participatory form of government, is the government wants to make a proposal for a regulation. The public gets to comment on whether the proposal is adequate to meet the requirements of the regulatory regime of the governing statute.

What we found out when the NRC finally proposed a rule was that, in fact, the NRC, while it said that it was strengthening the design basis threat, had actually weakened it with respect to the DBT for theft, and that is laid out in detail in our comments.

We only learned that because the NRC complied with the Administrative Procedure Act and published that proposed rule, and we hope that the NRC is going to pay attention to our comments and respond to them because that is a serious problem.

The weakening of the design basis threat in the post 911 environment is a very serious problem, and one of my concerns in coming here this morning was seeing that in March of 2006, the NRC issued yet another set of secret enforcement orders to licensees to upgrade the design basis threat.

Now, one would think that after having gone through the litigation with the Mothers for Peace and Public Citizen the NRC would say, "Okay. We're going to do this in a rulemaking." The NRC has the ability to make the rule immediately effective. It's not a question of whether, you know, if you go through a rulemaking you can't protect public security and safety by going ahead quickly. That's allowed.

But what's important is that you put the general contours of that so-called improvement out for public comment, and you're accountable to the public. Did we improve security or did we not? And that hasn't happened. It's just another example of how we, members of the public, are very frustrated by the lack of government response in procedural accountability.

Another concern that we have that the Mothers for Peace describe in our comments is that the design basis threat as it's set out in the proposed rule is based on what the industry can afford or what's considered to be affordable. Reasonable is really translated into affordable for a private security guard force.

Now, from the public standpoint, the question is not what can the industry afford, but what is the nature of the threat, and if the NRC thinks the threat is greater than what the private security forces can reasonably or affordably respond to, we, the members of the public, are entitled to know that and we haven't been dealt with straight. That's the frustration.

Now that's in our comments, and we're hoping to get a response to those comments from the NRC. So that's -- I know you can't talk about what's in the final rule. That's pre-decisional. So I think we have to wait to see what's in that final rulemaking, but I would really urge you. Read the comments because there were many individuals and public interest groups that spent a lot of time reviewing that rule and have very serious concerns about it.

Roy Zimmerman, Director, NSIR

I'm going to ask Vonna to respond, but first, I wanted to thank you. You went over that with me during the break and indicated that you really needed to be going. I thank you very much for staying, and I also thank you for being able to be patient enough to go through it again so that the rest of the NRC team could hear the concerns.

Diane Curran

Okay. Thank you.

Roy Zimmerman, Director, NSIR

Ms. Curran, I just wanted to mention we have received hundreds, almost 1,000 comments in particular on that rule. It's a very important rule to us as well, and we are in the process of finalizing the final rule package that as Glenn mentioned will be provided up to our Commission

by the end of October. And from a rulemaking standpoint as a whole, I also wanted to respond to Mr. Gunter's comments on the public confidence piece. Public confidence is extremely important to us as well. We are looking at the rulemaking process in terms of looking at ways to provide information out to the public as early as possible, including draft rule language that we have done on various security rules such that you can have an early review of the rules prior to it being published in the Federal Register for official public comment.

So we have done that with -- 73.55 has been out there in the public and other rules as well. So we're also looking at public meetings in terms of having more public meetings once the rule goes to the Federal Register for comment so that we can hear additional comments from you and include that as part of our open process, to solicit your comments early in the process.

And regulatory guides. Regulatory guides is another area, including 73.55, which is a very large package that you may have seen in the public domain. We're looking at putting out public reg. guides also so that the public has an opportunity to see that level of detail.

Of course, there will be a safeguards version as well because we do have to protect information under 10 CFR 73.21 properly, but we are looking at other ways to be able to provide information out to the public as early as possible so that we can get all of the comments that you have factored into our process.

Diane Curran

Thanks.

Roy Zimmerman, Director, NSIR

Thank you.

Lance Rakovan, Facilitator

Marjorie, if you have a comment, can you please go to the microphone?

Marjorie Rothchild, NRC Office of General Counsel

I would just add that the NRC will be responding to the comments made on the DBT rule and that will be in the Federal Register notice of final rulemaking. I just wanted to clarify that those comments and major issues raised, there are going to be responses to those in that notice.

PARTICIPANT

One disconnect for me, and I'm not sure if anybody here in the NRC can address it, but Diane has raised this issue that in her mind she's convinced that one of our actions weaken the design basis threat, and I'm just wondering if that's connecting somewhere because it didn't with me, and I said we would take that back. But being that you raised it, I just wanted to see if it's connecting here, and is this a forum that we can talk about it and maybe clarify it.

PARTICIPANT

Well, being pretty familiar with that, I can assure you we haven't reduced the level of the threat that's provided for that. The wording has changed, and it has reduced the emphasis on specific numbers in some cases, which perhaps could be perceived as a reduction, but that's not the case, and that is explained in the notice, and it is explained in the answer to your comments.

PARTICIPANT

Can we be any more specific here or we can't?

PARTICIPANT

I don't have the specific citation in mind, but it was a general theme throughout.

Rick Rasmussen, NSIR, DSP

Okay. So what I'm hearing, because I'm still trying to catch this issue, is that it's connecting a little how somebody can read it and think that there's a reduction, but in our -- in our response to comments, it should clarify.

Yeah, I believe it focuses on verbiage--excuse me while I ruffle papers. In terms of the internal threat, perhaps the vehicles, the use of the term "vehicles" was intended to expand the capabilities of those vehicles, not restrict it.

PARTICIPANT

Diane, can you?

Diane Curran

The language has to do with the number of groups.

Rick Rasmussen, NSIR, DSP

The number of groups, and one or more teams attacking from one or more entry points.

Diane Curran

What's the proposed -- it was -- I can't remember the exact --

Rick Rasmussen, NSIR, DSP

It was several, I believe.

Diane Curran

If you had the language of the current rule and compared it to the proposed rule, it has been weakened, and that is dealt with extensively in our comments. You know, I didn't bring my

comments. We could have a debate about it right now if I had all of that in front of me, but in my view it's very clear that the language has been weakened, and whatever your intent may have been, that language can be interpreted by someone who is responsible for implementing the rule as allowing a weakened response.

PARTICIPANT

Okay. Let me first say that in no way am I trying to debate it. I just wanted to try to clarify it, was the only driver here. And, again, we'll try a little bit more here and then, again, in our comments we should be explaining it more clearly, and if there's still an issue, then we would expect to have more dialogue on it.

Bobbie Warren, Chief of the Intelligence Liaison and Code Assessment Branch

I've been very involved with the development of response to comments.

One of the challenges in developing the language for the rule was how to best do a new rule that would not -- that would be open to the public, as we have been in the past, but that would address some of the challenges we had with specific words in the previous rule language, as well as looking at future rule -- the ability for the rule to stand for some period of time. And that definitely was a challenge, and I think that we made an attempt in this rule language to provide a -- and it may be interpreted as a weakening by some people reading it, but it was more of a generalization of some of the rule language, and I think that's the challenge that you're indicating here in your comments. But it was not an attempt to try and weaken the rule, but rather trying to address this ability to balance what we can provide to the public in the new, post-9/11 environment.

Jim Riccio, Greenpeace

It's not just what you have put in or done to the DBT. It's what we know is not in the DBT that gives the public cause for concern.

I've been cautioned not to speak out of school and so I won't, but you can find this information in the British study from the British PO Post, whoever that acronym stands for, but they quote NEI about what is not going to be included in the DBT.

So we know what's not going to be in there, and that gives us cause for concern, but it has also prompted the public to petition your agency to remove waste from the poll if it doesn't need to be there.

Again, unfortunately that petition has fallen on deaf ears, and if you're not going to protect against an airliner attack, why not at least reduce the consequences of a potential attack? It seems like a pretty honest and open question.

Roy Zimmerman, Director, NSIR

Thank you.

Let me address one aspect of aircraft now and then try to tie it into Dave's comments on new facilities.

One thing that I think we have shared in past gatherings like this is that the NRC, working with the national labs and using state of the art (inaudible) analysis, looked at the current designs for the current fleet to find out what would the impact be for an aircraft crash, and we learned a lot from that and identified that there are mitigating strategies that have been put in place at the licensees that if -- and this is what I was mentioning to be sort of practiced with the licensee -- that if they have incoming aircraft they are going to take these following actions, things that were not necessarily recognizable by us or the industry until after these analyses were done. And those findings have led to steps to be taken that would, although the emergency planning basis was not currently threatened, it added additional time, significant amount of time, for different plant designs based on what was learned.

So we have done a fair amount of work associated with the existing fleet on aircraft and candidly feel positive that it bore fruit in identifying some actions that licensees needed to take should that occur, and they have.

Now, if I move to Dave, so the staff looks at that and says, "Well, we have that information on existing, the existing fleet. Should we have a similar level of knowledge for the future fleet if there is going to be one?"

And that is a dialogue that has occurred within the staff, that is occurring with the Commission. The Commission has a policy statement that future reactors will be more secure than existing reactors.

You heard Commissioner Jaczko make the statement, and to the best of my knowledge all Commissioners agree, the staff agrees that the best way of doing this is to build it into the design and strengthen the design. The rulemaking that we're working on for security assessments will, I expect, accomplish that for the next generation of facilities that are being considered.

I'm leaving AP-1000 and others out of that mix. For the next one. But the question that the staff is asking -- I'll repeat it again -- is, "But we did this work on existing reactors. It bore fruit. Should the NRC be looking at doing something similar for the forthcoming fleet if, in fact, it materializes?"

