UNITED STATES NUCLEAR REGULATORY COMMISSION

BRIEFING ON OFFICE OF NUCLEAR SECURITY AND INCIDENT RESPONSE – PRORAMS, PERFORMANCE, AND FUTURE PLANS

+ + + + +

MONDAY

January 12, 2010

+ + + + +

The Commission convened at 9:30 a.m., the Honorable GREGORY B. JACZKO, Chairman presiding.

NUCLEAR REGULATORY COMMISSION

GREGORY B. JACZKO, CHAIRMAN

DALE E. KLEIN, COMMISSIONER

KRISTINE L. SVINICKI, COMMISSIONER

NRC STAFF

WILLIAM BORCHARDT, Executive Director for Operations

JIM WIGGINS, NSIR

VIRIGINA HUTH, NSIR

PATRICIA HOLAHAN, NSIR

KATHRYN GREENE, ADM

RICH CORREIA, NSIR

CHRIS MILLER, NSIR

\

P R O C E E D I N G S

CHAIRMAN JACZKO: Today the Commission will meet to receive its annual program briefing from the Office of Nuclear Security and Incidence Response, NSIR as we formerly know it.

NSIR's program responsibilities are vital to the safety and security of our nuclear facilities. Their responsibilities include providing security oversight of all the NRC regulated facilities, the development of emergency preparedness policies, and the coordination of our response to security incidents with law enforcement, intelligence agencies and other regulatory agencies.

In order to fulfill its security mission, the NRC has worked actively in recent years to tailor its policies to the potential threats facing our licensees. New security requirements instituted since the 9-11 attacks include increasing the number of security forces on-site, requiring greater training and qualifications for those personnel, strengthening the design basis threat, enhancing our force-on-force exercises, increasing cyber security protections and integrating response training with Federal, state and local agencies.

NRC has also made significant improvements to its incident response and emergency preparedness programs. The

agency is working on finalizing a proposed rulemaking for emergency preparedness. And we heard earlier this year from staff on that rulemaking.

These efforts reflect how seriously the agency takes its security incident response and emergency preparedness missions. The hard work and expertise of the NSIR staff and stakeholders in developing these policies and the diligence of their licensees in meeting their new responsibilities in these areas.

I would also like to acknowledge the hard work that's done on this side of the table and the dedication of my colleagues on these fronts. Certainly when I came to the Commission, a tremendous amount of work had been done by the Commission to respond to the incidents following 9-11. There is a lot of work that still goes on today.

Commissioner Svinicki has helped keep the Commission focused on the important implementation details and the development of the cyber security program which is perhaps one of the most important security programs that we deal with today.

The Commission has also benefited from Commissioner Klein's focus on incident response exercises and has worked to strengthen integrated response efforts. Before I turn to my fellow Commissioners for their

statements, I would like to note that over the past couple of years, the Commission has been able to focus greater attention on codifying many of the past orders issued in the wake of 9-11.

The rulemaking process provides a valuable opportunity for the Commission to clarify and strengthen regulations based on past experience.

And today's briefing I think is an important part of continuing this process. Although we have made significant security gains in recent years, we cannot allow those successes to lull us into a false sense of complacency. The potential threats that licensed facilities face are simply too real and evolve too quickly to let our guard down.

So I look forward today to hearing the update from staff on the progress and status of their important work and the programs that they deal with.

I now turn it over to my fellow Commissioners if they would like to make any opening comments.

COMMISSIONER KLEIN: I would just like to welcome Jim. It turns out that this is not the first time Jim has appeared before the Commission but it's the first time I believe you appeared in your new capacity. So welcome.

As we move forward in risk areas, I think risk informing our security is one of the areas that we should consider.

It turns out that you don't take an ax if a scalpel will do the work. And so I think as we have learned in our reactor oversight, risk informing has made us a better regulator and I think that is an area we should look at in the security arena as well.

COMMISSIONER SVINICKI: Thank you Mr. Chairman. I agree with you on all the important work that's being done in this area. And there are so may topics that I think as we ask questions today, it will seem to attendees as if we are hop scotching around on a lot of disparate elements but that's the nature of all the work that NSIR is carrying forward. And this is the first of this year's programmatic briefs and I think these are such an important part of the Commission's involvement in the day-to-day work of the agency. We have a chance to just sit and look at subject matter areas and office by office and program by program.

So I look forward to since this is the first of these, we have many months to go of these programmatic reviews but I think it is an important thing to focus our attention on. Thank you.

CHAIRMAN JACZKO: Bill.

MR. BORCHADT: Good morning. Before Jim goes over the agenda for today's briefing, I wanted to mention a few things. You will notice that we've chosen a handful of specific topics to focus on today's Commission meeting, but NSIR has a very unique and very important role within the agency as a point of contact for many issues that go across the entire agency, require the resources of the entire agency.

They're also probably the office that has more interface with other Government agencies and departments than any other office in the NRC. And part of that is all of the work that they do in the threat assessment and the coordination of security activities across the Federal Government establishment.

It is not an easy task. It's largely invisible to an awful lot of the NRC staff but it's very valuable nonetheless. They are also responsible for the information security program that is implemented by the entire staff. Then, also, the incident response program which requires the efforts of all of the technical staff in the regions and in the program offices and they do a remarkable job of coordinating a lot of very difficult activities.

So I would also like to welcome Jim to the table in his new capacity and to just take a moment to acknowledge the efforts and the contribution of Roy Zimmerman. Over eight years ago, Roy become the first office director of the newly established Office of Nuclear Security and Incident Response after the events of 9-11.

He has carried with him through the support of his entire office but carried with him the burden of the agency's efforts which were very stressful, probably the most stressful office director job within the agency over a protracted time period.

How he put up with it for over eight years, I have no doubt and I just wanted to acknowledge his contribution and let him realize how much we thank him for that dedicated service.

So with that, I'll turn to Jim.

MR. WIGGINS: Good morning. As you can see from the agenda on Slide 2, we are going to present a topical presentations.

There are eight topics that we will go over. Three are elements of what you would characterize as an integrated response to significant security threats that will be on force-on-force in the integrated pilot of

comprehensive exercise programs and hostile action based drills.

In addition, we will talk about the activity that allows us to share our safeguard information among the staff easier; we'll talk about cyber security, we'll talk about the actions to revise Part 73 which in this particular revision, there are actual physical plant changes that are involved and I think that part is noteworthy and significant.

We will talk about some of the facilities and the support that we get from the other offices, in this case, the Office of Administration. As you can see at the table, we have the division directors and Kathryn Greene from the Office of ADM here to make the presentation. And as you mentioned, Mr. Chairman and as Bill has mentioned, these topics are just a small piece of what the scope of NSIR's activities are.

While we are not a licensing office, we do licensing activities and licensing support. We are also similarly in rulemaking, we are a support organization, we provide the technical basis for security and emergency preparedness rulemakings. And we do oversight of the EP and security through inspection program development administration and we do perform the force-on-force inspections. And as Bill mentioned, we have a number of

stakeholder interactions which I will tell you has probably been the most difficult task that I have had coming into the job just trying to understand who we deal with, and why we deal with them and what we get out of it. But principally, we are dealing with in the emergency planning area, we deal with protective action decisionmakers in the state and local governments. In the Federal sector, we spend most of our time with Department of Homeland Security with Federal Emergency Management Agency, and with the Department of Energy and Nuclear Security Agency.

And we do have some international work that we do largely with IAEA, so it's a rather full scope.

During the eight topics, presenters will talk about what the status of some of those activities and some more noteworthy aspects of them and also talk about some accomplishments that occurred in these activities. I've got a couple that I want to highlight that are outside the topics we are going to discuss.

Bill did mention that we manage the incident response program for the agency. That includes continuity of operations and one aspect of that became especially relevant in the past year is preparations for the H1N1 potential pandemic.

NSIR was the lead office for the agency in developing the agency plan and providing support and oversight to the specific offices in the developments of their plans and we do have the plans ready.

In effect, we're ready to handle the pandemic of It as we said before.

We have piloted use of web-based technologies to gain some leverage and some improvement in external stakeholder interactions as we develop rules.

We piloted on the emergency preparedness rule that we briefed in the last Commission meeting.

Another accomplishment is we were able to work with the Department of Justice and Attorney General to get authorization for our site security people to use a higher grade firearms, special firearms. That puts them in a more even keel with what the threat would likely be. We have some rulemaking which will play out in the March time period to get the rule infrastructure in place that will be the next step and allowing sites go after these particular weapons. And lastly, we in the cyber security area, we chartered a Cyber Assessment Team. That's similar or analogous to our Information Assessment Team. This is for cyber issues. We take a look at cyber issues and have a single point in the

agency for assessment of cyber issues to decide what the threat is and what kind of actions we should be taking.

So with that summary, I will turn it over to our first presenter, Trish Holahan and she will talk about force-on-force.

MS. HOLAHAN: Good morning. As you may know, Section 651(a) of the Energy Policy Act of 2005 requires a Commission at least once every three years to conduct security evaluations to assess the ability of the private security forces to defend against the applicable design basis threat at licensed facilities.

