00:00:04.050 --> 00:00:15.980

OK good afternoon everybody. Thank you for attending and participating in this public meeting before we get started. I would like to mention that this meeting is being recorded, so that we can accurately capture and feedback that we received during the meeting.

00:01:29.430 --> 00:01:57.880

All that said, while we can accept comments and feedback during the meeting. Today, the best way to provide us with feedback on the draft regulatory guide is by providing that feedback through the regulations.gov website. And once you go website. Search for NRC-2021-0143 and then in the results. You'll see a comment button that you can Click to enter your comment. And those instructions also appear on the first page of the draft regulatory guide itself.

00:01:58.740 --> 00:02:17.870

And lastly if you'd like to provide feedback on this meeting. You can do so using form and or C 659 now would like to turn over the meeting to Jim Beardsley, who is the acting deputy director of the division of physical and cyber security policy. Thank you. Brian this is as Brian stated. This is a follow up meeting to our.

00:02:17.950 --> 00:02:47.930

We had a 2 months ago when we released the draft guide for comment. This draft guide has been in development for a number of years and Kim will talk about the history and the process we use for putting together. The changes that are in the draft guide. We're looking forward to stakeholder feedback and comments on the draft guide and hope to complete this update in a timely manner, and get the revision one to regulate 571 out for public use.

00:02:48.070 --> 00:03:04.470

And for use by stakeholders, both here in the US and abroad again. If you have any comments please. Please raise your hand or we will provide opportunities for people on the phone to provide comments as well. And we look forward to hearing from you and I'll turn it over to Kim.

00:03:10.800 --> 00:03:13.150

Thank you my name is Kim Lawson Jenkins.

00:03:13.310 --> 00:03:20.920

I am a staff member at the cyber security branch and the technical lead on draft guidance 5061.

00:03:21.950 --> 00:03:22.910

Next slide please.

00:03:34.660 --> 00:03:35.430

On this slide is the overview of this presentation is that first I will give a few key messages.

00:03:42.660 --> 00:03:45.310

First there is some background information.

00:03:46.000 --> 00:03:50.690

I will go through the updates per section in the document and.

00:03:51.190 --> 00:04:04.220

I will mention the conclusion which is pretty much restating the key messages and we'll have questions and answers at the end, so if people want us to go back and look at the certain slide. We can talk about the presentation then.

00:04:06.520 --> 00:04:07.540

Next slide please.

00:04:08.990 --> 00:04:39.440

OK, the key messages for this presentation is that since 2012. Licensees have implemented cybersecurity their cyber security programs and the NRC has provided oversight of these cybersecurity programs and the plans. There are no changes in the staff 's position in this draft guidance. Only clarifications and only one new NRC regulation, which is Title 10 code of the federal regulation 73.77.

00:04:44.270 --> 00:04:55.880

We're capturing all the lessons learned in this presentation and the guidance since the issuance of the original guidance in 2010 and we're preparing for the future.

00:04:57.110 --> 00:04:58.170

Next slide please.

00:05:03.650 --> 00:05:09.620

This slide - if anyone has been involved with it in their Cyber Security Program - has seen it many times.

00:05:11.000 --> 00:05:17.510

The cyber security rule was written in 2009.

00:05:18.270 --> 00:05:35.080

The NRC issued the original version of Reg Guide 5.71 “Cyber Security plans for nuclear facilities” in 2010.

00:05:38.980 --> 00:05:54.970

From 2013 to 2015, we had initial implementations of the cybersecurity plan milestones one through 7, which I'll talk about a little bit more in detail but all through the process of.

00:05:55.770 --> 00:06:08.450

From 2010 until today, we've had many engagements with the nuclear industry. We've had a lot of collaborative work on security frequently asked questions.

00:06:09.710 --> 00:06:11.050

The licensees have implemented NEI 13.10 assessments of security controls. We've participated in numerous workshops with industry and also tabletop exercises.

00:06:26.090 --> 00:06:27.180

Next slide please.

00:06:29.990 --> 00:06:45.390

And before I start talking about the guide itself, I always want to talk about the big picture because a lot of times when people think of implementation of cyber security plans. They only think of the security controls what security controls we have to implement.

00:06:48.530 --> 00:07:05.550

If you look at the cybersecurity rule, 10 CFR 73.54 section (e) says the licensee shall establish implement and maintain a cyber security plan that implements the cybersecurity program requirements.

00:07:06.370 --> 00:07:16.280

This is regulatory guide 5.71 is an acceptable way of implementing a cybersecurity plan that will meet the cybersecurity rule.

00:07:17.420 --> 00:07:27.440

In the NEI 08-09 it's another method to implement a cyber security plan that is acceptable for the cyber security rule.

00:07:29.960 --> 00:07:40.910

So, in this diagram, you see the cybersecurity plan I've just mentioned.

00:07:41.730 --> 00:07:55.140

Critical digital assets were identified and security controls or applied to those critical digital assets. And those critical digital assets perform SSEP function.

00:07:55.950 --> 00:08:12.560

One thing that we're highlighting definitely in the revision is knowledge of attack surfaces and pathways of seat of critical digital assets because we need that. You need that information. We need that information to adequately protect.

00:08:13.940 --> 00:08:14.810

Where's the security controls are applied?

00:08:25.590 --> 00:08:29.160

Those controls should be continuously monitored for effectiveness.

00:08:30.310 --> 00:08:37.510

So everyone should keep that big picture in mind because that's the goal that's how we protect the SSEP functions.

00:08:39.300 --> 00:08:40.340

Next slide please.

00:08:41.990 --> 00:08:42.440

Remembering what we just saw in the previous diagram, and the big picture. I want to go through some things about milestone one through 7 milestone. One was to establish a cyber security assessment team milestone 2, which was discussed in the previous slide identifying all critical digital assets.

00:09:06.540 --> 00:09:07.870

Milestone 3 was implemented using one way deterministic devices. This is important and affect wired pathways and wired connections.

00:09:20.690 --> 00:09:40.450

Milestone 4 addressed uh portable media and mobile devices, so that was another attack. Pathway milestone 5 was to implement observation and identification of obvious physical tampering for cyber so that's physical access that's another pathway.

00:09:41.450 --> 00:10:02.560

And then in Milestone 6 and 7, the licensees selected the most important, the most critical assets. I guess in the most critical digital assets digital assets in the plan to protect first and then to monitor those CDAs for the effectiveness of the protection.

00:10:03.440 --> 00:10:19.070

And that's really basically milestone one through 7 is the framework. The remaining security controls for full implementation of the cybersecurity plan so it was a good starting point.

00:10:21.210 --> 00:10:22.270

Next slide please.

00:10:25.400 --> 00:10:32.800

So a lot of the things that we discussed from from milestone one through 7 was implemented, which you see here on the defensive architecture.

And based on the guidance that was received in 2010.

00:10:40.030 --> 00:10:49.880

The most critical digital assets were located on Level 3 or 4 and controls were applied to those CDAs, and they were located behind a data diode.

00:10:52.030 --> 00:10:53.050

Next slide please.

00:10:55.970 --> 00:11:25.320

So the full program implementation is everything that I just previously discussed and then there were no other aspects of the program. We discussed you see defense in depth there, so to clarify defense in depth is not just having a a data diode remember to talk about that, more in in detail a little bit later, but it's layers of controls that being applied to protect the critical digital assets.