And that's an active discussion amongst the staff, and is now turning into an active discussion with the Commission. So I'm trying to readdress that. I wouldn't have expected you to have that information, the benefit of these kinds of meetings, but from my standpoint, I would hope that would move your comment a bit, Dave, that -- no, didn't move it. Okay. But it was intended to share additional information with regard to future reactors and aircraft.

Paul Gunther, Nuclear Information and Resource Service

I mean, that said, we have this dilemma where documents that are in the public arena contradict documents that NRC refuses to disclose. So if you have confidence in your analysis, the public needs to at least be able to challenge or verify, and under the current regime, we're

denied that opportunity.

Most appropriately, I think you know, specifically, for example, the December 18th, 2003, rule that denies public the ability to present contentions, and that is under challenge, but again, you know, if you were eager to engage the public in building confidence on these issues, particularly with regard to aircraft and plant vulnerability, you would provide us with a forum to address the disclosure of documents with regard to the EPR that suggest to the contrary; that new reactor -- this particular design is vulnerable. So until we can move around this impasse, I don't think we're going to make much gain in terms of both security and public confidence.

Roy Zimmerman, Director, NSIR

I'll make a comment and see if anybody else wants to comment as well.

I recognize the challenge that you're left with, you know, am I going to accept on face value when I don't have the ability -- I have the interest. I have the intellectual capacity, but I don't have the information in front of me. So I'm being asked to trust the NRC.

One of the things that we have done is we have been on the Hill a number of times with the representatives of the public that have the clearances for this information to brief them on the results of these studies. So their constituents don't have the specific information, but in a number of cases there have been briefings that have been done that have addressed the results of aircraft impacts associated with spent fuel pools or with the containment.

So we try to make inroads to share that information. I think, Paul, my recollection is I think you made that comment last year, too, and I respect it, and I understand it, and we try to work with some of this sensitive information that can't be shared broadly, but clearly there's interest that exists inside the Beltway, and we have shared those results in a number of different forums.

We tried to summarize it in the Protecting our Nation public document to be able to provide the bottom line that we came up with, but it doesn't scratch the -- you're raising is "yeah, but I'd like to see it for myself" or "I'd like to have it peer reviewed by my people."

So I understand that, understand that concern, but I did want to try to again address the fact that future reactors, there's still dialogues that are taking place within the agency on that.

Scott Morris, NSIR, DSP

I'm Scott Morris, Chief of Reactor Security Branch. I work for Glenn and for Vonna, and I just want to supplement what Roy said, and this isn't speaking directly to your comment, Paul, but with respect to the dialogue that we've had trying to convey what we've learned as a result of the detailed analyses that have been conducted on the existing fleets to an aircraft impact, we've not only shared that information with the -- with folks on the Hill and obviously with the Commission and other Federal agencies, but it has clearly informed our decision making and some of the requirements that we've instituted to address mitigation strategy, and Roy alluded to that. And it has added significant margin to emergency planning basis and other -- and other avenues, and also we've shared it in light of the fact that there is a lot of noise being made about new reactors.

We've also shared that classified information with cleared individuals who are -- you know, have proposed design, new reactor designs, including the major vendors like Westinghouse, GE, Areva. And so, they have the benefit of understanding some of the insights that have been gained from the current fleet. They have been advised about the Commission's policy statement on the expectation that new reactor designs be inherently more secure to arrange with threats. And so I think, you know, we've done due diligence in trying to convey the information that we've learned and to take action on it where we can, but it's exceedingly difficult as you might imagine to convey the level of information that's going to satisfy those in the public realm and maintain that balance that we need to maintain without giving away too much information.

So it is a huge challenge, but I can assure you that speaking for myself personally, and I know from my colleagues, that we have done what we think is appropriate. Now, obviously we're hearing something -- something to the contrary, and we need to consider that. So I guess we'll have to redouble our efforts to figure out how to do that.

Lance Rakovan, Facilitator

I've got a gentleman over here that's being very patient in waiting for a comment. So I'll get to you next as long as there are no further comments on this particular discussion or was your comment on this particular discussion? All right. You'll have to wait just a minute longer, sir.

Steve Dolley, Inside NRC

I can understand why if you revealed too much specific information about the design basis threats, say, that it anticipates X number of attackers, someone who wants to do less harm could use that information to plan an attack. But, if the analyses conducted by the industry and by the agency demonstrate that even crashing a full scale 767, or other large jetliner into a containment would not penetrate the containment, that it's physically and from an engineering perspective not possible, which is what at least the industry's position is, how does it increase vulnerability or jeopardize security by making those results public?

In other words, if it's just not possible to jeopardize a plant in this fashion, why does it jeopardize security to release specific information to that effect?

PARTICIPANT

Steve, I can take a crack at that, if you don't mind. Steve, I think it's a good question. The struggle that I referred to earlier applies to this case as well because we could make a statement such as that, but then the next question will be, well, how fast was the plane going in the analysis and what and how much fuel did it have on board. You know, it gets into -- and then you start going down a dangerous path of getting into too much information, and so the question is where you draw the line. But it's a good question. You know, I know that our folks in OPA working with our technical folks, you know, have tried to figure out what is the appropriate line, you know, between what we should make publicly available and what we should not, but it is a struggle. It is a definite fine balancing act.

Lance Rakovan, Facilitator

Any further comments? Okay. I'm going to go to the gentleman over here that has been patiently waiting for quite some time. Interested to see what he has to say.

Doug Walters, NEI

It's pretty dull, but – (Laughter.) -- I would maybe in response to your question

If you go to the NEI Website, public site, there is a little bit of information on the industry study that looked at constraints and fuel canisters. It doesn't connect the dots for you, but it will give you a sense of the scope of the study. It is just, I think, www.nei.org.

My question is regarding the future and enhancing effectiveness, and, John, you may address this in your talks. So if that's the appropriate place to answer it, that's fine.

We know that the NRC sits on a number of interagency working groups, whatever you may call them, that look at technology, and I wonder going forward if the NRC has considered a more structured approach for sharing technology with licensees and some of the insights you've gained from those groups.

Glenn Tracy, NSIR - DSP

Sure.

Doug Walters, NEI

Thank you.

Glenn Tracy, NSIR - DSP

There is a way to further enhance that. The building of those interagency technology groups is just solidifying at this point. I mean, charters have just been agreed upon, signed, and I've been sitting on several of those that (inaudible) now sit upon, and the bottom line is that the industry, the weapons industry is significantly enhancing its capability regarding remote systems and intrusion detection, assessment, communications, Web-based, wireless. I can go on and on, and the bottom line is the access to those is currently being assessed by those interagencies. And then the intent was to use the Nuclear Sector Coordinating Council and that joint effort between the Government Coordinating Council and Nuke Sector Coordinating Council to be the venue upon which we would share.

Now, as you well know, we're not going to endorse any specific product. That's the industry's business to decide what is the product, but the actual technologies that are multiplying at a rapid rate in terms of the means of affording such attacks across all of the sectors is just at the point right now of being "wow, there's a lot of technology out here. Let's get this out and see how it can be deployed in this sector." So you asked us the question. The answer is the NSCCGCC that I discussed previously.

Lance Rakovan, Facilitator

Anyone else have any comments on that one?

Roy Zimmerman, Director, NSIR

I would just add that as we would expect, there's an awful lot of enhancements in technology post 911 and looking at how to defend against various types of threats, and as Glen is indicating, we are very plugged into that, and I'll mention our new Chairman again.

From his background and what he has seen at DOD, that is a positive for us in terms of some of the things that he's aware of that he has seen from his walk of life that he's bringing forward, that we're also able to discuss in these interagency forums.

Scott Morris, NSIR, DSP

And in addition, I would -- I would offer that -- and I was going to speak directly to Dave Lochbaum's earlier comments -- but that to respond directly to yours first, Doug, and that is that the technologies that are now available, are becoming available or are being looked into, and as we expand our role in some of these interagency working groups to learn and understand how they have -- how they plan to deploy some of these systems, all of those things are going to be factored into the updated version of the NUREG that Mr. Lochbaum referred to, NUREG 1345, which is, in fact, a 26 year old document, which is, in fact, a set of design considerations that plant designers and licensees or future licensees should consider as they build security systems at their site.

That is a public document, and I know Dave has had it and has made some specific comments about it. The next version of that, however, won't be, and the reason is because of a lot of the technologies that are now becoming available and the tactics that some of the response and protective forces would use to employ, some of those new technologies, it's not something that we believe at this point should be in the public domain because then it helps the adversary plan how to counter that.

So I think, you know, again, this goes back to our continuing struggle with trying to establish and provide information and documentation that's meaningful enough to allow for public comment and ideally public -- aren't going to be able to use that to their benefit, so. And I want to also just suggest that -- I want to respond earlier to what you said, David, about our plans for the rule making for security assessments. You know, I don't share your views. I think that shouldn't come as any surprise. I don't think that we would engage in such a rule making if we didn't think it was going to be meaningful. I have far too many things on my plate personally to squander them on things I don't think are going to provide some value-added in the long run. And I think you had suggested that nothing is going to happen.