These evaluations shall include force-on-force exercises that to the maximum extent practicable, simulate security threats in accordance with the applicable DBT.

The current implementation of the force-on-force inspection program is highly effective. And I would like to emphasize that it's currently highly effective in meeting the objectives for the inspection of site security protected strategies at NRC licensed power reactor facilities and Category 1 fuel cycle facilities.

The force-on-force inspection program for power reactors continues to be implemented through the scope and parameters of the NRC reactor oversight process for the

security cornerstone.

And the primary objectives are to ensure licensees have target sets, they know what to protect, a strategy to defend against the design basis threat and adequate resources to conduct a demonstrated performance of their attributes.

And as an accomplishment, we did complete all required exercises every year since 2005 as reported to Congress in addition to some re-inspections. So we've had a very busy time over the past five years.

The current force-on-force uses the results of the triennial NRC evaluated exercises to demonstrate the overall adequately of the licensee's protected strategy and does not consider other aspects of the licensee's protected strategy prior to reaching a decision for the significance of certain findings at the culmination of the inspection.

Through the Force-on-Force Program, and this is another accomplishment, we have identified several sites at which the protected strategy required enhancements.

The exercises are currently assessed as a pass/fail process measuring the ability to protect a complete target set.

The NRC staff identified the potential for licensee exercise performances to influence the overall

protected strategy assessment in a false/positive or negative manner. An example of a false/positive would be inspection with marginal performance during the three exercises where they eliminated components of a target set but they didn't get to the complete target set. In this case, the current pass/fail process would result in a pass with no requirement for corrective action. But the marginal performance may truly indicate a poor overall strategy. An example of a false/negative would be an inspection with two exercises with strong performance and one exercise that resulted in destruction of a complete target set. And in some cases, the inspection team may have determined the overall strong licensee program and that one poor exercise performance was an anomaly due to controller issues or other artificialities. In the case of this type, the failing grade should be viewed as a false/negative assessment of the overall defense strategy.

Also the fidelity and artificiality of certain inspection objectives, equipment and activities during the NRC evaluated exercise may impact the NRC's ability to come to a realistic conclusion in a determination of the overall adequacy of a licensee's protective strategy and significance of findings. For example, use of explosives, simulation

of cutting fences requires a significant number of time outs which delays the momentum of the exercise.

In late 2008 through the first quarter of 2009, NSIR staff conducted a review of the force-on-force inspection program holistically and began to consider ways to enhance the assessment of the force on force inspection program results.

Staff has discussed the proposed enhancements for the force-on-force significant determination process, the STP to the Industry and the public. And we had a public meeting on November 19 to begin discussing it.

The proposed enhancements to the force-on-force assessment and significant determination process tool provide a process for assessing marginal performance that the current system does not allow.

The proposed approach is that exercise assessments will potentially be based upon the degree of adversary penetration into the protected area and power block and will be evaluated using a margin rating ranging from high margin adversaries neutralized in the owner controlled area or just inside the protected area to unacceptable margin where the adversaries achieve the complete target set.

And in addition, the staff has developed

protective strategy attributes such as target set assessments, how well licensees identify what to protect, controller training. Controllers are necessary to monitor the flow of the exercise and they are critical in both training and their performance as to the how the exercise evolves.

Scenario matrix development, that's necessary to ensure the time outs in anticipation of technical adversary movement is appropriate. And the appropriate briefings are done to the composite adversary forces, et cetera. And also, licensee exercise performance to evaluate licensee performance. That's a first for -- we have not really evaluated the licensee's exercises, but we are proposing to. So we are going to combine all that in addition to the data evaluated from the evaluated exercise results.

And attributes are given a weighted value for an overall assessment of the licensee performance during the target set review week, the planning week, and the exercise week.

The licensee performance during the NRC conducted Force-on-force exercises is still the most heavily weighted factor. So we are not eliminating to focus primarily on that but we are taking into account all these other things to make sure that licensees are defending the right targets.

And on the next slide, the path forward is to evaluate the comments from the public meeting participants and to continue to refine the process and conduct future public meetings. For example, there is a public meeting on February ten at the Marriott. And it is involving state and locals and all NGOs and all involved stakeholders.

And then, we will inform the Commission on the recommended approach for enhancements to the Force-on-Force Inspection Program and then conduct pilot inspections in the first and second quarter of 2010 comparing the current force-on-force program to the proposed enhancements for revised force-on-force programs. And with that, I will turn it over to Virginia.

MS. HUTH: Good morning Chairman and Commissioners. Thank you for the opportunity to bring you up-to-date on the safeguards information local area network, electronic safe. One abbreviation of it is SGILAN E-safe but we mostly call it SLES. It is pretty long.

It's genesis is a staff requirements memorandum of 2004, as you know. And it's basically a document management system that will enable vast improvements in the efficiencies and effectiveness related to the management of SGI

data.

For one thing, it is much more secure. For example, we have previously been engaged in sharing data through the regions through snail mail, trucks back and forth, not that that's insecure. But it's also slow, cumbersome and the electronic media is much more efficient and secure.

It also offers a good search capability, so staff are able to type in a key word and reference or research on the subject of their interest.

I will add that there is a need to know in the system so if they search on a document and they do not have access to it, they do need to contact the owner of the document for that access.

But it is a good knowledge management tool and also provides for the pre establishment of the dispositioning of records electronically consistent with requirements of the National Archives and Records Administration, so another efficiency for us. And finally, it offers the ability to reduce the numbers of lock-bar cabinets and safes throughout the agency.

It basically consists of the two parts. The SGI LAN component is the wiring or pipes, the infrastructure that the

system rides on or the application rides on.

The application known as electronic safe sits on that and that's where the functionality is that I described, the sophisticated file structure that profiles the information, the ability to collaborate or do version controls on the information, or to send an e-mail to another user in the system letting them know that a document is available for review.

It is also highly secure as we mentioned. And so it stands alone. It does not connect with any other system in the agency. It is configured so that it's available at the desktop for users who have a frequent need to access SGI information. And for those with the less frequent need, it is available at the kiosk and there will be one kiosk per floor in the agency.

In terms of a system operational experience, we since 2008 have been supporting 140 users within the Office of Nuclear Security and Incident Response and since that time, we have also inventoried, scanned and profiled over 12,000 unique documents. Many of those date back to the 1970's. Many were found only in paper formats in various safes and some in obsolete electronic media. So an enormous effort was undertaken to consolidate and inventory that data.

We believe that is arguably the bulk of that information is in the Office of Nuclear Security and Incident Response but we still do have some activity to search through the agency and regions for other records.

And we have also since that time been able to Reduce, since 2008, reduce the numbers of safes as well so significant progress so far.

In terms of deployment status and schedule, January 30 is our go live date to complete the expansion of the system to the One White Flint and Two While Flint Complexes.. So it will be available to the total of about 300 users, an additional 160.

Then, in the April time frame, we are expecting to complete deployment to the Executive Boulevard and the Church Street locations. It will be available there in the kiosk format. And our plans are also to complete the expansion to the regions by the end of calendar year, FY10, by December of this year.

Now, we had initially planned to expand to the resident inspector sites in 2011 and at this point, we are considering the possibility of accelerating that deployment into the 2010 time frame.

We are looking at the opportunity to achieve some

synergies in deployment. It's the same architecture and similar areas, saving on travel cost and so forth. And also, it will enable us to achieve earlier benefits related to sharing of information consistent with the various inspections I talked about.

So we are looking at those, that possibility and we actually have some pilots planned for April of this year and June with a couple of local sites to ensure that the connectivity will be sufficient.

Another area that we are kind of a decision point coming up is the possibility of expanding to external stakeholders. Initially, we had considered this as a possibility to expand to licensees as well as to various state, local, and Federal agencies as appropriate. And at this point, we are really looking closely at the cost effectiveness of that. I think with the other Governments, it's very much in question.

I will add that we do see benefits to receiving information from licensees because it eliminates the need for a lot of paper documentation that we will have to scan and so forth.

However, there are concerns with -- for example the costs of supporting equipment in licensee offices and

elsewhere for the long term, and also issues that we have to work through relating to ownership or the control of the information that is submitted and how that is handled.

So those are some issues that we are continuing to work on now and to study going forward. That concludes my presentation.

MR. CORREIA: Thank you. I have the next 3 topics. First is cyber security. Operating reactors were issued orders in 2003 and 2002 that contained certain requirements for cyber security.

Licensees currently have cyber security elements in their physical security plans and they implemented their plans using an NEI guidance document 0404. As you are aware, the Commission issued 10 CFR 73.54, the cyber rule last May.

These requirements in the new rule essentially codify the orders and added additional assurance to protect against the DBT.

The regulation required power reactor licensee to submit by November 23, 2009, their cyber security plan and implementation schedules.

The Regulatory Guide for 73.54, Reg Guide 5.71 was issued January 7th last week, provides licensees an

acceptable method for implementing the requirements of 73.54.

Previous, earlier drafts of the Reg Guide were provided to Industry for their use in developing their plans.

