Official Transcript of Proceedings

NUCLEAR REGULATORY COMMISSION

Title: Advisory Committee on Reactor Safeguards
Digital instrumentation and Control Systems

Docket Number: (n/a)

Location: Rockville, Maryland

Date: Wednesday, March 20, 2019

Work Order No.: NRC-0219 Pages 1-174

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

DISCLAIMER

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

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

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

UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

+ + + + +

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

(ACRS)

+ + + + +

DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS

SUBCOMMITTEE

+ + + + +

WEDNESDAY

MARCH 20, 2019

+ + + + +

ROCKVILLE, MARYLAND

+ + + + +

The Subcommittee met at the Nuclear Regulatory Commission, Two White Flint North, Room T3B50, 11545 Rockville Pike, at 1:00 p.m., Charles H. Brown, Jr., Chairman, presiding.

COMMITTEE MEMBERS:

CHARLES H. BROWN, JR., Chairman

RONALD G. BALLINGER, Member

DENNIS BLEY, Member

VESNA B. DIMITRIJEVIC, Member

WALTER L. KIRCHNER, Member

JOSE MARCH-LEUBA, Member

HAROLD B. RAY, Member

GORDON R. SKILLMAN, Member

MATTHEW W. SUNSERI, Member

ACRS CONSULTANT:

MYRON HECHT

DESIGNATED FEDERAL OFFICIAL:

CHRISTINA ANTONESCU

P R O C E E D I N G S

1:22 p.m.

CHAIRMAN BROWN: The meeting will now come to order. This is a meeting of the Digital I&C Subcommittee. I am Charles Brown, Chairman of this subcommittee meeting. ACRS members in attendance are Dennis Bley, Walt -- where are you, Walt? Walt Kirchner, Jose March-Leuba, Matt Sunseri, and who else did I -- Myron Hecht, our consultant who is visiting. Oh, and Ron Ballinger decided to attend also. Oh, I forgot Dick. Sorry about that, Dick. Dick Skillman is also with us. Christina Antonescu of the ACRS staff is the Designated Federal Official for this meeting.

The purpose of the meeting is for the staff to brief the subcommittee on cyber security oversight program to date and lessons learned from the staff's inspections. The ACRS was established by statute and is governed by the Federal Advisory Committee Act (FACA). That means the committee can only speak through its published letter reports. We hold meetings to gather information to support our deliberations.

Interested parties who wish to provide comment can contact our offices requesting time after the Federal Register notice is published. That said, we also set aside 15 minutes for spur-of-the-moment

comments from members of the public attending or listening to our meetings. Written comments are also welcome.

The ACRS section of the U.S. NRC public website provides our charter, bylaws, letter reports, and full transcripts of all full and subcommittee meetings, including all slides presented at the meetings. The subcommittee will gather information, analyze relevant issues and facts, and formulate proposed positions and actions, as appropriate, for deliberation by the full Committee.

The rules for participation in today's meeting have been announced as part of the notice of this meeting previously published in the Federal Register. We have received no written comment and requests for time to make oral statements as members of the public regarding today's meeting.

As always, we have one bridgeline established for interested members of the public to listen in during the open session. Also, the bridgeline will be open after the opening meeting session to see if anyone listening would like to make any comments.

The meeting will be open to public attendance with the exception of portions that may be

closed to protect information that is proprietary. We have received no written comments and requests for time to make oral statements from the public regarding today's meeting.

A transcript of the meeting is being kept and will be made available as stated in the Federal Register notice. Therefore, we request that participants in this meeting use the microphones located throughout the meeting room -- actually, there's only one -- when addressing the subcommittee. The participants should first identify themselves and speak with sufficient clarity and volume so that they may be readily heard.

And then please silence all cell phones, pagers, iPhones, iPads, and any other electronic devices or appliances which you have.

We will now proceed with the meeting. I would like to say that -- oh, Harold Ray also, another member, has also joined the meeting.

I call upon Ms. Shana Helton to make some introductory comments as Director of the Division of Physical and Cyber Security Policy in the Office of Nuclear Security and Incident Response for some introductory remarks. Shana?

MS. HELTON: Thank you very much. It's

a pleasure to be here addressing the ACRS today. With me is Eric Lee and Jim Beardsley from my division, and we hope that this will be a good opportunity to give an overview of where we're at with the implementation of the cyber program.

I recognize it's been quite a long time since we've addressed the Committee. Back in the early 2010, maybe 2013 time frame I think was the last time that we gave you an update. Around that time, we were in the midst of implementing Milestones 1 through 7, if you recall. We had eight milestones in our phased implementation of the cyber security program. It was a big lift for the industry.

We completed Milestones 1 through 7 in 2012, and we conducted inspections in 2013, 2014, and 2015 to verify that the most significant CDAs were protected and licensees were properly installing the deterministic data diode, which is very important, and you'll hear from the staff about the diode, to isolate the nuclear power plants from external networks.

Milestone 7 or, I'm sorry, Milestone 8, for full implementation, was complete by most licensees in December of 2017. We are actively inspecting the implementation. We'll get into the details of that. I think we've inspected about a third of the fleet

at this point. And so far, those inspections are going very well. We have a contractor who assists us on those to help bring some of the very specialized cyber security expertise to the table. We've been working closely with the regions and the regional inspectors to get them familiar with the program, as well.

And you'll hear more about it, but, just to tee it up, we are in the midst of a cyber assessment. We feel that we've got enough of the inspections under our belt with that first third of the industry having been inspected under Milestone 8.

To pause, not pause because the inspections are ongoing but to take the time now to have an independent team look at what we've done from the rule to the guidance to the oversight program, the entire cyber program, and to see what lessons learned we can gain. So today you won't hear the outcome of that. That self-assessment is ongoing. We anticipate it will be finished up in the June - July time frame and perhaps, if there's interest, we could come back and talk about some of our lessons learned and our planned activities going forward. Maybe in the fall time frame we can look for the right time.

Our goal today is to give a general overview to cover where we are at with the cyber security

oversight program. Our remarks are going to focus on the power reactors in general because that's the only area that has a regulatory requirement for cyber.

We will give an update later in the meeting, and there won't be a whole lot to say but we'll give an update on the status of the fuel cycle facility rulemaking. Not much going on there.

So for the following areas that we're going to cover in the brief, we presume that these are of the ACRS interest. This was our understanding from the planning meetings. But if there's any questions that you have, I'll just say that Eric and Jim are very knowledgeable and we're here to give you the information that you need. So if our agenda doesn't cover it, you know, I hope that we can answer your questions on the fly because we do have the right expertise in the room.

So with that, I'll just keep my remarks very brief and get right to the presentation. But thank you again. We look forward to having a good discussion today.

MEMBER BLEY: Before you switch off --

MS. HELTON: Sure.

MEMBER BLEY: -- from what you said, are there no requirements for cyber security for fuel facilities?

MR. BEARDSLEY: The post 9/11 orders for the fuel facilities did include mention of cyber security, but the details of that were not well defined.

MEMBER BLEY: Okay.

MR. BEARDSLEY: And I'll talk a little bit about what --

MEMBER BLEY: I know it's not pressing now, but it could be.

MR. BEARDSLEY: Sure. And we can talk some more about that when we get to that point. We can give you a little more background on where we believe that's going to go.

MS. HELTON: The rulemaking effort, to codify cyber requirements is, the rulemaking efforts to codify those cyber requirements for fuel facilities is not active right now.

MEMBER BLEY: Okay. And for me, if you would, I've looked through the slides. A lot of it looks very familiar. Some of our members weren't here the last time we went through it. Could you highlight, if you can, any areas where things have changed since the last time you came to see us --

MR. BEARDSLEY: Sure. I can do that.

MEMBER BLEY: -- in the requirements or others? And are you going to get into details on any

of the inspections? I think we'd be interested in that.

MR. BEARDSLEY: We will definitely talk about the inspections, and we'll talk about, at a high level at least, lessons we've learned so far and the things we're doing about them.

MEMBER BLEY: Okay. Very good. Thanks.

MR. BEARDSLEY: Okay.

CHAIRMAN BROWN: Before you get started, Jim, I'd like to highlight that Vesna Dimitrijevic has also joined us.

MR. BEARDSLEY: Well, good afternoon. My name is Jim Beardsley. I'm the Chief of the Cyber Security Branch in NSIR's Division of Physical and Cyber Security Policy. I've been the Cyber Security Branch Chief for three years. Prior to that, I had an extensive period of time in the NSIR as a force-on-force team leader, so I have a very strong background in both physical security and now in cyber security.

If there are questions about the program that relate back to long before my time, I brought my lifeline, Eric Lee, who has been our lead for cyber security basically since we stood up the post 9/11 orders and instituted our cyber security oversight program.

Based on the questions we received or the

outline we received when we started preparing for the brief, I'm going to try to follow this time line that you see in front of you, this is the first set of it, and base my remarks off the time line. So you're going to see slides sort of like this repeated as we go through the presentation, and I'm going to highlight where we are as we've developed the program and the lessons that we've learned.

Starting in 2001, after the terrorist attacks, the NRC issued orders to all the licensees and those orders included cyber security as a threat but did not provide much guidance or detail on what the licensees were supposed to do. Industry, the power reactor industry undertook a voluntary program to institute cyber security controls and try and put some guidance in place. The staff went out and did assessment visits to various licensee sites to assess how well the cyber security program was being implemented and, based on the results of those assessments, decided to pursue rulemaking for cyber security. That happened in concert with the update of the design basis threat in 2007 where cyber security was added as one of the five primary elements of the DBT.

In 2009, the cyber security rulemaking was

completed and instituted. And throughout that time period, the staff did work with industry and understand what industry had, what efforts industry had put in place, so we were observing industry and monitoring what they were doing but we were also in the process of instituting rulemaking to codify specific cyber requirements and try and firm up a little bit better what the licensees needed to protect.

So the next few slides are basically cut-and-pasted right out of the cyber security rule, 10 CFR 73.54. I just want to briefly highlight it because this helps provide context for basically the entire breadth of our discussion.

So operating reactors and licensee applicants must submit a cyber security plan. So that was the first requirement, and by November of 2009 they were all expected to submit their plans. Staff reviewed their plans and eventually approved all of the cyber security plans as a license condition to their license. So the plans themselves, in addition to the regulation and the rule, are specific aspects of their cyber security implementation. And those cyber security plans are somewhere on the order of 25 to 40 pages long, depending on the particular licensee.

The plans were based on a template that

came out of an NEI guidance document, NEI 0809. And that guidance document had been developed using the NRC Reg Guide 5.71 as a rough basis. So the regulatory guide provides guidance on cyber implementation. The latter part of the regulatory guide is a template for a cyber security plan. Most of the licensees elected to use the NEI template versus the NRC template, and there aren't a lot of significant differences between the two but they did elect to use the NEI template, and the staff reviewed and approved all of those cyber security plans.

What became very apparent after the implementation of the cyber security plans was that the industry and staff recognized that the cyber implementation was going to be very complex. There was going to be a lot of elements to it, and I'll get into the flow that came out of it. But we did divide up cyber security into eight milestones, and the goal of that was to help the licensees focus on the most significant cyber digital assets or critical digital assets in their initial implementation and then we would give them, arguably, a little more time to implement some of the other aspects of the program. But we recognize that those specific aspects, those specific subset of critical digital assets needed to be

addressed.

MEMBER SKILLMAN: Jim, what is the classification of the cyber security plan? Is it safeguards?

MR. BEARDSLEY: It is for official use only, security-related information.

MEMBER SKILLMAN: Thank you.

MR. BEARDSLEY: With the exception of the aspects of cyber security as they apply to physical security systems, those would be safeguards. But the remainder of our cybersecurity implementation is either public or OUO.

So as you see on the slide, the rule focuses us on safety, security, and emergency preparedness functions. And so as we've gone through implementation, and I'm going to talk about how that played out, those are the primary areas where we focused our attention and the licensees have focused their effort.

And then the bottom of the slide lays out the protection requirements, so they must protect from cyber attacks that adversely impact the elements listed here. And, again, and you're going to see this on the next two slides, the rule is very high level. So the rule doesn't provide a lot of infinite detail. When

you get into the cyber security plans, there is significantly more detail. But the breadth of a cyber security program is so broad that, even with a specific plan commitment, there's still a lot of, I'm not going to say interpretation but there's a lot of elements that need to be better understood that the licensees have then taken sub-tier documents for implementing procedures.

So as I get into talking about inspection, one of the lessons we've learned is there's a lot of documentation and a lot of requirements that inspectors have to dig through to really truly understand the licensees' implementation.

MEMBER BLEY: Jim, as you've begun to look through the individual plans, have you found any cases where the cyber security plan had conflicts with either safety or EP?

MR. BEARDSLEY: We have not. So one of the things we did look at initially in our inspection program and we continue to look at as the safety - security interface, it's one of the primary tenets we use in physical security and we've used that same construct as part of cyber security, and, in general, we have not found any significant issues.

MR. LEE: Also, in the cyber security plan,

if there's a conflict between safety and security, they're supposed to take the safety first, rather than security, and address the specific security issues alternatively or with different means.

MEMBER BLEY: Find some way to integrate them.

MR. LEE: Absolutely.

MR. BEARDSLEY: So this slide, this is slide four, goes into a little bit more detail on the protections and the methodology that the licensees are required to use. And what I want to highlight on this slide is at the bottom there it talks about applying and maintaining defense-in-depth. So it's relatively simple to look at putting a barrier up, and this is the same philosophical approach we take in physical security. You can put a fence, but, you know, if someone was to be able to defeat that fence, you need to have multiple layers and different aspects. And we do this in both physical security and in safety. Defense-in-depth is a very important aspect of what we've gone.

In cyber security, what we've laid out as a requirement for the licensees, and this is pretty well defined in their cyber security plan, is the concept of detection response and recovery or detection

response and elimination we call it. And so what we've done is the licensees have to demonstrate to us through the implementation of their plan and multiple controls in their plan how they can detect, respond, and then recover or eliminate, eliminate and recover from a cyber attack. And that has become somewhat challenging in some respects, and I'll talk about that as we get into it. But there's pretty, there are multiple places in their cyber security plan where they commit to defense-in-depth and we have focused on that in our inspections to make sure that there's no single answer, that there's a multiple layered answer, so, if a cyber attack was to get implemented, they understand the requirements they have to make to identify and then isolate the issue and then recover from it.

MEMBER BLEY: Jim, what kind of program do you have on the staff and does industry have to track and understand cyber security attacks in other industries so that you can refer that information back to make sure the plans are adequate?

MR. BEARDSLEY: That's a great question. So the staff works closely with our intelligence branch in NSIR to identify both classified and also unclassified law enforcement information as it would relate to a cyber attack. We also, the branch itself

works closely with our colleagues in the Department of Homeland Security to track potential issues with cyber attacks and, in particular, vulnerabilities. But the industry itself, based on a law, has a relationship with Department of Homeland Security that the regulator is actually cut out of, and the reason for that is they want -- and this is not just our industry, this is multiple industries. Most regulated industries have this established relationship with a center of expertise in Department of Homeland Security that allows that industry to feel comfortable to dialogue back and forth with DHS, and the concern would be is, if they potentially had an issue and the regulator was involved, there's concern that that would mitigate their communication with DHS. And we would prefer that they have an open dialogue and make sure that they can identify and resolve any potential cyber issues.

We do understand that, and we also coordinate with both industry and DHS to understand how that dialogue is playing out. And to date, we haven't had any issues with the open discussion between them, but the --

MEMBER BLEY: Has that mechanism been exercised much between the --

MR. BEARDSLEY: It has, it has. And I'll

talk at the end of the presentation about a couple of cyber incidents that have happened in our industry and how the dialogue between the industry, the staff, and Homeland Security played out and I can give you a little piece of that.

But for the purposes of threat warning, the way it's being viewed today is primarily the responsibility of the Department of Homeland Security. We understand threats, and we are prepared to send out a security advisory if it's appropriate. But the licensees, you know, either through their information technology and/or their industrial control system cyber security programs, have direct relationships with DHS, as do all the critical infrastructure, and they're going to get that information immediately. So we think that's a pretty healthy relationship, and we're pleased with the way that's working out.

MEMBER BLEY: The rule is high level enough I have trouble imagining a scenario that would crop up that wouldn't, you couldn't somehow say the rule covers that. But in implementation, maybe it doesn't, so I don't know if anything like that has occurred so far.

MR. BEARDSLEY: That's a great question. I'll talk about that as I get into some more of the

mechanics of the rule. But there are some areas where licensees, you know, have had cyber attacks that are not reportable to us because of the cognizance of the rule. I'll explain a little bit how that played out.

MEMBER BLEY: Thank you.

MR. BEARDSLEY: Okay.

CHAIRMAN BROWN: Before you leave that, go back a slide, back one. You talk about defense-in-depth and you say detect, respond, and recover. A key element that we've emphasized, and we've chatted about this before the meeting, was isolate. In other words, you never have a door that can be opened.

MR. BEARDSLEY: Sure, yes.

CHAIRMAN BROWN: And that's -- why isn't that explicitly stated as part of one of your general approaches from the defense-in-depth standpoint?

MR. BEARDSLEY: Well, I can't say how the rule was written and why the rule was written. I'm giving you the exact words out of the rule here. But when you go into the licensee cyber security plan that is part of their license, they do have a requirement to provide a deterministic boundary device that isolates the industrial control systems from the internet, effectively, in a cyber attack. So that's

a requirement. It's just not a requirement explicitly stated in the rule.

CHAIRMAN BROWN: Okay. Go ahead.

MR. BEARDSLEY: And on this slide, we just laid out a few more of the requirements, in particular the training requirements. And the training is one of the areas we do look at closely, we have in our inspection program and we'll continue to, not only just general training for the staff but also specific training in areas like configuration management, change management, and the operators who operate systems that will make sure the licensees are conducting a big picture review of potential cyber incidents.

So most of the licensees, in fact, I would say all of the licensees we've inspected to date have demonstrated that they have incorporated cyber security into their change management processes across the board. Any change they make, they have to check and make sure that there's no impact on cyber security. We think it's a very healthy program, and the industry seems to have implemented that sufficiently.

CHAIRMAN BROWN: Maybe you get to this later in a couple of slides. Do the programs account for insider possibilities and detection? If I raise anything that you shouldn't talk about in an open

meeting, just say so.

MR. BEARDSLEY: Sure, sure. Well, the licensees have insider mitigation programs that are instituted and inspected by the staff. And that's been well documented in physical security inspection space over the years, so we understand that. We also have included the critical group, which are the folks who are, part of that fitness for duty monitoring aspect of insider mitigation. And the implementers of cyber security programs, maintainers of cyber security programs are all included in that critical group, so anyone who has access to any critical digital asset is required to be in the critical group and monitored as part of their insider mitigation program.

MR. LEE: Additionally, in their cyber security plan, there are a number of security controls that monitors the unauthorized access and the logging in, things of that nature. That's why we have the detect and mitigate part in there, so there are a number of controls in addition to this access control, to address that particular issue.

MR. BEARDSLEY: Thank you. So at the bottom of this slide, I highlighted the cyber security program as part of physical security. If you look at the way cyber security is structured in the regulation,

10 CFR 73.55 which is our high-level physical security requirement, that is a higher tier to 73.54. So 73.55 leads you to 73.54, and the staff has approached cyber security implementation under the auspices of the physical security program. So I just wanted to make sure I highlighted that there because that's fundamental to the way we've approached cyber security as an entity.

MEMBER BLEY: Can I follow up on that --

MR. BEARDSLEY: Please.

MEMBER BLEY: -- insider question? Most of the questions I've asked I can imagine solutions. This one I have trouble imagining a solution. Suppose an insider did do something to the software in the plant. Is there anything within the plan that helps detect oddly-functioning software along the way?

MR. BEARDSLEY: The specifics of the defense-in-depth requirement in the cyber security plan don't get down to a finite detail, but they do require the licensee to identify deviations or malware, something like that, within the system. So if, for instance, if a licensee or if someone who didn't have authorization tried to access to a critical digital asset with a memory stick or trying to log in and change the settings, licensees are required to have password

protection, they're required to have locks and alarms, tamper seals and things --

MEMBER BLEY: These are all preventative.

MR. BEARDSLEY: These are all preventative. So in --

MEMBER BLEY: Protection is what I was asking.

MR. BEARDSLEY: But it all comes together. So some of the assets are not high-functioning digital assets, so they don't have a network or modern information technology such that we could install modern monitoring systems on them. In those cases, the licensees have elected, because they understand they have a requirement one way or the other, so in those cases the licensees have used locks and alarms and configuration management and work processes.

If the system is digital, and where we see it the most, to be honest with you, is in the physical security implementation system. Those are, in general, newer systems, fully digital, based on network technology. The licensees understand that they have to have protection response and elimination there, which includes network monitoring, host intrusion detection, the kind of techniques they would use.

So if someone, for instance, walked in and

tried to stick a memory stick into security computers, it would either not be recognized because it's not part of their system or there would be a cyber alert going back to the cyber folks saying, hey, there's something going on that's not authorized. So that is addressed within the bounds of the cyber security plan.

MR. HECHT: Those are really for TCP/IP-based systems, which are primarily information systems.

MR. BEARDSLEY: Correct.

MR. HECHT: That's not going to occur within the control or the safety side of the plant, is it?

MR. BEARDSLEY: For those critical digital assets that are network based, they have a requirement to have virus protection, host intrusion detection. They use whitelisting or blacklisting, depending on how -- so there are techniques and tools that they've installed. For those that do not, that don't have their own ability to detect, you know, some kind of malfeasant activity, the licensees have used other physical security boundaries, work control processes, and things like that to prevent someone from having access to the systems.

MR. HECHT: So by network based, you mean

specifically TCP/IP network based, as opposed to field bus-based systems, right?

MR. BEARDSLEY: Where a licensee can install those monitoring systems, they would. Where they can't because the technology doesn't exist, they would have to use other techniques. But that doesn't get them out of the requirement. They still have to address the requirement one way or the other.

MEMBER BLEY: Systems, like the reactor trip system and safeguard systems, are, they're custom designed. They might feed data to a network, but they are not network-based.

MR. BEARDSLEY: For most of the fleet we have in place today, that's correct.

CHAIRMAN BROWN: All you have there is, you don't have any internal mechanisms built into that other than you're supposed to, the check zone and basic redundancy checks, stuff like that, that you could periodically verify, which would be difficult to modify if you were doing something. You're largely relying on access of control --

MR. BEARDSLEY: That's correct, that's correct.

CHAIRMAN BROWN: There's no internal stuff to mess up the trip system algorithms.

MR. BEARDSLEY: That's correct.

CHAIRMAN BROWN: And they are not network based. I'm just addressing Myron's thought because he's right about the network stuff. There are other systems where your controls are actually embedded in a network, and there you do have concerns relative to how somebody could get in and take control of it.

MR. BEARDSLEY: That's correct.

CHAIRMAN BROWN: Okay. Thank you.

MR. BEARDSLEY: So slide six takes us back to the time line showing what has gone on since 2009. Some of this I've already covered, but I'll just run through it quickly.

So, again, in 2010, the NRC's Regulatory Guide 571 was put in place and followed up with NEI guidance document 0809. They are both reference documents and a template for a cyber security plan. The staff accepted NEI's document for use and, again, most of the licensees used that template as the template for their cyber security plans, which were subsequently codified as license conditions.