And I would tell you, and having been at the last public meeting when we discussed this rule, there was -- the industry, in advance of us even presenting the rule in the public in any kind of proposed way for public comment, the industry has already come forward and has said so in their meeting and provided us some details about what they would do to address the intent behind the rule. And I think that's very constructive, and it has moved the discussion forward, and from what I've seen in speaking directly with some of the new reactor vendors and

perspective applicants for new operating licenses, is that they are serious about it. Of course, it remains to be seen because we're not in a formal licensing process. But we're serious about new reactor designs being inherently more secure by design, that next generation that haven't, there aren't even plans for yet, I think clearly this rule is going to force some serious consideration of security at the very fundamental states of the design process. We are though kind of caught in the middle a little bit with AP1000, because it was in the design certification process when 9/11 happened and, of course, a lot of things happened in the security realm post 9/11. And it was a conscious decision on the part of this commission to license that particular design to the existing set of regulations and not what we had done by order.

However, this new rule that's being proposed is not just a design certification rule. It's also going to apply to combined operating license applicants such that if an entity were to come forward and propose or apply for a combined operating license that reference the Westinghouse AP1000 design for which you're absolutely correct, the NRC has already certified.

A couple of things still need to happen. One is when this rule gets put in place, security assessment is still going to be required, and that particular applicant, should the rule become final the way we've proposed it, is going to have demonstrate why that particular site and the design that's on that site are inherently more secure by design. So it's not a done deal just because the design cert is in the can if the rule goes forward the way it is.

Additionally, when we completed the design certification on the AP1000, since that was the plant that was referenced, there were a number of action items that we left on the table when we said this design is certified. There are bunch of what we call COL Action Items, and those COL Action Items, I can't remember the specific number, but I there were somewhere around the order of five or six in the security realm that any future applicant that references that design at a proposed new site has to address in their COL Application specifically with their security. And then the final point is when the commission provided it's guidance to the staff in licensing AP1000 in telling the staff, look, license it to the current set of regulations. The second half of the sentence was, and if anyone comes forward and applies for a combined operating license that references an AP1000, once that license is issued, we would then issue all the same orders that had been issued post 9/11 to the existing fleet.

So, I mean, again, I don't know if that moves you at all, but I just want to make sure the facts are understood by those in the audience of where we've been, but it's not to say that we can't do more to try to accommodate your issues and your concerns. And I, too, respect them. And to the extent we can do better in that regard, I mean I'm all for it. I mean I want to -- that's why we're having this meeting. That's why we have the meetings for the Security Assessment Rule Making in the public domain.

Lance Rakovan, Facilitator

I'll leave you all to determine whether you feel moved or not. I saw a number of hands come up here. Who wants to go?

Dave Lochbaum, Union of Concerned Scientists

The -- I don't know who originally prepared new Reg CR-231345, but I assume that person also didn't have an empty plan and had every intention in the world of having that effort lead to fruition, but it lead to nothing, so I'm just curious as to why or I -- I'm not curious to that -- poses an answer, but I don't see anything different today that would lead your effort to any more fruition than that past effort, which I assume was undertaken with sincerity and all the same emotions that you've spoke today. That led to nothing. I'm convinced that your effort will lead to nothing for the same reason. The track record is good intentions, no fruition, so I don't see any difference, but we'll see. Time will tell.

The fact that the commissioner ordered that the AP1000 if somebody comes in with a COL, it will have to apply to it, that just brings the reactors up to today's standard. That doesn't make them more secure. That just makes them less unsecured. So we don't give a lot of points for that one.

But turning to another subject, a lot of discussion in this session has been about public confidence, and I want to highlight an issue that, from Dan's talks, two different points, one that are completely opposite and are the basis for the public's lack of trust in this agency. They're not the only one but they're representative of that. One is your statement about if you go in and do a security inspection post 9/11, baseline or whatever, if you find a vulnerability deficient, whatever, before the NRC staff leaves, that problem is either fixed or a compensatory measure is in place to mitigate it or offset.

Right. That's for the force-on-force for any special NP. If that were true, and if the commission believed that were true, then the commission would have no qualms about posting findings on the website, because there would be no corresponding vulnerabilities that the bad guys could exploit, because they would have been addressed, either fixed or mitigated before you guys left. So the fact that the commission pulled the stuff off the website in August 2004 tells us that they don't believe that your compensatory measures are all that they're cracked up to be. So when the commission tells the American public that, why should I believe different?

Glenn Tracy, NSIR - DSP

Do you want me to take it? Well, I respect the point you're making about commensurate levels of compensatory measures. I'd just ask you to consider this comment, and that is that the day an inspector finds that, gee, that force-on-force indicated that while they may not have gotten the entire or complete target set, they certainly did damage to certain assets at the site that we would not warrant prudent or at some level of acceptability, the bottom line is that at that point, the inspector has to call back now to Dan, his staff, make an assessment, inform Roy, et cetera. Decisions are made that night about what interim compensatory measures should be made. We're going to put -- let's just do an example here.

We're going to be x armed responders that used to be at home watching TV no longer going to be there. They're going to be placed in certain locations. Interim defensive positions made to handle around to further protect the confidence level as well as the protection of that armed responder and other standoff things, and there's then a handful, quite frankly, only because it hasn't happened that often -- he gave you the statistics as Congress has -- the bottom line though is you and I, you can accept or not accept it.

The bottom line is that still, in my eyes, that day is an interim measure. The site hasn't had the time to fully think out exactly what its permanent measure should be. We have not fully thought out at that time what we will now accept as the permanent fix, especially if it's a more significant finding. And so, you know, I fully respect what you said, Dave. I want to make sure that's clear. But at the same time, an interim compensatory measure as compared to a permanent fix and the current deliberations that Roy has previously spoken to as well as myself about some months of time where you'll hear what actually happened, but we want the permanent measures in place so that there's not a spotlight on that particular site knowing that at that night, a certain Force-on-Force with a certain attack identified something.

You can consider it prudence. From our view, that's still prudent. Or otherwise, you say, go ahead, I don't accept it. You said there's interim measures there. You said you accepted those that night. One would have to admit that knowledge, even if you have an interim compensatory measure, is still not the same as the final fix to an issue that one has identified. That's true on both safety and security.

By the way, in my view, bottom line is if an inspector finds something, you expect to follow tech specs, you expect it to be operable. And the bottom line in that is that a permanent fix is often made as well to a further enhancement at the site. Your bottom line I understand though is hey, Glenn, can you say it's a safe site that night when the inspectors are now in the hotel room and the agency will state, yes, it's a secure site. There are interim compensatory measures in place. But that discussion, in our view right now, for prudence, should be that the permanent measures are put in place. I just wanted to indicate that to you.

Roy Zimmerman, Director, NSIR

A couple of other thoughts. You know, one of the things that you could come back with is Glenn just said after the permanent fix is made, and we're not coming out with a report after the permanent fix is made, we're coming out with our annual report to Congress, so as I indicated in my response to inside NRC, the agency has moved and could potentially move again as we get experience with what we've put out thus far. Don't know if we will or we won't, but to me it's an active talk like about can we go further and enhance public confidence by getting information out. We need to recognize also that the public is a large entity that the local law enforcement, they're there, they know the results. The state, in many of the cases, they're there, they know the results. So the representatives that are involved, which are members of the public, are in fact informed based on their role and their need to know.

Similarly, members of Congress get briefed on some of the detail specifics, so I recognize the interest that you all have in this area. I don't want to leave the sense that the only people that know this are the licensee and the NRC. That's not the case. The first responders, the state, the National Guard, there's a category of folks, plus those inside the beltway, that do get the information. And again, the report that we ultimately do send out annually does have a safeguards version of it that provides additional details to the elected representatives. But I still do go back that I think the concept of getting more information out to the general public is something that I would not draw a line through and say will never happen. I think it's up to let us live with what we've done for a while and see if the staff ends up making any proposals for further commission consideration.

Lance Rakovan, Facilitator

Okay. Did you guys decide who -- okay.

Paul Gunther, Nuclear Information and Resource Service

Well, really, obviously we're all concerned about the issue of getting more information out, but the old adage is action speaks louder than words I think applies here. And I can be specific because -- and I understand that you may not be able to reply specifically, but according to NRC's own documents from January of 2001 on the technical report on fuel pools and -- the issue is that specifically for the Mark I and Mark II, NRC has identified that the fuel pools are vulnerable, these elevated fuel pools are vulnerable. And yet on the surface, without seeing bricks and mortar, without changes to the Mark I Mark II, without seeing any changes to the high-density storage racks with a move to low-density open racking, without those specific actions, only to receive these superficial assurances, you're not going to move the public, you know, the -- which includes Princeton University, National Academy of Sciences, you know, on and on and on, and the Attorneys General from the State of New Jersey and Massachusetts and, you know, a growing public, that doesn't share your confidence or a trust without information or without even an avenue of engagement.

So I mean that, again, we're still at this impasse.

Roy Zimmerman, Director, NSIR

Again, I'll comment and then others may have some more details on it. On the National Academy studies, we responded to that, and I'm trying to recall whether that was a public document or whether that was a more sensitive response, and I honestly don't recall. If it was a public response, then we have at least weighed in so the public can try to form its opinion, and here's what NAS said -- we agree with much of what NAS said, but we don't agree with all of it - - so here's the issues that we don't agree with, and here's the status on the items where we do agree in terms of things that the licensees are doing, which are very appropriate reactions for the licensees to take.