At this time, I would like to acknowledge the exceptional support that we received from Research, NRR, NMSS CS0 OGC and ADM during the development and issuance of the Reg Guide.

It took quite an effort to do that because of the uniqueness of the topic. In reparation for the review of licensee cyber security plans; we developed a Standard Review Plan, and also instituted a team approach for the reviews working with NRR and OGC. This will give us better consistency, efficiency, and effectiveness.

Regarding the review of the cyber security plans that have been submitted, all licensees have submitted their plans by the November date. And the schedules for implementation range from 3 to 6 years after staff acceptance. All licensees follow guidance in NEI 0809, Rev. 3. This guidance was not endorsed by the staff.

We did review Rev 3 to 0809 and generated questions and comments which eventually evolved into Rev 4. However, due to time constraints of the licensees preparing their plans to submit

by November 23rd, Revision 4 was withdrawn.

Cyber security plan acceptance reviews are ongoing at this time. But as you would expect, licensees following Rev 3 to 0809 has generated questions and the need for request for additional information, which was essentially the same comments and questions we had on Rev 3 to 0809.

We have met with Industry senior representatives on this issue and are seeking ways to generically address these RAIs so that they could supplement their submittals so we will have a much more efficient method to reviewing and approving them.

Regarding inspection plans, we will develop an inspection procedure for the regulation and we are considering pilot inspections, one to validate the inspection procedure and also to give licensees a better understanding of what our expectations would be for the inspections once we get there.

Next, I will speak on Part 73 power reactor licensing activities. As you are aware, the revision to Part 73 physical security requirements became effective last May and are to be implemented on March 31st this year.

The tier one regulatory guides were issued last July. There remains two tier 2 Reg Guides that are in process

currently and we expect to have them completed by March this year.

There was a bit of a delay in working on the Reg Guides because of the unplanned exemption request that we received late last year. So we are working on those also.

As you are aware, last September, NEI submitted a request to change the implementation date for two provisions of Part 73.55, it's (e) and (i) to extend the due date, the implementation date rather to the end of this year.

Currently, that is being processed as a petition for rulemaking. To date, regarding the exemption request, we have 28 -- we have received 28 exemption requests. One has been issued. The rest are in various stages of review.

The essential requests are specific to very certain parts of 73.55 (e) and (i). And most of them are request for additional time to work on alarm stations, uninterruptible power supplies, relocation of detection equipment and adding video surveillance equipment.

Similar to what we've done with cyber security, we developed an acceptance criteria for these exemption reviews. And we've also developed a team approach to the reviews for consistency, efficiency and effectiveness.

Given that the rule has to be implemented by March

31st, we expect to start seeing revised security plans in about 60 days following. These are typically reviewed under 50.54 (p) which is licensee's way of submitting a plan without prior NRC approval because there is not a decrease in the effectiveness of their security plans.

Inspection procedures have been revised and we are working on inspector training. And we are also asking the regions to focus their calendar year 2010 inspections on changes to the regulations that licensees implemented.

Next, I'll speak about integrated pilot comprehensive exercise plans, or as the acronym spells out, IPCE. Integrated Pilot Comprehensive Inspection Exercises are voluntary, FBI led initiatives with support from NRC, DHS, local law enforcement agencies, power reactor licensees and NEI. IPCE's purpose is to design an exercise, an inter-agency plan that would enhance tactical take back capabilities that are one part of the integrated response relating to adversary attacks on commercial power plants. It includes an assessment of tactical capabilities of site security and local law enforcement agencies. And the first and only IPCE that we have had so far was at Limerick last year.

The Limerick exercise is considered a success in that it met its purpose but there was some lessons learned

that will be carried forward to the next IPCE.

Some lessons learned include the demonstration that an integrated response by local, state, Federal, law enforcement agencies and licensees' security personnel could occur. LLEA entered the nuclear power plant power block to conduct tactical operations training.

Some of the changes that need to be considered to enhance the IPCE's -- communication of operational expectations prior to the exercise need to be enhanced. Involvement with tactical teams at the lower levels also needs to be enhanced also.

The high level commanders of these teams were more involved with the planning phases but not as much for the actual implementers of the exercise.

Separate radio frequencies are needed for the controllers and the tactical team. More training for controllers needed to be provided. And lastly, observer access to tactical operation areas needs to be limited.

The next IPCE is planned for D.C. Cook sometime this year, this summer. FBI, NRC, licensee, local law enforcement and NEI had a kick off meeting at the site December 1st. It was an opportunity for each of the representatives to interact and

start planning milestones and dates for the exercise that is planned to be held this summer.

Future plans for IPCEs, we continue to work with F.B.I. and the power reactor Industry on scheduling, looking for other volunteers to schedule these IPCEs. And once sufficient experience is gained, these type of exercises should become a more routine training event.

That concludes my presentation and I will turn it over to Chris Miller.

MR. MILLER: Good morning. Another portion of the integrated response activities are the Hostile Action Based Drill and Exercise Program.

All 64 commercial plants have completed hostile action based drills. The last one was Palo Verde on December 10 of last year.

They used the guidelines from Bulletin, 2005-02 and completed these and we view this as a very successful activity. The effort brought together portions of operations, security and EP on the sites along with the off site response organizations in a way they really have not been brought together before to address the unique challenges that a hostile action event might challenge a plant with.

So, following the last drill and truly, all along, we been developing lessons learned that we been sharing with industry and with states and locals. Staff observations are summarized in Information Notice 2009-19. And that represents a lot of good work.

I would say that a majority of the 64 drills have been observed either by inspectors and other participants from NSIR but also from the regions. We had great support the regions on these hostile action based drills.

FEMA is also in the works of publishing the off-site response aspects of the lessons learned and they will put it up on their website, the lessons learned information sharing system on the FEMA website.

Of course, we are also in the process of working through how we incorporate the lessons learned from that 64 drill set into our proposed emergency preparedness rulemaking.

We are in the middle of that working with FEMA, working with our stakeholders to not only enhance the rulemaking but also the guidance associated with the rulemaking. NEI is also working the industry guidelines. Previously, they had developed NEI 0604 which gave some guidelines on how the industry should be using these drills

to enhance their programs and they are going to come out with a revision of that and we will work with them as far as any kind of endorsement to that document.

The next steps for this are to carry this momentum forward from what we learned in the drill program. And we need to carry it forward because the hostile action based will not be required by the EP rulemaking, the current rulemaking, probably not until some time in 2012, 2013 time frame is when the licensees will be required to conduct a hostile action based drill for the first time.

So we got a little bit of a gap there from December of last year through to 2012, 2013, how we keep that momentum going.

We are working with stakeholders, state, local, licensees and other stakeholders to develop the most effective way to keep this initiative hot basically and keep the lessons learned going. We are sensitive to the large effort that was required by the off-site response organizations for the Hostile Action Based Drill Program.

They have put a lot of effort and a lot of time and energy into it and there was some concern that maybe we don't want to do these -- you know, the follow on in a off year. Maybe we want to do it during some part of the

exercises. So FEMA and NRC got together to look at how we could incorporate some no-fault HAB practice into the existing exercise schedule that's going on.

Given that, we met with FEMA. We came up with some guidelines where we could lay this on top of current exercises and met with the industry but also with states and locals and we're going over some guidance that we had put out if we wanted to go in that direction. And I say "we". This is off-site on-site. This is states, locals. We need to get all the participants together.

So we really need to hear from our stakeholders on that one. We had a successful meeting on December 17 but we heard some other voices and they were saying you know, we can target better on an off year. We can target at each site how we are going to do these drills and exercises, so it may be anything from a table top to a drill to a full participation exercise and they would like to have the flexibility to do that and continue on this effort but maybe not lay it on top of a hostile action, or excuse me, a current exercise that has already been planned. They want some more flexibility in there.

We are currently working to hear from NEI and the

industry. NEI is going back to the industry and coming back to us in a working group meeting in February and they will discuss some additional options. In addition, FEMA is going to be getting with the states and locals and their stakeholders and discussing other options and seeing what the best recommendation coming out of the states and locals.

Once we do that, we will be looking forward to getting together sometime in February and developing the most effective way to keep this effort hot.

That's really what we are trying to do but we need to hear from all of our stakeholders. I think that the best way I can summarize it is we heard overwhelming response at that meeting that yes, it is a good idea to keep this forward. We didn't have anybody pushing back and saying I think it is a bad idea, too much effort, too much time. It is the details of how we move forward on it. So I think you will see something. We are looking for positive, something positive coming out in the February March time frame where we can work and craft this transition period for hostile action based drills.

We think it will continue this effort of positive engagement with operations, security, and EP.

With that, I would like to turn it over to Kathryn Greene of ADM.

MS. GREENE: Well, thank you and good morning.

My presentation is going focus on four areas, emergency preparedness and response, space planning, procurement, and rulemaking.

In the area of emergency preparedness and response: We serve in a complementary role to NSIR in our continuity of operations, planning, communication, training and exercises. Our focus is on agency operating status while NSIR's focus is on licensee's operating status.