In 2011, the staff agreed on a milestone construct, so a phased implementation of cyber security. And I'll talk a lot more in a couple of slides about what that phased implementation was and the things

we put in place early vice those aspects that were a part of Milestone 8 or full implementation, and I'll give you details on that as we go.

I think the big thing here is licensees all committed to have their initial milestones in place by the end of 2012, and they all completed that. And then the staff inspected that implementation between 2013 and 2015. So by 2015 we had inspected 100 percent of the operating units, interim implementation Milestones 1 through 7. We did identify a number of deviations or differences between the staff's expectation and industry's, and what we put in place was a process where we inspected and identified findings but we gave the industry -- what do we call it? Discretion. So the inspectors used enforcement discretion with the findings that we came up with, and the reason we did that is it became clear that the staff's expectation, the inspection team's expectation of how a licensee would meet a requirement wasn't clear to industry when they went and did their implementation. So we cited them, and they had to make corrective actions and fix those things. And none of them made their programs completely ineffective, but there were some implementation details the staff felt could have been done in a different manner or using different

techniques.

MEMBER MARCH-LEUBA: So in that light, now we're fully implemented since last year or two years ago. How is it working? And let me give you more specifics. When we discuss about this a couple of years ago, there was a concern that the licensing would have to spend so much time doing the paperwork for this other plant and they wouldn't have time to implement it. We were talking about you have 500 desktops, you have to do two pages for each desktop or kind of cluster it into 500 of the same.

MR. BEARDSLEY: Sure.

MEMBER MARCH-LEUBA: How did it work?

MR. BEARDSLEY: Well, it did create a lot of paper. And when we, again, do inspections, we do look through a lot of paper. So that all did happen.

But what, initially, the licensee is committed to Milestone 1 through 7 by the end of 2012 and Milestone 8, the full implementation, by the end of 2014.

All of the licensees subsequently submitted license member requests to shift their full implementation dates out. And most of them wound up in December of 2017.

So they recognized that this, in fact, I

think the Staff recognized too, that the scope of work was much greater than initially anticipated. And so, while we were inspecting them, we also gave them the relief to go do the solid job and complete the effort that they had planned.

MEMBER MARCH-LEUBA: So the licensees are still complaining about the effort or are they happy they did it?

MR. BEARDSLEY: Well, they completed it, so.

(Laughter.)

MEMBER BLEY: The same thing a little differently?

MR. BEARDSLEY: Sure.

MEMBER BLEY: Back when we last talked with you, as Jose was pointing out, the identification of critical digital assets was the whole world. Anything that could touch a network.

You had a line or two as an alternative to use some kind of --

MEMBER MARCH-LEUBA: Plastic.

MEMBER BLEY: -- I'll say risk-based --

MR. BEARDSLEY: Sure.

MEMBER BLEY: -- structuring. By the time they did Milestone 3 or 2, and identified all the

critical assets, did they do the world or did they do something focused that was defendable?

MR. BEARDSLEY: Well --

MEMBER BLEY: Was that all in place when you did your inspection?

MR. BEARDSLEY: Let me go onto the slide. That's a great question.

MEMBER BLEY: Thank you. You're welcome.

MR. BEARDSLEY: So, let's just talk about the milestones. So the first thing the licensee had to do was establish a multi-disciplinary team to go identify the assets.

So it wasn't just cyber folks, it was operations folks, maintenance folks, physical security and information technology. Because we wanted to make sure, and we still inspect those teams as part of our inspection to make sure they have, including an emergency preparedness as well, make sure they have a multi-disciplinary team because no one in the plants really understands all aspects of what they're doing.

So, they did the teams and then they identified the assets. And initially, the licensees had, initially we did not think the broad spectrum of the assets was going to be as large as it is.

And there's two reasons for that. One,

the true understanding of what a critical digital asset was probably wasn't exactly well understood, both by Industry and the Staff.

In the same time period, the NRC signed a memorandum of understanding with the Federal Energy Regulatory Commission to draw a line for cyber cognizance. We called it the bright line agreement.

And so, NRC has cognizance over all digital assets that are from the first intertie breaker and the transformer yard, back into the system. There's two reasons for that.

One is, the licensees had fear of being dual regulated. And they didn't want to have to be regulated and have to answer to two different regulators.

And it also helped us define, clearly, what were the licensees, because at the time, the NRC had our rules in place and FERC CIP standards weren't quite mature, so it helped the licensees understand, okay, yes, we can get to work on these while we're waiting for FERC to complete their CIP standards and what the bulks power system would have to meet.

When we did that, we added about 70 percent, somewhere between 70 and 80 percent more critical digital assets. So the average unit in the fleet today

has about 2,000 critical digital assets.

And I'll talk a little bit more about what we did about that in the future, but recognizing that, the Staff implemented a risk assessment and a risk-based methodology to reduce the number of controls that licensees had to address for many, many of those assets.

And I can get into some more detail on that as we go, but we did --

MEMBER BLEY: Has that been documented in the guidance then?

MR. BEARDSLEY: Yes, that is documented in NEI Guidance Document 13-10.

MEMBER BLEY: NEI document.

MR. BEARDSLEY: Which the Staff has accepted for use. And the Staff was heavily involved in that development. And the subsequent updates.

In fact, Eric is arguably one of the primary authors of that document.

MEMBER MARCH-LEUBA: Is that the public rule? I mean, I'm thinking it should be a safeguard sensitive.

If I tell you I am going to protect laptop but then I'm going to protect desktops, I know what I need to attack.

MR. BEARDSLEY: Eric?

MEMBER MARCH-LEUBA: Do you understand the question?

MR. LEE: Yes. But it doesn't tell you exactly, it provides a criteria by which a licensee can use it, therefore it's not a --

MEMBER MARCH-LEUBA: The answer, if you have thought about it and you have a, I don't need the answer --

MR. BEARDSLEY: Okay.

MEMBER MARCH-LEUBA: -- I just want to make sure you've thought about that.

MR. BEARDSLEY: Yes, we have. We have. And so, the specifics are not in the document. The methodology for making that determination is in the document.

MEMBER MARCH-LEUBA: Okay.

MR. BEARDSLEY: Okay. So, Milestone 2, download critical digital assets.

Milestone 3, implement a one-way deterministic device. And that's a requirement in their plan.

And that was inspected during the initial milestones. And I'll talk a lot more about how that played out and what those are as I go through it.

MEMBER BLEY: And really, the definition

of what that means?

MR. BEARDSLEY: Right. I will talk about that.

MEMBER BLEY: Okay.

MR. BEARDSLEY: The next one, access for portable media. This has become one of the major focus areas of our program.

Because all these assets, almost all of them, are going to require updates of some kind. Either software updates, virus protection updates, something. And so you have to have a program to screen those updates and anything else that goes beyond.

So once you have a deterministic device and build a wall, you have to be able to make sure nothing can get around the wall. And so, I'll talk about how that's implemented.

But those were all inspected in that 2013 to 2015 time frame.

MEMBER MARCH-LEUBA: We have heard from one licensee that they inspect EPROMs when they come into the plant.

MR. BEARDSLEY: They do.

MEMBER MARCH-LEUBA: They do?

MR. BEARDSLEY: They do.

MEMBER MARCH-LEUBA: And it's not just

laptop or cell phones --

MR. BEARDSLEY: Right.

MEMBER MARCH-LEUBA: -- USB drives, they go to the EPROM?

MR. BEARDSLEY: Yes. Anything that's identified as a critical digital asset. They have to inspect, and they have specific requirements in their cyber security plan and how they have to maintain control of and test that equipment.

And we've spent a lot of time working with Industry, both on a supply chain side and on a portable media side to make sure that, because we recognize that's probably the biggest vulnerability of the entire program.

MEMBER MARCH-LEUBA: Yes. And I'm sure they understand they have to do it, but my question is, are they complaining too much?

Is this costing them on FTE or 150 FTEs to implement?

MR. BEARDSLEY: Going back to your question before, along the same lines. The licensees did push back on some aspects of the program, and we have worked with them to try and develop guidance to be clear on what it is.

The bottom line is, they all went and

implemented it. So the program is in place today. So the hard work is done, and complaining or not, they've done it.

The issue they have now, and this is one of the reasons that Shana mentioned we're doing an assessment is, what's the sustainability of the program and did we miss something.

Did we either mischaracterize it in under control and asset or did we put too many controls on assets. And that's where we've really tried to work with Industry to say, okay, show us how you implemented and where did maybe the Staff's understanding and the Industry's understand not quite be in sync.

MEMBER MARCH-LEUBA: The issue is complacency, even on the TSA --

MR. BEARDSLEY: Sure.

MEMBER MARCH-LEUBA: -- at the airport. They push bad guys with the guns and bombs through once a month, so they stay vigilant.

MR. BEARDSLEY: Sure.

MEMBER MARCH-LEUBA: That might be something to do.

MR. BEARDSLEY: And that's another area where they're working Industry on as well.

MS. HELTON: Jim, and I'll just, and maybe

I'm jumping ahead, and I think we're going to cover this in the presentation, but I think so far, we've gotten a lot of positive feedback from the Industry about the work that we're doing and the cyber assessment.

Our team, our independent team that we have conducting the assessment, are doing visits with licensees to gather data. And I think so, yes, we're well aware of the complaints in the past about the number of analyses and the paperwork involved.

And I think there is a strong interest in leveraging the assessment that we're doing to make improvements to the program so it's a little more efficient.

MEMBER MARCH-LEUBA: Nothing, yes, noting teaches you the lesson as walking into your office and seeing all these screens saying, your computer has been ransomware.

(Laughter.)

MEMBER MARCH-LEUBA: You say ha --

MR. BEARDSLEY: That's right.

MEMBER MARCH-LEUBA: -- I need to avoid this. And this has happened to me.

MR. BEARDSLEY: Sure.

MEMBER BLEY: Have you found much

variability plant-to-plant in how it's been implemented?

MR. BEARDSLEY: There's some. It's usually --

MEMBER BLEY: Does it do any synthesis that more plants are --

MR. BEARDSLEY: Well, what Industry --

MEMBER BLEY: -- the Industry be sharing?

MR. BEARDSLEY: What the Industry did was they, through NEI they established a cyber security taskforce --

MEMBER BLEY: Yes.

MR. BEARDSLEY: -- that works very hard to develop guidance and share lessons learned.

We do meet with the taskforce on a relative routine basis, just so they can give us status on their initiatives and then we can talk to them about where we're going with whatever programs we have at the time.

We've continued to have those meetings. It's become a little more challenging when Entergy and NextEra like to delete NEI, but we've continued to dialogue with Industry and make sure we're sharing lessons, and they're sharing lessons. Because that's an extremely important point.

Is there variation, there is definitely

variation. And I'll talk a little bit about some of that variation as we go through. But none of it has deviated from the core set of requirements.

So, Milestone 4, I'm talked about Milestone 5. This goes back to your insider question. It's the monitoring of obvious tampering.

And so, they had to implement that program for the digital asset, the subset of digital assets, that they addressed in Milestone 1 through 7.

And then the final, Number 6, is applying the controls. So we actually went through and looked at, in detail, how they put controls in place for that smaller 20 percent of critical digital assets that they identified and protected in the first seven milestones.

And then the end, they had to implement an ongoing monitoring assessment program. So, not only did they have to put controls in place, but they have to monitor and assess to make sure those controls remained effective over time.

MEMBER BLEY: You said something of which I was not aware. Several of the larger utility companies have left NEI?

MR. BEARDSLEY: That's correct. Entergy and NextEra are two of the larger entities, left NEI --

MEMBER BLEY: So, any of those programs where NEI was coordinating things among utilities, they're kind of out of the picture now?

MR. BEARDSLEY: Kind of. So, one of the approaches is --

MEMBER BLEY: So even the flex equipment kind of stuff?

MR. BEARDSLEY: Well, one of the approaches that we've taken in cyber, I can't speak to the NRCs overall cognizance of that --

MEMBER BLEY: Yes.

MR. BEARDSLEY: -- but, when we receive a document from NEI for review, and subsequent approval for use, we ensure that that document is going to be publicly available. Or at least shared through an Industry's standard group.

So there's an information technology standards group that Industry has and they share all their documentation through that. So, we verify that those other two licensees have access.

MEMBER BLEY: That's good, but it's bringing up other thoughts.

MR. BEARDSLEY: Sure. All right, I've talked about this before. I talked about good faith and inspection.

And then in 2015, excuse me, in 2016, the Staff followed up the Milestone 1 through 7 inspections with problem of identification and resolution inspections.

So, I said before there were a number of findings at almost every site during the initial inspection program. We did a follow-up at every site in 2016 and early 2017, to verify that the corrective actions have been put in place.

So we feel very comfortable that Milestone 1 through 7 is a robust implementation and it does provide adequate protection for the sites.

So, let me just quickly run down, from a regulatory guide 5.71 point of view, what the requirement set sort of is.

First, they have to identify a team, as I said before. They have to identify all the critical digital assets.

And that's something that we focused our early inspections on. And we did review in the subsequent inspections, but we want to make sure they did not have a robust list, but they had a methodology for continuing to assess and identify critical digital assets as they made changes to the programs.

The next one, implement the defensive

architecture. And my follow-on slide shows this picture in the middle of a, this one, in a lot more detail. But this is fundamental to the approach that the licensees have taken.

And I think it goes back to Member Brown's concern about isolation and building a wall. And I'm going to tell you in a minute how licensees have done that.

And then finally, they implemented the controls. And so, again, we looked at the detailed controls they put in place for those most risk significant critical digital assets in the early part of the program.

MEMBER MARCH-LEUBA: I love this figure, but can you describe us this, you have four different types of walls. One of them is of a diode, the other one is probably a firewall.

Does it mean something or is it just a pretty figure?

MR. BEARDSLEY: You're playing right into my hand.

MEMBER MARCH-LEUBA: Okay, excellent.

(Laughter.)

MR. BEARDSLEY: So on this slide, Slide 9, I tried to breakdown, this is a generic topology.

Not every licensee has divided up all of their levels in the same way.

But for the most part, Level 0 is the internet. Level 1 is protected by a firewall from the internet, but that's a corporate network.

So for the larger companies that covers multiple entities, not just nuclear sites but any of their entities, they all have a firewall then between that and the site network. So that's the specific nuclear site.

Then all of the licensees have implemented a data diode right in the middle. And that meets that one-way deterministic device requirement that they have in their cybersecurity plant.

The way data diode works is, it's a hardware based tool that is basically laser implemented. So it's a --

MEMBER BLEY: So the light can only go from here to here.

MR. BEARDSLEY: Right. They only have a laser that fires from the high side to the low side. So you can't physically send any information the other direction.

MEMBER BLEY: They're all using the same kind of device?

MR. BEARDSLEY: Well, there's only two vendors in the U.S. that they're using.

MEMBER BLEY: Oh, I didn't know that.

MR. BEARDSLEY: And those vendors are heavily implemented within the DoD and the U.S. intelligence community. So, we feel comfortable based on our dialogue with those communities, that these are, these tools are going to do the job.

And if there was ever an issue with them, big U.S. government would have a much bigger problem in our Industry, and we would follow along with those issues. So, we feel pretty comfortable with that.

So, as you move up the levels, Level 3 and Level 4 are a mix of physical security and safety systems, depending on how the licensee elected to do their implementation. And they've documented in their cybersecurity plans the specific aspects of that. So not every licensee is the same.

The other aspect of this that is different is, if a licensee is not part of a large corporation, there isn't a Level 1. They go right from Level 0 to Level 2 because there is no corporate network for it to go to.

So, a lot of people have asked why even have a data diode, why not just have an island and put

all of those Industry control systems upstream in the island and you can't get anything there.

What we have found over time is the licensees that implemented their requirement for ongoing monitoring and, the question you asked before about, that alerting and making sure that any malfeasance that would happen on the systems gets identified.

Many of the sites don't have someone, a cyber person onsite 24 hours a day, 365 days a year. Especially the companies that are part of large corporations, feed those alerts down to a corporate cyber or security operation center that's monitored by cybersecurity professionals that are, not only are they monitoring the industrial control systems, but they are monitoring the whole corporate network.

And so they're going to get alerted to cyber-attacks nationwide, cyber-attacks on the company. And they're going to get alerts and then they'll call back to the licensee site and say, hey, we got an alert on this piece of equipment, you might want to go look at that.

MEMBER MARCH-LEUBA: Yes, we were told back in the time that fewer fabricators needed to give access to their customers, direct access to the

fabrication as part of the quality control. So, have then been able, they said they couldn't do it?

MR. BEARDSLEY: To our knowledge, they have not. But we'll talk about field facilities a little bit later.

MEMBER MARCH-LEUBA: So that's not this?

MR. BEARDSLEY: They are under a different regulatory construct.

MEMBER MARCH-LEUBA: Yes. And second, Level 2 or Level 3 are likely co-located in some places? Meaning, that the cables run --

MR. BEARDSLEY: Absolutely. Absolutely.

MEMBER MARCH-LEUBA: So, there's always a possibility of a Bluetooth tunnel?

Meaning, you put a Bluetooth device here, a Bluetooth device here that goes over?

MR. BEARDSLEY: Yes.

MEMBER MARCH-LEUBA: Are they cognizant of those things?

MR. BEARDSLEY: To a great extent. Level 1 and Level 2 implementations are not part of our regulatory cognizance, so we don't inspect those.

MEMBER MARCH-LEUBA: No, I'm wondering about Level 2 to 3.

MR. BEARDSLEY: So, from Level 2 to 3, that

is where we focus 90 percent of our inspection time. We're looking at controls on the systems, Level 3 and Level 4, and then bypasses. And so, any type of bypass, we look for those.

There also, the licensees have a requirement to eliminate any wireless networks. So they are not allowed to have wireless networks. And they're required, on at least a 30 day basis, to scan for wireless networks. So they're looking for that.

MEMBER MARCH-LEUBA: That's --

MR. BEARDSLEY: Right.

MEMBER MARCH-LEUBA: -- I think a facility is where there is a van that goes around and if you turn your cell phone --

MR. BEARDSLEY: Sure.

MEMBER MARCH-LEUBA: -- they come and zap you.

MR. BEARDSLEY: Sure.

MEMBER MARCH-LEUBA: Based on a facility where they have a classified network and an unclassified network and every IT technician carries a six, a ten centimeter piece of metal. Because that's the distance that the cables have to be checked.

MR. BEARDSLEY: Sure. Right.

MEMBER MARCH-LEUBA: Everywhere you walk

by. Yes, you're okay.

MR. BEARDSLEY: Right. And the licensees have those same type of requirements when they're implementing their networks.

MEMBER MARCH-LEUBA: Okay.

MR. BEARDSLEY: And so, we have found a number of times where there are potential bypasses as we get into inspections. And we've identified that.

That operation and experience has been spread throughout Industry. So, early on in the inspection activity we found some. We find very little to none now.

So, as I said before, bypasses and then the portable media program are two of the most important pieces of our inspection program, because one you have the data diode in place and we've inspected all of them to make sure they're properly implemented, now bypassing it is the only way you can get any kind of malfeasance into the system.

MEMBER MARCH-LEUBA: Or portable media.

MR. BEARDSLEY: Right. So, portable media is extremely important. And I think we'll talk a little bit more about it as we go.

But, as I said, the big picture here is, all of those critical digital assets, almost 100

percent, with the exception of a couple of the emergency preparedness computers, are on the Level 3 and Level 4 protected by the data diode.

So that includes power production, balance of plant, important to safety, safety and security systems. All those assets are behind the data diode.

CHAIRMAN BROWN: Question. Why is the log with flames coming out of it between --

(Laughter.)

CHAIRMAN BROWN: -- and 3?

MEMBER MARCH-LEUBA: It's working so hard.

CHAIRMAN BROWN: It's obvious we have firewall --

MR. BEARDSLEY: Because it's a super important firewall. Because I have Staff that are --

CHAIRMAN BROWN: If it's not a one way, it shows one way, but it could be a software-based firewall --

MR. BEARDSLEY: It could be a two way --

CHAIRMAN BROWN: -- data diode.

MR. BEARDSLEY: -- but the way it's implemented at the sites, and we inspect it as such. And we do look at the configurations of those firewalls to verify that they are designed to only pass the information in one direction.

Now, as I said, this is a generic topology --

CHAIRMAN BROWN: Now, the other key issue there is that orientation, or the directionality, is not controlled by software. In other words, fixed by a hardware arrangement, it's only one way.

MR. BEARDSLEY: Well, in the firewalls it is controlled by software. And that's one of the things that we go look at.

CHAIRMAN BROWN: Yes, that's a problem.

MR. BEARDSLEY: Well, and in some, this is a generic picture. Some of the licensees do have two-way communication, depending on the way they've structured their networks and the controls they have in place.

And, again, we've inspected that and verified that it's acceptable based on what they've committed to and how they have structured their networks.

So, there is no single picture once you get upstream of the data diode. They have different, depending on the way their sites laid out and the different requirements they have.

CHAIRMAN BROWN: Well, I understand that data diode, but I think, I've been trying to relate,

not just today or the last few days, but ever since we issued this thing back in 2000, 5.71 back in 2010. With the four levels.

We didn't have the little fiery brick or the log and then the, that data. That was just, those were all just white lines with one-way arrows. We argued about it then.

But I keep trying to relate this to the plants that we look at. What is a Level 4 system, what is a Level 3 system?

In other words, I look at it, I don't know what my patriots do, but I look at trip systems, safeguards, right control, all those pumps, all those basic plant controls are in Level 4.

And I view, this is a personal opinion, that that fire, that burning log, anything going out of that ought to be hardware. No software control on the directionality of it.

And that's been maintained in all the new designs. I'm not talking about existing plants. Not many of the existing plants, in fact, that a reactor trip systems or others, with microprocessor, computed based systems, there's only a few. A handful at most.

Like there's, I think there's just Oconee and Diablo Canyon.

MEMBER BLEY: But all of, this is a question.

MR. BEARDSLEY: Sure.

MEMBER BLEY: All of Level 3 and Level 4 are within the plant.

CHAIRMAN BROWN: Yes. Yes.

MR. BEARDSLEY: Correct.

MEMBER BLEY: It says security system/safety. Is that on both sides or is security systems in Level 4?

MR. BEARDSLEY: It depends on the specific licensee's implementation.

MEMBER BLEY: So, what's the difference between Level 3 and Level 4?

MR. BEARDSLEY: It depends on how they define, they broke apart their networks.

MEMBER BLEY: Okay.

MR. BEARDSLEY: Some of them use Level 4 to isolate safety systems.

MEMBER BLEY: I mean, I'm kind of happy as long as the combination of Level 3 and Level 4 can't be affected from the outside.

MR. BEARDSLEY: Right. That's the big picture we inspected.

CHAIRMAN BROWN: And by the way, Dennis,

if you just, without talking about who, the last argument we went through where we were looking at it --

MEMBER BLEY: Yes.

CHAIRMAN BROWN: -- the Level 3 to Level 2 communications was a firewall software program.

MEMBER BLEY: No, I, this is different.

CHAIRMAN BROWN: I know, but if you relate it to our last letter --

MEMBER BLEY: Yes.

CHAIRMAN BROWN: -- you relate that, this diagram to the last thing we looked at, the big fight was the Level 3 to Level 2.

MEMBER BLEY: Yes.

CHAIRMAN BROWN: It was a software-based firewall. They changed --

MEMBER BLEY: So, I'm happy.

CHAIRMAN BROWN: We're happy now.

MEMBER BLEY: But I'm not, I don't think I'm worried about level 3 to level 4 since they're kind of not clearly defined in there.