Similarly, this was an issue on Capitol Hill as well where a number of briefings were done for the NRC to explain why we are in a different place than the National Academy is on certain specific items, and that vetting took place. So we've tried to play it out in as much in a public venue as we can. But we were not totally at odds with the recommendations that came out of the NAS report. There were some that we felt were not appropriate. But we respected their effort, and we aligned on a number, and we tried to explain the areas we were in a different place. Anybody else wants to --

I would also just quickly add that, you know, that this agency has done a lot of research studies over the years for a variety of different purposes, some of which were for licensing, some of them were -- you know, and different standards were applied to the assumptions that were used. You know, one only needed to look at how power reactor, you know, reactor coolant systems and emergency cooling systems have to be designed under Part 50 in relation to, you know, and the studies upon which those requirements are based compared to where we are in 2006 with looking at more risk-informed, more precise studies and understanding real reactor response to various scenarios.

And so I think the same principal is applied to when you look at studies that were done -- for example, the one you referred to, Paul, from I think it was 2000, 2001, but it, you know, that study that you referred to on spent fuel, if my memory serves was to try to deal with an issue in licensing space. There were a lot of conservatisms in that study. But then with the post 9/11 mind set thinking well, now what does this really mean, not just from a licensing where there's lots of design margin that gets factored in, but what does it really mean when you really look at what is likely to occur, how is really going to respond, requires a whole different level of sophistication, in the modeling and the engineering, and we've done that. And I think the results of those subsequent studies that have had more precision and less of the design margin sort of -- probably not saying this exactly right -- but the point is they are far more realistic studies, and they will cost a whole heck of a lot more money, but they're done for a different reason. And I think it's because of those subsequent studies that we have added confidence and perhaps why, you know, we may say one thing and stand behind a certain path or position and yet what's in a public domain may not be consistent with that. And I don't know to what extent that's playing a role in this, but I suspect it has at least some. And, Dan, you may want to add to that.

Dan Dorman, NSIR - DSO

Yes, just a couple of things relative to follow-up of the NAS study is while there has not been a move to low-density racking or movement of fuel out of the pool, there have been a number of mitigating strategies that have been put into place, relocation of how the fuel is distributed within the pool, additional cooling capabilities that have been put into place that do align with the NAS study. The NAS study suggested that based on further plant specific studies, the NRC might determine that movement of fuel out of the pools was warranted. The NRC has worked with the industry and done the plant specific studies at all of the facilities. Mitigating strategies, more cooling capability either has been or is being added in all of those circumstances taking into consideration the very severe environments that could be associated with a severe terrorist attack.

So while I acknowledge the petition that came in, the concerns that the Attorneys General has raised, and the ongoing interest that you have expressed on moving the fuel out of the pools, that has not been the conclusion of those studies, but there have been additional measures put in place. So I know that doesn't get where you want to be, but I just want to put those points on the table.

Jim Riccio, Greenpeace

You've mentioned Congress a couple of times already, and we are looking forward to working with Congress to do more legitimate oversight of this agency which is desperately needed. I don't want to pick on a particular licensee, but we do know that you have had some problems with force-on-force tests at a specific licensee. I think GAO couched it this way, that -- and you have been very circumspect in your providing information to the public. You know, like I said, we have not been getting, you know, much information from the NRC. But you have not been as circumspect apparently with the information you're providing the industry. And, at least according to GAO, you, you know, basically when you ran the force-on-force tests, they, you know, the people running it already knew the nature of the attack. They lapsed in the protection of information about plant scenarios for a mock attack, GOA observed, may have been given to

the plant security officers knowledge that allowed them to perform better on the test than they otherwise would have.

I don't even know if that refers to the plant in Texas. But, you know, GAO always pointed out problems with force-on-force. I wish you'd address at least that, if not the other specific things we know about the plant in Texas.

Dan Dorman, NSIR - DSO

Let me take up the GAO part. There have been two GAO reports, and I'm not sure of the dates. There was one in 2003 or 2004, and one in 2005 or 2006. The issue of telegraphing scenarios is one that we take very seriously in the Force-on-Force Program. It's one of the activities that the NRC evaluators are looking for - any indication that the licensee's response force have prior knowledge of the attack scenario. You've got the response force at the site; you've also got several dozen controllers who are there to control the simulation of the exercise and make sure that the key events are communicated among the controllers so that they get communicated to the players at the appropriate point for things that get simulated. And then there are a number of evaluators that are there as well, and so there is a large group of folks who know before they exercise what's going to be happening. And they are all signing trusted agent forms that acknowledge their responsibility to control that information. And then our evaluators, among the things that they're looking for is indications, that the scenario has been telegraphed in some way. So that's an area that we take very seriously.

The specific issue, you know, I won't get into the one specific plant where the issue was raised. I think there were a number of issues at that plant that related to the control of the exercise and in at least one of the evenings, as I recall, invalidated the exercise. At that particular plant, we ended up going back and redoing the Force-on-Force because of that.

The control of the scenario information prior to the exercise is an area that we do take very seriously.

Roy Zimmerman, Director, NSIR

Well, it's a Federal offense. I mean that's why you sign the trusted agent form in the very beginning of the Force-on-Force. That would be an OI investigation upon which is a significant thing to go through if you were on the side of a licensee as it would be for IG on any Federal employee. Bottom line is that I assure you, though, I've been on several of these as I know several executives have, and we want to invite others to watch, from other agencies. You name it. We invite them constantly. They are attending. We're trying to get other external insight. Dan's very much on top of that, and the truth of the matter is, though, Jim, while I don't disrespect the raising of that, I would not want the public -- and it's my responsibility to ensure -- to think that's a widespread issue of any type out there. I'm not going to counter, you know, specifically to the GAO and the specific instance. I just try to make sure I affirm to you that it is not an acceptable practice. That would be a significant report back from the inspection team, and it would result in an OI investigation with a Federal offense.

Dan Dorman, NSIR - DSO

Let me add one more thing. Jim, you mentioned the recent assertions on the South Texas Plant. One of the assertions was that the licensee had directed its adversary to basically fall down during the exercise that was observed by the NRC and FBI.

We're looking at all of the issues that came in, but we cannot discuss details here. The one thing I can tell you here is in the triennial Force-on-Force Program, the NRC-evaluated program was not at South Texas in 2005. So if that happened, it was in some sort of training exercise or something that the licensee had set up. We're looking into the aspect that it was observed by the NRC and the Bureau. We're looking at what did that refer to. But that was not one of my evaluated exercises.

Roy Zimmerman, Director, NSIR

Couple more comments. First, I want to reiterate that we do look for this and we have not seen this and that we're watching for it. I think in the GAO report, I think the words you read that maybe they thought something could have occurred. They never came to a conclusion that there really was a tip-off. But on the other hand, when I was speaking earlier about Force-on-Force and inspection programs and how they were in the implementation phase, but there are still areas for improvement.

One of those areas for improvement is with regard to the controllers. We're still dealing with that issue that the controllers really need to be on target with their calls and well trained. And we expect that the realism will continue to improve as they continue to perform their role better.

We have, you know, less concern -- we used to have concerns with the adversary force. We've been pretty pleased with the adversary force. Right now we've got our focus and attention on the controllers.

Jim Riccio, Greenpeace

Just to add. Peter Stockton is usually here from POGO, and either he's given up on you guys or he had something better to do. But, you know, I know he has repeatedly raised that issue in regards to Wackenhut. They've produced reports in terms of Wackenhut. I don't even know if it was Wackenhut. Oh, it was. Okay. So, I think we've raised this issue. We've pointed out it was going to be a problem. It has now become a problem. I trust that you, you know, want to make sure that it doesn't happen elsewhere. But given the history that the public has already had with your force-on-force tests, when you fall down on this, it just -- it gives us amazing ammunition to question what else is going on within the agency on this issue. And, again, it just doesn't put us in a place where we can feel confident that the issues that we've been raising on security for the last five years have been adequately addressed.

Rick Rasmussen, NSIR, DSP

One thing about this I'd point you to, in the 73.55 rule making which is currently available under SECY-06-126. It specifically addresses a lot of the aspects on Force-on-Force testing, the combined adversary force requirements, and the training qualification issue on the controllers. And so that's all included in that now.

Jim Riccio, Greenpeace

That doesn't change the (inaudible) --

Roy Zimmerman, Director, NSIR

Sure. Let's go with a couple of more questions. I'd like to give Mr. Tomlinson a chance to give his presentation at some point.

Paul Gunther, Nuclear Information and Resource Service

Really quick. Just to follow-up on Jim's reading from the GAO report and their cite of telegraphing. Is there currently Federal prosecutorial action as a result of this GAO finding?

PARTICIPANT

If I understood the way that was worded, it says, may. They didn't confirm that there was something there. They just --

Paul Gunther, Nuclear Information and Resource Service.

Is there an investigation or?

PARTICIPANT

There was a discussion. Dan, I don't recall the specifics, so I don't want to mislead. If we're talking about the one that was conducted in this year's or the previous?

PARTICIPANT

This year's. The current one.

PARTICIPANT

Then you would -- I don't know.

Dan Dorman, NSIR - DSO

Well, it was the most recent GAO report, but it was -- the direct answer. No, there is not a Federal investigation on this. The issue was discussed, and there was not deemed enough there to go -- to even start down that path. But let me just briefly touch the question that went back and forth there on Wackenhut. I think the answer over there was, yes, South Texas, I believe, is a Wackenhut-served site. But, I think, you then linked that to the adversary force Wackenhut. If it wasn't my exercise, then it wasn't the Wackenhut adversary force, it was the licensee's training adversary, so I just wanted to make that clarification.