In the area of space planning, we've worked collaboratively with NSIR to improve our information security capabilities within headquarters, with the regions, and with our appropriate Federal partners.

We expanded and refurbished the secure compartment information facility here in One White Flint North Building. In addition to enlarging its size, we added homeland security data network terminals and other communication capabilities.

These improvements enhance our discussion of classified information including threat assessment analysis among headquarter staff and regional staff with a need to know and with our pertinent Federal partners.

And as Virginia mentioned, we are expanding our

safeguard local area network capabilities by constructing safeguards LAN kiosk workstations throughout the White Flint complex In Executive Boulevard and Church Street and eventually, we have plans to expand that to our regional offices.

In the area of procurement, we are moving to a more strategic approach to our procurement of goods and services here at NRC. We want to align our division of contracts branches along our budgetary lines of business.

This means we will leverage our purchases to aggregate similar purchases and to enterprise wide procurement. So for an office like NSIR that crosses many business lines, they won't have a single focus which they do now, a single branch in the division of contracts. They will be working probably across all the Branches.

But we think that the efficiencies that we gain through this consolidation of procurements for like services and goods will mitigate any concerns we have with the organizational approach that we have now.

We also are strengthening the capability of our acquisition work force. The EDO signed out Revision 3 to our acquisition certification and training program in late December.

It requires additional mandatory training classes

for our project managers and technical monitors across the agency. And this training initiative supports one of the President's initiatives to strengthen the acquisition work force.

We also have developed strategies to implement a second presidential initiative aimed at improving government acquisition.

In the area of rulemaking, we were given authority for the oversight and coordination of rulemaking activities about ten years ago. This was assigned to us so that we could ensure proposed and final rules met their intended purposes, that there was process and content consistency across the program offices involved in rulemaking activities, that schedules were met and that our rulemakings conformed to Federal Register content and printing requirements.

To perform these responsibilities, we formed the Rulemaking Coordinating Committee of which NSIR is a member. We also support the agency's openness goal by ensuring the availability of all public documents associated with rulemaking activities and if you go to regulations.gov, you can find the regulatory history of all NRC rulemaking dating back to 1999.

We have provided support to various rulemakings

involving NSIR including the power security requirements rulemaking mentioned earlier that affects Parts 50, 52, 72 and 73. And also, the subsequent NEI petition on that rulemaking and the emergency preparedness regulations found in Part 50, and 52 of our regulations. And that concludes my remarks. Thank you very much.

MR. WIGGINS: That concludes our presentation of the topics. It dawned on me, I was a bit remiss in the beginning of the presentation, I recognize that Chris Miller was a late fill on your agenda, should have shown Mel Leach but Mel Leach had a sudden medical condition and required some hospitalization so he was unavailable. We just hope we get him back quickly.

Some issues going forward coming out of the presentation that we will need to keep the Commission informed of either formerly or through our normal routine communications with the Commission would include maintaining momentum in the comprehensive exercise and hostile action based exercises. As I said, they are part of the integrated response and I kind of view these things baring safety term as a defense-in-depth strategy.

We assessed a threat, we set a DBT, we set up a licensing

and inspection process to make sure licensees responded to DBT correctly and we tested through force-on-force.

But it's possible we are not in the right place. So we have to be able to handle things that are either beyond what we said is the DBT or to make up for some uncertainty in the process of determining it so when you start looking at these other two off-site factors, they provide back stops. And you can get in the same analogy that we do on safety with the 3 tiered force-on-force with emergency planning as a fourth tier back stop.

Also going forward, you heard about cyber plans. This is a matter that is a tough issue and potentially controversial between us and Industry. And we have talked and we have engaged the senior executives in industry particularly the fleet operators. And we just did that yesterday, in fact.

And I'll just tell you, based on our conversation, I can tell you that both Industry and we are committed to getting this thing done and get it correct.

But getting it correct is going to be a challenge. So, we will have to monitor that carefully and see how that goes going forward and make sure the cyber plans are appropriate and serve us well.

We talked about force-on-force. To borrow a term that industry uses, we are going to continue to work on stabilization.

I work for a boss that told me something when I was working for Hub Miller, I learned a number of things working for him. And one of things he did and you actually had to think about a lot of what he said, you not only need to be good but you also need to look good. And to look good is not for cosmetic reasons but it buys you credibility and it buys you space to operate.

Force-on-force, we are good. We need to work on making sure people think it's good. I talked to the staff a lot, sometimes at great length, I'm told. But I'm told that in my former life, I would tell them sea stories. In the current vernacular, it is story telling and knowledge management. But I kind of compare what we are doing in force-on-force to things that we lived through before. And one of the things I think is a good model is where we lived through was operator licensing and requalification. We have a lot of the same issues after Three Mile Island as we decided to fundamentally change how we approach operator requalification activities. And it was a rocky road initially but we made our way through it and there are some lessons you can learn and apply about having good infrastructure, good processes and a real strong change management program that both industry and regulator both agree to implement.

And I think we can make some progress in there.

There may be some more fundamental changes in how we do Force-on-force that might be appropriate, but we will deal with that later and that will be something we'll come back to the Commission if we reach the conclusion that's the direction we need to go.

In the last Commission presentation, you know we currently are working on a revision to the emergency preparedness regulations. We need to keep momentum on that and get that through in a good way, need to make it a sound regulation that serves the interest of safety and of the regulator but also of the other stakeholders including the states and locals who are part of the protective action decisionmakers and Industry.

One thing we have not really discussed a lot of in this meeting and I don't want it to go un-noticed is we did do a lot of work with the Offices of Federal and State Materials Materials and Environmental Management Programs or FSME and Nuclear Materials Safety and Safeguards, to look at security issues mostly.

In a materials area and waste area for instance in the waste we recently just published a draft technical basis for some potential proposed rule changes affecting security for independent spent fuel storage installations. And we also work on fuel facility security so there will be some issues in there.

We will talk about one particular issue later this afternoon in the afternoon's briefing. There is IOU to the Commission that we will mention that comes up and we will update you on where we are with responding to that Commission request.

So with that, that completes the NSIR side presentation.

MR. BORCHARDT: The staff is complete.

CHAIRMAN JACZKO: Thank you Bill, We appreciate the presentation it certainly covered a wide variety of areas. I thought I would just start with a question in an area that you didn't necessarily touch on but I think it is certainly an important piece of our program for emergency response capabilities and that is the emergency response data system which I think the staff is in the process of providing a new or transiting to a new system with perhaps a more updated hardware infrastructure than what we have been accustomed to. And I was wondering if you can tell me how that transition is going and if there are any issues that are coming up from a policy perspective, the Commission will need to address when its comes to that.

MR. WIGGINS: Let me try that and if we need more detail, Virginia and Brian McDermott can add in: Our current system is archaic. It's based on modem transmissions

over telephone lines.

The existence of the system traces back to an element in the planning standards in Appendix E that talks about a reliable system for transmitting of data.

As doing this incident response thing for some years, I recall a time when we didn't have this type of system and we tried to get the data over the emergency notification, the ENS phone lines. And there is only so much data that can come over a phone that way with a talker trying to tell you what data you need.

So this system is important to our response. These modems are failing and they are unreliable and we have a more reliable, more secure solution that we have created and we funded. And we would actually provide the equipment for licensees to install something that's called a virtual private network, an internet based solution using encryption to provide security in information transfer.

So far, we have asked licensees to voluntarily contact us and sign up for the installation. And I guess we are to be truthful, we are under subscribed, dramatically under subscribed. We have a handful, maybe 6 or 7 licensees that have stepped forward.

We are going to work with the executives in

Industry to try to raise the profile on this issue a bit.

We are thinking of some correspondence that both I would send with Pat Howard so we can attest to the information security provisions of the fix.

So we need to work through that because like I said, the current system is not sustainable in the long run.

CHAIRMAN JACZKO: There is nothing right now in the rule that you feel needs to be changed to accommodate the new system?

MR. WIGGINS: No., nothing in the rule.

CHAIRMAN JACZKO: Certainly from my perspective, this is one I've see move forward and I think it is important to having traveled to other countries and seen the kind of response and data systems that they have, I think it's certainly about time for us to have the similar capabilities and not be relying on such an out-dated and outmoded technology but be able to take advantage of the more secure as well as more reliable forms of communication for really what is an important function.

So I look forward to again, seeing how that moves forward and again, if there are areas where the Commission can support or play a role in moving that forward, let us know.

Jim, I'm going to go back to a statement that you made about cyber security plans. And I think cyber is certainly an important piece of security and may as time goes on become the dominant piece in security as we go forward. And I think one of the things you said is that this needs to be done correctly.

Well, what in your mind does that mean for this to be done correctly? And where are we -- are we doing it correctly and if not, what do we need to do it correctly?

MR. WIGGINS: Well, the staff would say we are doing it correctly and it has not gotten up to Bill Dean and myself yet to look at it.

Industry right now has some trepidation as you can well imagine. If -- I don't want to take too much time to answer. Let me try to hit a couple of key points.

We are regulating this differently than we would approach most of the other things that we regulate. Typically, there is some sort of consensus standard or guideline we could adopt. Our Regulatory Guide would be a rather brief document that adopts the standard possibly with some caveats. That's not the case we are in.