CHAIRMAN BROWN: Well, we did --

MEMBER BLEY: And they're all inside the plant.

CHAIRMAN BROWN: Well, one of the things

you like to do is, there can be networks, as we have seen in 1, inside the Level 3. And you don't want bidirectional communication from that network back into the reactor trip systems and safeguards, where we also have a data diode.

MEMBER BLEY: I don't know for sure reactor trips in Level 4.

CHAIRMAN BROWN: Yes, it is.

MEMBER BLEY: I don't know what's where.

MR. BEARDSLEY: Well --

CHAIRMAN BROWN: You know, reactor trip and safeguards and all the ones we've talked, every time I've asked a question, they've been in Level 4.

MR. BEARDSLEY: A lot of it depends on the licensee's specific implementation. So, what they commit to in their cybersecurity plan we then go in and inspect.

Some of them initially have their physically security systems on an island or connected to nothing. But we recognize that, hey, if there was an attack on that, you'd still want to alert like you would with anything else. So it makes sense to do that conductivity.

And when the licensee makes a commitment to say, we've put the safety systems, the core safety

systems on Level 4, or Level 4a and there's a firewall that protects it, we then go look at, during inspections, show us this specific configuration of your firewall.

That's one of the reasons we have contractors out with us during the inspections. And they have tools they use to screen through the configuration data to ensure that the firewalls are configured appropriately.

MEMBER BLEY: But the NRC and NEI don't, I think I'm hearing you say this, told people what systems they ought to put in Level 3 or Level 4.

MR. BEARDSLEY: We do not.

MEMBER BLEY: I don't disagree with what Charlie says --

CHAIRMAN BROWN: No, I know.

MEMBER BLEY: -- that makes a lot of sense.

CHAIRMAN BROWN: All I've done --

MEMBER BLEY: And I don't know what 100 plants out there have done.

CHAIRMAN BROWN: Oh no, we do not know what the existing plants have done, we only have seen the plants that we've been reviewing. Those new designs. And where we have a --

MR. BEARDSLEY: Right.

CHAIRMAN BROWN: -- pretty clear delineation of where they are.

Diablo, two of the existing plants, at least one of them I know, is configured this way.

MR. BEARDSLEY: Yes.

CHAIRMAN BROWN: One of the other ones --

MEMBER BLEY: It would make sense, but there is no guarantee of it.

MR. BEARDSLEY: Right.

CHAIRMAN BROWN: No, there is no guarantee based on the back fit for the existing plant. They have to be done on a review basis.

If they implement computer-based systems for those systems, you have to go back and look at it. And you have to ensure there's associated systems, with their analog units, you can't compromise something.

MEMBER BLEY: But if Plant 66 out there, when you go look at it, doesn't have S-PRESS (phonetic) and emergency core cooling and reactor trip in Level 4, you wouldn't, that isn't something you would inspect for.

MR. BEARDSLEY: It would depend on how they structured it in their cybersecurity plan, which was reviewed as part of the licensing basis. So we inspect

them to their licensing basis.

MEMBER KIRCHNER: Now, doesn't that fall under your definition of most important critical digital assets?

Wouldn't you use that logic then to zero in on, I'll pick something, the reactor trip system or --

MR. BEARDSLEY: We did in the initial inspection program. So we based it on an analysis of those systems that were the smallest subset of critical systems and that's what we looked at, during the initial program.

Now, since that time, they've fully implemented and now we look at everything. But yes, we did give those, a focused look during the initial inspection and every licensee was inspected.

Any other questions on this picture? I know there's a lot here and this is the focal point of our program.

CHAIRMAN BROWN: I just had one other. When, this is me just asking the question personally, okay.

If I was the inspector, if I was in your all shoes and I wanted to go out and do the assessment, don't you have to have the app, not the app but the

licensee provide some boundary conditions or something?

MR. BEARDSLEY: We do.

CHAIRMAN BROWN: How do you get the bad things up, boundary condition wise, relative to the 5.71 level so you can see how they picture their stuff?

And don't they have to setup these bins that this stuff is in this and this stuff is in this and these, and they meet, so that you know what you're looking at, otherwise it's spaghetti.

MR. BEARDSLEY: No, we do. And I'll talk about it a little bit more when we get into inspection. But we have a structured process we've agreed to with Industry, after the lessons we learned from the initial inspection program.

And the three-phase request for information that the regions use to gather information from the licensees to based their inspection on, the first phase includes network topology diagrams.

And we do a detailed look at their cybersecurity commitments and then compare sort of, this is what they said they're going to do, this is how it's laid out, do those all match up. So we are looking very detailed way at that.

CHAIRMAN BROWN: Okay. To me a picture is worth a thousand words --

MR. BEARDSLEY: Right.

CHAIRMAN BROWN: -- circumstance, if you can draw a architecture --

MR. BEARDSLEY: Yes. If you --

CHAIRMAN BROWN: -- their architecture arraignment of their critical digital asset and which ones are less and where they fall within that architecture framework, it's much easier to assess how much effort you ought to, or even they ought to put into it.

MR. BEARDSLEY: Yes. If you were to observe one of our inspection teams in the field, and I had the opportunity to do that a number of times last year, in almost every room they have huge plots of the networks on the wall. And the teams use that as the basis for what they're, for electing their sample for inspections and then conducting the inspection activity.

So, that clearly is one of the focus areas that we used during inspections.

MEMBER BLEY: Not to beat this to death, but your burning firewall there, when you go plant-to-plant, are some people using the laser diodes in that?

MR. BEARDSLEY: We have seen

implementations where licensees have used more than one data diode, yes.

MEMBER BLEY: Yes.

MR. BEARDSLEY: I can't say the exact details of it because I didn't spend a lot of time, but yes, there were definitely some that have more than one data diode.

MEMBER BLEY: So it's been implemented in different ways?

MR. BEARDSLEY: Yes. Absolutely.

MEMBER BLEY: Okay.

MR. HECHT: Can I ask a question about the data diode devices?

MR. BEARDSLEY: Sure.

MR. HECHT: I've seen them described in various industrial control system conferences, and I was surprised to learn this, but one of the vendors did have the arrangement that there was actually data going the other way, they needed to accommodate things like data historians and remote diagnostics.

Are these truly one-way diodes, and if so, what makes a nuclear plant different from other places where are also pretty important that people use data diodes for?

MR. BEARDSLEY: So, you raise a great

point. In the intelligence community, they use two-way data diodes and they have logic systems that they use to ensure that the data that gets past is appropriate.

For the implementation in our nuclear sites they only have one laser. It only fires in one direction.

So it is impossible, physically, for any data to pass from low to high because there is no methodology for that to happen. Through the data diode.

MEMBER BLEY: So people in those other fields think they're smarter.

(Laughter.)

MEMBER BLEY: And they've learned otherwise.

MR. HECHT: I'm just following up on that. Does that mean that there is no way for somebody in Level 2 to make a query of a Level 3 system, and if so, how do diagnostics and other commands get run?

MR. BEARDSLEY: So there is no, I would say, to my knowledge, there is no instance in our current construct in the fleet, where there is a digital communication between Level 2 and Level 3.

MR. HECHT: That means that the control room is basically Level 3 or Level 4?

MR. BEARDSLEY: The control rooms are all Level 3 and Level 4, correct. That is absolutely correct.

MEMBER BLEY: What about the tech support centers?

MR. BEARDSLEY: The tech support centers do have Level 3 and Level 4, level 3 and/or Level 4 connection.

MEMBER BLEY: No Level 2 tech support --

MR. BEARDSLEY: We've also found instances where they have connected Level 3 out to the metrology building out in the OCA and then we inspect to make sure that they've provided adequate controls on the conduit, on the access control on the system.

So, I mean, those are areas we do look at. The physical security system in some instances is connected directly to their access points, where they issue badges. Because they have to connect, you know, talk to the physical security system.

And, again, we inspect all of that communication path to make sure that it's adequately protected.

All right, moving on. So one the things we identified, once the rule was in place, was the licensees had a requirement to notify the Staff, but

it was unclear exactly what level of notification they had to do.

So, in 2015 we implemented this 10 CFR 7377. It's the cybersecurity notification rule. Here you go.

And so, the rule went into effect in December. The implementation date was in 2016. The Staff released a regulatory guide, 5.83, that described in detail what the licensee's commitments were.

NEI turned that around into a NEI guidance document that the Staff accepted for use, that provided some of the details on implementation. And I'll just sort of walk through a couple of examples of that.

So, right now the licensees are committed to a one hour notification to the Staff of any cyber attack that adversely impacts a safety, security or emergency preparedness function.

If they find one that could have adversely impacted or suspect that there was physical and electronic access to a critical digital asset, they have a four hour notification requirement.

And after receipt, an intelligence gathering, they find that there is potential that they would be attacked, they have an eight hour reporting requirement.

Anything beyond that is a 24 hour recordable that the Staff looks at, both in inspection space, and our resident inspectors would monitor. So, that is the structure of the reporting role.

It is loosely based on our physical security reporting requirements. And so, the methodology is basically the same.

And one of the things we do look at during inspection space is, show us your procedure, show us how you would make those notifications. Some of the inspections have actually observed the licensee conducting cyber security drills and walking through the process of where they, and identifying the issue, making notifications and those kind of things.

CHAIRMAN BROWN: So, your last bullet says you've received no notifications.

MR. BEARDSLEY: Yes.

CHAIRMAN BROWN: That kind of says to me that they haven't been hacked.

MR. BEARDSLEY: To the best of our knowledge --

CHAIRMAN BROWN: That they know of.

MR. BEARDSLEY: To the best of our knowledge, no critical digital asset has had a cyber attack or even a potential cyber attack since the rule

went into place.

MEMBER BLEY: But the utilities may have? Other computer systems.

MR. BEARDSLEY: Yes.

MS. HELTON: The corporate, yes.

MR. BEARDSLEY: Yes. And we'll talk about that.

MEMBER BLEY: Shana, I couldn't hear you.

MS. HELTON: Oh, I'm sorry, the corporate networks. We have seen some corporate networks attacked but nothing inside of the data diode.

MEMBER BLEY: Do they report to you?

MR. BEARDSLEY: Well, we have some examples of that at the end of the presentation. And we'll talk about that process.

MEMBER BLEY: Okay.

MR. BEARDSLEY: But that is not included in the cognizance of the rule, so they don't have a regulatory requirement to report to us.

CHAIRMAN BROWN: Okay, Shana, I didn't understand you. You said nothing inside the data, inside the Level 3, in other words, equivalent to Level 3?

MR. BEARDSLEY: Right.

MS. HELTON: Correct.

CHAIRMAN BROWN: That's all they're required to, that's what this rule applies to?

MR. BEARDSLEY: Well, it's safety, security, emergency preparedness asset.

CHAIRMAN BROWN: Yes, okay.

MR. BEARDSLEY: Wherever they are. We do know that most the sites have two or three computers in their emergency preparedness implementation structure that would be included in the scope of the rule but are not in Level 3.

And so those have to be protected by firewalls. And that they're also monitored with some extra monitoring.

CHAIRMAN BROWN: Okay.

MEMBER BLEY: I know you don't generally work with INPO, but are they involved in this somehow or you hear from them on this sort of thing?

MR. BEARDSLEY: To the, I guess it depends on the question. So, does INPO monitor licensee's implementations and sort of observe that --

MEMBER BLEY: Sure.

MR. BEARDSLEY: -- I don't believe they do. They are working with INPO on methods to improve their lessons learned. And in particular, the vulnerability assessment area --

MEMBER BLEY: Okay.

MR. BEARDSLEY: -- which we'll talk about in full implementation here in a minute.

The licensees basically have a requirement to monitor any alert or potential vulnerability on any one of their critical digital assets. Well, trying to monitor potential alerts on 2,000 assets is an incredibly difficult challenge.

And so, what INPO has done is setup databases that the licensees can register all of their critical digital assets. And then they, INPO draws in the alerts from DHS and from other sources, and then the licensees then get a report on a daily basis of any potential vulnerabilities, viruses, hacks, anything like that, that potentially makes their digital assets vulnerable.

And then they would have to do an assessment to decide whether they would make changes, install upgrades, that kind of thing.

But that's really, that and the, INPO has some efforts in place to help licensees characterize the level of controls or protection their assets need. But that's really a future effort that, to be honest with you, is, to some extent, focused on the Vogtle 3 and 4 implementation. And so, INPO is involved in

that effort as well.

So that brings us to 2017. In mid-2017, our first two licensees committed to completed full implementation. And the Staff then embarked on our full implementation inspection program. And I'll talk a lot more about the program that's in place.

There are a few licensees that did not complete full implementation in 2017. There were very particular reasons for that.

And the primary one was, we had some licensees that had planned on decommissioning. So they stop worked on their cyber programs, and then either because of interactions with the state or because the licensee was, that particular unit was purchased by another licensee, they then were not going to decommission.

And there was no way they could finish their cyber security implementation in the time frame that they committed to, so we then reviewed and approved license amendment requests to extent those.

MEMBER BLEY: How many of those are there?

MR. BEARDSLEY: I believe there's four --

MEMBER BLEY: Okay.

MR. BEARDSLEY: -- but I would have to get you an exact answer.

MEMBER BLEY: Okay.

MR. BEARDSLEY: Most of them have completed their implementations now. I think there is maybe one that hasn't.

MEMBER BLEY: Okay. Just ballpark, that's all.

MR. BEARDSLEY: It's a ballpark in that period. And we also looked at those licensees that were in the process of decommissioning and evaluating whether or not we felt it was appropriate for them to go through full implementation with the fact that they were going to decommission.

And some of them did not fully implement it. And most of them have decommissioned at this point as well.

So let's just talk a minute about what full implementation is. I said before that the interim implementation, Milestone 1 through 7, accounted for about 20 percent of their digital assets.

So they expanded the scope to, with another 80 percent of digital assets. That's a lot of assets when you look at 2,000 overall.

And as we did that, the licensees recognize that, and the Staff recognize that's a lot of work. And so, we developed, in concert with the Industry,

they developed NEI Guidance Document 13-10, that we mentioned before.

And what that does is it breaks down the critical digital assets into a series of classes. If it's a safety asset but it's very low functioning, in other words, there's just not a lot you can do to it, there's a subset of the 138 controls you have to put in place.

If it's an emergency preparedness asset or important to safety or balance of plant, there's a smaller set of controls you have to put in place as compared to a safety system or a physical security system.

And so, the 13-10 process goes through a mythological assessment and tiers your way down to decide what level of controls you have to put in place.

We've spent a good amount of time in inspection space looking at the licensee's processes for dividing up their critical digital assets, to make sure that they're properly classified and that the right controls are put in place.

MEMBER BLEY: Is this covered in the NEI guidance document?

MR. BEARDSLEY: It's covered in NEI 13-10.

MEMBER BLEY: It is, okay.

MR. BEARDSLEY: Yes. Yes. And the Staff has approved that for years.

MEMBER BLEY: And there's an inspection guidance as well I assume.

MR. BEARDSLEY: The inspection procedure does cover the details of this and directs the, so, in an inspection space, which I'll talk some more about it in a minute, there's a structured process for selecting samples.

And so, the inspectors are going to look at a sample of sample systems, security systems, and then we're going to give them options on different levels of the indirect critical digital assets. Which are sort of a gross approximation of all of these.

And so, they do look at, not only how the licensee choose them, but then what they did to protect them.

Going beyond the controls for critical digital assets, full implementation included a significant number of programmatic implementations for the licensees. And so, there is a couple of different examples here.

The first one is incident training and drills. They are required to do training and run drills to demonstrate their cyber security response

capabilities. We have observed some of those drills in inspection space.

Continuity of operations in training and testing is another one, where they have to identify, this is part of that protection response elimination, how do they recover from a cyber-attack, what systems do they put in place, what backup pieces of equipment do they have. And they have to document those processes. We inspect those as well.

The bottom here I mentioned earlier. It's the vulnerability assessment and mitigation process. And this is an area I'll talk about later that we've struggled a little bit with Industry.

Because they didn't fully implement it until December of 2017, some of their digital assets had arguably thousands of updates or alerts that had been identified. And they're digging their way through and assessing those.

We have agreed to a methodology, so, DHS has a hierarchy they use to classify the urgency of different alerts and changes and updates. And so, we've worked with Industry to try and identify, what's the right threshold that you should be focusing your effort on by spending a lot of time and effort on changes that may or may not be of value.

And so, we're working with Industry to try and find the right place in that particular area. What we have asked them to do is make sure that they focus their effort on boundary devices.

So those devices that would prevent any malware or malfeasance from getting from the low to the high. We want to make sure that we're getting the strongest review and understanding.

Secure communications pathways between the CDAs is another area that's very --

(Off microphone comment.)

MR. BEARDSLEY: Oh, I'm sorry. Go ahead.

MR. HECHT: Yes, I'm sorry. A question on NEI 13-10.

MR. BEARDSLEY: Yes.

MR. HECHT: I tried to follow it, it's pretty complex, at least for the simple example that they included there of the emergency notification system. It is, it seems almost that you could base an intelligence test on whether somebody could follow it.

I guess, what is the state of the Industry's knowledge of that and proficiency with that document?

MR. BEARDSLEY: Today we've conducted 23 full implementation inspections. And I think we've

had two findings associated with their critical digital asset assessments in their NEI 13-10 process.

So, the majority of the licensees either didn't use it and just classified everything as direct, although there's very few of those at this point, or they did understand and implement it in accordance with the intent of the program.

MR. HECHT: Okay.

MS. HELTON: Can I?

MR. BEARDSLEY: Yes, go ahead.

MS. HELTON: It's an interesting point though, and we heard about this. We had a session at the RIC on cyber and one of the Industry representatives, and I can't recall who it was on the panel, but they did have a good bit of their presentation focused on the Industry's efforts to ensure they've got the right skill sets of Staff employed to successfully carry out their cyber programs.

Because it is an interesting mix of engineers and IT specialists. You need both the nuclear and plant operations expertise, along with some computer savvy.

So, I think you were raising your comment in the context of the NEI 13-10 document specifically and how complex that document is. But I just wanted

to note that I think that is a focus.

And it's a focus for us too, to make sure that we keep the right skill set of Staff onboard at the agency for our programs.

MR. BEARDSLEY: So, moving onto slide, supply chain is an area that we did not look at closely in the initial implementation, but we spent a good deal of time looking at it and working with Industry to understand the requirements for.

This is one of the areas where we realized that the requirements in the cyber security plan were not specific enough to really help both the inspectors and the Industry to understand what our expectation was.

NEI has developed an addendum to NEI 08-09 that specifically talks about supply chain and the service maintenance of different assets. And that's an area that we look at closely.

During 2018 inspections we didn't have a whole lot of run time, if you want to call it that, with supply chain. Just because they hadn't been implemented all that long.

But the Industry is working through that and they're developing processes to work with their vendors, to provide cyber requirements to their vendor

base and include those in contracts, so they can make sure that they're getting cyber safe assets as they purchase them.

Let's see, on this slide. Another big one here is configuration management. I mentioned that before.

We look closely at configuration management to make sure that the licensees have basically spread that cyber discipline throughout all of their processes and make sure that they understand the potential ramifications of changes or issues with any system and make sure cyber is included in that.

It goes sort of back to your question about safety, security interface. And you could almost argue its safety, security, cyber interface.

How does those three disciplines mix together and make sure that they don't impact each other's ability to perform their task.

I'm going monitoring and management of cyber risk. That's an area that we've looked hard at. The licensees have made a number of commitments in our cyber security plans to ongoing monitoring and assessment requirement.

Ninety days for this, 30 days for that. Some of those requirements the licensees committed to

on the plan and then when they got into implementation, they realized that it's not really realistic.

For instance, if you have a critical digital asset that's in containment and you have a 30 day password change requirement, it's just not realistic to think we're going to shut down and go into containment to change passwords.

So, we've agreed with licensees, fundamentally, on some control deviations or, what do we call it --

PARTICIPANT: Waivers.

MR. BEARDSLEY: They're not waivers, alternate. So, in the cyber security plan the licensees are authorized to use an alternative approach to a particular control.

And so, there's a serious of these timing and monitoring requirements that we've agreed, yes, that's reasonable. If you have a critical digital asset that sits in the control room and is being monitored by the operators 24 hours a day and you have work controls before you open the box and go work on it, you probably don't need to change passwords every 30 days.

Or you probably don't need to go in and check the logs on that system every 30 days because

you'd know if someone opened the box and went and did something to it.

Those are a couple small examples of where we tried to be reasonable with Industry and help them focus on those things that really are vulnerable vice the things that maybe they've already covered with other programs of other systems.

MEMBER BLEY: Can you say a little more about supply chain?

The reason I'm asking is, I did some work with railroads and I've done some work with electrical folks and I know both cases they got and installed equipment that looked right.

MR. BEARDSLEY: Sure.

MEMBER BLEY: Everything about it was right. Expect when, if you opened it up and got inside, it was bogus. And some of the things in the railroad Industry had the wrong software running --

MR. BEARDSLEY: Sure.

MEMBER BLEY: -- and they didn't find it out until they had it in the systems for a while.

So, are we going all the way back to the inspectors out at the manufacturing facilities or --

MR. BEARDSLEY: To the licensees, again, they have a requirement to go maintain their systems

is cyber safe. So, it's not the government's responsibility.

But we are involved, the Staff is involved in a number of inter-government agencies that are looking at the cyber supply chain issue, government and critical infrastructure wide.

So, in particular, they have a requirement to contract, to include in their contract stream cyber requirements for their vendors. They also have requirements to do robust testing, both receipt inspections and then testing of their systems.

So if for instance, so, on the day they committed to be fully cyber implemented, they had a warehouse full of parts. And there was no requirement to do any cyber verification on those parts when they purchased them, because they had not fully implemented their program.

So they have, so there's, in the guidance that we've agreed to on supply chain, there are requirements for them to do detailed bench testing, verification of software, do that kind of effort on the things they already have.

They can also use that on new purchases if it's just not possible. If it's a commercial off the shelf piece of software, there's only so much they

can do to verify its capabilities and that it came from the right place.

But they do have technics they can use to verify receipt of updates to make sure that they are signed and properly documented so they're not getting some kind of malware.

MEMBER BLEY: Thanks.

MR. BEARDSLEY: But it's a big challenge for sure.

So, not only within inter-government, but we also are involved in IEA forums to look at the supply chain problem worldwide and understand how different countries and different industries are implementing it. Because it's not easily a solvable problem.

MEMBER BLEY: No, I agree.

MR. BEARDSLEY: So, full implementation inspections, let me get into that a little bit. So, the full implementation inspections started in July of 2017.

We did two inspections and then we took three months off to sort of take a look back at the inspections and make sure that the inspection program was effective, was being operated in a way we expected it to. And we got feedback, both from the inspection teams and the licensees.

So we understood sort of whether or not everyone was on the same page, if you want to call it, with respect to the inspections.

In January of 2018 we went into full inspection mode and we conducted 20, 18 inspections in 2018. And we've gotten three more inspections done so far through February. So we have 23 complete so far.

And the list here provides you some insights on the things that we found as relatively, sort of repeatable or consistent challenges that both the Staff and Industry have seen in the implementations.

The first one is the quality of the critical digital asset assessments. And this really comes down when the licensees are documenting their reasons for, their implementation for alternate controls.

We have found that the licensee's documentation has not been as clear and consistent as you would expect if you were using this documentation as part of your configuration management process. And the licensees have acknowledged that.