00:11:27.890 --> 00:11:37.950

Things such as training programs, where we're looking at the record retention with modifications are made to the systems how that's recorded.

00:11:38.690 --> 00:11:45.290

And maintain so everything all the controls were in place for the full program implementation.

00:11:46.970 --> 00:11:47.950

Next slide please.

00:11:50.070 --> 00:11:50.420

OK.

00:11:51.760 --> 00:11:54.750

So once again this, this timeline of everything that we've done.

00:11:56.800 --> 00:12:13.200

From 2009 on and in 2016. We started the revision of the original guidance that we gave in 2010 of the regulatory guide, so that began in as I said in the spring of 2016.

00:12:15.890 --> 00:12:16.870

Next slide please.

00:12:19.380 --> 00:12:24.090

OK, so I'm going to go through some of the some of the updates that we made.

00:12:24.750 --> 00:12:26.470

Next slide.

00:12:31.580 --> 00:12:38.890

Based on that work that we started in 2016, we issued a version of the draft guidance in 2018.

00:12:40.760 --> 00:12:46.600

It was based on providing more clarification of the things that we learned in milestone one through 7.

00:12:47.760 --> 00:12:55.170

It included the only new regulation that we've had since 2010, which is the cybersecurity event notification.

00:12:56.570 --> 00:13:08.170

Because the original version of RG 5.71 was a tailored version of the NIST special product, 800-53.

00:13:09.450 --> 00:13:17.150

We based it on we updated the guidance to make sure that we were in alignment with what they had in there for revision 4.

00:13:18.620 --> 00:13:29.130

The IAEA was generating new security guidance for cyber security at the very same time, we were doing it. So we were cognizant of the work that they were doing and we updated.

00:13:29.280 --> 00:13:36.470

We added guidance to deal with balance of plant equipment, which was not in the original guidance.

00:13:38.020 --> 00:13:38.990

Next slide please.

00:13:45.710 --> 00:13:57.220

Well, once we made the updates and we got public comments back in 2018, there was a pause decided not to go forward at that point with issuing the final version of the guidance. It was decided to wait until the full implementation. Full implementation inspections were not completed, so in the meantime. There was there was still changes going on. We added more information to the draft guidance. We added a discussion of a risk informed cybersecurity.

00:14:19.690 --> 00:14:27.480

We emphasize and this was a lesson learned the need for accurate CDA assessments because everything really hinges on that.

00:14:31.330 --> 00:14:33.470

The guidance that I spoke of earlier that the IAEA was doing was actually finalized during this period. So we are actually citing that guidance in this new document.

00:14:50.150 --> 00:14:56.820

Issue a new version of NIST SP 800-53 again so we are referencing the latest version of the document.

00:14:58.420 --> 00:15:05.130

And we addressed the public comments that we received in 2018 in this version of the document also.

00:15:06.380 --> 00:15:07.440

Next slide please.

00:15:12.380 --> 00:15:21.170

There were 57 inspections full implementation inspections completed from 2017 to 2021.

00:15:22.670 --> 00:15:47.470

The most important insights that areas that we saw that we can just still do improvements, especially on the guidance was to emphasize the quality of the licensees critical digital assets and the system assessments were important. They were actually the foundation. You have to know what you have in order to protect it adequately.

00:15:48.690 --> 00:16:00.170

Because a lot of the equipment in the of the program was going into the maintenance phase, we saw a need for a stronger emphasis on vulnerability assessments.

00:16:01.550 --> 00:16:08.560

And also for this very same reason we needed to look closer at the periodicity of ongoing monitoring.

00:16:09.920 --> 00:16:14.950

And monitoring of the of the program and monitoring specifically of security controls.

00:16:17.120 --> 00:16:18.640

Next slide, please.

00:16:20.960 --> 00:16:48.450

So now I'm going to go into each section of the document where we made changes. I'm giving an overview of that, but obviously I'm not going to go line by line but I'm going to go on the specific sections. The first section was Section C.3 in establishing and implementing a cybersecurity program where we added content about risk informed cybersecurity.

00:16:51.090 --> 00:17:01.690

To do risk informed type of security of cyber security plans should characterize the facility functions.

00:17:10.300 --> 00:17:27.860

A plan should also characterize the threats to the facility and this is especially important going forward where the new applicants and the plants that are coming forward may not face the same threats that we see today in the currently current currently operating fleets.

00:17:30.020 --> 00:17:52.410

To the plans just these specify the requirements, including obviously, the cybersecurity plan itself. The defensive architecture, and the defense in depth methodology.

00:17:55.120 --> 00:18:01.050

There should be a discussion that the implementation of the requirements based on consequence analysis.

00:18:02.010 --> 00:18:10.070

And also there should be information about validation and verification of the implementation of the cybersecurity program.

00:18:16.110 --> 00:18:17.060

This slide talks about balance of plant, which was not in the original guidance.

So there was new text as I said added for that.

00:18:31.130 --> 00:18:31.470

NEI is issuing a new version of NEI 10-04, which will give more information about balance of plant information and it's going to be cited in the revision of RG 5.71.

Next slide please.

00:19:23.140 --> 00:19:27.300

This slide, which talks about the identification of critical digital assets.

00:19:28.760 --> 00:19:30.280

We have the more diamonds here.

00:19:31.020 --> 00:19:35.000

And the reason we added more diamonds is because the identification of critical digital assets is, is obviously very important, but it's also important for licensees to understand that attackers don't look at what's labeled as a critical digital asset. They look at the functions that are performed by a digital asset, so it's very important when we're identifying critical digital assets that you look at it from the attackers point of view. What does the device do?

00:20:15.000 --> 00:20:24.520

Just identifying the devices that protect other critical digital asset and whether the pathways that have been analyzed for this - so it is really important to understand that calling something a critical digital asset is very important because it is in a way a bookkeeping exercise because it lets people who maintain the equipment and protect the equipment to do things in the consistent manner.

00:20:44.420 --> 00:21:06.950

When you apply controls, you'll do it in a consistent manner based on whether it's you know how you define the asset. But at the end of the day, the attacker doesn't use this CDA labeling information. They

attack based on what the device is doing and what is protecting and when you identify critical digital assets it's very important to keep that in mind.

Next slide.

00:21:14.030 --> 00:21:18.330

We updated information about defense and depth protective strategies.

00:21:19.020 --> 00:21:19.590

The defensive strategy includes defense in depth is the strategy that employs multiple diverse and mutually supported tools technologies and processes that will be needed to perform timely detection for protection against and response to a cyber attack.

00:21:42.770 --> 00:21:45.180

If you look at the cyber security rule it talks about detecting, responding to and recovering from a cyber security attack. So the defense in depth protective strategies will do that. But in the in our guidance also talks about how to use multiple the various mutual supporting tools, technologies and processes to do that. And we give examples of this throughout the guidance. Next slide, please.

00:22:22.060 --> 00:22:24.800

In this section about defensive security levels.

00:22:25.670 --> 00:22:26.920

We discuss allocating the devices that perform functions at the appropriate security level, so it's commensurate with their safety or security significance and you allocate that to their appropriate security level.