We build a Regulatory Guide in many ways looks similar to a ANSI standard in terms of the level of detail in it and

it is essentially a very complete cyber security program.

Now, how that gets built into the plans and Industry's trepidation is, what is their exposure to the level of detail that is in this Regulatory Guide.

Now, it gets to the other question, what does it mean to be doing it right? Cyber is interesting because it evolves very quickly, probably quicker than most other things we do either on the safety or security side.

You can basically see a threat building and safety side you can sort of accumulate operating experience, you see where it is pointing you. But in cyber, it seems the type of threat, what it's going after, how it works, you see just in looking at a trade press, if you build an internet base solution, firewall or something like that, you just get smarter hackers. The figure out a way through or around it. So we have to have a program that is adapted. We can't have one that the regulation locks something in so tightly that it restrains industry or restrains us from being able to adapt or to handle the new threat.

So as I've said before, I think there is a lot in it in terms of assessment and testing that's going to be the real key parts of this. You need to test against what the

threat is and see how your systems behave.

Dr. Klein mentions risk assessment. This is an interesting issue too because you have heard from ACRS about the difficulty of doing risk analysis for digital systems.

That's because to me, a lot of times when we talk about risk assessments in the agency, we start looking at PRA, diagrams and things like that. This may need a different type of risk assessment, like a risk management, assessment not a PRA. You are not going to get a 10 to the minus exponent answer on this. What you're going to get is what does the system do? What is its failure mode? What are the effects of the failure and the consequences and what do you think are the ways around it.

So, my view of the way to do it right is to have a program that's adaptable. Although it's tied to regulations so it is a hard and fast requirement that this exist. It's flexible enough to deal with this threat. It doesn't lock you in to do things that are not smart as you go down a range.

CHAIRMAN JACZKO: One of the big issues that are out there and I don’t know that we have fully grappled with yet is how this ties in with the enemy of the state provisions.

And certainly, I think from the perspective of all

of our security requirements, we have the enemy of the state provisions is kind of a back stop that ultimately limits licensee's responsibilities in dealing with any kind of security intrusion and much as electrons don't really have a tag telling them what particular plant they were produced in or what type of energy source created them, the cyber world is one that also does not easily tag sources of attacks or those kind of things.

Have we had any discussions about whether or not we need to consider looking at the enemy of the state provision to ensure that we are not overlapping with our limitations in enemy of the state when we are dealing with some of the cyber issues? Is there a consistency there?

MR. WIGGINS: It think it would be fair to say it's more work on that. Personally I haven't heard that issue raised at this point. I don't know that we have gotten there yet. I understand the point. I would agree with you, this is the same as -- the agency I think correctly treats cyber as a security issue. It is not an engineering issue. And there's implications that affect the licensing offices, particularly NRR and NRO and we believe we have straightened that out.

The engineering issue would be the unintentional

human act. The cyber issue is an intentional malicious act so it's rightfully a security issue that brings in this construct of the enemy of the state or line of demarcation that is fuzzy at best about what you can expect an industrial facilities to protect against verses what you have to get outside help to protect. I don't know that -- I'm dancing around the issue frankly.

CHAIRMAN JACZKO: It's okay if you don't have an answer.

MR. WIGGINS: We're not there yet, Chairman. I think we are at the crawl stage trying to get the plans in place to meet the regulatory due date.

CHAIRMAN JACZKO: I have several other questions but I'll wait for a second round.

Dr. Klein?

COMMISSIONER KLEIN: Thanks for a good presentation. Normally, I start asking questions from either Bill or Jim but I'm going to deviate and go to Kathryn first, and the reason for that you talked about part of your responsibility was space planning, when are the cement trucks coming for White Flint Three?

MS. GREENE: We are working with GSA and the developer LCOR to schedule ground breaking in April, 2010.

COMMISSIONER KLEIN: You have a date?

MS. GREENE: No.

COMMISSIONER KLEIN: Just checking. Then I was going to ask what time of day they were coming.

MS. GREENE: No, we will certainly work with the Commission's calendar on that event.

COMMISSIONER KLEIN: Thanks. Now, I will go back to my normal mode.

Jim, in terms of the NSIR organization, you have a lot of divisions within NSIR. When I talk to the Utilities, they sort of feel as soon as they get finished with one issue, here comes another one.

So I guess my question is, who in your office is responsible for looking at a systematic approach in how we deal with our licensees so that we don't just as soon as we come back with them on one issue, you come right back on another one?

MR. WIGGINS: The obvious answer is Bill Dean and I have to integrate this all together. If I had to pick one, I will go the policy direction which is Rich Correia would be further along. He is the one that does most of the rulemaking and licensing activities. so that's where you would get the start of this.

But, as you know, the idea of the integrated impact is a generic issue that goes beyond just what goes on in our office and it's something that we are getting to look at. It needs to be looked at broadly, it's both a safety and security issue. You will be hearing something on that at some point.

COMMISSIONER KLEIN: Soon?

MR. WIGGINS: Yeah. It needs to be soon because we have some major activities that we ought to decide what the implementation dates are which I think is really there is a question about what to do and that gets into security to where is the line in demarcation, how much is enough? What is realistic for a licensee to protect against. And then you get an issue of now I need to decide the what, and the next question is the when.

That's where this integrated approach can help.

You can look at what we are asking the regulated entities to do. We have got a pretty good estimate of what type of resources are needed to do it, whether it's engineering, security or quality assurance or licensing. You can get at least a good approximate picture of what the workload is out there. I think there is a framework and I don't want to pass this off on anyone but I think Eric Leeds would be much more able to talk about this than I am.

COMMISSIONER KLEIN: Trish, I have a question for

You on the force-on-force. Clearly, if you look at a lot of our utilities now, they have plants that cross our definition of regions so they will have plants in more than one region.

How do you coordinate and standardize the force-on-force in the various regions to ensure we have consistency in actions and responses?

MS. HOLAHAN: Well, obviously, inspections are currently let out of headquarters but we are looking at -- we coordinate with each region and we are involving the regional division directors now and the nuclear security working group so they can hear the discussions with industry that we are having so we are getting the message out and we have communication with the regions through security issues forum.

We are communicating with the regions on a division level, at a branch level. So we are communicating with the regions of issues that come up with force-on-force.

COMMISSIONER KLEIN: So at this point, do you feel you are pretty consistent on security issues force-on-force across the various regions?

MS. HOLAHAN: Yes.

CHAIRMAN KLEIN: Virginia, I got a question on the electronic safe. I assume that at the present time, it is

only safeguard information; is that correct?

MS. HUTH: That is correct.

COMMISSIONER KLEIN: What is your schedule to get classified information on there?

MS. HUTH: We do not have a schedule at this time. I think our expectation was we would complete deployment of this but then start budgeting and thinking about it for the 2013 budget. We will start looking at the exact schedule in anticipation of budgeting for it in that time frame.

COMMISSIONER KLEIN: You talked about the electronic safe as a stand-alone system but at the same time, we access it through our desk tops, rights?

MS. HUTH: Yes.

COMMISSIONER KLEIN: Jim talked about cyber security a little bit. How will you know if someone has hacked into that system?

MS. HUTH: We do have audit logs available on a daily basis as part of the system administrator function.

It is when I say "desk top", it is separate from the desk top you have right now. It would be at the individual's desk, a separate monitor and system. So they could not get at it through the existing NRC network. They would have to actually hack into SLES itself and because of

it stand alone capability, I think it's very challenging.

COMMISSIONER KLEIN: And then when do you go out to the regions? Obviously they would be remote systems as well. I assume that you will know if someone has broken through that system?

MS. HUTH: What we will do is we will be using a virtual private network which is a very secure technology similar to what we will be doing for ERDS actually. As you may know, many other Federal agencies, industry and the NRC itself uses Verizon as its service provider and we lease dedicated lines that are double encrypted. So those lines will be the primary network and in fact, that's how we are connecting to Executive Boulevard and Church Street, over those dedicated lines. However, separate from the existing NRC lines for say our email and other functions, double encrypted on a dedicated line. Does that answer your question?

COMMISSIONER KLEIN: I guess, Jim, you had talked on the ERDS system that there was a lack of rush to volunteer to change the system.

Is that lack of rush to voluntarily participate due to cost or is it due to uncertainty on security?

MR. WIGGINS: I can't think it's cost since we bear

the brunt of it. As we've looked at it and walked this through in the pilots, it takes maybe a day's work of the licensee's IT staff to check data points. We pick up the rest of cost. It isn't that.

I think my feeling based upon some tidbits of information I have gotten is it's sort of concern or ill ease over the internet structure. There may be concerns about cyber which is an issue we think we are going to put to bed in the next -- shortly, next couple of weeks. In terms of the -- while the ERDS system itself is a device that helps us, it would not necessarily be covered under 73.54 of the Cyber Rule. It connects into the process computer which I would presume it might be an asset on the licensee's side that they capture in there, at least thinking, with regard to this plant, we need to give them the good argument that exists that we have not given them yet about why this thing is secure.