Glenn Tracy, NSIR - DSP

This telegraphing matter, I just want to make sure whatever the specifics up to the '05, to give a

crisp aspect of an example where if you were witnessing these, and I wish the world could get to see it, and then not know the DBT, because then you could witness this and make comments. But for example, formal safety inspections have to be conducted, you would understand why full-out gear, full running, wet floors, something out of place, so the safety inspector for the licensee has accounted for any safety concerns. However, if the safety inspector takes a tour of the proposed route, you could telegraph where there might happen to be an attack that night. So, therefore, our inspectors are out there making sure that the safety route encompasses the entire site, and it is not -- you know, and these are the kinds of things not only do you learn, but the possibility of telegraphing is why there's an oversight team with team leads keeping an eye on exactly that matter.

Regarding a specific action like a Federal offense, if I were to tell a licensee what tonight's scenario is, that destroys hundreds of thousands of dollars of the Government and licensee's money. It invalidates the entire test. That's why it's a significant offense and obviously a criminal sanction. I do not know personally of a specific activity that has occurred.

John Tomlinson, Director's Office, NSIR

Jim, let me add one thing if I may just on balance. Obviously, you've read the entire GAO report. Those in the audience and perhaps those on the phone have not had that opportunity, but in there you'll see that the conclusion the GAO draws is that the force-on-force program is a good solid program. It needs to continue to move forward in terms particularly limiting artificialities, et cetera. But clearly, GAO, if you would accept that they're an objective organization, gave the effort -- gave the force-on-force program good marks.

Lance Rakovan, Facilitator

Was there one additional?

Jim Riccio, Greenpeace

I'll just read you what the title says. Plants have upgraded security, but the Nuclear Regulatory Commission needs to improve its process for revising the design basis threat. So --

John Tomlinson, Director's Office, NSIR

Yes, sir, you're absolutely right. That is the title, but the substance that pertains to the Force-on-Force gave them good grades. So I think, in fairness, we'd like to take credit for the efforts of those that have worked to make it successful noting that --

Jim Riccio, Greenpeace

You can take credit for any --

John Tomlinson, Director's Office, NSIR

-- there's (inaudible.) Noting that the job is never done and it's a continuous improvement, but let's take credit for what we did.

PARTICIPANT

No. Indeed.

PARTICIPANT

You know, though, that we had problems with Force-on-Force in the past.

PARTICIPANT

We did.

PARTICIPANT

Absolutely.

Jim Riccio, Greenpeace

We now have at least -- you know, GAO felt it was important enough to raise it in a GAO report. Whether or not it's been verified.

Roy Zimmerman, Director, NSIR

And we welcome it.

Jim Riccio, Greenpeace

We know they also had their problem with South Texas, so at least two instances you've had problems since the revised force-on-force, at least in the perspective GAO and in the perspective of I know at least UCS and on NC Alerts. So improvement, potentially. We don't know. We haven't been able to see. But we do know that in your improvement process, at least twice you've had problems that have gotten others who have had access to the information to raise issues.

Dan Dorman, NSIR - DSO

Yes, let me touch that briefly and say, you know, I mentioned the two GAO reports. I think the more recent GAO report paints a much more favorable picture of the program and acknowledges significant improvements in the program. I think that was the point that John was trying to bring across, and the other point that I would just go back to, Jim. As you said, you've got two data points. You've got the GAO report. You've got South Texas. And I would just reiterate that the comment on South Texas was specific to 2005, and I wasn't there in 2005. So whatever happened there in 2005, which we're looking into, wasn't on our program.

Roy Zimmerman, Director, NSIR

Any further comments on this before we go to Mr. Tomlinson?

Okay, John, you're on.

Lance Rakovan, Facilitator

Okay, John, if you want to take things. It looks to me like you're going to be talking about related security topics.

John Tomlinson, Director's Office, NSIR

Here we go. Good morning. When the staff within the Office of Nuclear Security sat down, they saw obviously program areas that were covered by (inaudible). But we also identified some areas that didn't fit into a particular bin. But we thought they were worthy of being noted to those in the audience and the viewing audience as well as those on the phone.

We also recognize that different people in an audience have different levels of involvement with NRC activities. So while we certainly want to challenge those folks that interface with us more often, we want to make sure that we bring those folks that perhaps don't have the inclination to engage as often, along with us. So for that reason, we're trying to be inclusive here versus exclusive.

So the first topic that we wanted to just touch on is the Energy Policy Act that was, for those of you that follow NRC activities understand, passed in 2005. One of the tenets in the sections that were addressed in that, there is, if you look at the entire Act, there are about 28 or 30 sections that have some nexus to security, either directly or indirectly, counting subsections, of course. About half of those relate to security activities. So I would offer to you that Congress has a focus on nuclear security as well as on the other pieces of the Act.

One of the issues, one of the first items in there is the DBT. Clearly that included basically every form involved with DBT, whether it's enforcing it, whether it's implementing it or whether it's continuing to challenge the precepts of it.

But in that particular act, it identifies 12 factors and requires comments on each, and requires the commission to consider each of those 12. Now again, those of you -- bear with me those of you that commonly know this -- can read it from memory, I'm going to have to resort to the page, but those factors that are being considered would be the events of 9/11, cyber, biochemical and physical threats, attacks on facilities, plural, by multiple teams, water craft-based attacks, insiders, suicide attacks, large explosive devices, modern weaponry, insider with sophisticated knowledge of plant operations, the potential for fires, specifically long duration, attacks on spent fuel shipments, adequacy of planning to protect health and safety, and last, but clearly not least, is theft or diversion from such facilities.

So those are the 12 items that the NSIR folks, which are involved in the rule making, have taken on board together with colleagues from the other offices here in the NRC. And as understood, they have received 919 comments on those particular 12 factors. The other folks that clearly have a better skill set in terms of rule making can perhaps address any of those that come to memory. Some have already been raised here this morning. But that's the first example that we wanted to raise. The other one, again, in this legislation is, I term it enhanced weaponry. And when you say, you know, is there a need to enhance weaponry, what are we doing today? We want to make sure that we don't leave anybody in the audience with the perception that our personnel are outgunned. The men and women that stand watch at these facilities have weapons and have a defense in depth that can withstand attacks.

Given that, we don't want to play to today's level. Adversaries, as you read in the newspapers as well as I, adversaries are always getting the potential, always trying to plan how to advance their cause, advance their tactics. So we want to make sure that as they leverage technology in their behalf, we leverage it in likewise fashion on our side of the fence so to speak. So the legislation specifically talked about the ability to have the commission identify advanced weapons given a variety of considerations that the commission will take on board.

Since last year, we've been in constant dialogue with our friends from Alcohol, Tobacco, Firearms and Explosives, our friends at the Department of Justice as well as our friends at the FBI trying to craft some guidelines that are being written by the Nuclear Regulatory Commission that will ultimately have to be approved by the Attorney General's office. Those guidelines will form the framework under which we can pursue the next step in terms of acquiring other weapons in a responsible way.

Inherent in that is a couple of issues. Number one, this has never been done before, so our friends at those external agencies as well as here within the Office of General Counsel are faced with a brand new issue. You may know from personal knowledge that there are individuals who work for private contractors, for instance using Department of Energy as example, who protect facilities. But they protect Government facilities. So this is the first time this legislation impacts private security entity protecting a private facility. So it's new virgin territory. It's new ground. So it's incumbent that we get it right, because we're going to be setting a precedent for what's going to happen down the road so to speak.

So that dialogue continues. There have been iterations back and forth between DOJ and Office of General Counsel here. We're making progress. Are we doing it as quickly as we'd like? Absolutely not. But everybody is making a solid effort to advance the ball. So while we're trying to be patient with ourselves as well as our partners here, it's taking a while to move forward. But we're certainly encouraged. We haven't been discouraged since the first meeting. And we're going to see some results here that folks will be satisfied.

Related to that, the Federal Security Coordinator -- let me just change it a little bit in the interest of time here so we can have some discussion here afterward perhaps -- Federal Security Coordinator, the legislation requires us to put one in place at each of the four Regions. Those individuals have been named.

The process is underway where their specific jobs and job details are being delineated. The idea is for those individuals in there, as we term them here, backups, or their seconds, their lieutenants, whatever term you choose, have an opportunity to interface with licensees, not just at nuclear power plants but other licensees. And at the same time, we have an opportunity to work with State, Federal and local law enforcement and emergency preparedness individuals so that we have a consolidated approach with a focus on both security and emergency preparedness.

Subsequent to this legislation being passed, there was another player so to speak that came on to the scene. Those individuals are called Protective Security Advisors. They're individuals who in the neighborhood of 60 or 65 have been hired. They come to the DHS family with a variety of security backgrounds, military, local law enforcement, Federal law enforcement, and it's their role to act as an interface between State, local, and Federal entities and DHS to make

sure that the avenues of communication are as open as they can be in terms of what's being shared. So we see these, PSAs as they're now known, as adding to the efforts in the four regions as well as they've been adding to efforts in comprehensive reviews and other activities that the NRC participates in. I think as those PSAs get their legs under them -- a lot of them come from organizations with a premium on liaison -- so as they get their legs under them, they're going to establish their own constituencies up there in the various regions. And I think it's going to be a plus.

The other piece is that they're accountable to the Department of Homeland Security, advice, directly accountable to gubernatorial offices. So it gives DHS much more control. DHS is signing the check, and they've got to report back through the DHS piece.

Roy Zimmerman, Director, NSIR

Let me stop you just for a second.

John Tomlinson, Director's Office, NSIR

Yes.