They had a, as you brought up, a huge number of assessments to do. It's a lot of paperwork. And we found multiple examples where the licensees, for instance, cut and pasted huge pieces of matrixes.

And then when you ask them questions about it, oh yes, maybe we should have, maybe that one wasn't quite right.

So, there have been some findings in this area. But for the most part, it's really just a lesson learned on making sure that those assessments have quality, are endearing for the future.

Some of the licensees hire contractors to do the assessments. They did them. They put the controls in place, they put the assessments on a shelf and then the contractors were let go.

So then we come in two years later to do an inspection and we say, can you show us the assessment for critical digital asset X, and they're like all right, let us find that for you, and then they get it and you say, well, why did you do this. Hmm, Bob did that, he doesn't work here anymore.

And so, that level of documentation just wasn't up to the expectation of the licensees, to be honest, and the Staff.

MEMBER BLEY: Jim?

MR. BEARDSLEY: Yes.

MEMBER BLEY: Have you folks, or do you plan, to put together some kind of summary report on the inspections?

MR. BEARDSLEY: We have not to date. We do have a routine dialogue with Industry on these areas.

MEMBER BLEY: Okay.

MR. BEARDSLEY: And in fact, NEI is conducting a cyber workshop next week where we're going to get into some detailed discussions on these various areas. Because Industry, for the most part, they agree.

And in some cases, they, it's clear that there is, just, the guidance isn't there. We didn't identify this particular area and so either Industry or the Staff needs to work on guidance.

And on other areas, Industry just acknowledges, we didn't do as good of job as we could have. And that's operating experience that they're working on.

So, after finding it at a site or two, they'll put it in their corrective action program. So we'll show up for an inspection and they're like, yes, we acknowledge this is here and we need to work on it, and they're getting better at it.

MS. HELTON: And the only thing I'd add is that with our assessment going on, we don't know yet what the outcome of our assessment --

MR. BEARDSLEY: Right.

MS. HELTON: -- will be and --

MEMBER BLEY: I'm sorry, I couldn't --

MS. HELTON: I'm sorry, I keep turning my head and looking at Jim instead of looking at the microphone.

With our assessment that's ongoing, that started in January, and we've let that team be very independent. These preliminary insights that we have shown on this slide are based on our own observations as we've moved through the oversight program.

We will get additional insights from our assessment. So that could very well inform something.

But I think it's safe to say that with all of the communication that we have with Industry, and Industry is talking as well, we see good communications happening, for the most part, on how the inspections have been going. Sites are trying to learn from each other. Especially for those within the same fleet.

The focus, as Jim was saying, the focus, where we have placed uncertain guidance documents, is reflective of those issues, that they keep coming up in inspections.

MEMBER BLEY: I got another question on NEI. I think you told us that all of the guidance documents are public now, so the utilities who no longer

belong to NEI have access to them. Do they also have access to the workshops?

MR. BEARDSLEY: So, the, not all of the documents are public, but we've verified with the other licensees that they have gained access to the documents. So some of the time they do it through an Industry consortium.

MEMBER BLEY: Okay.

MR. BEARDSLEY: So, I just want to make sure I'm clear on that. Because some of them are, for professional use only, security related information because it's sensitivity of the particular information details.

The workshop, next week that I mentioned, all licensees are invited. If you're not an NEI member you have to pay a higher fee, but anyone can go.

And the Staff has maintained a dialogue with those other two licensees that split from NEI. So any information or any dialogue that we have Industry through NEI, we also make sure that we communicate with the other two entities so that we make sure that they're getting all the same information.

MEMBER BLEY: I just had a, I've been around long enough that I remember when EPRI reports were free, and if I did one for them, I get a whole

box of reports, and then people left EPRI and all of a sudden the free documents turned into $50,000 documents, and if you weren't offered you got one.

(Laughter.)

MEMBER BLEY: So, maybe the fees will go up.

MR. BEARDSLEY: And that's a challenge that is not a cyber challenge. That's an NRC and Industry challenge. And NRR has an initiative to look at, how are we, what's the right way to communicate with Industry and those two entities as a whole.

But we recognize, with the dialogue we've had going with the Industry over the years, that we need to at least make sure that we're doing our part. And I think we're being effective.

And I think if you asked the cyber security leads for those two companies, they would agree that we're making the effort to try and keep them involved.

The third item there, guidance for portable media and mobile device program. So, I talked about the importance of making sure that the bypasses for any software or any updates, making sure that no malware could pass from low to high and get to the critical digital assets.

This is the barrier that stops that. So

what we have is, what the licensees have implemented for the most is a kiosk. They either purchase it from a vendor or they develop their own set of computers, that basically takes a piece of software from the internet and screens it to make sure it's what it's supposed to be, that it doesn't have any viruses or anything like that on that.

Where we've run into a challenge with Industry is, the box itself, what controls have to be on that box. Because the box is not a critical digital asset. It provides protection. And it also, it inherits protection for critical digital assets.

So, if you have a CDA that doesn't have the capability to run virus protection, it's just a low function, but you still have to install updates on it, we're relying on that kiosk to provide the protection. And so, the Staff has looked closely at the kiosk to make sure that they are robustly built and that they will perform the task.

And we've sort of gone back and forth with the Industry on, what are the proper sets of controls on those boxes. And we've just recently had a public meeting with Industry where we provided them some feedback on guidance they developed, and we think we're in the right place in this area as well.

But that's, there's been a number of findings in this area because the Staff and Industry were clearly not in sync on this particular requirement. That's the last, no it's not, that's this one here.

CHAIRMAN BROWN: You made the comment earlier --

MR. BEARDSLEY: Yes.

CHAIRMAN BROWN: -- in the session about wireless has not been implemented inside the Level 3 and Level 4. At least that's the implication I got from your statement.

MR. BEARDSLEY: They, in their cyber security plans, commit they have no wireless connected to Level 3 and Level 4.

CHAIRMAN BROWN: That's, okay, that's what I thought you said.

Now, that's, does that fundamentally prohibit cell phones and other types of devices like that?

MR. BEARDSLEY: It does not. And in fact, they do have wireless networks for monitoring, for performance monitoring and things like that in this plant.

But those networks are not connected to the CDAs or the networks associated with Level 3 and

Level 4. And they are required to not only show that to us, but they're required to scan a minimum of every 31 days to make sure that there is no wireless networks connected to those assets.

CHAIRMAN BROWN: Yes, but wireless is wireless, it can penetrate.

MR. BEARDSLEY: But you have to have something that will receive it. So they're required to disable --

CHAIRMAN BROWN: -- the point is, inside Level 3, Level 4 parts of the plant, cell phones aren't allowed then?

MR. BEARDSLEY: No, they are.

CHAIRMAN BROWN: Well then, you've got wireless.

MR. BEARDSLEY: You do but you have, so wireless sending and receiving from a phone is one thing, wireless capability in the system is, so Level 3 and Level 4 are --

CHAIRMAN BROWN: Yes, I understand that.

MR. BEARDSLEY: -- yes, they're not physical. So, within the physical boundary of the plant, there's Level 3 and Level 4 assets in various different places.

They're required to make sure that those

assets, and the networks associated with them, have no wireless connections. That doesn't limit wireless --

CHAIRMAN BROWN: So a phone can't send something to --

MR. BEARDSLEY: Right.

CHAIRMAN BROWN: -- the systems that are within that boundary condition?

MR. BEARDSLEY: Right. So one of the things we look at in inspection space is, show us how you've disable USB ports, wireless ports or any other way that that asset or that network could communicate in and out. So we do look at that. And they're required to verify that those networks are connected there.

MR. LEE: Additionally, we, as we have mentioned previously, there are a number of security controls to monitor the access to these devices so that the, if somebody tried to do unauthorized access or try to get at it, and the, you'll get alerts and also requirements for detecting such a thing.

And also, we have a number of controls to prevent unauthorized connection to these devices.

MR. BEARDSLEY: Right.

MR. HECHT: Can I ask a question about the

digital kiosk?

MR. BEARDSLEY: Sure.

MR. HECHT: Are there any standards or requirements that are placed on the capabilities of the device and not interested so much in the controls protecting the device, but what functions must the device do? For example, antivirus, what else?

MR. BEARDSLEY: There are. So, there are specific requirements that I, and I'm not conversed to them just off the top of my head, but they do commit to a serious of controls or the number of virus engines that have to run.

And then we have some guidance that we've approved that give a little more definition to that, on white listing and making sure that the controls, that they have a number of virus, different search engines or different virus protection engines that have to be updated at a certain period. So, there are very specific requirements to that.

All right. So, I talked about full implementation. So, I'm going to shift now to the future, and let's talk about the cybersecurity assessment that Shana has teed up and we've touched on over time.

So, our intention with the assessment is

twofold. In 2014, the nuclear energy institute submitted a petition for rulemaking to change the scope of the cybersecurity rule.

In their opinion, the scope of the rule was too broad and could potentially lead the licensees to be distracted from what they believed was the core safety systems that needed to be protected.

The Staff elected not to make a decision on that petition, but to defer a decision on it until we the licensees had fully implemented and we started our inspection program.

And the commitment we made was, after we were one third of the way through the inspection program, we would do an assessment of the rule and then make some decisions on the petition.

The Staff took the opportunity, given the fact that we were ten years in from implementation, to expand that assessment. And not only look at the rule, but look at the guidance associated with implementation, both the Staff and the Industry guidance, the inspection program and any other external factors or lessons learned.

So, the team that is conducting the inspection is a team of NRC Staff and one engineer from the Idaho National Lab. All of whom had little to no

interface or experience with the inspection program.

So we brought in people with really a fresh look. We wanted them not to have any preconceived notions.

They have gone out to, in the process of meeting with all of our licensee community, we decided that any licensee that had three, four units or more, we would go visit their site and talk to their cyber engineering teams and get feedback from them individually.

The team is going to attend the NEI cybersecurity workshop next week and they're going to spend the day and allow any other licensee that's interested in coming and talk to them to provide them feedback.

We've done one public meeting to kick off the process. We're going to do another public meeting on the 9th of April.

We're also going to send the team down to FERCs headquarters and meet with FERC to talk about the CIP standards and our requirements and make sure that nothing's changed in the last ten years that made us basically to be out of sync between the two.

We're also going to meet with the Staff and our contractors who are conducting the inspections

to make sure that there's any feedback from them.

MEMBER MARCH-LEUBA: So, the petition is to relax the rule or to relax the inspection --

MR. BEARDSLEY: No, that petition is to relax the rule. To change the scope of the rule. And they give some specific examples in the petition. But really, that's what they're looking for.

So, after all that data is collected, the team is coalesce and put together an assessment summary report that's going to identify all the areas that we're identified as potential lessons learned on the implementation of the cyber oversight program for power reactors, from 2009 all the way through to 2019.

We expect the team to finish that assessment, that summary report, at the end of this June and early July. And then the Staff will use that information to make some decisions on guidance changes, inspection program changes. And to inform the final decision on the NEI petition for rulemaking.

MEMBER MARCH-LEUBA: So I guess, without changing the rule, you can change reviews caused by making Regions III and IV smaller. Is that the trend?

MR. BEARDSLEY: I would argue that's what Industry would like. If we change the scope of the rule it can reduce the number of assets that have to

be included in the program and then it would save them money. I think that's, you'd have to ask NEI.

MEMBER MARCH-LEUBA: I can understand if we were too generous in their location of assets because we wanted to be overly conservative. And maybe we're doing a lot of work on something that is not critical.

MR. BEARDSLEY: Right.

MEMBER MARCH-LEUBA: I don't have any problem removing it.

MR. BEARDSLEY: I think there's another aspect of your question that's very important. There is a rule question there and then I think there is a deeper implementation question.

And I think what we will, I think what we'll find from the assessment, because I've spent a lot of time talking to licensees over the last three years, is that the licensees arguably took a very conservative approach to determining their critical digital asset pool.

They arguably had a little bit of fear that the inspectors were going to take that more conservative approach in what they should have included, so they over assessed.

MEMBER MARCH-LEUBA: Yes.

MR. BEARDSLEY: And I think that that's

what we're going to learn. And that's one of the reasons we wanted to go out to the sites, to sit down with the engineers that did those assessments and say, hey, explain to us the methodology you use to decide what was included in the program.

And then we talked to the Staff that had some expectations of how the program would turn out. And if the licensees were sort of out of sync with what we expected, we may, in the scope of guidance, without changing the rule, be able to provide some relief or help the licensees focus their effort on those assets that are most important.

MEMBER MARCH-LEUBA: And I don't know it will work, but often they become too hard headed as a user. I want to have accurate control to that switch jab (phonetic) sensor, which then becomes a critical asset.

Where if you can put the little diode on the sensor and say, sure, you can have it, but you cannot modify it. A small hardware change, Charlie will tell you, can save you a lot of money.

MR. BEARDSLEY: Sure.

MEMBER MARCH-LEUBA: And if, then if they were to think outside the box like that, they can maybe do it. I will not relax the rule, I will give guidance.

MS. HELTON: And like Jim said our look at what is appropriate to do with that petition for rulemaking is on hold until we get the results of the assessment.

But I think, you know, what you are saying resonates well with us and we heard it also at the Regulatory Information Conference, was it last week, and the quote that I think kind of sums up what you are saying is we took a good performance-based rule and layered a lot of deterministic guidance on top of it.

So I think that's really the fundamental question that we will be looking at as we are reviewing the petition, you know, are there things that we can accomplish without a rule change or do we really need to go back and change the fundamentals and the regulations, but we'll need to decide.

MEMBER MARCH-LEUBA: Mm-hmm, right.

MR. BEARDSLEY: So the other aspect of the assessment that I think is going to be very important is in full implementation inspections we are sending out two inspectors and two contractors for two weeks.

They are also doing on the order of 12 weeks worth of preparation for those inspections. That is a lot of work on our part and the licensees are devoting

significantly more assets than we are.

And so the question is are we getting the bang for the buck from them? I think we are today because we need to do a deep dive and make sure that they have implemented this vast program in an acceptable level, but do we need to continue that level of effort over time.

And licensees have some strong ideas. Arguably the Part 73 rule is a performance-based rule. We have not done a lot of performance-based looking at the implementation so the question that we have talked to industry about but where we're really expecting them to come in with some ideas is what could you do to help, you know, change the scope of this or at least some of the focus into a more performance-based type methodology.

Are there performance indicators? Is there some level of testing they could do? Things along those lines that the staff could use to inform us as part of our inspection program and verification of their implementation.

You know, I can't say what the industry is going to say as part of their proposal but I think they recognize that there are aspects of their programs.

I mean we know today that that reporting

process I talked about where they are sending alerts and logs down to analysis systems and then alerting them to potential issues, they are collecting an immense amount of performance and health data on their systems.

Would it make more sense for the staff to review that health and performance data over time or to go look and make sure they had, you know, 138 controls on an individual asset properly configured?

If we could look at health data we might be able to see how they have put the controls in place for all the assets in a significantly less period, you know, shorter period of time.

So those are some of the things that we have thought about. We are waiting to hear what industry's thoughts are and then we are going to evaluate that as part of the future of inspections.

So we are committed to conducting the inspection program we have today through 2020. At the end of 2020 we will have inspected all of the fleet and then we need to make some decisions in the interim on where we go with inspections from there.

MEMBER BLEY: What you are describing here is interesting. Now how do you see it resolving? Would it likely be a SECY paper with recommendations to the Commission or is this something you might handle

--

MR. BEARDSLEY: That's a great question.

MEMBER BLEY: What might we look at --

(Simultaneous speaking)

MR. BEARDSLEY: In general the staff does not inform the Commission on changes to individual inspection procedures, but --

MEMBER BLEY: If there is a rule change here?

MR. BEARDSLEY: Well if there is a rule change -- So the petition for rulemaking has to result in a recommendation to the Commission and the staff is committed to making that report to the Commission by the end of 2019.

So by December of this year some recommendation from the Petition Review Board will be transferred up to the Commission. That is the commitment we have right now.

That would not include details like the inspection program necessarily or some of the guidance --

MEMBER BLEY: Well it seems, and this is just off the top of my head, it seems that since there is a recommendation in from NEI your recommendation might be to do what they suggest or if it isn't it

probably needs to be backed up by some of these other arguments.

MR. BEARDSLEY: Without a doubt.

MEMBER BLEY: Yes. Well that could all be in the paper that goes --

(Simultaneous speaking)

MR. BEARDSLEY: So if the staff sends a paper up to the Commission that says we don't believe that changes are necessary for the 7254 rule we would have to back that up with why based on NEI's request do we think the current program can be, you know, managed to gain the same level of efficiencies that they were looking for.

And that is definitely something that we have talked about, but we have to get -- I mean, you know, the petition review process is a very structured process, it's part of rulemaking, and we have to work our way through that process as we communicate with the Commission.

MEMBER BLEY: In any case, the end of this year you have to do something?

MR. BEARDSLEY: Right.

MEMBER BLEY: Yes.

MR. BEARDSLEY: So there will be a Commission paper by the end of 2019 that makes a

recommendation to the Commission on NEI's petition.

CHAIRMAN BROWN: The petition is in the package that Christina sent out to you. Look at Pages 11, 12, and 13. They eviscerated the rule. That's my personal opinion.

Okay, I mean they took all the stuff on reactor safety out and put in system structures and components and then they took, they deleted two of the rule items in 73.54(a)(1)(ii) and (iii) and --

(Simultaneous speaking)

MEMBER BLEY: But still the focus I was going at --

CHAIRMAN BROWN: Yes.

MEMBER BLEY: -- when will the staff have something put together?

CHAIRMAN BROWN: Yes. They said, you know, as they noted they are going to do something. I think we are looking for some additional interaction later in the year once they come to grips with what they are doing so we'll have some idea where they are going on this.

MR. BEARDSLEY: And so --

CHAIRMAN BROWN: NEI was very aggressive.

MR. BEARDSLEY: And what we talked about before the meeting was after the assessment is complete

and the staff has had time to look at, you know, what do we think we can do within the bounds of what we found it would probably make sense for us to come back and update the committee, or the subcommittee anyway, on, you know, where we think we're going to go, and I think that is well within the bounds of what we can do.

CHAIRMAN BROWN: You know, both the rule and the -- You're also looking at changes to Reg Guide 5.71 if I -- I saw that you all have a draft guide that was floating around.

I don't know whether you have issued --Have you issued that for public comment yet?

MR. BEARDSLEY: You're a great straight man.

(Laughter)

CHAIRMAN BROWN: Okay.

MR. BEARDSLEY: My last bullet talks to Reg Guide 5.71.

CHAIRMAN BROWN: Oh, yes, too bad I didn't read forward.

MR. BEARDSLEY: We do have a Revision 1 to Reg Guide 5.71. It went out for public comment last summer. We collected a number of comments in the fall and the staff has been reviewing those comments.

We have -- We are in the process of

finishing up that review, but based on the fact that we are going to do the assessment and there is potentially a lot of changes to the program we're working with NSIR management to make some decisions on whether we even move forward or do we just put on hold the Revision 1 and then re-issue it with a new set of guidance based on where we go with the program, and that's a management decision that we need to get through.

MS. HELTON: Yes. And just for absolute clarity on the path forward, there is a lot of the path forward that I don't think we can put products associated with quite yet.

So there are certain things that are in play that we know we are going to need to do something with. We've got the cyber assessment, we'll get the results, that will result in some recommendations, and that's really going to drive a lot of our specific products.

We've got the petition for rulemaking, we need to resolve that. That will certainly result in a communication to the Commission with whatever recommendation we come to as a result of the petition process. We are not there yet.

And the Reg Guide 5.71 that has been issued

for comment. We need to in some way decide what we are going to do, and as Jim said before we know what we are doing with the petition for rulemaking, I mean any time you update if we do wind up making a rule change you always update the guidance along with the rules.

So it wouldn't make sense to put Reg Guide 5.71 ahead of that if that's where we go, and I don't even know if we are going to go there yet.

And then we have lower level documents as well. Our inspection procedures probably, you know, sometimes they do go the Commission if it's a significant change to the reactor oversight process the Commission likes to be engaged.

So we just have to see what the nature of the changes are and which regulatory products they impact to have a good sense -- And, again, in the fall timeframe after we have completed our assessment and we have our recommendations and we align in what actions to take we'll have a better picture of what SECY papers, what rulemakings, if any, what regulatory guidance, if any, what inspection procedures, if any.

CHAIRMAN BROWN: If I read you right the game plan would be finish the assessment, is that number one?

MR. BEARDSLEY: Correct.

CHAIRMAN BROWN: Okay. And number two then would be take care of the petition in some way, shape, or form, resolve that?

MR. BEARDSLEY: Yes.

CHAIRMAN BROWN: Either do it, reject it, whatever you end up doing?

MR. BEARDSLEY: Right.

CHAIRMAN BROWN: Number three would be then do we change the rule in some other way based on even though we didn't accept the NEI thing, do we make another rule change based on our assessment?

MR. BEARDSLEY: I think that would be a result of the petition resolution.

CHAIRMAN BROWN: Yes, okay.

MR. BEARDSLEY: Yes, if there is any changes to the rule that would come out in our recommendation to the Commission.

CHAIRMAN BROWN: Okay. And then the last part would be do we need to do something with RG, the Reg Guide 5.71 depending on how the rule, if we do a rule change or what have you, or any other reason for it?

MR. BEARDSLEY: Sure. I think there is two other aspects. One is are there ways within the bounds of the current rule and the guidance that is

implemented to address some of the concerns with either over assessment of CDAs or implementation clarity that could assist both the staff and industry in the implement, and we can do that without changing the rule.

CHAIRMAN BROWN: Yes. You're really talking about calibrating --

MR. BEARDSLEY: Right.

CHAIRMAN BROWN: -- what you, how you implement?

MR. BEARDSLEY: Right. Right, and that could either be --

MS. HELTON: We have to use the current rule.

MR. BEARDSLEY: Yes. That could be either be staff, informal guidance through the Security Frequently Asked Questions Program, or NEI guidance or industry guidance they have submitted to us that we have approved for use and the other aspect of it that I think is very important is the potential changes to the future inspection program.

And so that's another aspect that is going to come out of the assessment that we are going to have to make some hard decisions and we have to do that before the end of 2020 because right now the provisional

inspection procedure we are using is really only expected to be used until every licensee has received one inspection.

CHAIRMAN BROWN: Could you us -- Since I can't write fast enough could you kind of write down your path forward at some point with the stuff you just talked about and just give a copy to Christina so that she can send it to us to see and we'll --

MR. BEARDSLEY: Sure. Yes, we can do that.

CHAIRMAN BROWN: I'm not -- I can't ask you to do anything. I'm just -- It would be useful for us in our further deliberations and when we do anything would be to have a little bit of clarity, because there is not kind of a path forward that is in one of your slides here.

All you have talked about is piece parts of it and I'm not sure I've got them in the right order.

MR. BEARDSLEY: Okay.

MS. HELTON: Okay.

MR. BEARDSLEY: We can do that.

CHAIRMAN BROWN: So if you -- And I'm not saying you have to follow that order, it's the game plan. It's kind of a game plan thing, what's your thought process.

MR. BEARDSLEY: I think you ask a reasonable question and it probably behooves us to write some of that done, yes.

CHAIRMAN BROWN: But, yes, that would be helpful. And, again, it's not official that you have committed, it's not in your list, it's just kind of your thought process.

MS. HELTON: Correct. And we would be happy to provide that and I think it would actually be helpful just in looking at what's the next appropriate time to engage between the staff and the ACRS.