00:22:47.720 --> 00:22:57.370

The function may an SSEP function may be performed by one of the most critical systems and they allocated are allocation of the systems of to a security level is determined based on the highest function, the function that has the highest level.

00:23:06.380 --> 00:23:06.910

So it is very important to make sure that you're protecting that function at their appropriate security level.

00:23:16.960 --> 00:23:17.890

Next slide please.

00:23:23.650 --> 00:23:42.480

One of the lessons learned from the vulnerability updates is that when we said that well. I just said about protecting things on the appropriate security level when vulnerability updates are initially received obviously they aren't received at the same level that the asset that you're protecting.

00:23:44.080 --> 00:23:53.530

So when they we have defensive architecture that goes from a lower level to a higher level and you're restricting communication from the lower level to the higher level.

00:23:55.070 --> 00:24:07.240

That should stay in place, but because you have to do vulnerability updates. You may have to have a denial, but permit by exception and the exception is forming the bulk phoner ability to the update.

00:24:08.060 --> 00:24:11.140

OK and if whenever they are exceptions.

00:24:11.990 --> 00:24:20.810

To sending things from a lower level to a higher level, it has to be supported by complete justification and security risk analysis.

00:24:22.700 --> 00:24:23.660

Next slide please.

00:24:27.720 --> 00:24:29.370

This is really one of the newer sections in the document. it's very significant about minimizing attack surfaces and pathways.

00:24:41.330 --> 00:24:42.620

A lot of times when everyone talk about cybersecurity controls they try to get the top 20 controls or the top 10 controls.

00:24:51.950 --> 00:24:53.960

What should be among all of them?

00:24:55.260 --> 00:25:14.650

Any kind of grouping that you do with the top controls should be controls to control that will minimize and attack surface of pathway – such as least functionality hardening the device - because there are benefits for maintaining the program and maintaining the protections by doing that.

00:25:16.380 --> 00:25:20.410

Application services and protocols that are not necessary to support.

00:25:21.050 --> 00:25:24.310

The functions that that CDA is performing should be eliminated.

00:25:25.950 --> 00:25:31.320

And implementation of multiple diverse technologies used within the plant should address the attack surfaces and environments associated with the technology so that the protections of the defensive architecture are not bypassed.

00:26:07.850 --> 00:26:22.600

In the system and the creases that ability of the license fee to identify normal communication and and activities. It's really hard to identify anomalies if you have a lot of noise. A lot of things going on that you don't need to monitor.

00:26:23.980 --> 00:26:26.150

And reducing the attack surface helps with the effort of vulnerability management. You don't have to look and see if something has a vulnerability if it's not on your network if you don't need it and it's not on there.

00:26:40.520 --> 00:26:45.990

So it really is a significant security control that should be implemented consistently.

00:26:47.090 --> 00:26:48.080

Next slide please.

00:26:57.200 --> 00:27:01.530

We added a new uh some new text that whenever update this made, especially with something that's updated behind the data diode, it has to be ensured that the update does not the pathway that you're using what doesn't contain malware and that the integrity of the update is maintained during the transport when you're doing the vulnerability update. This change was added due to a presentation to and the comments from the NRC Advisory Committee on Reactive Safeguards.

00:27:37.090 --> 00:27:50.350

It was always implied in the guidance, but we explicitly put that in because they wanted to make sure that the protection behind the diet data diode was maintained during vulnerability management updates.

00:27:51.820 --> 00:27:52.750

Next slide please.

00:27:57.290 --> 00:28:01.440

We added some information to the use of alternate controls.

00:28:02.450 --> 00:28:20.500

And one of the main things that we added was that for the security objectives. For every control that we have in Appendices B&C were given the why these security controls were there? What was the intent of the control?

00:28:21.960 --> 00:28:42.240

And if a security control can not be implemented and alternate controls or used, what kind of security measures are used. Those measures should provide at least an equivalent level of protection against threat or attack vectors and the weak and vulnerabilities or weaknesses.

00:28:43.640 --> 00:28:49.500

So if an alternate is used, it has to provide at least the same level of protection of the control that is being replaced.

00:28:55.020 --> 00:28:56.390

Next slide please.

00:28:58.940 --> 00:29:00.930

Consequence based graded approach.

00:29:01.750 --> 00:29:07.980

This was always in the document, but we added more text to clarify this topic.

00:29:08.860 --> 00:29:20.780

When we talked about the defensive architecture and how you protect the more consequential assets at the higher level, the text was always there in the original RG 5.71.

00:29:21.710 --> 00:29:22.240

So the analysis done to support consequence based greater approach should be rigorous and repeatable so that could be. An example of this would be in NEI 13-10, which was generated after both NEI 08-09 and NRC Reg Guide 5.71 were released. Within the last 10 years that it was deemed an acceptable for implementing a cyber security plan using a consequence based great greater approach.

00:30:02.740 --> 00:30:03.580

Next slide please.

00:30:09.260 --> 00:30:12.080

Technical security controls.

00:30:14.460 --> 00:30:22.850

Quite often in many operating plants alternated controls are usually used for technical controls because of the age of and limited digital functionality in the equipment in the plants.

But as we introduce more digital equipment in existing plants because the newer plants will have a lot more digital equipment. It's really important that there's a dialogue going on with the vendors and the applicants or licensees early in the process so that technical controls can be implemented in the device.

00:31:09.820 --> 00:31:12.190

Like I said in the current operating fleet, there are a lot of controls that cannot be implemented because the devices are older.

00:31:17.810 --> 00:31:20.300

But in the newer devices that are coming along that will that probably won't be the case that a lot of vendors are looking at how to provide security in their devices that it won't be just added on at the end after the device has been bought.

00:31:34.330 --> 00:31:38.460

So the section that's been updated in the technical security controls in this section C.3.3.1 in the staff guidance.

00:31:48.510 --> 00:31:59.740

It says that the applicants for design certification may incorporate technical security controls as a part of it of the nuclear power reactor, have discussions with the vendors early, get these security controls that you need and then use those controls as a part of your cybersecurity plan.

00:32:14.080 --> 00:32:25.210

Because we foresee more technical controls being used in the future, we added more guidance to section C.3.3.1.

00:32:26.280 --> 00:32:36.600

In sections C.3.3.1.1 to C.3.3.1.5 we discuss more about why technical controls are needed for access

control, audit and accountability, system communications protection, identification and authentication, and system hardening.

00:32:45.810 --> 00:32:53.120

We really went to more detail about why these controls are need into the purpose of them so that when you have the discussions with the vendors there will be more helpful guidance.

00:32:58.270 --> 00:32:59.320

Next slide please.

00:33:03.680 --> 00:33:29.420

For incident response we updated for guidance based on the new rule that was added for cybersecurity event notification and their associated guidance with that. In addition, we updated references to incident response documents that we had from this and from DHS cybersecurity and infrastructure Security Agency.

00:33:31.060 --> 00:33:31.920

Next slide please.

00:33:36.360 --> 00:33:39.900

Section C.3.3.3.1 referenced Section2.1 through Section2.5 of NRC RG1.152, Rev.3 - Criteria for use of Computers in safety systems of nuclear power plants.

00:34:05.030 --> 00:34:10.820

In that document, we cited sections 2.1 through 2.5 specifically, because of applicability to the supply chain and when you can have discussions with vendors for the concepts phase, requirements phase, design, implementation. and test phase of a product development.