Roy Zimmerman, Director, NSIR

As I think back on the meeting, one area that I'm not sure that we really stressed enough -- we covered it quickly -- but it's the amount of time and effort that we have spent with DHS working on this comprehensive review to get the grant funds out to the areas where there is enhancements that can be made, but this money is going to go directly to work on those areas. That's been a significant initiative of ours with DHS since we last met. And it's coming to fruition.

I just wanted to make sure -- we only had a little bit of dialogue on it, but that's an important part, to make sure that the first responders have what they need when they get there. There's talk about well, they'll never come into play, the firefight will be over so fast that, you know, they'll never be seen. I know in one of the force-on-forces that I attended, they definitely would have gotten there, because the firefight went on for a long, long time. They had them pinned down. It went on for 45 minutes or more. But we keep track. In our force-on-force, we keep track of all the times so that we're able to indicate how long it takes from when the adversaries are seen until the firefighters' firefight is over. So we're tracking that type of information as well.

John Tomlinson, Director's Office, NSIR

The next action that we wanted to touch on -- and, again, these are examples. Obviously, it's not meant to be all inclusive of what the Energy Policy Act brings to bear.

The next one is the fingerprinting requirement. As most of you are aware, those with unescorted access are required to provide fingerprints, which serves as a tool to confirm their identity as well as confirm any criminal history. This particular section advances the ball significantly, because it requires those individuals -- it requires licensees and certificate holders, but it also talks to entities who are filing either category of application to provide fingerprints. It

goes a step beyond and says once these categories of applicant make aware or inform the NRC of their intent to file an application; they're required to start the process for providing those fingerprints.

So what's the -- you know, what's the use? What's the deal? The deal is that it's important to identify somebody early on in the process, and if there is anything to be concerned about, if there is anything to be reconciled, we have it well in advance so that person or those individuals don't have an opportunity to interface in activities that could be problematic or criminal. So, again, it's a step forward.

This particular section also applies to individuals who have access to SGI unless they're exempted. Now I know there are comments here that the rule has already been filed. So my interest here is just noting in terms of truth in advertising. There's two different pieces to the particular fingerprinting or environment enhancement.

The next two sections are basically very similar in terms of their intent. For the first time, the introduction of weapons or explosive provision was incorporated. That's not to say that the FBI, who has primary jurisdiction for investigating acts of terrorism -- that's not to say that somebody bringing in those instruments or bringing those explosives into a facility would not be chargeable.

But the Congress wanted to make sure that there would be no consideration otherwise, giving us the tool and giving the Federal government, Federal law enforcement the tool to prosecute under a specific section.

The same principal applies to sabotage of facilities. Clearly, sabotage of facilities but also it goes on to materials and property. So clearly, it gives the FBI specific jurisdiction, specific piece of legal material that they can pursue. Again, that's not to say that in either circumstance, state and local as well as other Federal statutes couldn't be brought to bear on these particular offenses. So the rule making will start on implementing these two pieces as it relates to the NRC.

The last one is consultation that Glenn Tracy certainly covered very well, as he always does, but the one piece that I just wanted to kind of drive home is as you read this, it doesn't say anything beyond the term "consultation." Now our General Counsel is working, as it was mentioned, with our office as well as counterparts in DHS to come up with the protocols as to the advancement here. In no way is this going to be a paper exercise, so for anyone who has that opinion, I think they'll fall short.

So we're aggressively and professionally working with DHS. DHS also has stakeholders that they need to satisfy on this, so it's kind of a mutual arrangement that this thing needs to work for everybody to come away a winner, and it should. We all have communities. We all have organizations that we take our respective (pie) in. So those particular pieces are going to be a step forward.

Let me just take a break here. As it relates to the legislation, I may not have the answer, but there may be some folks here that do, so the (plants), if we could just ask any questions just regarding those slides that I could amplify or give it to somebody smart to answer.

Lance Rakovan, Facilitator
Anyone want to respond to –

Dave Lochbaum, Union of Concerned Scientists
It's not so much on that slide, but it was on Roy's inject.

I just had a question on the time lines you said during those exercises. Is it when the security event -- the notification goes out, or is it the six weeks or six months before when these local law enforcement and all the other responders are notified that the drill is occurring? What starts that clock?

John Tomlinson, Director's Office, NSIR

I understand your point and, again, there's -- as you know, we're very focused also on personnel safety and the logistics to be able to make this go correctly, so there's a weighing that's done. We give much less advance notice now than we did pre-9/11, and as time moves on, if we're able to satisfy ourselves that we can cut it back further, then we will. But we don't want anyone getting killed out there. So I understand your point. It's one of those artificialities. It's not a minor artificiality, but having somebody shot is something that has occurred on force-on-force. We don't want it to happen in one that we're involved with.

Dan Dorman, NSIR - DSO
Not in ours.

John Tomlinson, Director's Office, NSIR

Yes, right. But it has -- well, I thought I added that with a sentence -- one of ours.

Jim Riccio, Greenpeace

Yes, John, I have no question you guys are working hard to try to meet the bar. We have a question whether the bar's high enough. We are placed in a very uncomfortable position of not knowing what's actually in the DBT rule, which members of the media have been very pointedly asking your Commissioners, you know, how you can comment on something you can't see, but we don't get to that. I just -- a couple of things you said. You said it's going to include advanced weaponry, and you said it's going to include the events of 9/11. Now, for those members of the public who watched the planes impact the building, we take that to mean airliner impact. When I read in the British analysis of what is going to be done, I read from NEI that you're not going to include advanced weaponry and your not going to look into an airliner impact, I think NEI has better information than I do, I want to know is NEI just wrong or we have different definitions here.

John Tomlinson, Director's Office, NSIR

Sure. Jim, let me go back. Those 12 items as per the statute, yes, those 12 items are to -- actually, they call them factors in the legislation, are to be considered, and the Congress --

that's not my term, that's the congressional term, "considered" -- that doesn't say that any of the 12 would necessarily be included in the new product. Clearly, you know that, you don't have to be in SGI space to know that there is going to be inclusion of items within that list of 12. But if I misled you, it was clearly inadvertent.

Jim Riccio, Greenpeace

There's a juxtaposition between what you're telling us and what's in the rule and what NEI has told the British, and I'm just trying to determine where the reality lies. You know, you were very up front in saying that, you know, we're not going to be outgunned, but I wasn't quite worried about that they would have a better machine gun than our guys with pistols. I was more concerned about advanced weaponry that might be used to take the facility without getting too specific.

John Tomlinson, Director's Office, NSIR

Understood. And those are being and have been considered, each of those 12 factors. Clearly, one of those, I think the term is modern weaponry, is among the 12.

Paul Gunther, Nuclear Information and Resource Service

You know, according to Congressional testimony before Shea's subcommittee, part of that modern weaponry was referenced in testimony as rocket propelled grenades and 50-caliber rifles, yet as the GAO reported, it seems that this level of modern weaponry is not being considered. And, again, that speaks to, you know, is the bar appropriate, particularly when we're faced with this in modern warfare on the fronts that we're engaged in today. But the other -- you know, again, this whole issue of considering is very vague and disturbing.

You've been asked to consider fires of long duration, and in fact the agency has been considering enforcement issues about fire protection since 1980. And we, the agency and the industry, are still at an impasse today with regard to protecting say shutdown capability through enforcement of Appendix RG-32. So, you know, it seems like the public has to see more than just consideration that can go ad infinitum and see some action.

John Tomlinson, Director's Office, NSIR

I would just suggest to you Mr. Gunter that the term consideration was something that was given to us by the Congress versus the NRC saying what it should be. I would also say that while, you know, you and others here that have the right skill sets might disagree with the outcome, I would tell you that the approach to each of these 12 has been professional. If it wasn't professional, I wouldn't be in the organization.

So while the end result might not be what you would like, clearly it might not even be what I like, as long as it's done professionally, in a professional way, then I think we owe some respect to the process. If the language, if the Congress decides to change that language, then clearly they're not bashful about dictating other language to us. But I think, John speaking, not the NRC, John speaking, that they had some respect for the NRC and for its ability to do those analyses that have been done or are in the process of being done. That may not be the answer

you're looking for, but that's heartfelt.

Paul Gunther, Nuclear Information and Resource Service

Well, again, it was the professional assessment of NRC staff to include RPG and 50-caliber, you know, armor piercing incendiary munition, and it appears to have been a financial decision that eliminated that from the DBT.

John Tomlinson, Director's Office, NSIR

I think you can respect that it wouldn't be prudent on our part to say what is or what isn't in the DBT.

PARTICIPANT

That's correct.

John Tomlinson, Director's Office, NSIR

It just doesn't make sense, because while we certainly respect you and your intentions as well as those other folks here, that same information would be available to adversaries who could exploit it, so I understand your interest in knowing, but I'm not going to go either way on it.

Paul Gunther, Nuclear Information and Resource Service

It speaks more to the issue of professional input versus financial considerations.

John Tomlinson, Director's Office, NSIR

Yes, sir, I take your point. I understand what you're saying.

Eric Leeds, NSIR - DPR

Paul, you talked fires a little bit through the morning, and I think you've gone back to some other operational safety issues with regard to fire analysis, but I'm pretty confident that you're aware that post-9/11, licensees are required to be able to deal with large fires and explosions. So I think you're trying to tie those two together, but licensees need to be able to deal with large fires and explosions.

Glenn Tracy, NSIR - DSP

Can I speak to that?

John Tomlinson, Director's Office, NSIR

Sure.