You'll want to have a sense of when we can complete the assessment, when we are going to the Commission with our determination, what to do with the petition for rulemaking, and, you know, everything else is really a question mark on the path forward because of those two products. They are going to determine our next steps.

CHAIRMAN BROWN: Yes. Two big items, final assessment and the petition.

MS. HELTON: Two big items.

MR. BEARDSLEY: Right.

MS. HELTON: Correct.

CHAIRMAN BROWN: And the other things if,

the other thought you -- You tossed in a couple over, not corrections but expansions relative to how do you make the current rule work better, which is a good plan.

MR. BEARDSLEY: Right. And industry had recognized that while they stand by their petition that there are potential areas where in the interim of rulemaking -- because even if we agreed to NEI's petition and made a recommendation to the Commission in December that the rule should be changed it would be a few years before that rule change goes into effect.

And, you know, if we could provide some of what they are looking for in guidance space within the cognizance of the rule we could do that, you know, in a few months potentially.

MS. HELTON: If we feel it's appropriate.

MR. BEARDSLEY: If we feel it's appropriate. I mean it's what we could do. I am surely not saying we are going to do that.

MS. HELTON: Right.

MR. BEARDSLEY: But we have worked with industry over the last six or seven years to help them develop guidance, not help them, but they've developed guidance, we have worked with them on it, we have approved it for use, they have submitted it to us and we have approved it for use, and I think that has really

helped us to provide clarification in the current inspection program.

So I talked a little bit about the milestone one through seven inspections and some of the challenges we had with the staff and industry just not being in sync on a number of areas, we have not seen that in the full implementation inspections.

We are not without findings. You know, most of the inspections have had one or two findings, but in general the staff has found that the industry understands the requirement and has implemented it with, you know, with a reasonable assurance that we don't have significant issue with.

A number of years ago the staff issued a paper to the Commission called the Cyber Security Roadmap. We updated the roadmap in 2017 and much of what's on the slide here is documented in that paper.

So we talked initially about fuel facilities. The fuel facility rulemaking has been briefed to the full committee I believe back a number of years ago.

The staff submitted the draft rule to the Commission for release, you know, public release. The Commission has that draft rule and has not made a decision on it, so we've --

MEMBER BLEY: A question though --

MR. BEARDSLEY: Sure.

MEMBER BLEY: Given all the lessons learned you've seen and are developing are you happy with the draft rule you sent up?

MR. BEARDSLEY: We informed the draft rule significantly based on the lessons we learned and the feedback we received from the power reactor industry.

MEMBER BLEY: You've had enough experience --

(Simultaneous speaking)

MR. BEARDSLEY: So we believe that that rule includes, you know, a robust set of lessons learned.

MEMBER BLEY: Okay.

MR. BEARDSLEY: I mean the structure of it is arguably different in many areas than the power reactor, but the fuel cycle facilities are very different than the power reactors as well. So we are waiting for direction from the Commission on where to go with that rule.

For non-power reactors, those are primarily the research and test reactors at universities. The staff went out and did a survey of that community and the cyber controls they had in place

and found based on the arguably very analog technology that are implemented in a low security risk that the protections they had in place were adequate.

They did collect a number of lessons learned from the different reactors and sites they visited and published those in a best practices guidance document for industry, so that's been provided to the non-power reactor industry.

MEMBER BLEY: There is a couple of isotope generation facilities, medical isotope generation facilities that might be getting built in the near future. Did you consider those as well? Do you think you can say the same thing about those?

MR. BEARDSLEY: You are almost as good a straight man as Member Brown. That's my next bullet.

(Simultaneous speaking)

MR. BEARDSLEY: So the non-power production utilization facility --

(Simultaneous speaking)

MR. BEARDSLEY: Yes. So our challenge there is it is unclear to the staff the digital nature and the safety sort of level of some of those facilities, of the moly-99 facilities for purpose of discussion.

MEMBER BLEY: Yes.

MR. BEARDSLEY: So we did make a

recommendation to the staff, to the Commission, excuse me, that we wait on cyber security decisions for that set of licensees and, you know, right now that's where we stand.

We are waiting to see detailed design information. Some of those digital systems, I mean we know they're going to be digital.

I mean there is no question about that, virtually everything that is designed today is digital, but what's the risk significance of them, you know, the reactors they have or the production facilities, and we just need to make some decisions on that.

MEMBER BLEY: So let me ask, and I'm not, you know, NRC looks at the risk arising from the facility, but if a facility is one of a limited number of sources and medical isotopes interruption of the supply of isotopes is a really major risk to the country and maybe the world.

MR. BEARDSLEY: Sure.

MEMBER BLEY: Is that part of the calculation?

MR. BEARDSLEY: Well --

(Simultaneous speaking)

MR. BEARDSLEY: -- based on our mandate it probably isn't, but we recognize in engaging with

those licensees they recognize that they have, arguably, a fiduciary responsibility to make sure that they are building a robust cyber implementation so that their systems can keep running.

I mean we're really going to be focused on the safety nature based on our mandate, but what we have done is looked at in conjunction with the facilities and sort of understand what are those sort of risk points.

Our intent would be not to do a rulemaking for these licensees but to develop a cyber security plan that would be included as a license condition in their license and that would be how we implement any requirements as we move forward.

MEMBER BLEY: Given the nature of their product and how it's used and how significant it is to the health and welfare of people is there some other agency who looks at that that you are aware of?

MR. BEARDSLEY: I can't answer your question, but we would have to -- I mean I would have to -- I'd have to get a lifeline to answer your question, I don't really know.

MEMBER BLEY: If you find out I would be very interested. I mean that's a significant --

MR. BEARDSLEY: Sure, absolutely,

absolutely. It's a worldwide challenge.

MEMBER BLEY: Yes.

MR. BEARDSLEY: Okay, moving on. Independent spent fuel installations do not have any cyber requirements to date.

The staff has taken a look at safety and security for ISFSIs and stands by that position and has been given direction by the, or has informed the Commission that we don't intend to make any changes in that area.

For nuclear materials the NMSS did a very broad survey of the materials community, you know, because it's a very wide community, and they found that most of, or they found adequate the cyber controls that were in place for the various facilities primarily based on their insurance or fiduciary responsibility to maintain the safety of their systems.

They did collect up a number of best practices and also communicated with the Department of Energy to get access to best practice guidance documents that have been put together form their surveys worldwide and that is being put together in an information notice that is going to be sent out to the entire nuclear materials licensee community.

MEMBER BLEY: So a question on that one,

I haven't thought a lot about it, but it seems that perhaps one of the most important ways in which this could be significant would be if through software for cyber attack you could delete the records of sources and they would disappear.

If you lose track of all the sources there is a lot of -- and now that, of course, they are distributed in many different organizations, but I am not sure how much, what they looked at for consideration that their cyber security is good enough.

MR. BEARDSLEY: I'll be honest, I don't have access to the final results of their assessment but when it comes to recording sources and in managing that I think that's a little different than the licensees themselves.

I think that's, you know, the NRC has processes we use to track sources throughout the country and that's an NRC-managed database. It would be under our won cognizance. It wouldn't be included in his particular are of rulemaking.

MEMBER BLEY: Well that opens a whole new can of worms.

MR. BEARDSLEY: Probably.

MEMBER BLEY: What about NRC databases and your resistance to cyber security attack on those

databases?

MR. BEARDSLEY: Well, you would have to talk to NMSS and the Office of Chief Information Officer because that's not under --

MEMBER BLEY: That doesn't come under cyber security?

MR. BEARDSLEY: It does not come under the cyber security oversight program that we have here, that we have here, that we have at NSIR.

MS. HELTON: Well, and --

MEMBER BLEY: You look at everybody else but not yourselves.

MS. HELTON: Correct. Well, right, so for the focus of what we are doing and physical and cyber security policy we are looking at implementation by the licensees.

So we have started having more conversations I can just say from the management level about, hey, what about cyber security and the NRC. We're not subject as the agency to the requirements in 73.54, which is really the focus of this presentation, you know, implementing NRC requirements.

MR. BEARDSLEY: Yes.

MS. HELTON: We have other requirements that we need to meet. So we are starting and we are

just at the early stages of coordinating more between OCIO admin, NSIR, because we recognize that with staff the limited skillsets that we have there is probably some ability to be growing and sharing across the business lines.

But, yes, right, so the focus of this presentation is --

MEMBER BLEY: And there is information that needs to be protected from getting out --

MS. HELTON: Right.

MEMBER BLEY: -- and there is information that needs to be protected to be preserved.

MR. BEARDSLEY: Sure.

MS. HELTON: Correct, right.

MEMBER BLEY: So you are -- Somebody is beginning to look at that?

MR. BEARDSLEY: Right. The Office of the Chief Information Officer and then the information security program that is run out of NSIR both have a primary responsibility for those areas.

But what we have found through some management things that we have been doing under OPM is we have identified all of the cyber specialists in the agency and NSIR has been working very closely with admin and OCIO to develop training programs, to bring

in commercial training programs for the cyber specialists because we don't have enough of them to, you know, to build up a training program here.

MEMBER BLEY: Sure.

MR. BEARDSLEY: And that's provided two benefits. One, arguably it's going to save us some money because if we can bring training in-house it's cheaper than going outside and taking a $5000 or $6000 class.

The other thing it does is it allows the specialist from OCIO and the offices in the regions to take classes together and share lessons --

MEMBER BLEY: Yes.

MR. BEARDSLEY: -- because there is a very small subset of information technology-trained cyber folks in the agency and we recognize that we want to share those resources.

And so when we have had some of the challenges, and I'll talk about it on the next slide, in industry NSIR and OCIO have communicated back and forth to make sure that we understand the specialties and some of that background that the different staffs have and we can take advantage of that.

MEMBER BLEY: Great.

MR. BEARDSLEY: All right, let's go to the

next slide. So cyber incidents, there is two particular cyber incidents that I will highlight here.

The first one has gotten a lot of public attention. It was initially identified in the Summer of 2017 but the advanced persistent threat attack by the Russians had been going on for well over a year at that point.

The attack focused on a number of critical infrastructure industries, including the energy industry, and when it first came to light it was actually the cyber incursion into one of licensees that first went public in this. It was identified --

MEMBER BLEY: That was in the electrical systems or something?

MR. BEARDSLEY: It was in the --

MEMBER BLEY: Distribution I mean?

MR. BEARDSLEY: No, it was in the site network, the Level 2 network --

MEMBER BLEY: Okay.

MR. BEARDSLEY: -- at a licensee that was not part of a major corporation, so they did not have a Level 1.

MEMBER BLEY: Yes.

MR. BEARDSLEY: And it was identified based on information traffic leaving the site. It was

picked up through the intelligence community and then was identified to the FBI and eventually to DHS and to the staff, so let me just talk a little bit about that.

I am not going to talk about the details of it. The Russians got into their corporate network, their business network, but what happened afterwards is Homeland Security notified the staff as part of the FBI -- So the FBI took the lead because they have the lead for a criminal act or a terrorism act.

They worked with Homeland Security to put together a team to go out and assist the licensee with basically doing forensics on what happened. In concert with all that the other agencies communicated with the staff and let us know what was going on.

We actually helped facilitate access to the site with the licensees because we have contacts, we have residents, so we help them. We also sent some of the cyber engineers in our branch out to observe that forensic analysis so we got a feel for what are they doing, what are their capabilities, and what happened there.

And we have continued to dialogue both through the region and with the other government agencies to understand what happened and how to

potentially prevent that.

There was a security advisory that went out following this incident to all of the power reactor industry just informing them, although most of the information was probably already made public, about a year, about six months later DHS actually stated it was the Russians that did it.

Up to that point it was an unknown adversary, but that's pretty public and well understood.

Based on that forensic analysis the adversary was not able to penetrate past the data diode to gain access to any of the safety security or merchant preparedness systems that are under our cognizance.

So going back to our discussion when we talked about the reporting role, although we were cognizant of what happened and the licensee was, you know, spoke to us with candor about the challenges they had, they had no requirement to make a report to us. So this was not a reportable incident.

The second incident on the slide happened just about a year ago. Entergy had a malware attack that penetrated an internet-facing website. So one of their websites that was connected to the internet, they penetrated the website, penetrated the firewall,

and installed Bitcoin mining malware on their computers.

So if you know what that is we can get into a whole different discussion, but what it did was it spread throughout their corporate network and they identified it at night and we found out because our resident inspector showed up at work the next morning and they heard site-wide announcements telling everyone not to turn their computers on.

So the residents called the regions, the regions called NSIR, and then eventually we made contact with the IT folks and the licensing folks at Entergy to find out what had happened.

At that point they were still doing forensic analysis and we basically came up with an agreement with the licensee that the staff would stand off and give the licensee 18 hours to go figure out what happened and clean it up.

They were able to isolate the infections and clean them off their networks. Again, based on forensic analysis of the attack there were no, none of the regulated critical digital assets were impacted.

There was the potential -- Remember I said before that some other EP assets were on Level 2?

MEMBER BLEY: Yes.

MR. BEARDSLEY: So they did detect an area where they thought the malware tried to gain access to some emergency preparedness assets, as it turned out, and although I did say it on this slide, the licensee made it a recordable event and then later came back to the staff and said based on their further analysis they found that that was not, in fact, true.

It was an indication that they thought they had. It was a false positive basically. But this is another example of where we believe that the controls have been in place with the data diodes and the other controls that we have inspected and we're taking a strong look at are protecting the critical digital assets from, you know, internet facing attacks and that kind of thing.

Any questions about those?

(No audible response)

MR. BEARDSLEY: Both of these are public. They are not professional use only. They have been acknowledged by both the licensees publicly. That completes my remarks subject to your questions.

CHAIRMAN BROWN: Before I got to public comments -- or should I do that first?

MEMBER BLEY: Go to public comments and then get the phone line open.

CHAIRMAN BROWN: Yes, okay. I'm pretty sure it's -- Is it open Paula?

(No audible response)

CHAIRMAN BROWN: Yes, it's open. I'd like to know if anybody is on the phone line listening to this subcommittee meeting. Could you just say hello or something?

PARTICIPANT: Hello.

CHAIRMAN BROWN: Okay. Now that we know that somebody is there was there anybody on the public line that would like to make a comment?

(No audible response)

CHAIRMAN BROWN: Hearing none I will now ask the audience, the public attenders does anybody want to make a comment?

(No audible response)

CHAIRMAN BROWN: It doesn't look like we have anybody. I will now transition to the staff and we'll make a round from the staff starting with Vesna.

MEMBER DIMITRIJEVIC: I have none.

CHAIRMAN BROWN: Myron, do you have to leave?

(No audible response)

CHAIRMAN BROWN: Oh, okay. Go ahead, Vesna.

MEMBER DIMITRIJEVIC: No, nothing.

CHAIRMAN BROWN: Ron?

MEMBER BALLINGER: This is very cool. I appreciate it.

CHAIRMAN BROWN: You are a welcome member of our committee any time you want to attend. Jose?

MEMBER MARCH-LEUBA: I don't have any comments. I just wanted to thank the staff. It is a pleasure to have a presentation by people that actually know what they are doing and enthusiastic about it and understand my questions.

MR. BEARDSLEY: Thank you.

MEMBER RAY: I'll just add to what, or agree with what Jose said.

CHAIRMAN BROWN: Okay. Dick?

MEMBER SKILLMAN: I agree with Jose. Thank you.

CHAIRMAN BROWN: Boy, you're popular. Dennis?

MEMBER BLEY: I looked at the slides last week and sent Charlie a note, I don't think there is anything in here we didn't hear before, why are we having a meeting.

I take it all back. There were excellent discussions, excellent response to all the questions

and thank you. It was a good afternoon.

CHAIRMAN BROWN: Walt?

MEMBER KIRCHNER: Just thank you for the presentation.

CHAIRMAN BROWN: Okay. And I don't have anything else other than just if you could write those kind of a path forward type thing down and then we can maintain some communications and determine when we'd like to have another update or what have you or what our next actions or appropriate actions would be.

I mean we certainly don't have anything to deal with right now other than to let you finish your work and we'll try to stay out of your hair. I say that figuratively.

MS. HELTON: Yes.

CHAIRMAN BROWN: Other than that, thank you very much and I thought it was an excellent presentation by the way. I do appreciate you all coming in and giving us this update.

It has been a long time and I have to agree wholeheartedly with Jose and Dennis, particularly Dennis, in that it was very, very insightful and provided a lot of very good information.

The fact is I think I've about gone into brain overload. Anyway, now the meeting is adjourned.

MS. HELTON: Thank you.

CHAIRMAN BROWN: All right. Thank you.

(Whereupon, the above-entitled matter went off the record at 3:26 p.m.)

NRC Cyber Security Oversight Program Status

Jim Beardsley, Chief

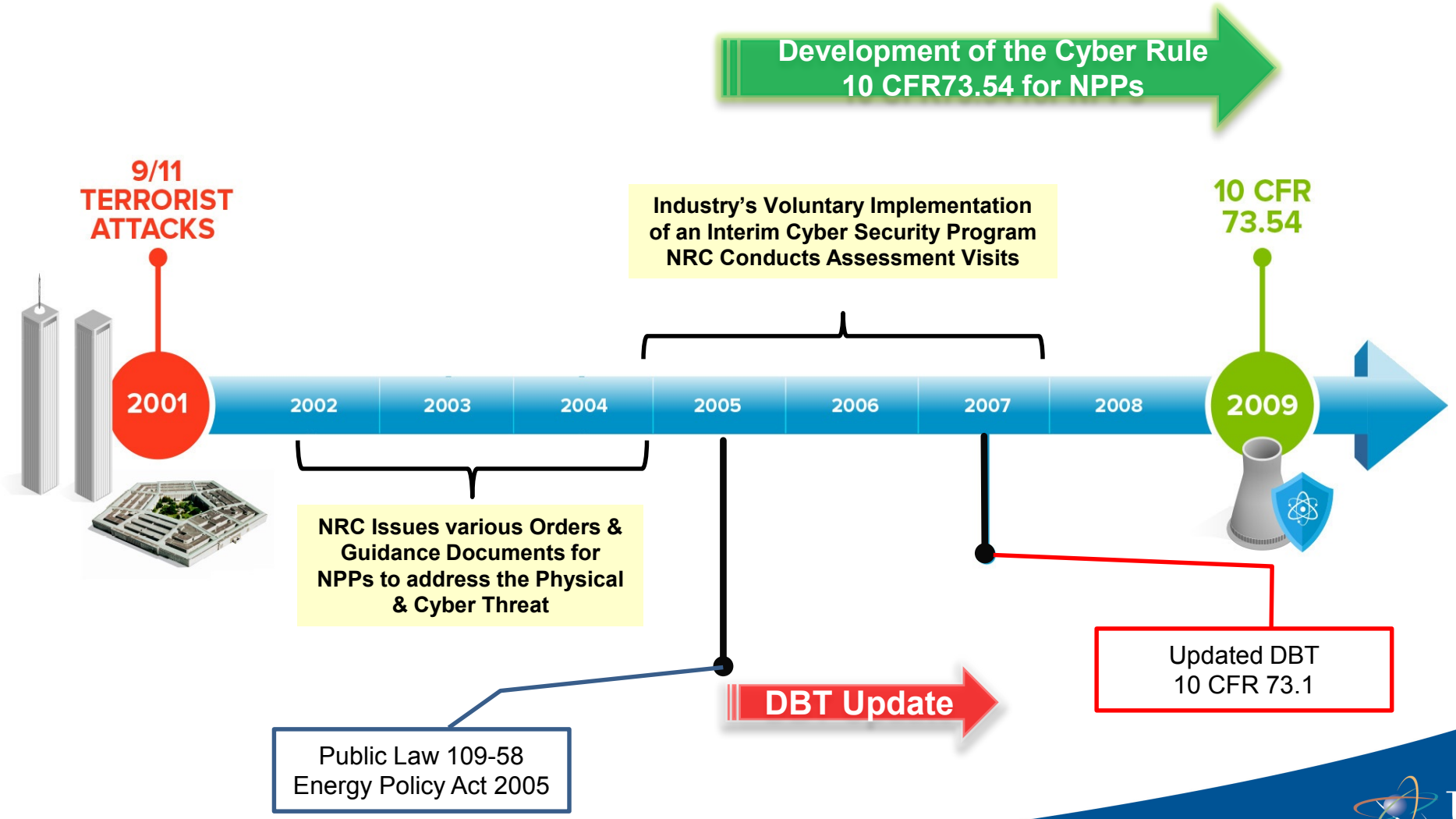
Cyber Security Branch (CSB)

Division of Physical and Cyber Security Policy (DPCP)

Office of Nuclear Security and Incident Response (NSIR)

james.beardsley@nrc.gov

Overview of US NRC Cyber Security Program



10 CFR 73.54 Protection of Digital Computer & Communication Systems & Networks

- **Op Rx and license applicants must submit a Cyber Security Plan by November 2009**
  - Protect digital computer and communication systems and networks associated with
    - **Safety, Security & Emergency Preparedness (SSEP) functions**
    - **Support systems** and equipment which, if compromised, would adversely impact SSEP functions
  - Protect from cyber attacks that adversely impact
    - Integrity or Confidentiality of data and/or software
    - Deny access to systems, services, and/or data
    - Operation of systems, networks, & associated equipment

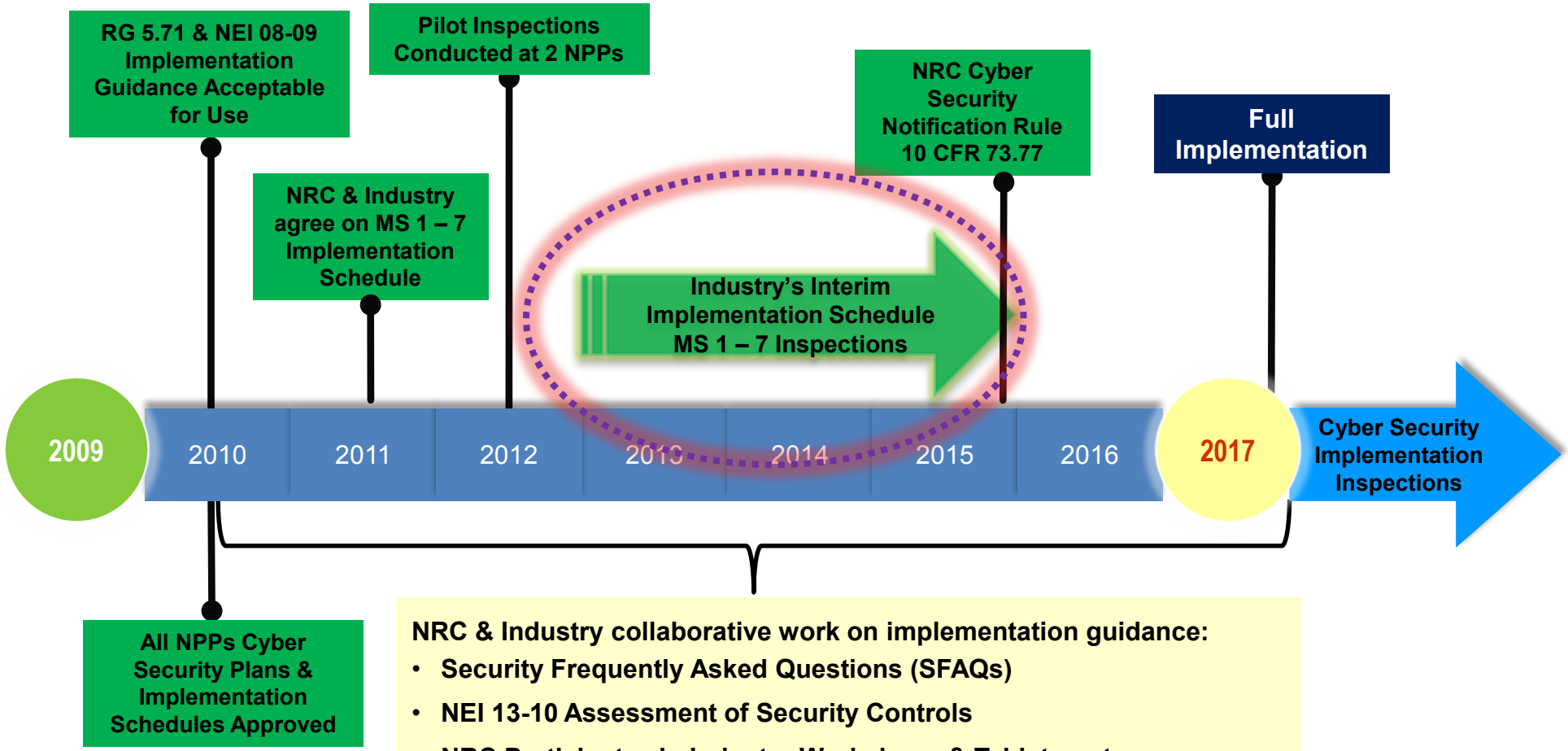
10 CFR 73.54 Protection of Digital Computer & Communication Systems & Networks