00:34:30.930 --> 00:34:39.210

It is very important to get have these discussions early with vendors because that would allow these technical controls to be added to their products.

00:34:42.870 --> 00:34:43.890

Next slide please.

00:34:47.390 --> 00:34:51.240

As I said, now we've gone through 2 rounds of inspections with licensees.

00:34:52.060 --> 00:34:52.630

So.

00:34:54.060 --> 00:34:57.230

Continuous monitoring and assessments, we added more information there, we gave additional examples of what we saw as continuous monitoring.

00:35:05.440 --> 00:35:13.110

Which are here continuous monitoring of inbound and outbound network traffic and analysis of an event logs?

00:35:14.180 --> 00:35:20.350

Periodic vulnerability scans and assessments ongoing verification.

00:35:21.230 --> 00:35:33.910

Using established baseline configurations of CDAs that are being protected that commiserate with the safety and the safety and security significance So what we're saying here is CDAs that are considered higher value assets that are protecting critical safety and security functions.

00:35:49.000 --> 00:36:19.150

Those you should have more ongoing verification of the baselines is very important to understand have a current view of the configuration of those devices because one of the things we see in cyber attacks is when they modify the configuration of something you really want to know that when that occurs or if someone is attempting to do that. And we expanded text to discuss the importance of anomaly detection. We really didn't talk very much about that in the original version, so we had some more text on that also.

00:36:23.480 --> 00:36:24.420

Next slide please.

00:36:29.830 --> 00:36:35.530

For effective in that analysis of security controls we, we updated some of the texts we.

00:36:36.330 --> 00:36:47.100

Mentioned in there that you could there's a lot among the ways that this could be done is to do performance testing modeling and also to have cyber security metrics.

00:36:48.150 --> 00:37:01.570

So as information for an option of using cyber security metrics. We added more information about that? What is being measured? Why it's being measured and what do the metrics mean we gain more guidance on that.

00:37:02.480 --> 00:37:03.040

The information that we put in for the metrics do a better job of tying the specific protections of the measurements that you have to do already for auditing to understanding the the effectiveness of your controls and your plan.

00:37:27.370 --> 00:37:28.390

Next slide please.

00:37:32.120 --> 00:37:32.850

I put this slide in here to show asset management is critical to the licensees programs is and how you have insight to the asset procurement and identification process.

00:38:11.650 --> 00:38:21.410

How you maintain securely maintain the asset? How this fits in with the procedures of plans you have at the plant and how to do vulnerability assessments?

00:38:22.410 --> 00:38:25.050

All of this plays into asset management and it is important to do all of these things to have an accurate view of the security posture of your plant.

00:38:34.540 --> 00:38:38.370

00:38:41.350 --> 00:38:55.750

It has to be a current view, not something that was done months ago, a years ago, depending on the how important those assets. Do you really not want to have a current view because if someone 's attacking your network. They most likely have a current view.

00:38:57.540 --> 00:38:58.520

Next slide please.

00:39:02.560 --> 00:39:10.240

As I said, before we updated the security controls in Appendices B&C to add the intent of every control.

00:39:13.410 --> 00:39:19.570

We added text regarding reducing or eliminating a tax surfaces and attack pathways.

00:39:20.600 --> 00:39:29.590

And we made sure that the new text any text. We had in there align with new versions. The new latest version of NIST SP 800-53.

00:39:33.550 --> 00:39:34.470

Next slide please.

00:39:37.640 --> 00:39:42.790

I've shown this slide previously while go over it one more time because I wanted to clarify again. In changing removing or adding controls we did not add any controls at all in the guidance OK but we did remove a few.

00:40:01.430 --> 00:40:15.030

We didn't that change the numbering because if a licensee or someone was using automated tools to maintain the view of other controls what we're in there, renumbering would affect the automated tools.

00:40:15.100 --> 00:40:22.320

So when we delete a control the numbering of the of the remaining controls remain the same.

00:40:23.330 --> 00:40:24.960

So we felt that.

00:40:27.190 --> 00:40:44.550

Previous log on notification and uh supervisory supervision and review of asset control. Those are covered by other controls. We already had in there and the same thing for automatic automated labeling OK resource priority.

00:40:45.470 --> 00:40:49.600

That would be done probably more through the safety requirements.

00:40:50.160 --> 00:40:54.670

If that was done it will also be done during the design phase of the device.

00:40:56.620 --> 00:41:11.700

For the control for Thin Nodes we took out because we felt it would be covered in removal of

unnecessary services and programs. There were 2 controls that were removed in NEI 08-09 that remain in Reg Guide 571.

00:41:15.940 --> 00:41:16.610

We keeping the control for heterogeneity and diversity because if you really need to look at both of those issues, based on safety and security context and there may be a trade off.

00:41:32.140 --> 00:41:42.190

But we didn't want to remove that completely it's really important just because you're doing, it for safety. You must look at it from the security context off so, so that's why it's still there.

00:41:43.560 --> 00:41:50.530

And there was there's a control that we have in for a device to fail in a known state. NEI 08-09 made it to fail in a safe state, but failing in a safe state is different from failing in the secure state.

00:42:01.960 --> 00:42:17.990

So it's important to know when a device fails, with a known state with the state of that device is from a security and the safety perspective because unless you know that you can't recover which is part of the cybersecurity role.

00:42:25.290 --> 00:42:36.390

For Supply chain, we removed a lot of the prescriptive guidance that we had, and we added text to evaluate the attack surface and attack pathways.

00:42:37.690 --> 00:42:49.840

We had numerous changes to the glossary we had a lot of changes for references and from the different round of reviews. We've had on the document. We've had numerous editorial changes also.

00:42:51.850 --> 00:42:52.910

Next slide please.

00:42:57.010 --> 00:43:00.720

So I'm going to talk to a few slides about the next steps for this guidance.

00:43:01.690 --> 00:43:02.600

Next slide please.

00:43:05.450 --> 00:43:10.380

As I said, this when the process began in 2016.

00:43:13.990 --> 00:43:19.460

We've made it right now, we are in the 2nd public comment period, which is going to end very soon.

00:43:20.160 --> 00:43:24.950

And next slide, please will be working on this guidance once we get the comments.

00:43:25.860 --> 00:43:26.400

For probably almost 9 months, not just making updated based on the comments but having internal reviews. The goal is to publish revision 1 of the Reg Guide in the first quarter of 2023.

00:43:50.620 --> 00:43:54.330

I think the next one should be the last almost the last the last slide the conclusion.

00:43:55.660 --> 00:44:00.950

I'm going to restate right now, the key messages that hopefully people would take away from this presentation.

00:44:01.650 --> 00:44:16.140

That since 2012 licensees have implemented their cyber security programs and the NRC has implemented effective oversight of those cybersecurity programs.

00:44:17.370 --> 00:44:31.700

We have no changes in the staff 's position on the guidance that we've been generating only clarifications and one new NRC regulation that was see if 10 CFR 73.77.

00:44:35.080 --> 00:44:42.030

The attackers and with the techniques. They used they have changed since the original version of RG 5.71.