Paul Gunther, Nuclear Information and Resource Service

(Inaudible) -- issued in 1998 to have substituted without NRC approval and largely without analysis actions that are legal, namely operator manual action, which don't consider the issue that these are security infrastructures, and so, I mean saying one thing and doing another are in stark contrast right now. And, you know, it seems again that we've -- you know, if the agency wants to get beyond this lack of trust that it has the ability, it has the authority to move into enforcement action. And if you can demonstrate that you in fact have the willingness to enforce your own regulations, then we can begin to take steps towards real security and building public confidence.

Glenn Tracy, NSIR - DSP

Got your comment. Thank you. Mr. Gunter, let me offer one thing that Vonna Ordaz was good enough to pass to me. We owed the Congress a report on EPA-05 which was delivered and is in the public domain. Her recollection is that includes a better sense of how we're attacking "considering," so I might make reference to that if you have an opportunity in the public forum. I'm not saying that's going to win the day, but at least in terms of truth in advertising here, it's at least a step to either confirm what you're arguing or perhaps mitigate it.

Vonna Ordaz, NSIR - DSP

And more broadly, it's my understanding we're reporting back to Congress on how we're proceeding with all the items within the EPA-05.

Roy Zimmerman, Director, NSIR

Although, John, I had one final slide and it's in your package, I think our sense is that the next five minutes is best left for topics that you all want to raise to us that you haven't already touched on. What we have done is we have taken down the comments -- we didn't maintain the parking lot of the issues, but I've got probably a dozen items here, points that you raised that I want us to respond back to you on that in our minutes and on our website, we'll respond to these points including, Paul, the one you just raised, but we've been taking them through the morning. So I'm pretty confident that between us, we have those issues that you've raised covered that we can respond to even though we didn't put them up on the board. But other areas where we haven't gone or other topics you want to punctuate or anybody else that hasn't spoken or would like to speak, try to use our last few minutes for a wrap up.

Lance Rakovan, Facilitator

And that includes people on the phone.

Roy Zimmerman, Director, NSIR

Thank you.

Mr. Bione. Al Bione (phonetic) with Paralex (phonetic)

On the slide we were last discussing, it talks about the new reactor NRC consultation, and Scott

had earlier talked about how in the design certifications, there were some action items associated with security provisions that are to be determined. The question I have has to do with regulatory certain aspect and not knowing any of the details associated with future security changes, modifications, and so on, could you talk for a minute about to what degree future security related design changes may have impact on the regulatory certain issue.

Glenn Tracy, NSIR - DSP

Let's see. To repeat back -- What future a new reactor will have on design changes. Is that what the basic question is? Well --

Mr. Bione

To the degree you have a certified design and there are action items.

Glenn Tracy, NSIR - DSP

Okay, so you've the certified design.

Mr. Bione

Those are clear, because they're written. To the degree there's some future consideration. As Scott discussed, the COL, there will be additional site specific review.

Glenn Tracy, NSIR - DSP

Correct. Those have been delineated as Scott articulated.

Mr. Bione

I'm just trying to appreciate the degree to which a licensee can appreciate today what that might be vis-a'-vis a licensee might be surprised by changes or new considerations brought up at a later date, possibly subsequent to decisions to build.

Glenn Tracy, NSIR - DSP

Okay. Let me take a stab at it and allow Roy to calibrate it as well as my own staff. But a Commission can make a decision on policy at any point in time, overriding global obvious. Okay? The bottom line is design certifications have been made at this point. The COL process of specific aspects of security are delineated in specific applications that were certified.

You've already understood that, as Scott has said, there will be a requirement for a security assessment and a proposed rule. Again, proposed rule. Those decisions are going to be voted upon, so we can't make policy at this table. Only the Commissioners can and will, and those assessments are to ensure that the designs of the future -- I'm sorry to be redundant, but I want to repeat it so you can -- are in fact incorporating the design in order to further enhance their ability to promote security. And so there is going to be a time period upon which policy makers are going to be not only discussing these aspects, I think it opened even with even

Commissioner Jaczko's remarks on 73.62. And then ultimately the guidance that we received in terms of those assessments and how much operational programs, the current fleet and how not only design changes were made, you could go to the fleet and see that, but how they're going to be mandated for the design as compared to operational programs. And I think Roy hinted at, and I'm going to allow him to summarize my statement, is that as your designing the new fleet and whatever design is chosen, whether it's a certified or not yet certified design, there's going to be elements of the future where designs are going to incorporate this immediately, you know, or at some point in time, and others are going to have operational programs that will be acceptable.

And if you're talking about again AP1000 that's been bantered out tremendously in this meeting, the bottom line is they have to meet COL, or they have to meet the orders that were delineated. And future policy decisions associated with the rule makings before us will determine how the security assessments show that they will in fact meet the design basis threat that is imposed as well as aspects of B5B or shall I say mitigative measures for large fires and explosions. Scott, could you clarify anything and then give it to Roy?

Scott Morris, NSIR, DSP

Let me try to understand the question. Is the question really come down to the NRC has certified the design, but are we -- I think your question is, are we planning to not uncertify it, but, add things to it at some point in the future? You're looking at regulatory stability in the design? Is that basically your question?

Mr. Bione

Yes, that's my question.

Scott Morris, NSIR, DSP

Okay. Just a brief history lesson, and this won't take but 15 seconds. When AP1000 was in-house and 9/11 happened and we started issuing orders, we provided the vendor the latest iteration of the design basis threat. And when they -- the target they were aiming at when they made that design was what they perceived the previous design basis threat. Okay?

Well, then they looked at the new one and said, we're not going to address that in our current design, we're going to leave that to the COL applicant, this Combined Operating License, not to say that it's never going to have to be addressed. It's just business decision, whatever, and commission policy licensed the existing set of regulations and then issue orders at a later point, that's how it occurred.

So the Deltas, things that they thought were going to be captured that suddenly weren't going to be able to be handled appropriately once they saw the revision to the design basis threat, rather than -- I mean I'm putting words in their mouth and I don't mean to do that, because I wasn't directly associated with that design, but it's my understanding that there were a couple of things.

They said, you know what, good issues. The COL applicant's going to have to address that.

And that we've captured those. They're available. I believe they're in the public record. And so those things, before just one of those designs is ever actually built and operated in this country, those issues are going to have to be resolved.

Now, whether they get resolved in the design itself –

PARTICIPANT

Exactly. This is the –

Scott Morris, NSIR, DSP

-- or in how that design is ultimately employed on a real piece of property and its proximity and, you know, other barriers that may be applied, really the issue comes down to does one go back and address the concerns through the specific concrete and steel and typing arrangements that's in the certified design or does it get dealt with the addition of additional barriers, guns, guards, or other means. And so that's -- if your question is what is the regulatory -- I mean is it a certified design and is always going to be the way you certified it, that's up to the COL applicants to decide how they want to deal with that issue. But our standard is the same. That, whatever ultimately gets licensed has to be able to -- there has to be a demonstration at that site -- that licensee, that new site has to be able to defend against the design basis threat with high assurance, otherwise it doesn't get an operating license.

Mr. Bione

That answers my question. Thanks for that background.

Scott Morris, NSIR, DSP

Okay.

Jim Riccio, Greenpeace

Just one thing. My understanding of the SECY paper on that was that you wanted the industry to consider security at the design phase. So if you're going to consider it and then not require that anything be done, that's just, you know, what basically we come to expect of the agency. But that's irrelevant at this point. I want to go back to the point also –

Scott Morris, NSIR, DSP

Well, I don't know, Jim. I mean let's stop, because you just made an important point.

Jim Riccio, Greenpeace

Well, this is going to get to it.

Scott Morris, NSIR, DSP

Okay.

Jim Riccio, Greenpeace

Your Dense Reactor Policy Statement says up front, thou shalt be less resistant to a meltdown or safer, however you want to couch it. Your Security Statement says you're going to be more secure. Are you going to be allowed to take credit for the design in saying you're more secure as well? Again, my question is the new design going to mask things you could improve upon (inaudible) the reactor design itself supposedly is an improvement?

Scott Morris, NSIR, DSP

If the new design makes for a much more complicated target set, and you've got thicker walls and things of that nature, to me it would be appropriate to give an appropriate consideration for those design enhancements. We feel that's the best way to go about it.

Jim Riccio, Greenpeace

I'm not -- Maybe I have to explain. I mean, yes, I hope you would do that on the security side. Are you taking credit for like a lesser core damage probability is what I'm asking at the front end to say the plant is more secure now?

Glenn Tracy, NSIR - DSP

No. The concepts and the rules that are before you and will be before you are still relying on the concept of target sets in the same construct that we have in our regulatory regime that we talked about for two hours here. What I want to make sure you understand though is that let's make sure we're not misaligned, because I'd like to hear you say otherwise if we are.

We are hoping that future designs, and much to your comment not relevant, it is extremely relevant on the ones that have certified designs right now, because that's your point. Well, there's this issue here that we have to, you know, have on the table associated with has that design been informed by the commission's intent by 73.62 that even Commissioner Jaczko wrote up, and that is that we hope the designs are going to be inherently more secure, and therefore the adversaries, whatever number there are, are going to have a more difficult time getting to target sets in order to cause a core melt scenario. Probabilities are not a part of that.