- **The licensee shall:**
  - Analysis of equipment that needs to be protected (SSEP)
  - Establish, implement, and maintain a cyber security program for the protection of the assets identified
- **The Cyber Security Program is designed to:**
  - Implement security controls to protect the assets
  - Apply & maintain Defense-In-Depth
    - Detect, respond, & recover from cyber attacks
    - Mitigate adverse effects of a cyber attack
    - Maintain SSEP functions

10 CFR 73.54 Protection of Digital Computer & Communication Systems & Networks

- **The Cyber Security Program must include:**
  - Training for all Personnel, including contractors
    - Awareness
    - Specialized training commensurate with roles & responsibilities
  - Evaluate & manage cyber risks
  - Evaluate modification to assets
  - Conduct cyber security event notifications
- **Review the cyber security program as part of the physical security program**

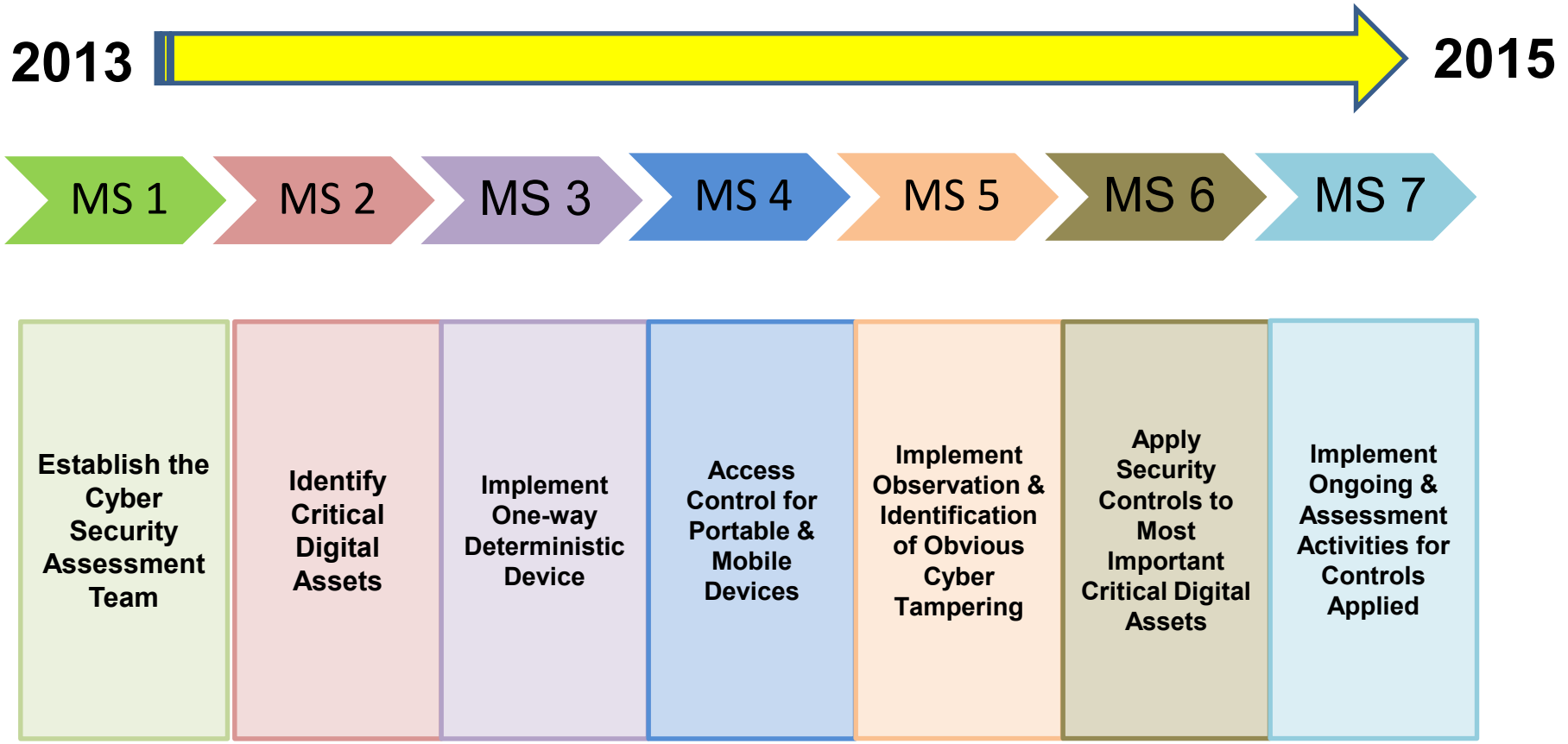
Overview of US NRC Cyber Security Program



NRC & Industry collaborative work on implementation guidance:

- **Security Frequently Asked Questions (SFAQs)**
- **NEI 13-10 Assessment of Security Controls**
- **NRC Participates in Industry Workshops & Tabletops to assess inspection procedure**
- **Development of Additional Guidance for Implementation Schedules**

7 Interim Milestones

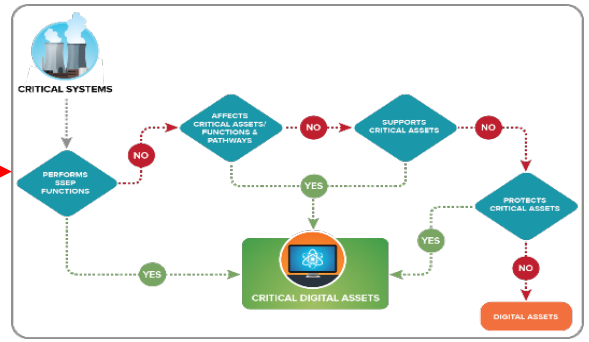


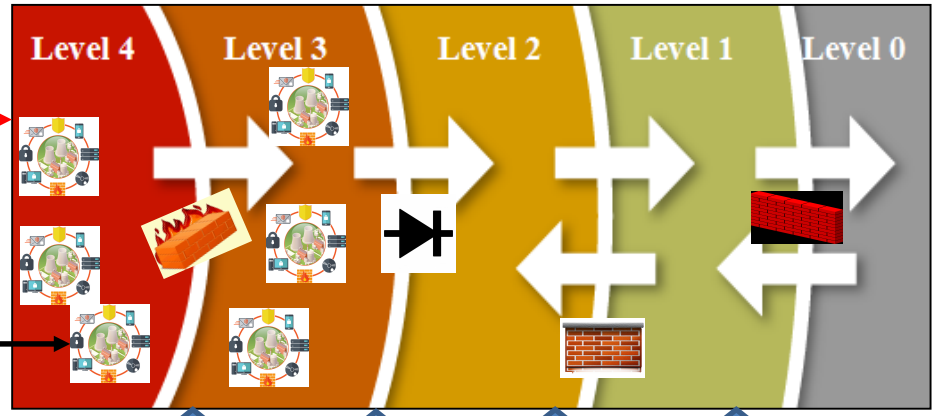
- Inspections conducted using a Temporary Instruction
- Good Faith Enforcement Direction used for findings
- Findings followed-up through Problem Identification & Resolution Inspections

Regulatory Guide 5.71, "Cyber Security Program for Nuclear Facilities"

1. Cyber Security Assessment Team
2. Identify Critical Digital Assets (CDAs)
3. Implement Defensive Architecture
4. Apply Security Controls

Most Risk Significant CDAs

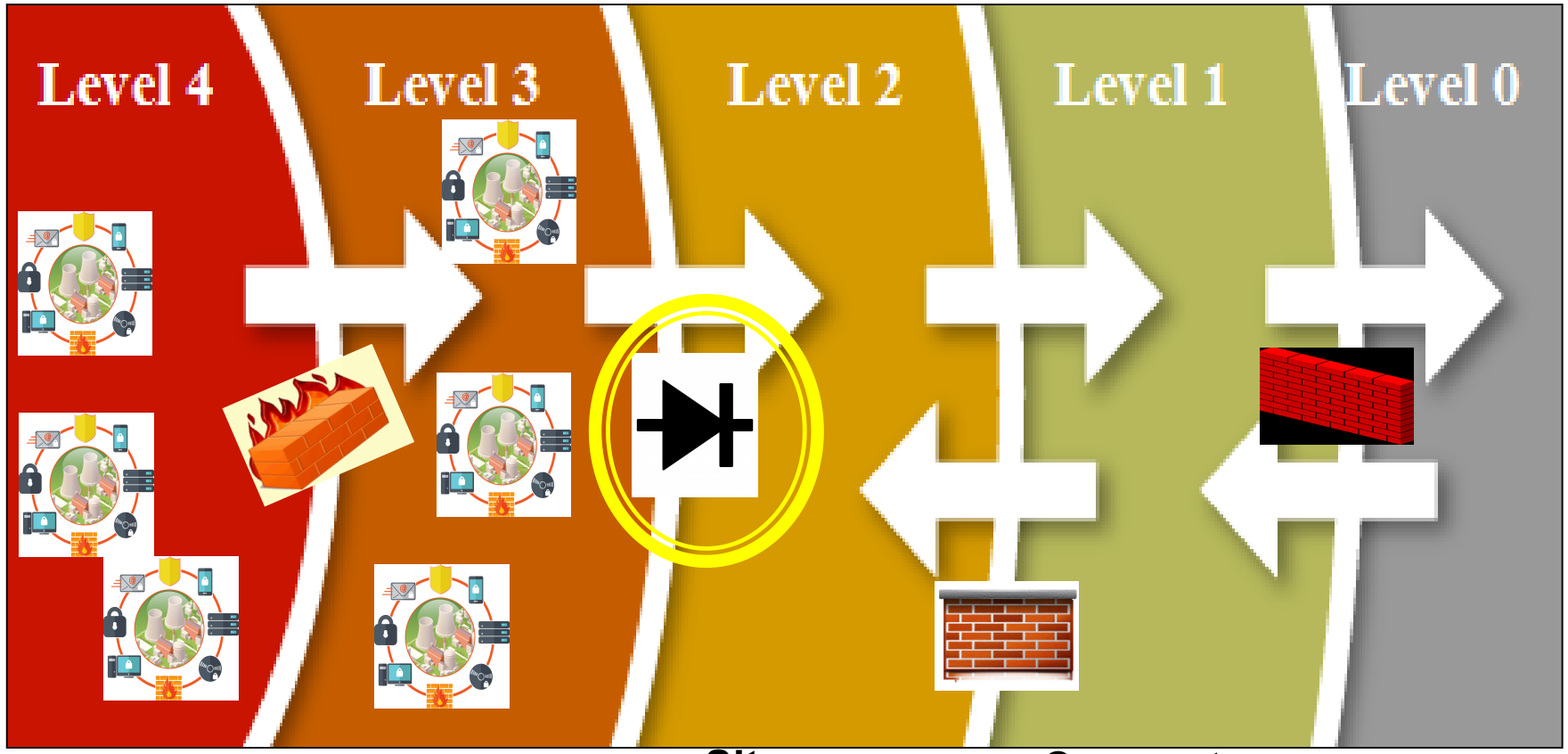




CYBER SECURITY PROGRAM

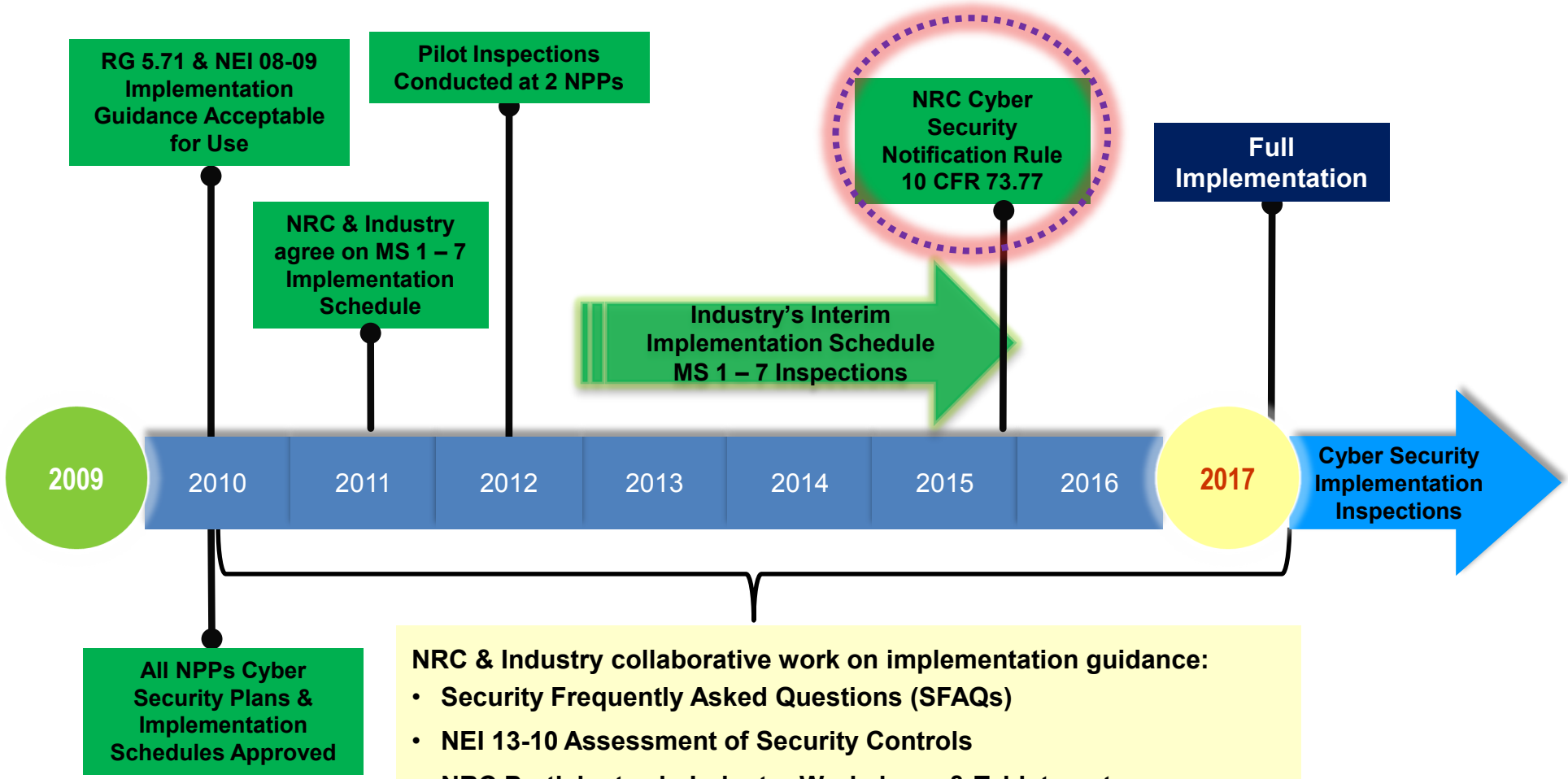
- Defense-in-Depth
- Security Controls NEI 13-10
- Mitigation Strategies
- Training
- Manage Cyber Risk
- Periodic Review
- Modification Evaluation
- Incident Response
- Procedures
- Records Retention

Generic Defensive Architecture



One-way Deterministic Device

Overview of US NRC Cyber Security Program



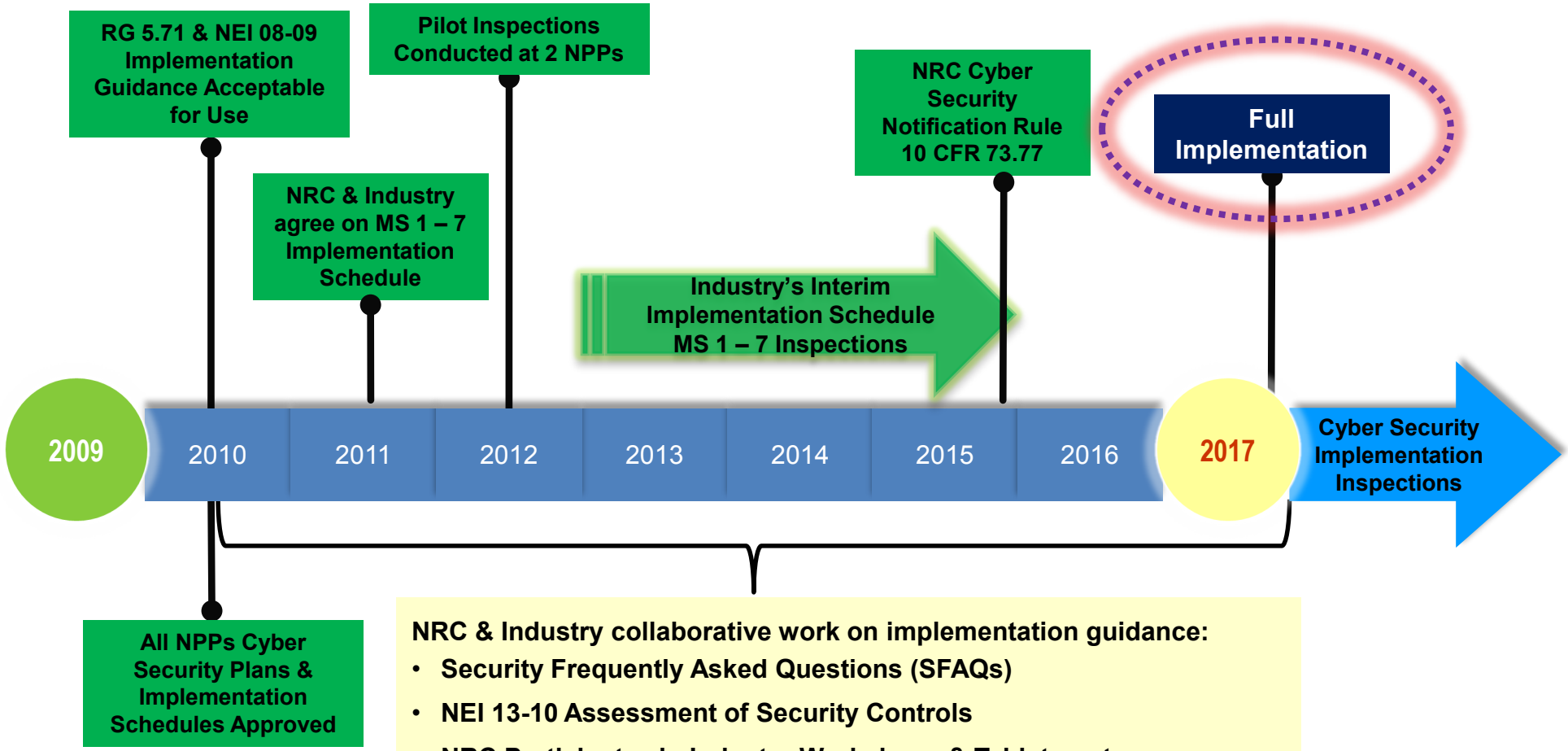
NRC & Industry collaborative work on implementation guidance:

- **Security Frequently Asked Questions (SFAQs)**
- **NEI 13-10 Assessment of Security Controls**
- **NRC Participates in Industry Workshops & Tabletops to assess inspection procedure**
- **Development of Additional Guidance for Implementation Schedules**

Cyber Security Notification Rule, 10 CFR 73.77

- **Effective on December 2, 2015**
- **Implementation date – May 2, 2016**
- **Requires licensees to notify NRC of certain cyber incidents within timelines based on the severity of the incident.**
- **Associated Guidance:**
  - NRC Regulatory Guide 5.83
  - NEI Guidance Document (NEI 15-09)
- **The NRC has received no 10 CFR 73.77 notifications to date**

Overview of US NRC Cyber Security Program



NRC & Industry collaborative work on implementation guidance:

- **Security Frequently Asked Questions (SFAQs)**
- **NEI 13-10 Assessment of Security Controls**
- **NRC Participates in Industry Workshops & Tabletops to assess inspection procedure**
- **Development of Additional Guidance for Implementation Schedules**

Full Implementation Details

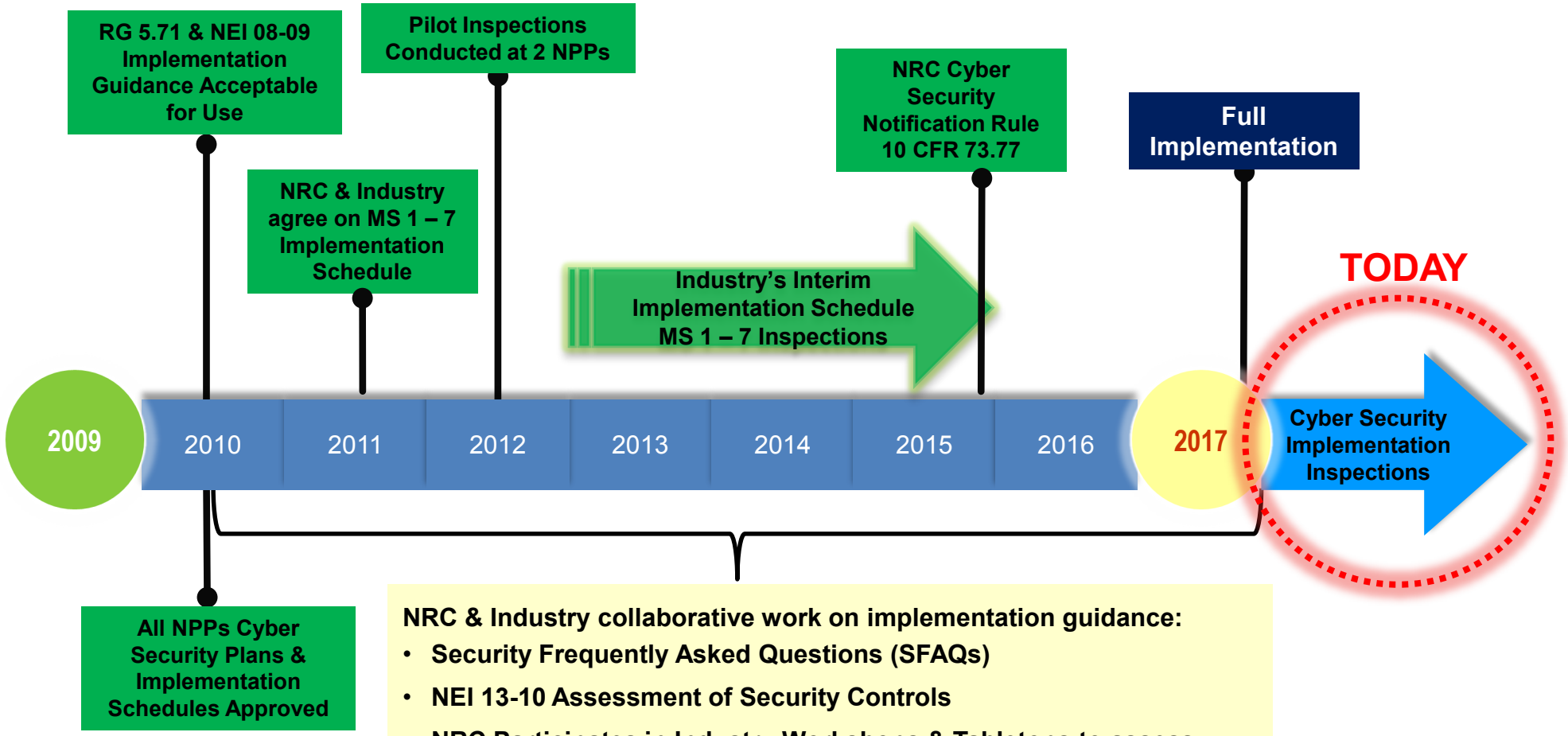
- **Expands scope to include all Critical Digital Assets (CDAs)**
  - All Safety & Security – Full Cyber Controls
  - Graded Approach for Important-to-Safety, Emergency Preparedness (EP) & Balance-of-Plant (BoP)
    - Some Important-to-Safety, the EP and BoP CDAs are evaluated as Non-Direct and have a minimal set of controls applied
- **Attack Mitigation and Incident Response Testing and Drills**
- **Continuity of Operations Training and Testing**
- **Vulnerability Assessment and Mitigation**