00:44:46.000 --> 00:44:46.790

We have learned a lot of lessons from the inspections and the implementation of licensees programs and we documented in this in this guidance and we're preparing this document to reflect the those lessons learned and to prepare for the future so that future life applicants and licensees can use this document they will be more relevant.

00:45:13.410 --> 00:45:17.580

One of the things that I was you preparing some of these presentations. I saw where The Department of

Energy and DHS were citing that interim the early version of our draft guidance in several of their presentations.

00:45:30.850 --> 00:45:39.600

So it's very important for us to get this document finalized so people can actually use the latest version of it.

00:45:41.810 --> 00:45:47.300

I would like to strongly encourage comment written comments to this document.

00:45:49.070 --> 00:45:51.110

The original version of RG 5.71 talked about what the licensee needed to do to implement the cyber cyber security regulation. The revision of the Reg Guide 5.71 goes into more detail about why these things should be done.

00:46:09.040 --> 00:46:14.640

Please if you're going to provide comments go to regulations.gov.

00:46:15.670 --> 00:46:29.220

Search for NRC-2021-0145. That's the docket number for this Reg Guide and then your search results you'll see.

00:46:30.780 --> 00:46:49.890

A notice for this, this Reg Guide cybersecurity programs for nuclear power reactors. You and there's a button there to Click to say uh comment OK and that will put your comment officially in in the system.

Comments are due by May second.

00:47:07.810 --> 00:47:27.550

Next slide is questions so if you have questions on the presentation. We'll take some more questions at the very end about things in general. If you have any questions, but if there was something in the presentation that you had a question please. Raise your hand. Let us know. And we'll answer those questions.

00:47:32.940 --> 00:47:33.650

On the bridge.

00:47:34.780 --> 00:47:35.180

You can have.

00:47:38.680 --> 00:47:39.950

Or is it that's going on right now.

00:47:41.790 --> 00:47:42.880

Plus, a couple so.

00:47:45.780 --> 00:47:46.600

You wanna go to?

00:47:47.360 --> 00:47:49.250

OK, so rich.

00:47:50.080 --> 00:47:51.770

Which you can then mute yourself?

00:47:52.620 --> 00:48:08.660

Thank you. Kim I may have some additional questions at the end, but specifically related to the presentation so good morning. My name is rich McGovern from nuclear Energy Institute. I'm senior project manager and Kim. Thank you again for the very detailed insightful presentation today.

00:48:09.200 --> 00:48:40.030

You know one thing I heard you say uh that this you know, although this guys applicable power reactors. There's other statements that you made that it may be used as a resource for power reactor. Applicants also licenses during design development of digital safety systems. It almost implies that the guidance can be used by advanced reactors without truly providing that guidance with the technologies that might be in mind for some of those technologies or or advanced reactor types did the interoc intend on setting up an expectation that.

00:48:40.100 --> 00:48:46.190

Advanced reactors need to meet this guidance.

00:48:49.020 --> 00:48:49.990

So my question was did the NRC intend on setting up an expectation that advanced reactors need to meet this guidance as well as it likely can be very burdensome that's my question can thanks.

00:49:02.410 --> 00:49:15.390

OK, thank you. My colleague Juris Jauntirans will answer that question specifically on the advanced reactors.

Hi Rich, I am Juris Jauntirans with the cybersecurity branch and rich thanks for the question.

00:49:16.060 --> 00:49:30.810

There is a guidance that's being developed. In addition to the part 53 rulemaking process and that if you if you choose to use uh you know as was discussed several times during the part for the process.

00:49:31.310 --> 00:49:53.750

Industry asked if a 10 CFR 73.54 based framework would be appropriate for future commercial reactor licensees and at that So what we have done and you may have seen the second iteration of the part 53 rule and that states that you know future commercial reactor licensees can develop a cyber security program.

00:49:57.860 --> 00:49:59.230

You're as he went back to mute.

00:50:08.300 --> 00:50:09.570

Can you hear me Rich?

00:50:10.400 --> 00:50:19.090

Now I can OK, yeah, I know where I got cut off, but uh in the second iteration. The public rule based on comments that we received from industry.

00:50:19.880 --> 00:50:29.110

A future commercial reactor licensee can use either 10 CFR 73.54 framework or the proposed 73.110 framework in order to set up their cybersecurity program.

00:50:33.900 --> 00:50:45.600

If they choose to use a 73.54 framework, then Reg Guide 5.71 would be applicable if they choose to go that way. The 73.110. It will be the new reg guide that we are currently drafting at this point does that answer your question.

00:50:47.790 --> 00:50:48.620

Yes, thank you.

00:50:53.550 --> 00:50:56.690

Brad Yeates, you have question?

00:50:58.390 --> 00:50:59.390

Yes. Can you hear me?

00:51:00.790 --> 00:51:05.690

Yes, we can hear you OK well thank you. Kim appreciate your presentation.

00:51:06.710 --> 00:51:09.890

I wanted a little more clarification about.

00:51:11.850 --> 00:51:22.230

Allowing communications from lower to higher security levels to support normal ability updates at this in action and that kind of thing.

00:51:24.740 --> 00:51:25.670

Are you saying that uh we would allow a bypass to evade the diode to support the vulnerability updates?

00:51:45.140 --> 00:51:49.800

If you're going if when you're receiving any vulnerability update from a vendor.

00:51:50.450 --> 00:52:08.300

If that suppose you're sure, it's not a bypass because if you're select. Let's put it like this, if you receive a vulnerability update from a vendor. It's not at level of the highest level already of your unless you had a direct tie to that vendor and they had a very high security facility.

00:52:09.420 --> 00:52:17.060

You have to take it from a lower level, with your call it 012. Whatever from the fleet is a lower level than probably what?

00:52:17.740 --> 00:52:33.840

Protect the behind the data diode so we've come up there's already established in SFQ guidance from NEI on how to do vulnerability updates from a lower to a higher level. That's been accepted by the NRC.

00:52:34.560 --> 00:52:36.110

That we agree with that process.

00:52:37.260 --> 00:52:53.120

So we're not talking about uh wired connection that would allow that to come in; that is absolutely not. What we're talking about so we're talking about possibly using alternate methods. Just like we you do on other things when you have multiple diverse ways on how you do something if you're going to have

an update you won't be doing it with a wired connection. You could do something with physical security and portable media for instance. That's an acceptable way of doing it, but not with a wired connection.

00:53:12.770 --> 00:53:22.870

Is that clarifying that a little bit and? And like I said there's a there's the guidance that's already given out by NEI regarding software updates.

00:53:23.840 --> 00:53:24.240

OK.

00:53:27.000 --> 00:53:28.830

Did you did, you have something else in mind?

00:53:31.110 --> 00:53:31.960

I just wanted to.

00:53:33.070 --> 00:53:33.960

It wasn't clear to me what you were saying there.

00:53:40.130 --> 00:53:47.250

It fits spawned another question in my mind that this is a challenge is that the industry is facing today.

00:53:52.790 --> 00:53:57.170

Inquire some sort of an online verification or software licenses and Able to Activate the software license in an isolated environment is becoming the increasingly difficult.

00:54:20.730 --> 00:54:21.750

So there is a need to have some temporarily connections to be able to support that functionality.

00:54:30.510 --> 00:54:36.820

Serious if you have considered that and you could provide some additional guidance.