Scott Morris, NSIR, DSP

Well, let me try at this. And I want to try to take this out of the abstract, because it makes it harder to understand. But let's just -- I mean every -- the design basis threat makes reference to vehicle born explosives, vehicle bombs. It's no secret. That's in our rule. So in the case of AP1000 for example, you know, they made an assumption that the size of the explosive or that bomb would be some number, and I'm not obviously going to say what it is, so that this -- the placement of various safety-related components for a safe shutdown and a long-term cooling of that facility would be located within the facility in a way that it would be resistant to that size explosive either because the concrete and steel was, you know, resistant enough or because of

the placement or the redundancy of the systems or the fact that they were passive in nature or not active. Then we tried out a bigger bomb or a different size bomb, and they say, hadn't considered that; we're not going to change our design now; we're in the middle of the process.

We recognize that anybody who ever builds one of these is going to have to deal with that issue. Okay? So the issue is not lost. The question then becomes when the applicant shows up and says I want to build an AP1000, and we say well, how are you going to deal with this threat, the question is, the decision that has to be made at that point is are they going to change the design, or are they going to put greater standoff distance between external vehicle barriers or whatever it is. But we're not going to prescribe what that is. We're going to say here's the threat, you got to deal with it and explain to us and give us high assurance that your design ultimately will be able to deal with it, and then we'll come visit you, and inspections, and force-on-force, et cetera. So hopefully that helps explain the nature of what occurred with AP1000.

Roy Zimmerman, Director, NSIR

The only other thing I want to add is -- I want to go back to what I said before on aircraft that there is a certified design, but we learned a lot and enhanced safety working with the industry based on the results of those studies. We haven't done those studies on the next fleet, and that's something that is under consideration, that the NRC is thinking to do to see if we can have the same benefit that we gained for the operating fleet.

Glenn Tracy, NSIR - DSP

Okay. Before we end this conversation, I want to go to the phones really quick, because I've been told that we might lose the phone line fairly soon since we're over our allotted time and just make sure that nobody there has any questions.

Brian Miller, Progress Energy

I have no questions, Glenn.

Lance Rakovan, Facilitator

Speak now or forever hold your peace. Okay. Moving on.

Dave Lochbaum, Union of Concerned Scientists

The problem I'm struggling with, Scott, is that approach seems to provide equivalent to today's reactors, because it's bigger bomb that today's reactors have to (inaudible). You're looking at the AP1000 and future reactors, so the Policy Statement says more secure, and what you continue to outline says equal –

Scott Morris, NSIR, DSP

Yes. I'm glad you brought that up. In fact, I meant to address this early, and I just forgot. And the Policy Statement, you're correct. It says inherently more secure through the design. The

way -- What the commission intended, and this is something that we wrestled internally, because that does seem ambiguous when you look at how perhaps you've heard it discussed today -- the best way I can explain it to folks -- the commission was also very clear that future generations will still be held to the same standard, i.e., the design basis threat. So the commission was very clear. New reactor designs don't have to deal -- there won't be a different design basis threat for new reactors. The design basis threat is what it is. It applies to the operating fleet as well as to any applications for future designs. So given that and the expectation in the Policy statement to which you referred, the best way I can explain it, and I, again, we've struggled -- I've struggled to explain it to folks internally and externally. If this piece of paper were the design basis threat, this box that's represented by this sheet of paper were representative of every one of the characteristics and attributes that comprised the existing DBT, what the commission is asking that there is a certain percentage of that box that can be addressed by the physical and design and layout of the facility. The rest have to be accommodated by operational security programs: guns, guards, barriers, you name it.

Dave Lochbaum, Union of Concerned Scientists

Potentially human errors being removed?

Scott Morris, NSIR, DSP

Right. And so what they're now saying is that we expect that a larger percentage of this box beyond what is currently in the case at the operating fleet is accommodated to the physical design and construction of the facility. The box size itself doesn't change. It's just the percentage of the box that gets accommodated by the design to handle security. The expectation is that goes up.

Now the next question is well, how in the heck do you do that? And that's what all the guidance documents that we're working through and the process, consideration of the industries' proposals, et cetera. And, you know, we haven't even put the rule up for public comment yet officially, but that'll be up.

And we intend to have many more public meetings and discussions to get to the end point on that. But I hope that answers the questions. It's not that we're changing the DBT and making it more secure, just the percentage of the DBT that gets accommodated by design.

Paul Gunther, Nuclear Information and Resource Service

You would think that would accommodate bunkering and enhanced fire protection for safe shutdown, but are we going to see that?

Scott Morris, NSIR, DSP

Well, I think, you know, Paul, it's a good question. And I think that the strategies, the processes, the guidance that we're developing in support of this new rule needs to consider those things. So to that extent, I'm glad you raised it. Because the fire protection piece wasn't right directly on my radar screen, but, you know, certainly the advanced weapons were.

But, yes. The answer is yes. It needs to be factored in and it will be factored in. You know, again, I don't know how to pinpoint exactly how at this point, because it just hasn't been a discussion element up until now.

Roy Zimmerman, Director, NSIR

I think it was a good explanation you gave, Scott. I want to give another opportunity to see if there are any remaining questions. Otherwise, I'm going to do a quick wrap up. Jack Goldberg.

Jack Goldberg from the Office of General Counsel

I just want to put in context a lot of the discussion that's taken place today in connection with ongoing rule makings, and in particular the design basis threat rule making. It's been a good exchange. A lot of useful information and viewpoints expressed, but in those discussions, a lot of imprecise statements and mischaracterizations which I don't want to leave unaddressed.

We are in the midst of a rule making. In particular, for example, the design basis threat rule making. A proposed rule was published for comment. Comments have come in, close to 1000 comments. They're being evaluated. The Energy Policy Act requires the commission to consider 12 factors. Consideration of those 12 factors is ongoing.

A lot of statements have been made that suggest people know or organizations know what the final design basis threat is going to be. Those are incorrect. NEI does not know what the final design basis threat is going to be. Roy Zimmerman does not know. No one in this room knows.

Roy Zimmerman, Director, NSIR

Thank you, Jack.

Jack Goldberg, OGC

Because the staff has yet to make a proposal to the Commission, and the Commission will decide what the final design basis threat will be, it may include one or more or all of the 12 factors that the Congress directed the commission to consider. But we don't know yet. The staff has to make a recommendation, and the commission has to make a decision.

When we talk about the DBT, we can talk about the DBT in its entirety in the public context, because the current DBT is in the regulations in 73.1. The revised DBT will be in the regulations. There is nothing secret about the DBT. It's a public statement of what the licensee must defend against by high assurance as provided by 73.55.

There are things associated with the DBT that are not able to be discussed in public. Those are a level of detail which are safeguards information for the power reactors and classified for the Category 1 facilities. Those are things which have been called adversary characteristics, and when you get to that level of detail, there cannot be a specific detail public discussion because of the sensitive nature and the classification or safeguards information categorization

for those details.

But the DBT is public. We're in ongoing rulemaking. There is consideration being given to all 12 factors in the Energy Policy Act. And every comment that has been submitted by any member of the public, they will all be considered and addressed appropriately in the final rule. I just want to make sure that everyone understands the context. Okay? People may believe they know or suspect or have a hunch or make a prediction, but no one knows. I don't know. No one in this room knows, because it's not yet been determined.

Lance Rakovan, Facilitator

Thank you, Jack. Any other comments before we go to Roy for closing?

Roy Zimmerman, Director, NSIR

Okay. A few comments that I'd like to share and then we'll wrap up. To repeat what I indicated before, I think we have good notes. And you should see your notes up here in our minutes. We'll look at what we can do with the website. Things that you don't see, that you raised, that you want to put on our screen, work with us. Give us the feedback so that we can have an accurate record of those items.

I'm not sure you maintained time, but you did maintain distance and shielding in this meeting. But you did engage with us, and I thank you for that, as you have in past years. You gave thought to your comments and you constructively provided those to us, and we've done our best to capture those. And in areas where we felt perhaps we could clarify, we tried. In some cases, it may have helped. In others, perhaps not.

We tried to provide a lot of information to you as we have in past sessions. And hopefully you heard some things today that you haven't heard before. And the lines of communication are important to us. So we want to continue to have opportunities to meet with you. We can think about frequency change. We can think about how we can make these meetings better. We're open for, but what we don't want to do is shut down communications. That's something that we very much don't want to do. And I iterated a number of times that I recognize the frustration, not just in this meeting but in other meetings, that you want the information, you want the information. There are efforts where we've been trying to move in that direction in small steps, and we've made some headway since the last meeting. And we tried -- I tried to articulate the fact that I recognize that you all may not have gotten that information and told you something you already know, that there are other representatives of the populous that are getting the information and interacting with us and asking us the tough questions. And if they're not satisfied, they let us know. And if they are satisfied, we move on. And, you know, NAS was one of those examples.

The last area I want to go if you'll just indulge me for just a moment. I do want to recognize Glenn Tracy. Glenn Tracy is a tireless Federal manager, leader that I believe you all, through all your interactions you've had, may not agree in every point, but I believe you would agree with me about the work ethic that Glenn has brought to the job. He is a man of action. He is a man of decisions. There were many actions and decisions that were made before NSIR was ever created that Glenn was in the middle of. And he has put in amazing hours and has served

the public extremely well. And I want to thank him for everything that he's done.

(APPLAUSE)

Roy Zimmerman, Director, NSIR

We wish him well, and at our next meeting at the Regulatory Information Conference, Trish Holahan, we will welcome you to the group. Thanks very much. Thanks for your patience. It was, you know, a long morning, and we appreciate it. Have a good day.

(Whereupon, the foregoing meeting was concluded.)