I think that's what it is and frankly, some of the people I talked to at the operations end of the industry are not as aware that we are doing this.

And that's why one of the things that we are considering doing is having Pat Howard and myself send a letter out to the CNOs that -- a short letter asking to

spend a little bit of time on this and let's see if we can get moving.

Basically we won't really know if there are real issues until we get more participation.

COMMISSIONER KLEIN: Well, Rich, I have a question for you on timing. You commented that our Reg Guide just came out in January of 2010 but yet, we required the utilities to turn in a plan in November. That seem as little backwards.

Why did we do that?

MR. CORREIA: When the Part 73 was under Development, the changes to Part 73, it was a conscious decision to accelerate the rulemaking at the cost of slowing down the Reg Guides. We did get the physical security Reg Guides done last summer. With cyber, we spent a lot of effort working with industry to hopefully get to where we could endorse their guidance document. I think we were close but, we ran out of time frankly.

So, once we realized that we needed to have a Reg Guide in place, it was last May. So the time to develop it, put it together, go through ACRS reviews, et cetera, it took some time. That's essentially what happened.

Commissioner Klein: It almost seems like that

process will create RAIs?

MR. CORREIA: It will given that industry has used Rev 3 to their guidance document, but the questions and the comments are well-known. We have had marathon meetings with Industry to go over the comments. They had generated a Rev 4 which we looked at for a short time that looked very promising but given the time constraints, they withdrew it.

Optimistically, I'm hoping we can get back to a Rev 4 that will get us closer to what we need to approve these plans.

COMMISSIONER KLEIN: Do you have many RAIs at this point?

MR. CORREIA: We have started to develop them and we are being very careful to focus the RAIs on the rule requirements and not anything that we have in our Reg Guide. It is going through management review as we speak. So we are getting close. We are very close. At that point, we both share those with the Industry so they can start working on generic responses.

COMMISSIONER KLEIN: i have got some more questions but will wait for the next round.

COMMISSIONER SVINICKI: Thank you. I thank all the presenters for your informative presentations this

morning. Before I start with specific questions, I want to Jim, take your taking over the helm of NSIR to make a more general point.

You come into an organization like NRC and you are struck by certain things. One of the things I was struck by when I came here is that it is an expression of succession planning and an organizational value here to rotate the senior leadership and as you look at the resumes of senior managers at NRC, you often find that they have worked in a lot of the different organizations. And you know I was struck by that. A skeptic could say what's with the big musical chairs that goes on at the NRC and I'm very grateful for Roy Zimmerman's stewardship over the creation of NSIR and all the contributions he's made as Bill mentioned, but Jim as I listen to you talk this morning, I feel like the expression of the value of having people move about the organization, we already heard from you this morning, you compared force-on-force exercises to reactor operator licensing. You compared the cyber issues to ANSI standards. You compared risk informing security to digital I&C. And so I think that's the real strength and the value of the way we do succession planning and the way we move managers about the organization because what you're bringing to these issues is a fresh perspective of course, but you're bringing

your extensive background at NRR and I think that's really going to prove valuable on a going forward basis.

I just wanted to make that comment. I appreciate all the new perspectives you are bringing in.

Maybe that's why when you talk to staff, your stories take a long time because you have your translation step, maybe that's why.

MR. WIGGINS: I think they have a different view on that.

COMMISSIONER SVINICKI: We will go with mine because it's more flattering. Everybody talked about ERDS. I'll just share with you a perspective. If you feel under subscribed in volunteers, I am hearing that cyber security concern. As I move about in the regulated community and I flat out say your cyber security requirements, your own ERDS VPN system would not be in compliance with your own requirements as a regulator.

So I'm going so suggest to you the sooner you can run that to ground, you said we owe them the answer that is the good answer that they are looking for. I think the sooner we provide that, but I'm fully on board that what we have is not sustainable. If I have this right, I think NRC was ridiculed in Wired Magazine over how archaic this was. Maybe

that's folklore but I think I heard that where you put the phone in the cradle, I'm told that that was a subject of ridicule for being such an antiquated system so we clearly we need to move forward. But if there is any kind of concern that our own ERDS upgraded system would not comply with our requirements as a regulator, that is ours to resolve that and run that to ground. So I agree with you, you're on the right path. The sooner you resolve that, I think we can just move forward as again, the Chairman mentioned, we need to be doing.

I might turn Rich to the cyber plans that we have in house and you talked a little bit about as a kind of a broad range, the plans we have would have implementation periods of between 3 and 6 years. Did I have that right?

MR. CORREIA: Yes.

COMMISSIONER SVINICKI: I know that you send a letter recently regarding some feedback to give licensees about NRC's expectation, interim milestones and other things like that, but it concludes with a statement and again, this went out under your signature, it says, "The provisions of 10 CFR 73.54 are not significantly different from any of the previous requirements." It goes on to say "many aspects of the program should be already in place."

Can you help me understand why is there such a range and why are -- staff has suggested maybe 36 months is the right number. Why is there such a big difference here?

MR. CORREIA: We asked that same question Commissioner. Now that we have the plans in place, even though they do not detail that kind of information, that will be on specific RAI – please explain to us, why it is going to take 3, 4, 5 or 6 years after we approve the plans to implement them? We did have an opportunity to meet with one fleet operator recently. They did share with us their plans which I think would take three years. There is a lot of design and engineering and physical plant changes that are required per their vision.

COMMISSIONER SVINICKI: I was going to offer that as a cautionary tale. As incredulous, as I might sit here and say that is a huge range and if it is really true that many aspects of these programs are in place, speaking of organizational values, we are a learning organization and we talked also this morning about all the exemptions on Part 73 because I think we carried around the kind of knowledge internal knowledge that it was going to take licensees a certain amount of time to get those in place. I think hopefully, there would be agreement that where we don't want to end up on cyber with exemption requests. And I will get to a question about how much unplanned labor is that between

NSIR and NRR on the exemption requests that we had on Part 73?

So that -- it complicates our planning, our Budgeting, if in cyber we can avoid that and take a lessons learned, I think that would be really useful for us to do. And you said some things that I'm very hopeful about. Rich, you mentioned piloting of inspections. We want to take this and maybe this was Jim's crawl, walk, run is where we need to go on cyber but the Chairman has mentioned such an interesting point about cyber is that it is very dynamic as well. The technology, the threat and then, the protections against the threat, I think are going to be very dynamic.

So if it takes a licensee two years to change a protected area, fence or something, we can all kind of understand that. We are getting into some highly technical areas on cyber. So that will be very hard to stay on top of that. As I saw a 6 year implementation plan for cyber, I was thinking to myself, if I wrote you today a white paper about the capabilities of my iphone, six years from now, I very positive it will have very different capabilities at least, I hope so since I'm kind of into technology.

MR. WIGGINS: That is 72 months from approval of

the plan, so it's actually worse. It could be 7 years. When we started seeing these implementation dates, and it was helpful to talk to the one fleet operator, this was a status kind of conversation. He showed us what the long pole in the tent turns out to be is after they go in and decide what are in fact these critical assets applying the guidance that we agreed to in the plan, then if there is a physical plant change, you're talking usually about a three year activity for that. There is a planning year and then you have to wait up to two years for an outage, if you need an outage to put it in.

So you've got this rolling three year period that runs down from the last time you decided what you have to do. When we saw these late times, I asked Rich -- and one of the things we have to get to after we get over this current issue with the plans, we have to figure out a way that we can say we got most of the rule in place.

Having a six year or seven year waiting time until you have a rule that you say is in force does not make good regulatory sense. I think there is a way we can work with Industry. There is a way we can get the large amount or the vast majority of much of the critical stuff in and there will be individual things that you can say are exceptions and I think we can deal with it that way and say it's in

force, and mean it.

COMMISSIONER SVINICKI: And I notice I think in Rich's communication, it talks about having licensees provide when they can have some of these interim steps in place and complied with, not just when they plan to do it but when will it really be in place. I thought that was a good intuitive common sense way to approach that.

On force-on-force Trish, I would say on the enhancements, you mentioned and I know you are always using the parallel of examples is that people will latch on to your one example of something, and then ask a bunch of questions about it and you just meant it to be a notional example of what staff is considering. But you talked about assessing things in a force-on-force like degree of adversary penetration. When I heard of that, I reflected on the sites that I visited that even just their physical geography is so different.

So when I thought about your example of degree of adversary penetration, what that pointed out to me was the more general notion that any approach to the force-on-force with these enhancements has to be sensitive to the fact these sites are all different. And I'm sure that's part of what you're struggling with or one of the challenges you will deal with.

MS. HOLAHAN: Yes and that's exactly it because different sites have different footprints and so we take that into account.

COMMISSIONER SVINICKI: Certainly the recommended or smart protected strategy for one would not work for another. So we have to have the kind of regime in place that would acknowledge that.

MS. HOLAHAN: Yes, and that's why we asked the sites to identify the individual target sets and target set components because that will vary from site to site and that's what's planning their protective strategy as to what to protect.