00:54:38.950 --> 00:54:42.650

It's about you know what we would find acceptable to that.

00:54:44.990 --> 00:55:04.920

As we typically say during most public meetings that we aren't going decide policy if the meeting, but I

understand the concern. We can have future discussions with industry. But we obviously aren't going to make that decision here.

00:55:05.680 --> 00:55:07.700

No, I'm not asking you to make a decision.

00:55:08.600 --> 00:55:16.330

00:56:31.180 --> 00:56:34.210

Comments right now that the.

00:56:42.480 --> 00:56:49.250

I think one thing that we would like to make clear at least I would like to make clear as far as the what information we have in this guidance.

00:56:52.000 --> 00:57:00.570

It is a lot of the information. We've gathered over the last 10 years and what we could see going forward. There will never be a finished document.

00:57:01.210 --> 00:57:06.230

OK, I can see another version. NIST generates revisions of NIST SP 800-53 every 2 to 3 years. OK this document. We waited quite a long time to regenerate because of the different inspections. But going forward I don't see such a long period between versions of the documents. I'm not saying what it will be, but I think it's quite unlikely it will be 10 years 12 years.

00:57:36.860 --> 00:57:45.290

Anything that we possibly won't have in this document doesn't mean it won't show up in the next version, so please go on and add your comments.

00:57:52.310 --> 00:57:52.600

Sure.

00:57:54.110 --> 00:57:55.560

I agree OK.

00:57:57.550 --> 00:58:19.520

A colleague just mentioned that which I agree normally every 5 years. Every 5 years. Keeping generally

the guidance revised or at least and looked at to see whether revision is needed. I can almost guarantee for cyber the way they attackers. So our operating it will probably have a reason to update the guidance within every 5 years.

00:58:25.140 --> 00:58:27.590

Bill Gross you have your hand raised.

00:58:30.440 --> 00:58:36.010

Yeah, thanks I so slide related questions. I have 21 on slide 14.

00:58:37.620 --> 00:58:43.750

Slide 14, you were, We refer and it just took a note. I don't have the slide in front of me about threats to the facility.

00:58:45.350 --> 00:58:58.330

And I guess this as your remarks indicated that the licensee could kind of consider threats to the facility. I think maybe in the process of implementing cyber security controls. I wonder if you could elaborate on that a little bit and then I probably have a follow up based on that.

00:58:59.290 --> 00:59:03.250

OK, like I said, we're keeping this not just in mind for the current operating fleet, but future applicants and licensees where the threat environment for them because of what they're doing, and the type of facility that they're building and the protections they have in place physical protections will be different for than what we currently have for the operating fleet so that is what it was really made that why that statement was really there about looking at the threat environment for the facility.

00:59:39.220 --> 00:59:50.080

So is it your intent that licensees would be able to tailor their operating power reactor cyber security plan based on what they believe the threat is.

00:59:54.910 --> 00:59:59.480

I'm saying that the facility threats based on how they build it is going to be different.

01:00:00.470 --> 01:00:06.870

The light water reactors for the different types of advanced reactors, you're using so.

01:00:09.170 --> 01:00:20.070

That's information that will be and obviously that's going to be discussed. When the NRC is having dialogues with them too. But it isn't going be a one type of model for threats to the facility. I think

because we're going be seeing so many different types of facilities. Alright I can. I understand where you're coming from. I think you know since this guidance appears to be tailored for large light water reactors. I think it's probably reasonable to at least include a reference to NRC regulatory guide 5.69, which provides the adversary characteristics.

01:00:44.850 --> 01:00:56.420

Umm and you know, I would encourage the NRC if they believe that the characterization of the cyber threat in regard 5.69 is not adequate that that's that that's the place that that should be adjudicated.

01:01:00.320 --> 01:01:07.140

I understand your comment. Thank you then I as a second comment on slide 20.

01:01:08.400 --> 01:01:12.060

Use this expression multiple and diverse.

01:01:12.620 --> 01:01:32.300

These terms don't appear in current reg guide 5.69 and they are 5.71. They also don't appear in the in the world. I wonder if you could kind of elaborate on your expectations with respect to you know your protective strategy in cyber security controls and this the terms multiple and diverse.

01:01:33.630 --> 01:01:33.870

OK.

01:01:35.440 --> 01:01:47.570

OK, I know we gave us and the actual guidance specifically where I talk about the different types of security controls. I I gave it. We gave examples of what we meant by that, then for instance.

01:01:49.460 --> 01:01:57.670

There are cases where you have to do malware protection, but you also have to do vulnerability updates.

01:01:58.060 --> 01:02:10.220

You might have technology to monitor changes in your baseline, which you configuration is so my point is there are different ways of protecting.

01:02:11.250 --> 01:02:13.140

The asset and sometimes we've had comments that well if we did. One thing we don't have to do the other. But when the intent of the control is really looking at something very specific for the type of attacks we've seen.

01:02:29.760 --> 01:02:37.230

We wanted the licensees to be cognizant of that that when you're looking at.

01:02:39.690 --> 01:02:45.420

Saying and the control is not applicable or they don't need to implement it. It's really going be based on what the control what the function is and what you're trying to and the configuration of the device itself and then how you're trying to protect it and.

01:02:58.780 --> 01:03:08.730

OK, so that's why we added the intent to the control there, which is I think it makes it very clear what we mean when we say multiple it'll make it more clear what we mean when we say multiple protections because sometimes if you're looking at a physical protection.

01:03:16.610 --> 01:03:23.200

And you take credit for that which is usually fine, especially for lower for assets, which don't have a lot of functionality.

You may not have a lot of the controls that you can implement.

01:03:32.690 --> 01:03:43.570

There are technical controls that you can't that can be implemented that will give you more insight or granularity of to what's going on with that box with that device that you're protecting.

01:03:44.530 --> 01:03:48.560

It would be good to have that insight for situational awareness.

01:03:49.500 --> 01:04:00.700

So as I said in the in the actual guidance. I know we give examples of controls that are complementary that you know they they don't look at the same thing, but they?

01:04:01.420 --> 01:04:17.940

Do it in the they perform it all, an overall view of the box and we want to make sure that people understand that it's just because you do one control or 2 controls. Whatever they may be to look at the intent of the controls that they is that area covered.

01:04:18.620 --> 01:04:21.700

For protecting a device.

01:04:22.480 --> 01:04:37.440

It really is on a case by case basis. You have to look if you're looking at all. The controls you really need for like a direct CDA and you're looking at all the controls that to look at the intent of the control because as I said.

01:04:38.870 --> 01:04:41.880

Some attacks you won't have insight of visibility to the attack because the alternate may not capture the control.

01:04:49.330 --> 01:04:58.240

You know that was being used and substituted am I correct I can. Uh you are uh trying to expand the definition provided in the uh defense in depth.

01:04:59.160 --> 01:05:04.490

And Reg Guide 5.71 does talk about the multiple level of security and methods deployed to guard against the failure or one component or you know, so that was in the in the in the original too. Right so that's why I said, We're expanding on the clarifying with within the original document.

01:05:27.280 --> 01:05:29.530

Well, you have mute, yeah, OK.

01:05:34.080 --> 01:05:35.090

Build everything else.

01:05:37.240 --> 01:05:40.720

No, I'm trying to lower my hand and having a hard time with that. Thank you.