Non-Direct CDA: CDAs that cannot have an adverse impact on Safety or Security functions prior to their compromise or failure being detected and compensatory measures being implemented by a licensee

Full Implementation Details

- **Secure Communication Pathways to CDAs**
  - Ensure only authorized, protected communication from known devices is permitted
- **Supply Chain**
  - Adds security requirements relevant to vendors, contractors, and developers
- **Ensure Availability and Integrity of Information to, from, and on CDAs**
  - Prevent CDAs from accessing, receiving, transmitting, or producing unverified or untrusted information
- **Configuration Management**
- **Ongoing Evaluation and Management of Cyber Risk**
- **Audit and Accountability**
  - Validates effectiveness of the cyber security program and controls

Overview of US NRC Cyber Security Program



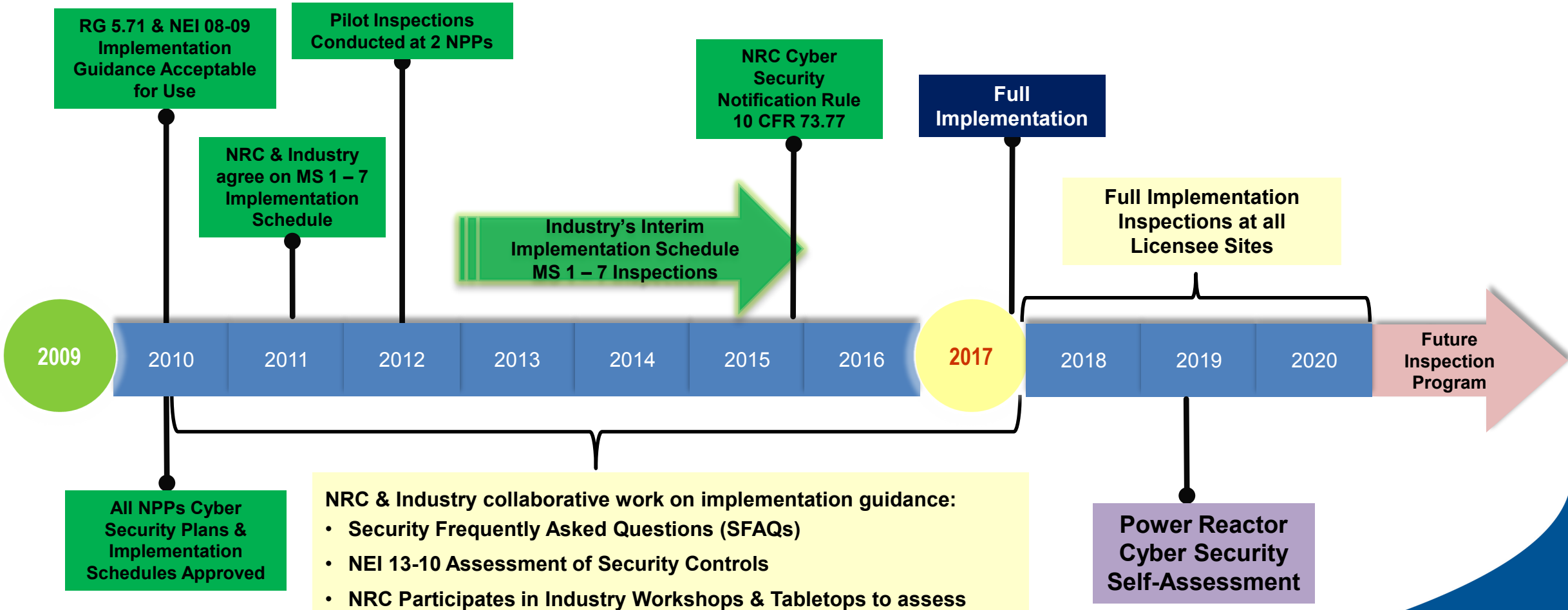
NRC & Industry collaborative work on implementation guidance:

- **Security Frequently Asked Questions (SFAQs)**
- **NEI 13-10 Assessment of Security Controls**
- **NRC Participates in Industry Workshops & Tabletops to assess inspection procedure**
- **Development of Additional Guidance for Implementation Schedules**

Full Implementation Inspections

- As of February 2019, 23 inspections are complete.
- Preliminary insights on potential areas for improvement:
  - Quality of licensee critical digital asset and system assessments
    - Quality of description / justification for the use of alternate controls.
  - Implementation of the licensee's vulnerability assessment program, including past vulnerabilities.
  - Guidance on portable media & mobile device program, in particular configuration of transfer kiosk.
  - Guidance on periodicity for ongoing monitoring & assessment modifications.

Future of US NRC Cyber Security Program



Future Plans

- In 2019 the NRC plans to conduct an overall assessment of the power reactor cyber security program to include:
  - Effectiveness of the 10 CFR 73.54 rule
  - Effectiveness of the guidance and licensee implementation of the rule
  - Effectiveness of the full implementation inspection program
  - External factors and lessons learned over the course of program implementation
- The assessment will inform the staff's evaluation of the NEI Petition for Cyber Security Rulemaking.
- Assessment results will be used to evaluate future inspection
- Regulatory Guide 5.71 Revision 1 in comment resolution

Other NRC Cyber Initiatives

- **Fuel Cycle Facilities**
  - Cyber Security Rulemaking in progress
  - Lessons learned from power reactor implementation
- **Non-Power Reactors**
  - Best Practices Guidance
- **Non-power Production or Utilization Facilities**
  - Under evaluation by the NRC staff
- **Independent Spent Fuel Storage Installations**
  - No cyber requirement, may re-evaluate in the future
- **Nuclear Materials**
  - Best Practices Guidance
- **Decommissioning**
  - Cyber Security is included in the decommissioning rulemaking

Industry Cyber Incidents 2015-2018

- Advanced Persistent Threat (APT) campaign targeting energy sector (2016-2017)
  - Well publicized attack on multiple sectors of the critical infrastructure.
  - March 15th, DHS identified Russia as the source of these incursions.
  - Staff follow-up the incident with a security advisory for industry.
- Malware Event impacting multiple Entergy facilities, including nuclear sites (2018)
  - In February 2018, malware was detected on Entergy's business networks
  - Attempted access of EP CDAs identified as a recordable event at two sites.
  - Attack attributed to hacking an internet facing company site.

Questions

NRC Cyber Security Oversight Program Status

Jim Beardsley, Chief

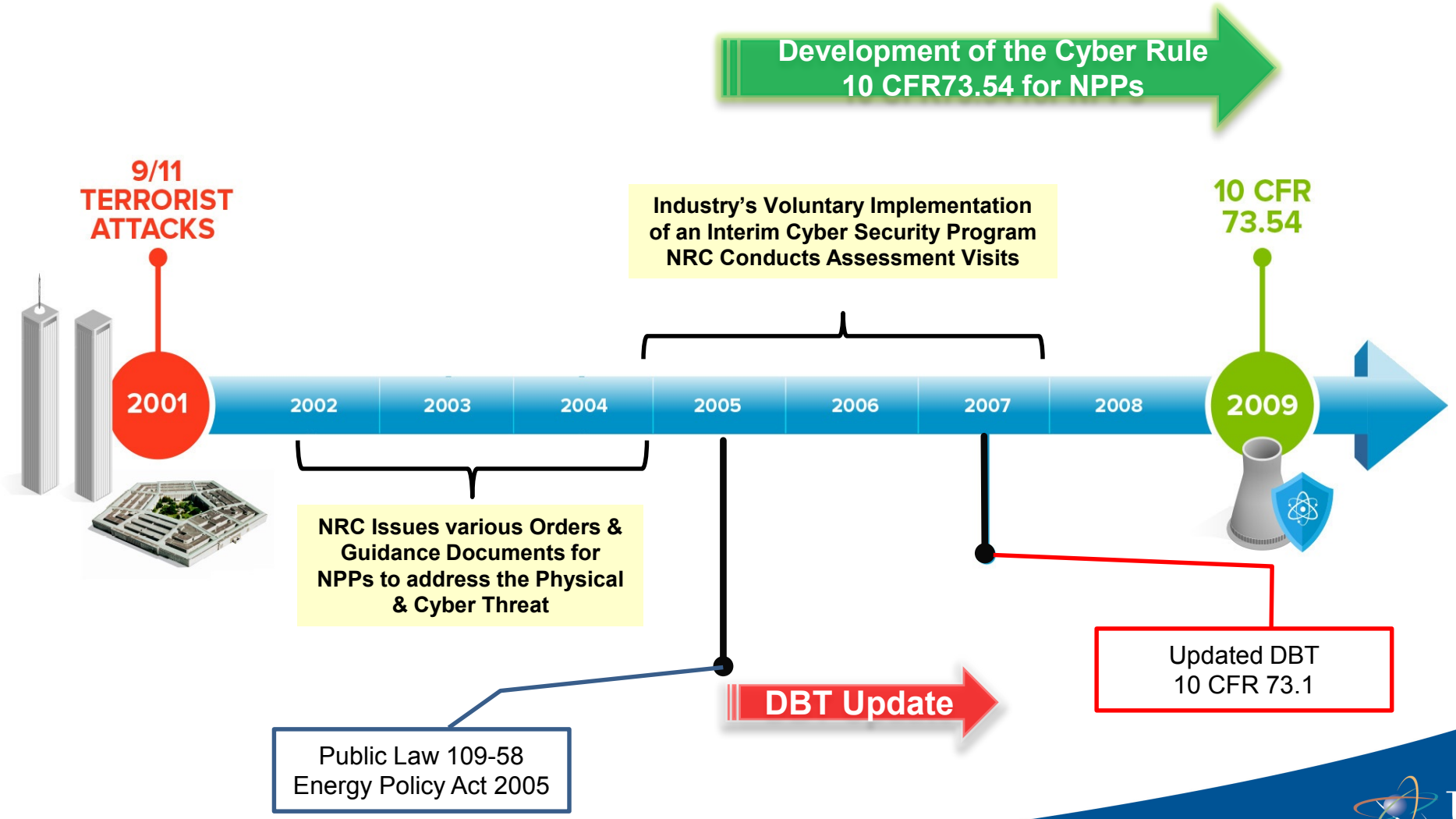
Cyber Security Branch (CSB)

Division of Physical and Cyber Security Policy (DPCP)

Office of Nuclear Security and Incident Response (NSIR)

james.beardsley@nrc.gov

Overview of US NRC Cyber Security Program



10 CFR 73.54 Protection of Digital Computer & Communication Systems & Networks

- **Op Rx and license applicants must submit a Cyber Security Plan by November 2009**
  - Protect digital computer and communication systems and networks associated with
    - **Safety, Security & Emergency Preparedness (SSEP) functions**
    - **Support systems** and equipment which, if compromised, would adversely impact SSEP functions
  - Protect from cyber attacks that adversely impact
    - Integrity or Confidentiality of data and/or software
    - Deny access to systems, services, and/or data
    - Operation of systems, networks, & associated equipment

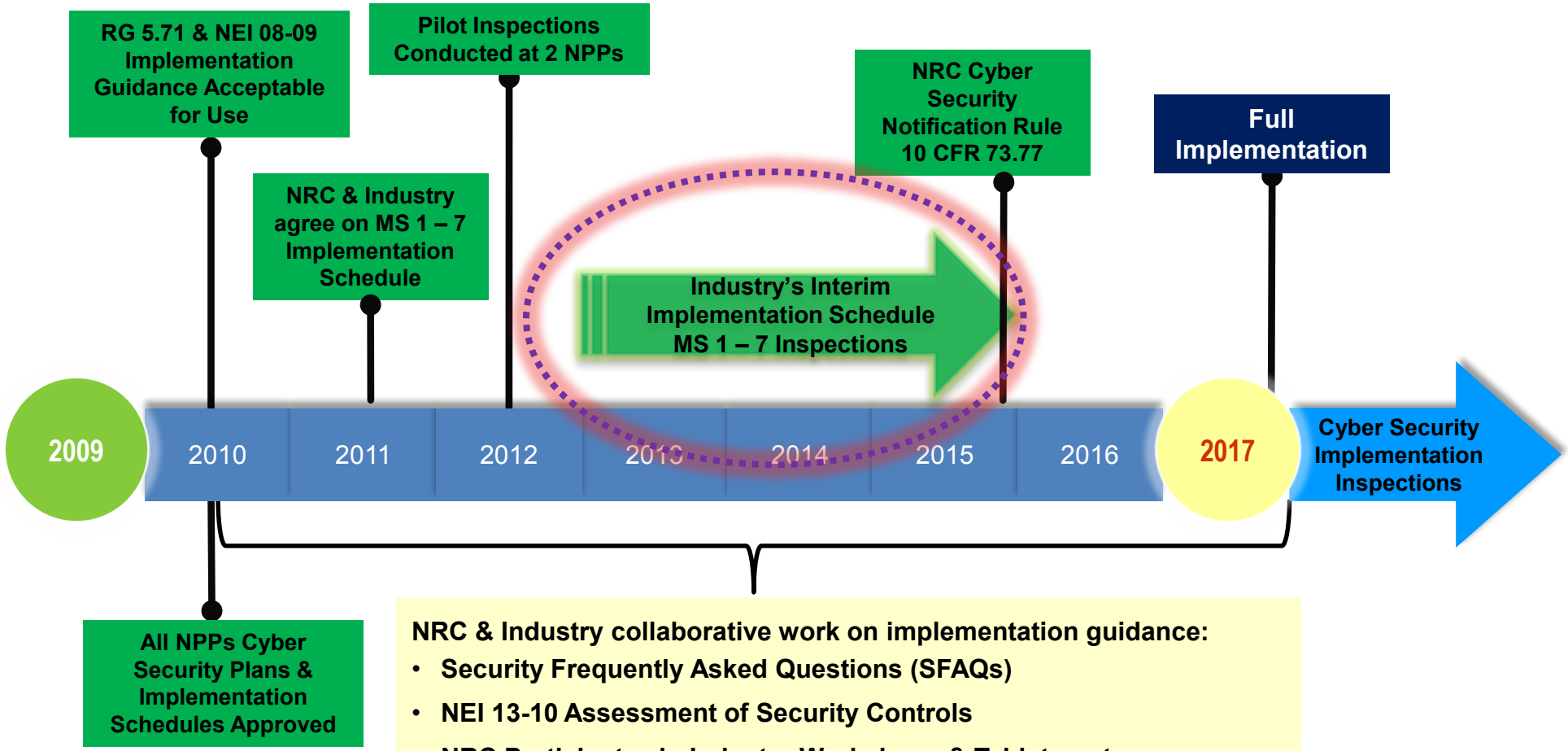
10 CFR 73.54 Protection of Digital Computer & Communication Systems & Networks

- **The licensee shall:**
  - Analysis of equipment that needs to be protected (SSEP)
  - Establish, implement, and maintain a cyber security program for the protection of the assets identified
- **The Cyber Security Program is designed to:**
  - Implement security controls to protect the assets
  - Apply & maintain Defense-In-Depth
    - Detect, respond, & recover from cyber attacks
    - Mitigate adverse effects of a cyber attack
    - Maintain SSEP functions

10 CFR 73.54 Protection of Digital Computer & Communication Systems & Networks

- **The Cyber Security Program must include:**
  - Training for all Personnel, including contractors
    - Awareness
    - Specialized training commensurate with roles & responsibilities
  - Evaluate & manage cyber risks
  - Evaluate modification to assets
  - Conduct cyber security event notifications
- **Review the cyber security program as part of the physical security program**

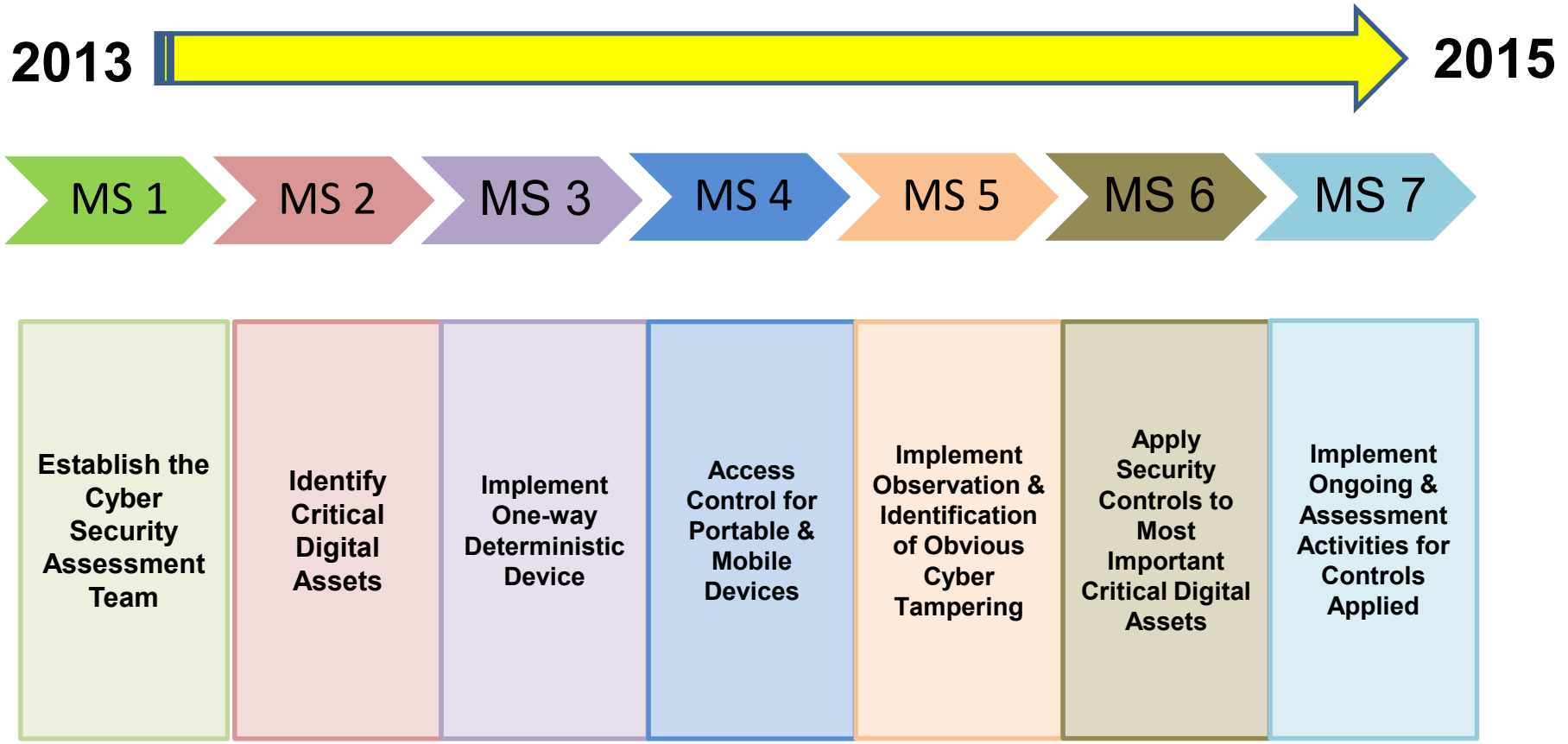
Overview of US NRC Cyber Security Program



NRC & Industry collaborative work on implementation guidance:

- **Security Frequently Asked Questions (SFAQs)**
- **NEI 13-10 Assessment of Security Controls**
- **NRC Participates in Industry Workshops & Tabletops to assess inspection procedure**
- **Development of Additional Guidance for Implementation Schedules**

7 Interim Milestones

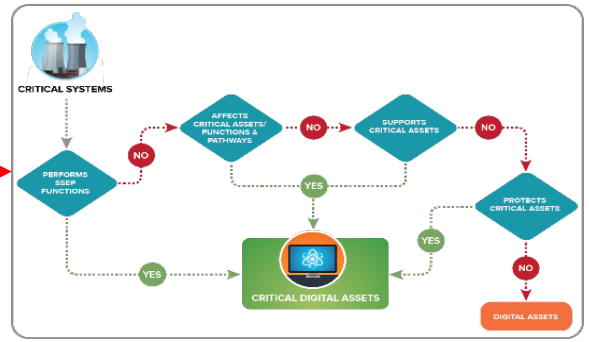


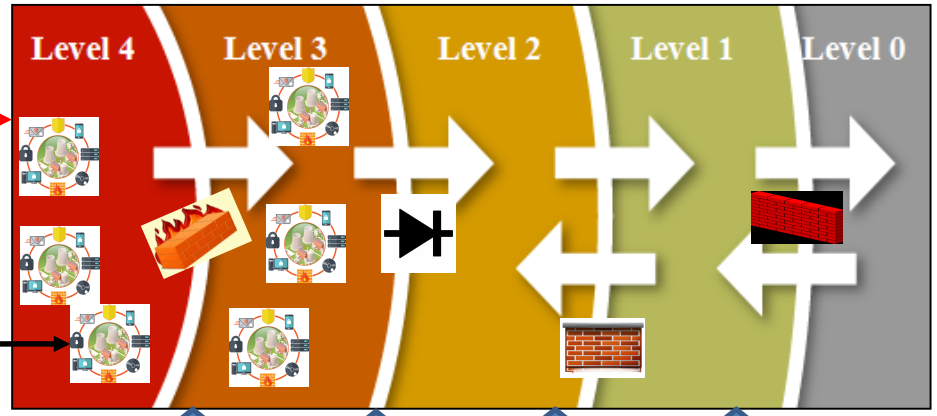
- Inspections conducted using a Temporary Instruction
- Good Faith Enforcement Direction used for findings
- Findings followed-up through Problem Identification & Resolution Inspections