COMMISSIONER SVINICKI: And just returning to the exemption process in Part 73, do we have any sort of estimate of how much unbudgeted staff time was then spent on that process? This would be more than just NSIR? And I know one has been approved, you said you have 28 in total were submitted. Are we able to get more efficient in that process as we have reviewed later ones?

MR. CORREIA: Yes. That was the concept of using the team approach, the first one with Farley we followed a series process verse a parallel process. Typically, they take 90 days to review.

I think we're down to less than 60 days now so there is efficiency gained. Using the same people to do the reviews over and over again, there is efficiencies gained there also. I don't have a FTE estimate at this time. It's something we can provide though.

MR. BORCHARDT: I'll just add one thing. As we budget three years into the future, we don't try to predict what licensing actions we will be working on three years from now so we budget in categories. So and although we can't predict that these would be the licensing actions we would be working on this year, this activity is budgeted. NRR has a large responsibility in this so it is within budgeted work and might displace some lower activities, but it's not a resource problem for us now.

COMMISSIONER SVINICKI: Thank you. I'll look forward to another round.

CHAIRMAN JACZKO: I think this issue of exemptions is an Interesting one and I think as I was looking at this Meeting, I went back and looked at the Commission's Approval of the rule and there's been a lot of discussion about the need to have an idea and concept of how all these activities are planned and quite frankly, that is fundamentally the responsibility of the Commission. All of these rules ultimately go through the Commission.

The Part 73 Rule was not a surprise, it didn't materialize in 30 days. I think in fact it took the Commission about four or five months to actually approve it. So to a large extent, the Commission in fact discussed the issue of the implementation date and what the Commission said was at that time there was an implementation date but as consideration went on, the Commission said we give one year from completion of the Reg Guides which were anticipated to be completed in March. The Reg Guides were done about June. I think so there was a little bit of slippage but not a significant amount.

So I think we are very easy on the E word sometimes but very difficult on one E word is the EN one which is enforcement.

Fundamentally we put implementation dates in the rules. And the simplest and perhaps the least resource activity for the agency was to actually enforce the implementation date.

We talked a lot and Dr. Klein raised questions about cyber and the Reg Guide and I think a fundamental principle of regulation that I think we have applied and that I think licensees would prefer that we apply is that we regulate to rules, we do not regulate to Reg Guides. Reg Guides are there as an enhancement to help the licensees and as an agency, we do very well in the

Reg Guide area. Many Federal agencies don't even do Reg Guides at all for their rules.

So I think it's very easy to get caught up in the concern that somehow we did something wrong here. But all of these issues were laid out very clear and I think licensees had a good understanding. We do a draft reg analysis which looks at implementation issues, implementation questions that went out with the draft rule package. They have an opportunity to comment on that.

So we gets lots of information and I think there is a good opportunity licensees are going to have these challenges. There are lots of places in the process where they can interject and I'm not sure in this case -- I think they were reluctant to move forward with changes that were likely going to come because they didn't want to spend the money and hoping they would get change and they didn't.

The Commission finalized it and then they weren't ready. So we do in fact have the exemption process in our rules that allows them to use it. They did and we have approved some and I think the staff will or hopefully be very cautious in the ones that it does. I think the other important point to remember is we have approximately 28 and I don’t know if that is 28 facilities, I think it’s 28 facilities, but let's say conservatively,

it's 28 facilities, that means there are still another 40 or so facilities that have managed to comply with the rule, have managed to meet the implementation date.

So, again, I think the focus we're missing the forest for the trees here because for those licensees that it, they perhaps were more proactive, spent resources earlier. We should not be penalizing them for having done the right thing by necessarily granting extensions to others.

So all of these issues do sometimes get looked at more easily and in hindsight, people were concerned about the rule, but I think they were going to be concerned about the rule no matter what. So, in my mind, the simplest way would have been to approve no exemptions and start enforcing and I think we would have seen to some extent what the real issues were and what could, and couldn't be done in the implementation period that we had.

So, I would like to turn to another issue: The integrated pilot comprehensive exercises. I had a chance to go to the exercises in that was Limerick and I think it was a very good program. The one concern I have with this and it's clearly not for NRC a regulatory program.

Personally, I don't know that's the right

answer, I think maybe there is a way to develop some kind of regulatory clarity here or some kind of a regulatory program that puts us on par, with, I think Jim, as you said in this context that we have a EP program that is kind of a defense-in-depth. This is in many ways a defense-in-depth for our security program.

Absent us doing that who long term is the steward for this program and who has responsibility for it? Is it DHS? Is it FBI? Who is kind of the Federal owner of this going forward?

MR. CORREIA: FBI is. Given the nature of this exercise, the technical take back, they are best equipped to deal with that. They train on it. They can train local law enforcement to be able to deal with it. So they are the lead.

CHAIRMAN JACZKO: Do we have the sense that FBI intends to continue it long term, that they are committed to it from a budget perspective, from a resource perspective?

MR. CORREIA: Based on what we know today, yes, sir.

CHAIRMAN JACZKO: Good. It's certainly good to see and I think it is an important program and we will get a lot of the next exercise and be able to really improve this integrated responded activity.

As you look at the hostile action based exercises,

and again, I think you talked about the interest in continuing to move that program forward and there's been a lot of discussion about how we should do that; is there a regulatory impediment to simply doing it as one of the exercises? You talked about kind of having it as ancillary element, I think of a current exercise pending the rule change. But is there anything right now that would prohibit us from actually doing this in the exercise program? Are the rules restrictive enough that they would be violating FEMA requirements or our requirements if they actually did one of these that way?

MR. MILLER: We looked at what's an elegant way, a good way to just go ahead and try to practice these within the exercises and there are some limitations. First of all, they are working to existing emergency plans and their existing emergency plans don't have certain elements in them like the incident command elements and some of the other features

So if they were to plan an exercise and then, we were to evaluate them, you get into what part can we evaluate and can FEMA issue a deficiency on and can we --

CHAIRMAN JACZKO: Regulatorily, it can't work?

MR. MILLER: It was a gray area and was difficult. We

looked at that with FEMA, put together a set of guidelines that would try to get you through that, break up the gray area and say okay, you would be able to for example, enforce this part or issue a deficiency FEMA for this part. This part would be tested out and we're going to make no comments in our inspection report.

We laid those guidelines out and what we found is not only licensees but states and locals were saying, the reason why we're hesitant about that is because when you lay it on top of an exercise, there is a lot of angst, a lot of the gain even at the local and state level, if they get a deficiency from FEMA, they really are concerned about that. They don't want that hanging over their head.

CHAIRMAN JACZKO: Does FEMA have the discretion to not issue them a deficiency? If the purpose of the exercise were different, do they have that authority or is that something FEMA didn't feel comfortable? .

MR. MILLER: There is different thoughts in different places in the REP organization with FEMA but there was a lot of angst about that, whether they can actually observe something, see them and something that they would normally issue an deficiency for, but because this was a practice, they are not going to it in the exercise because you don't have – you've got another two years until they can evaluate that area again. if they

didn't issue the deficiency then they would have another two years and they were uncomfortable with that approach.

I think we're going to get to a place where we want to be and that -- we weren't sold that you have to do it with an exercise and it's different at each site.

You heard Trish mention that on the security side, but on the EP side it's different at each site. There are some sites we would hold up right now and say, they got a great program and other folks ought to look at those but there are other sites that are way behind and so there is -- each one should be tailored a little bit differently. So it might be a table top at one facility and it might be an exercise or drill at another.

That is what we are working through right now. What is the best approach to get through this at all 64 sites?

CHAIRMAN JACZKO: I appreciate that and I think it's good to see that everyone seems to agree on the concept which is to get it done and keep doing it because it has been a very successful program and one that continues to make our sites better and better prepared. So I think it is good to keep working to find a solution.

Patricia if I could ask a question on force-on-force program. And I think it's really two elements to it.

One, as a simple kind of performance measure for the new changes, in light of the new significance determination process, have you gone back and looked at -- would any other findings that we've previously made that have been identified as white findings not be white findings? And would any previously identified green finding be white findings with the change?

MS. HOLAHAN: We haven't gone through that exercise yet. We can go back and look at the last year and see if -- that's what we are planning on doing in the near term.

CHAIRMAN JACZKO: What's your sense? Would you anticipate something happening that way or not?

MS. HOLAHAN: I'll say yes because it can go either way.

Some may have had a great than green finding whereas some may have just been a green finding.

CHAIRMAN JACZKO: As part of that then, what conceptually are the kinds of things that would lead you to a red -- would it be possible under the new SDP to get a red finding here?

MS HOLAHAN: Yes, it would.

CHAIRMAN JACZKO: Conceptually, if you could go into what it would involve in a red finding

MS. HOLAHAN: I don't think we can go there in this forum.

CHAIRMAN JACZKO: And finally on this issue, have we gone back and confirmed that the changes we're making are consistent with the statutory direction on the program?

MS. HOLAHAN: Yes we have

CHAIRMAN JACZKO: And OGC is comfortable with that.

MS. HOLAHAN: Yes.

CHAIRMAN JACZKO: Fine. Dr. Klein.