01:05:42.120 --> 01:05:43.950

OK uh rich was next.

01:05:50.220 --> 01:06:09.180

Rich Mogavero. Just a general comment came at a high level. It's sort of appears that the guidance is is becoming a little bit more prescriptive and less performance based which is a trend. We really don't want to go in that direction.

01:06:09.660 --> 01:06:40.370

We've seen in the NRC IP 7113010 cyber security inspection procedure as an example. Part of what you were just talking about with this. The control control intent is a is an example of sort of looking at so I

want to segue into there so with the revised guidance, adding that word in control intent to each of the Appendix B and see operational management cyber security controls there are some concerns.

01:06:40.460 --> 01:07:11.280

This added wording will create uh some inspection concerns and maybe unnecessary burden during inspections where the licensee program documents and procedures may not have? What the inspectors may be looking for in terms of control intent because it seems new recognizing that, Red Guy 571 is one way to implement the cyber security program. What should licensees expect with the new wording being added to The Reg guide such as control intent.

01:07:15.660 --> 01:07:19.090

On the current inspections, we actually have.

01:07:22.680 --> 01:07:29.150

Question some implementations of controls or alternates based on the fact that.

01:07:31.680 --> 01:07:35.990

Whether the whether the overall protection was adequate because.

01:07:37.200 --> 01:07:40.950

Alternate controls were used that didn't meet the intent of the original controls, which is why we added that for the clarification. So we, we really, and a really if you look at even in NIST documents, they have intent. You know of the objective of the control, so this is not something new in computer security at all, and like I said it was more of a clarification in order to do an alternate?

01:08:12.210 --> 01:08:21.780

And you're saying, You're taking the alternate for control. You almost need to know why the control is there, you do need to know that to do it adequate alternate.

01:08:22.840 --> 01:08:33.490

So it is as far as being prescriptive like I said, We're far from our perspective we're providing clarification if someone can make the case that what they did was adequate based on the functionality of the device that's performing the SSP function.

01:08:47.450 --> 01:08:49.090

And attack surface and the attack pathway that that's what we're going for here.

01:08:57.300 --> 01:09:18.650

As we keep saying the Reg Guide is just one way to implement a cybersecurity plan OK. We wanted

when especially for new applicants and licensees when they come along to look at why they're doing something and why they apply control. This guidance will tell you what the control is meant to do.

01:09:19.370 --> 01:09:44.280

OK, because I know on my original inspections really as an observer when I as a computer scientist when I would go on an early inspections and I would see protections apply to certain devices. My first question is why did you pick that control? Why is that control on this device based on what it's doing it's a very basic question and so like I said, We're providing clarification.

01:09:45.070 --> 01:09:57.590

Of the controls that we have in Reg Guide 5.71. If you look in this documents. They talk about the objective of their security controls so this is not really a new prescriptive way of doing something is saying.

01:10:01.300 --> 01:10:02.840

It is clarifying why you're doing something.

01:10:03.750 --> 01:10:06.960

And so everyone could have a general agreement about that.

01:10:13.550 --> 01:10:24.720

We still welcome your comment and please put it in writing, but it really isn't saying, you have to do the security control. But if you're taking an alternate to the security control. This is why this control is there.

01:10:26.700 --> 01:10:27.800

Understood thanks Kim.

01:10:32.030 --> 01:10:34.980

Yeah, hello. This is Margaret Ellenson, I'm with Kairos power. I wanted to. Thank you for having this conversation today and walking us. Through this DG 5061. I appreciate the conversation. I was thinking of this and I thought I would chime in from the perspective of an advanced reactor developer.

01:10:57.890 --> 01:11:03.120

One of the things that came to mind as I was listening to the presentation and walking through the guidance that it's unclear to me as an advanced reactor developer how I would implement this guidance.

01:11:11.460 --> 01:11:40.510

The language in the front which talks about how new applicants may consider the guidance. It's not clear about how an advanced reactor would do that specifically how an advanced reactor who is implementing the LMP process would demonstrate compliance with 73.54. It's clear that the guidance would provide one at least from my perspective. I shouldn't speak for other folks, but from my perspective. It's clear that it that the guidance.

01:11:40.590 --> 01:11:54.460

Weeks to how an existing light water reactor might be able to demonstrate compliance with 7354. But the guidance doesn't really say anything about how a new applicant using the LMP process would.

01:12:10.200 --> 01:12:36.180

So I think what we're going to be looking at how we would provide a comment on this draft guide. I appreciate the opportunity to do that. But I might encourage the NRC staff to look a little bit harder. About the guidance. That's in this draft guide and how an applicant using the LMP process would be able to demonstrate compliance.

01:12:39.670 --> 01:12:43.380

OK, thank you. Margaret this is you're Asian Trans again.

01:12:45.320 --> 01:13:15.620

Appreciate the comment we look forward that you, you know if I we, we hope you can put together a formal comment and and we look forward to seeing that. I just want to just a little bit of clarification. You know part 53? Is is currently in development and we do address specifically quote Unquote Advanced. You know reactor future commercial reactor designs in part, 53 in in regard 571 and and 7354. It's very difficult to have one rule and one red guide able to encompass all of these technologies at this time without uh going through our normal rulemaking process and everything of that nature. I think that the guidance at this point is.

01:13:28.120 --> 01:13:47.820

If you are under the 73.54 framework that you use the right guide as best you can and look for exemptions for parts that do not apply as long as there's an analysis and uh an explanation for why that exemption is being sought, then we, we believe that that's the way forward for.

01:13:49.820 --> 01:13:51.910

Future commercial reactor designs.

01:13:53.110 --> 01:13:57.960

Hmm yeah, I appreciate that and I might also comment on that.

01:13:59.210 --> 01:14:19.540

You know the part 53 rulemaking while it. It's tackling some important issues. The timeline for that rulemaking may not be consistent with what an advanced reactor developer might need so that guidance may not be an even you know, applying under that part of the rule may not be something that is timely.

01:14:21.750 --> 01:14:42.600

So in that case, it's what we're what we then uh are left with to consider is the guidance that is available out there and this is one guidance document that would be out there and when the when the guidance document makes a statement up front that says that any power reactor applicant should be consider the guidance in this Reg guide it without any further clarification in the rest of the guidance about what might be different under an LMP process. It doesn't really add any clarity to new applicants.

01:15:01.490 --> 01:15:06.190

So, but you know, I appreciate the opportunity to comment on the guide.

01:15:07.880 --> 01:15:10.370

Yes Margaret this is Jim Beardsley.

01:15:11.460 --> 01:15:34.650

I think that you going to remember a couple things that Kim said. When she started the brief so the template for a cyber security plan and regulatory guide 5.71 is a method to meet the requirements of 70 through 54. Any licensee that comes in prior to any reactor license that comes in prior to part 53 being put in place would have to meet the requirements of 73.54.

01:15:35.580 --> 01:16:05.130

So the question is how do you do that and I think the answer to your question is early engagement with the staff so we are willing to meet with licensees and talk to them about what their designs are how their designs might be different from other reactor designs and how the requirements that are in the regulatory guide may or may not apply now as yours, pointed out there may be opportunities for you know for requesting.