Regulatory Guide 5.71, "Cyber Security Program for Nuclear Facilities"

1. Cyber Security Assessment Team
2. Identify Critical Digital Assets (CDAs)
3. Implement Defensive Architecture
4. Apply Security Controls

Most Risk Significant CDAs

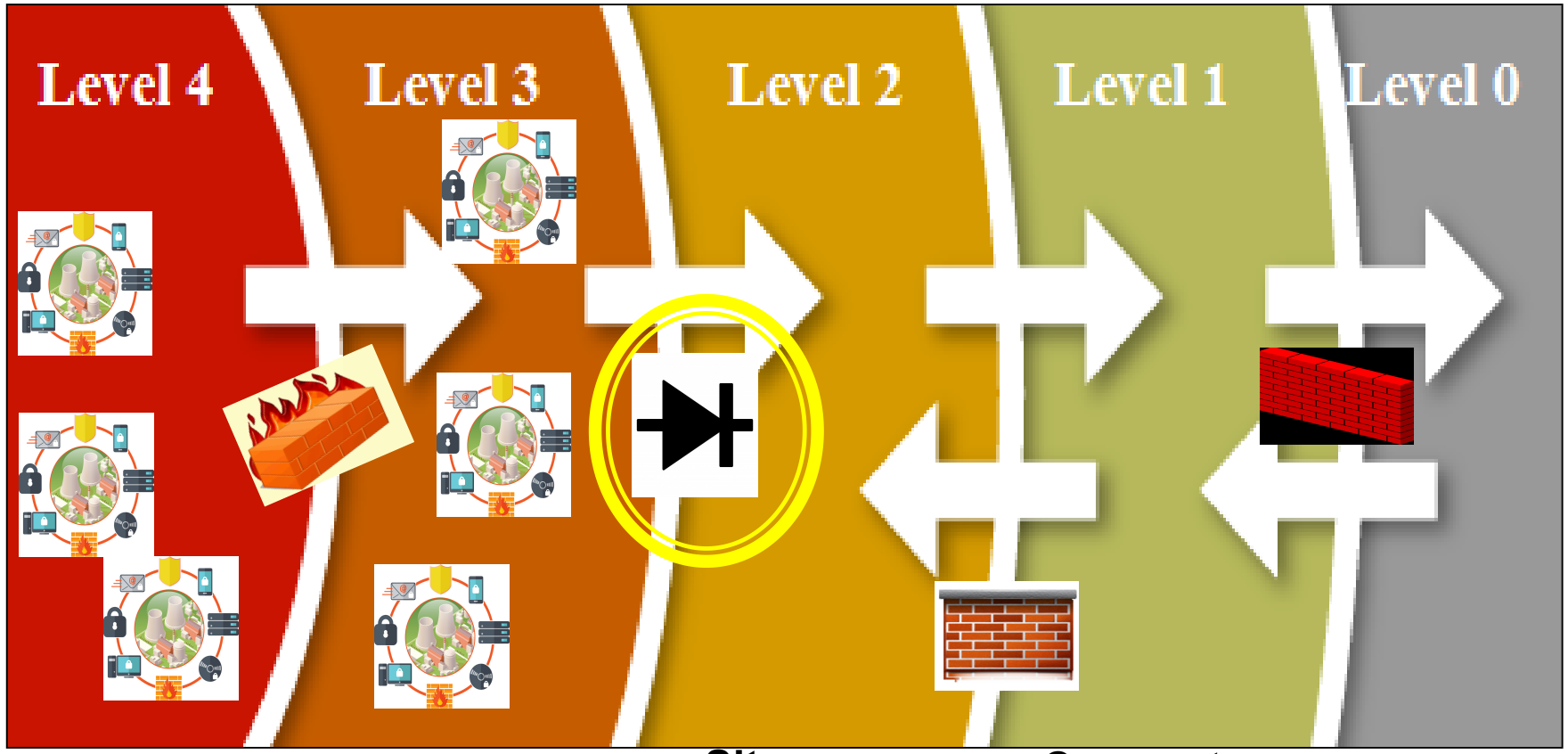




CYBER SECURITY PROGRAM

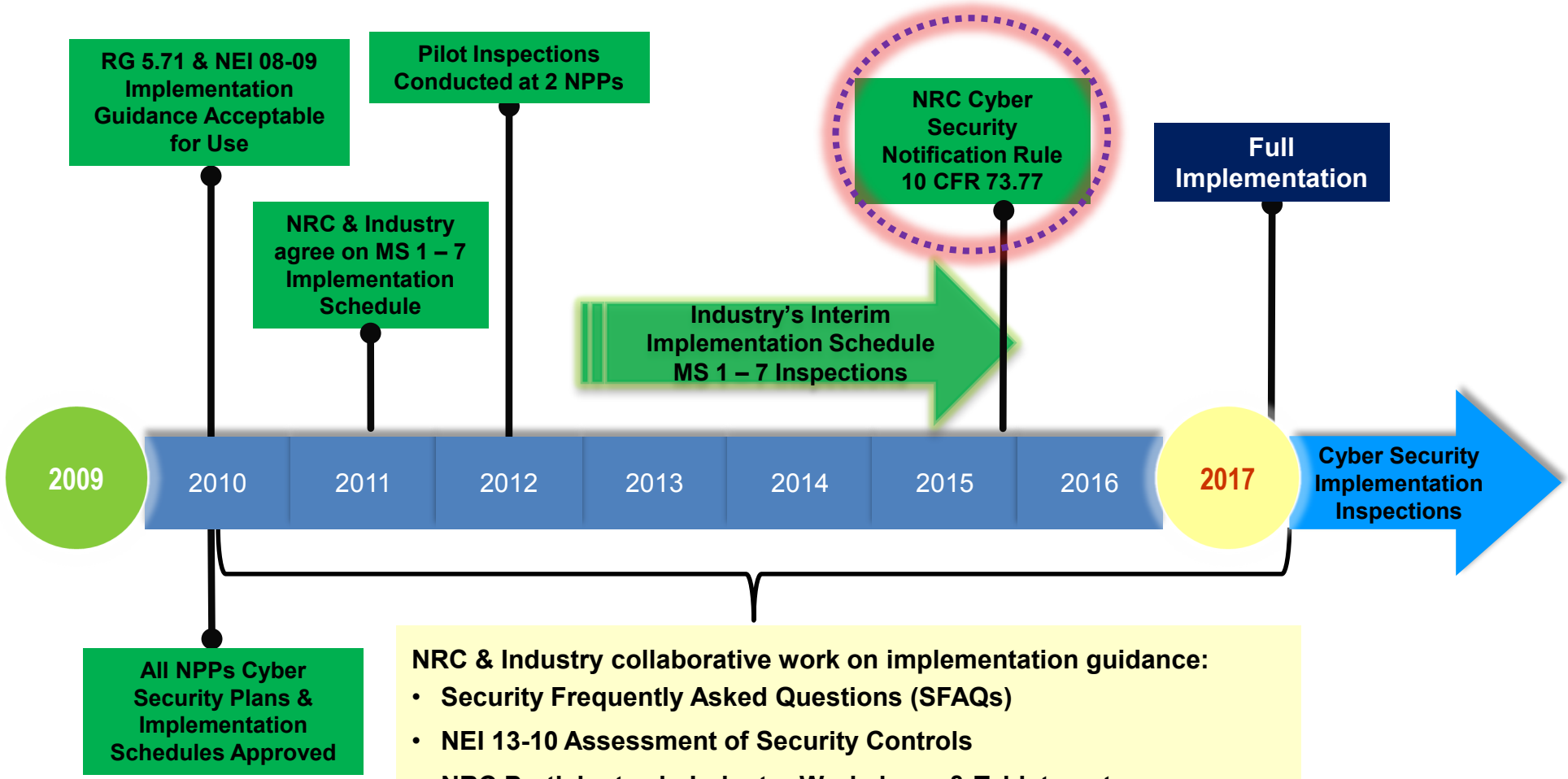
- Defense-in-Depth
- Security Controls NEI 13-10
- Mitigation Strategies
- Training
- Manage Cyber Risk
- Periodic Review
- Modification Evaluation
- Incident Response
- Procedures
- Records Retention

Generic Defensive Architecture



One-way Deterministic Device

Overview of US NRC Cyber Security Program



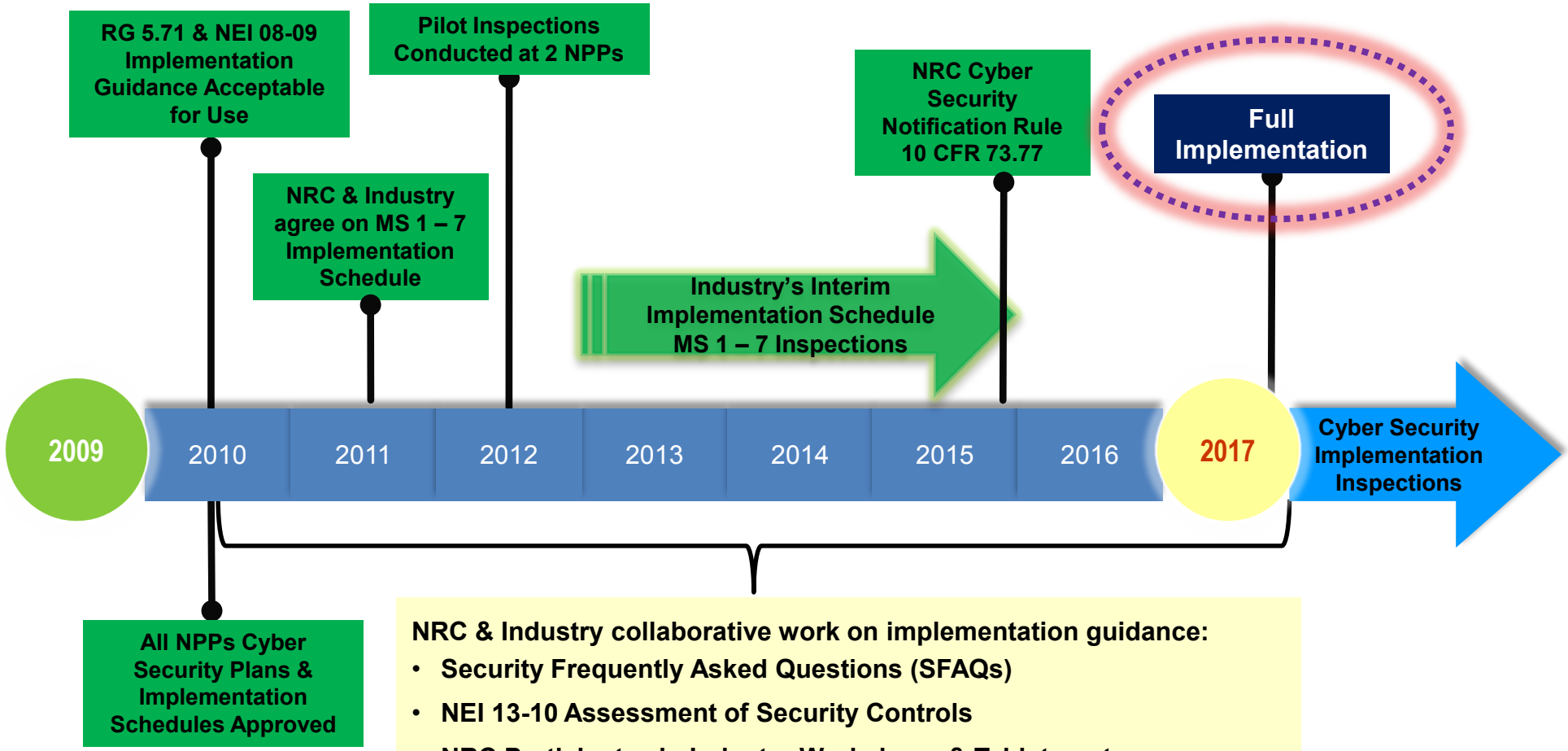
NRC & Industry collaborative work on implementation guidance:

- **Security Frequently Asked Questions (SFAQs)**
- **NEI 13-10 Assessment of Security Controls**
- **NRC Participates in Industry Workshops & Tabletops to assess inspection procedure**
- **Development of Additional Guidance for Implementation Schedules**

Cyber Security Notification Rule, 10 CFR 73.77

- **Effective on December 2, 2015**
- **Implementation date – May 2, 2016**
- **Requires licensees to notify NRC of certain cyber incidents within timelines based on the severity of the incident.**
- **Associated Guidance:**
  - NRC Regulatory Guide 5.83
  - NEI Guidance Document (NEI 15-09)
- **The NRC has received no 10 CFR 73.77 notifications to date**

Overview of US NRC Cyber Security Program



NRC & Industry collaborative work on implementation guidance:

- **Security Frequently Asked Questions (SFAQs)**
- **NEI 13-10 Assessment of Security Controls**
- **NRC Participates in Industry Workshops & Tabletops to assess inspection procedure**
- **Development of Additional Guidance for Implementation Schedules**

Full Implementation Details

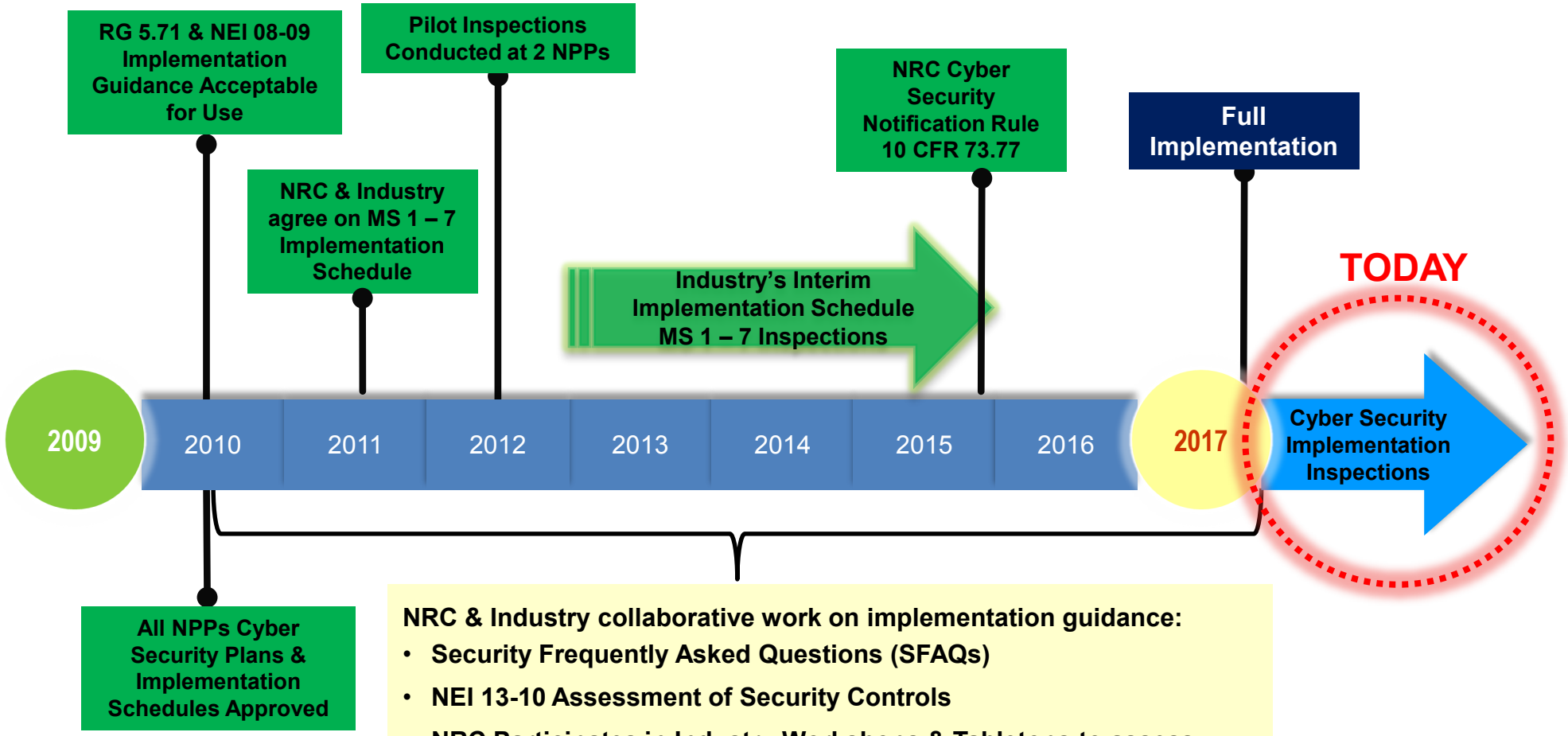
- **Expands scope to include all Critical Digital Assets (CDAs)**
  - All Safety & Security – Full Cyber Controls
  - Graded Approach for Important-to-Safety, Emergency Preparedness (EP) & Balance-of-Plant (BoP)
    - Some Important-to-Safety, the EP and BoP CDAs are evaluated as Non-Direct and have a minimal set of controls applied
- **Attack Mitigation and Incident Response Testing and Drills**
- **Continuity of Operations Training and Testing**
- **Vulnerability Assessment and Mitigation**

Non-Direct CDA: CDAs that cannot have an adverse impact on Safety or Security functions prior to their compromise or failure being detected and compensatory measures being implemented by a licensee

Full Implementation Details

- **Secure Communication Pathways to CDAs**
  - Ensure only authorized, protected communication from known devices is permitted
- **Supply Chain**
  - Adds security requirements relevant to vendors, contractors, and developers
- **Ensure Availability and Integrity of Information to, from, and on CDAs**
  - Prevent CDAs from accessing, receiving, transmitting, or producing unverified or untrusted information
- **Configuration Management**
- **Ongoing Evaluation and Management of Cyber Risk**
- **Audit and Accountability**
  - Validates effectiveness of the cyber security program and controls

Overview of US NRC Cyber Security Program



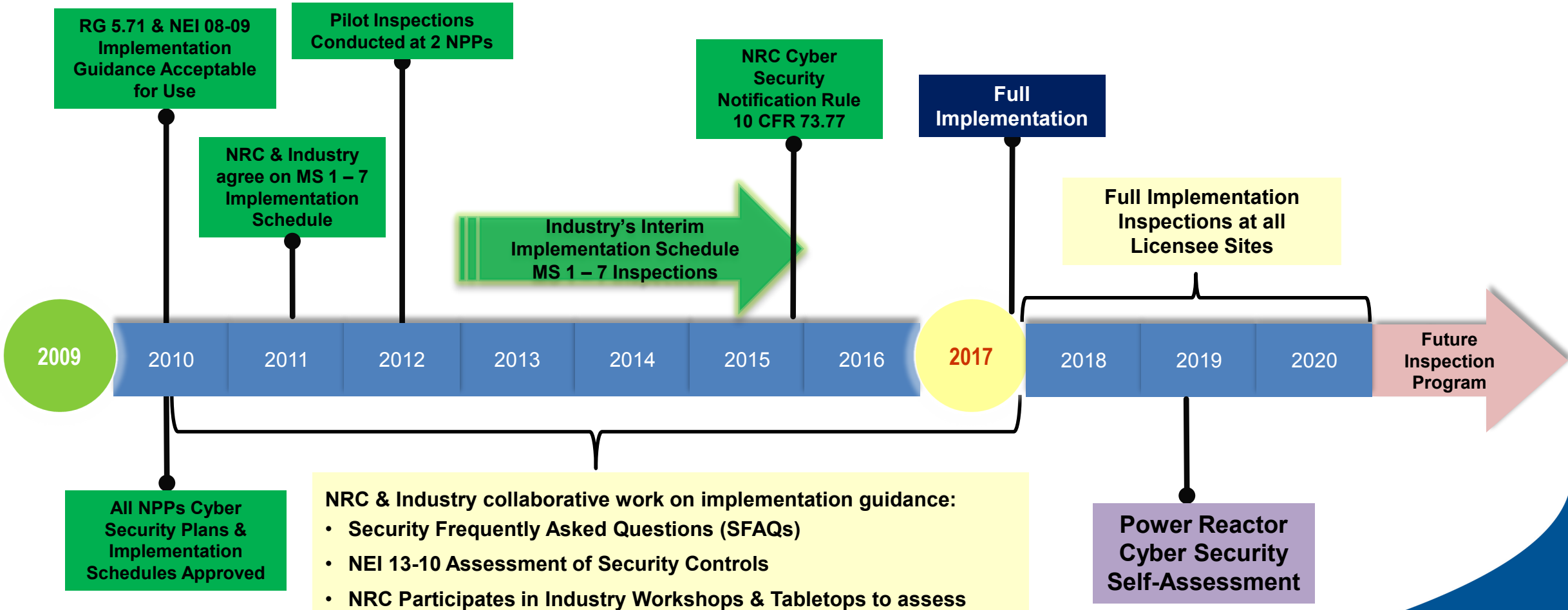
NRC & Industry collaborative work on implementation guidance:

- **Security Frequently Asked Questions (SFAQs)**
- **NEI 13-10 Assessment of Security Controls**
- **NRC Participates in Industry Workshops & Tabletops to assess inspection procedure**
- **Development of Additional Guidance for Implementation Schedules**

Full Implementation Inspections

- As of February 2019, 23 inspections are complete.
- Preliminary insights on potential areas for improvement:
  - Quality of licensee critical digital asset and system assessments
    - Quality of description / justification for the use of alternate controls.
  - Implementation of the licensee's vulnerability assessment program, including past vulnerabilities.
  - Guidance on portable media & mobile device program, in particular configuration of transfer kiosk.
  - Guidance on periodicity for ongoing monitoring & assessment modifications.

Future of US NRC Cyber Security Program



Future Plans

- In 2019 the NRC plans to conduct an overall assessment of the power reactor cyber security program to include:
  - Effectiveness of the 10 CFR 73.54 rule
  - Effectiveness of the guidance and licensee implementation of the rule
  - Effectiveness of the full implementation inspection program
  - External factors and lessons learned over the course of program implementation
- The assessment will inform the staff's evaluation of the NEI Petition for Cyber Security Rulemaking.
- Assessment results will be used to evaluate future inspection
- Regulatory Guide 5.71 Revision 1 in comment resolution

Other NRC Cyber Initiatives

- **Fuel Cycle Facilities**
  - Cyber Security Rulemaking in progress
  - Lessons learned from power reactor implementation
- **Non-Power Reactors**
  - Best Practices Guidance
- **Non-power Production or Utilization Facilities**
  - Under evaluation by the NRC staff
- **Independent Spent Fuel Storage Installations**
  - No cyber requirement, may re-evaluate in the future
- **Nuclear Materials**
  - Best Practices Guidance
- **Decommissioning**
  - Cyber Security is included in the decommissioning rulemaking

Industry Cyber Incidents 2015-2018

- Advanced Persistent Threat (APT) campaign targeting energy sector (2016-2017)
  - Well publicized attack on multiple sectors of the critical infrastructure.
  - March 15th, DHS identified Russia as the source of these incursions.
  - Staff follow-up the incident with a security advisory for industry.
- Malware Event impacting multiple Entergy facilities, including nuclear sites (2018)
  - In February 2018, malware was detected on Entergy's business networks
  - Attempted access of EP CDAs identified as a recordable event at two sites.
  - Attack attributed to hacking an internet facing company site.

Questions