COMMISSIONER KLEIN: A few more question but I'd like to make a general comment. I would encourage Rich and Jim and Bill to continue using your professional judgment on enforcement and discretions and exemptions.

There is a big difference between the theory of rulemaking and the practice of regulation. As a former licensee, I can tell you that when you read those rules, it is oftentimes difficult to really determine what the intent was or what you're after. And that's why Reg Guides are so important. So as an former licensee, I can assure you that from the licensee standpoint, it's difficult to speculate on why they take action and when you speculate, oftentimes, you're wrong. So I would continue to encourage you to use your professional judgment in this area.

Rich, on a question that I have in terms of cyber

security plans, if we look at a plant that is considering expansion, so we will pick Vogtle because it's out there.

If you look at the cyber security for Units 1 and 2, will the cyber security be similar or the same for Units 3 and 4, and how do you evaluate those?

MR. CORREIA: They could be similar. Actually, we are evaluating both Units 1 and 2 and 3 and 4.

Units 1 and 2 follow the operating fleet guidance through NEI 0809 Rev 3. The newer plants have taken a different path and we are working with them to try to understand exactly what they want to accomplish.

They are going down a unique avenue, I must say. In fact, we are meeting with them this week to explore again, how their cyber security plans for the new reactor are acceptable that meet the regulations.

COMMISSIONER KLEIN: On the new plants, are you going to try to look at cyber security generically like for the AP 1000 and the EPRs to look at a generic --

MR. CORREIA: Vogtle is the lead plant for their plant design. So others could follow suit. It turns out the South Texas plant, they followed our Reg Guide exactly so that was a relatively easy review so there is not consistency on the new fleets -- new plants.

COMMISSIONER KLEIN: On the MOU with NERC, obviously a press release came out about that recently. Any open items, any surprises still lurking or do you think it's pretty well --

MR. CORREIA: I think it's pretty well understood. We worked hand in hand with OGC and NRR to establish that MOU. I think we understand what their responsibilities are and what ours are. There is -- excuse me -- there is still some question exactly where that bright line is at any one plant where their jurisdiction begins and ours ends, but we will work that out as we go forward.

COMMISSIONER KLEIN: The last question I had was was on the DETRA take back activities.

I know there was some apprehension about how that information was controlled and Utilities had some concerns about that access falling into the wrong hands.

Are those issues pretty well resolved?

MR. CORREIA: Yes, we worked with FBI to rewrite their standard operating procedure. We've been at every site giving training on safeguards control and so far, it has worked very well.

The goal was to limit very much who had access to that information.

COMMISSIONER KLEIN: Thanks, no more questions.

COMMISSIONER SVINICKI: Just a couple of more areas that I wanted to talk about. Kathryn, I know we referenced a little bit the planning, the infrastructure planning for the new building, and often that clean sheet of paper having a -- building out a new facility is a unique opportunity in terms of cyber requirements and other planning for the future. Retrofitting is always kind of sub-optimal when you have to retrofit new requirements in a older building. And so my question is really on the theme of in the experience we're having and certainly working with GSA, are we able to be forward looking enough?

I'll use as an example, our circumstance here, our IT needs have certainly grown over the time that NRC has occupied these two buildings. And so when we have a summer power outage, you think to yourself, well, at least, we have things like blackberrys and people can work from home. And then, you find out our server farms can't be chilled because we lost our power and remote computing capability as well.

It would seem to me that a building is an opportunity to appropriately size things and really plan for our needs going forward. Is that the experience -- are you confident that we are capturing those opportunities as we

plan for the future things like our operation center and other kind of core mission areas that we need to cover? Are we looking forward appropriately in your view?

MS. GREENE: I think so. We are in the process of formulating several teams to work on the project. We have a project team which is NRC, GSA and the developer LCOR. We have a core team which are the various elements of the Office of Administration, Facilities, Security, our space planning, our administrative services and also, the Office of Information Services. They will play a critical role in developing our requirements for electricity and power and across Marinelli is another grid. So we can lose power here but not there. So that's very beneficial to us. And that was part of our consideration as we and GSA evaluated the selection of the site for Three White Flint North.

That was very important to us. Then we have a occupant team composed of the offices that will be going into Three Flint North and the National Treasury Employees Union will play a critical role in providing us input in that regard as well. And with the Chairman's recent decision to relocate the Operation Center, we be inviting NSIR to join us on the core team because they will play a critical role in that.

As part of our program of requirements, we did

identify the need for a data center in Three White Flint North, so that will be a part of our planning.

COMMISSIONER SVINICKI: And then again, I don't know what the right answers. It's more the broad theme of you know, you kind of only have one shot when you have an opportunity like this. And the windows to make these decisions and consider alternatives are often narrower than you think. You think you have all this time but you really don't. So I'm glad that we have teams looking at that and we are getting the right involvement across the organization.

Another topic you mentioned that I think is really important but didn't know would come up today is strengthening the NRC acquisition capabilities, our training of acquisition officials and I know that is a government-wide initiative but with the growth in NRC's budget, we certainly have – we're doing more procurement and acquisition than ever before in the agency's history as a percentage of its budget. So again, another organizational value is training. So we are a training organization and it is good to hear.

Do we have access to good vendor training services there? Are you happy with the kind of capability of

training that's available to our employees?

MS. GREENE: We developed an in-house acquisition certification and training program geared to the NRC environment. So we use NRC examples so that it's easily relatable to our project managers and technical monitors and we have had that program in place for many year and we are augmenting that program.

We also rely on the Federal Acquisition Institute which provides Government-wide training and there are several vendors in the metropolitan area that offer very good and competent procurement training which we send our contracting staff to. So we use a mix of training providers.

COMMISSIONER SVINICKI: Thank you for that. In a couple of the topics, the issue of controller training came up. That's not our training but the one force-on-force that I observed, I think it was Trish you mentioned or you were setting some context for the importance of he controller role, those type of exercises. And in my case, all I needed to do was observe one in order to have that point hit home to me of how important that is. It's also of course part of the artificiality of what we are doing is that the participants and the exercise having controllers kind of

jogging alongside of them. So I took away from the force-on-force I observed the importance of that. But where do you go to really develop good controller training? It seems to me we are kind of on the cutting edge of his notion.

Are there other institutes and knowledge management or knowledge centers that would be able to guide us and help us and therefore, we could work to help licensees have better training?

MS. HOLAHAN: Well, there are private entities that have offered to the industry to help them with controller training. And we encourage the licensees to take advantage of that.

We have -- with the new Part 73, the requirements are in place to make sure the controllers are properly trained and can perform their tasks. And what happens is often the licensees use a different licensee to provide controllers because their security forces can't support everything else.

So within a fleet, you can get controllers from various organizations.

But I think we are working with the licensees to make sure that the controllers are being trained appropriately and they are performing their tasks. And it's

just a matter of getting the right entities to put the time and effort into it, rather than because oftentimes we find out that they throw the controllers under the bus and it is an artificiality of the exercise. And if the controllers can be trained appropriately, then we get fewer time outs and fewer misunderstandings.

COMMISSIONER SVINICKI: That was clearly the lesson I took from it. It can be a key determining factor, the quality of the controller's training and experience can be a key determinant in the quality of the overall exercise. Chris, I think you were the other person or maybe Rich mentioned it.

MR. CORREIA: Yeah, I mentioned it as part of the lessons learned from Limerick. The individuals that were chosen to be controllers, they were more safety conscious, not getting into the wrong areas of the plant versus security. So you need that mix. You need to understand both safety and security to be a good controller.

COMMISSIONER SVINICKI: And then for those that don't operate a fleet, I mean, what are their alternatives in terms of having quality controllers? Do they face a much larger problem?

MS. HOLAHAN: Yes and no because the new requirements provide and the Reg Guides on physical security

provide guidance to the licensees as to how to train the controllers and what to put in the training program. And the nuclear security working group is a mechanism that they can reach out to other entities.

COMMISSIONER SVINICKI: Thank you. Thank you Mr. Chairman.

CHAIRMAN JACZKO: This is an interesting topic that Commissioner Svinicki raised. With the new force-on-force significance determination process, will you look at controller issues as an element of the evaluation?

MS. HOLAHAN: Yes. Both the controller training and the controller performance.

CHAIRMAN JACZKO: It is a way to enhance or try to at least provide an opportunity to encourage licensees to make improvements in that area. I think that is certainly one of the benefits of the new program. It does as she said come up quite often in exercises if there are challenges. It is often that their can be controller issues that go with it.

I want to thank everyone for a very informative briefing and very good presentations about all the work that goes on.

It demonstrates that we continue to be an agency that is at the forefront of addressing and dealing with

security issues.

These are not simple issues. I think just as you hear the discussion among the Commissioners, these are complicated issues with a variety of different solutions and I think it is important that we continue to explore them and continue to look for the right solutions, we continue to talk to stakeholders and talk to licensee and get good feedback.

I want to thank everybody for a very productive meeting and we will adjourn until we have a closed discussion this afternoon on our threat assessment. Thank you.

(MEETING ADJOURNED)