01:16:05.770 --> 01:16:21.330

Yeah, deviations from the requirements 73 to 54, but 7354 quite frankly is pretty high level and it's performance based and so what that cybersecurity plan looks like is something that would have to be determined as part of the licensing process.

01:16:22.100 --> 01:16:24.930

I don't know if that helps, but that's a little bit of a different viewpoint.

01:16:32.150 --> 01:16:34.510

OK, it is Dr. Lyman.

01:16:38.700 --> 01:17:07.390

Hi yes, Ed Lyman from Union of Concerned Scientists. I was actually going to make a remark. Similar Mr. Beardsley and that everything I've seen today. I don't see anything that is reactor design specific at all, and the things that are relevant to new reactors or associated with you know, incorporating security design features from the beginning, so that I think is something should be highlighted and frankly, I would like to see a more prescriptive requirement for that kind of activity to be performed for the new reactors. But I don't understand the concern that's been expressed because if the advanced reactor developer. Somehow think their designs are going to be immune to a cyber attack. I think they have something else coming thank you.

01:17:38.160 --> 01:17:44.860

OK, I don't see any other hand, raised at the moment. Somebody came up from you on the phone for a while.

01:17:45.750 --> 01:17:48.050

Is there anyone on the phone who may not be using teams want to make a comment or question about the flies.

01:18:02.670 --> 01:18:06.210

You know, but Brad Yeates, who you have one additional comment.

01:18:08.780 --> 01:18:20.490

I don't know which slide this is on uh probably here. The slide where you're showing the defensive architecture with the arrows going from the different.

01:18:22.530 --> 01:18:24.600

OK, you go to that slide.

01:18:32.220 --> 01:18:34.490

So yeah, one of the early slides, Yeah.

01:18:39.660 --> 01:18:44.550

People are more keep another one, yeah, OK yes.

01:18:45.690 --> 01:18:46.600

Oh OK.

01:18:47.840 --> 01:19:00.570

Yeah, I just misremembered what you had on that and I was looking in the guidance of using 5061 and I thought there was a mismatch between what's in the document.

01:19:23.530 --> 01:19:33.460

So we want to give NEI an opportunity to make any other comments that on that specifically tied to this, the slides, but on the on the guidance in general.

01:19:36.580 --> 01:19:38.030

Sure can this Rich Mogavero.

01:19:39.240 --> 01:19:51.180

One last one last thing is uh looking forward as the industry seeks to innovate using new uh new and innovative technology for improved safety and efficiency of operations.

01:19:51.720 --> 01:19:52.230

We're looking for the NRC to possibly consider removing the prohibition for wireless communications in terms of uh controls associated with safety related and important safety systems and essentially allow its use with appropriate cyber security controls that are in place that was my last comment. Kim and all the open, it up if Bill Gross has anything additional.

01:20:22.460 --> 01:20:31.290

Now I don't necessarily have anything additional can I you know we the NRC and the industry have been working on cyber security for the better part of a decade and a half.

01:20:32.010 --> 01:20:36.440

As you indicated a lot of lessons have been learned.

01:20:37.910 --> 01:20:39.070

One of the things that I think we see and you've talked about it during your remarks is that the cyber security threat evolves and it progresses and the types of tactics that they use change.

01:20:51.380 --> 01:20:55.830

And it begs the need for cybersecurity programs that can be flexible.

01:20:56.780 --> 01:20:59.350

And just adjust and adapt overtime.

01:21:00.220 --> 01:21:09.970

So I think Rich has comment earlier about Prescriptiveness is you know after the decade and a half of operating experience. You know, we're seeing more guidance put in this document that over the long run is going to end up with a program that is static.

01:21:18.770 --> 01:21:25.630

And licensees will evolve it just to the minimum degree necessary to comply with the requirement.

01:21:26.370 --> 01:21:30.250

And that is not necessarily the state that we want to be in.

01:21:30.480 --> 01:21:48.250

Umm to have the NRC kind of focus on having cyber security guidance. That's much more focused on identifying undesirable outcomes that have to be precluded in the context of a cyber attack.

01:21:49.460 --> 01:22:03.010

And allowing the licensees the greatest degree of latitude with how those performance criteria are met is the most desirable possible outcome. So you know when rich talks about Prescriptiveness. I think what he's referring to is.

01:22:03.960 --> 01:22:34.630

Try you know, rather than guidance that tries to answer every question try to have guidance that provides a very clear indication of the performance objectives that must be met and minimal guidance on exactly how those performance criteria should be met, so for example, you know just at a very high level. This kind of continued adherence, both in any guidance documents and the NRC documents on the cyber security controls from NIST.

01:22:36.140 --> 01:23:05.690

Is over the long term is just not kind of trying to include that much level of detail is the wrong approach right. You've got companies like Mandiant and others that just constantly doing response and recovery to cyber attacks on industrial facilities. They're putting out reports on what's working and not working you know it'd be much better to have licensees have enough latitude to make rapid changes as needed to their program based on that emergent information.

01:23:06.350 --> 01:23:14.810

Then kind of being adherent to a guidance document that nest puts together that's principally designed for IT systems and federal agencies.

01:23:15.520 --> 01:23:19.400

So you know that that's at it just at a very high level.

01:23:20.700 --> 01:23:48.190

Recognize that the staff is trying to incorporate lessons learned from a lot of operating experience and there's a balance that has to be met and I think you know you guys are kind of at the middle of that. You know it's just Bill's perspective is that we should be focused on adaptability and flexibility in the program, not trying to write a guidance document that you know can only lead to a single kind of static implementation of the cyber security program.

01:23:51.200 --> 01:23:51.530

OK.

01:23:52.680 --> 01:23:54.540

Thank you for your comments.

01:23:57.040 --> 01:23:57.560

From my perspective the guidance that's given in this draft guidance Is Comprehensive.

01:24:13.370 --> 01:24:24.590

OK, that whenever new licensees or new threats or new new attacks arise that it, it could be used to tailor the plan that's going be implemented, So what I what I really I guess I want to say is that.

01:24:36.310 --> 01:24:40.520

We don't know what we don't know, but we know what we've seen.

It is usually something that we've known about for a long time. There have been very, very few attacks that we've seen where there are exploiting a vulnerability that we had never seen before. If something totally new and there's no control for it. There's no cybersecurity control for it with something and that's one. One reason why we haven't had to add any new cybersecurity controls because the ones that we actually have a pretty comprehensive. They work pretty well. It's the implementation of things that matter.

01:25:15.130 --> 01:25:31.140

And and that's why we like I said, we mentioned the attempt of the control when applicants or licensees come with their cybersecurity plan. They should look at the controls as a toolbox. These are the things we have to protect the system.

01:25:34.580 --> 01:25:45.630

And most certainly they should not be looking for the minimal number of things in the toolbox. Because you don't know what's coming. In 5 years in 7 years or whatever, so.

01:25:46.390 --> 01:25:52.300

Just because you have a control in your plan doesn't mean it's going to be implemented every time for everything.

01:25:53.030 --> 01:26:11.080

But you do want that toolbox that contain those controls so as I said, I what we really want people to understand what was and we don't focus a lot of the guidance that we like I said the lessons learned that we put in are based on what we've seen and why certain controls.

01:26:17.970 --> 01:26:25.440

There'll be something new, but it's unlikely the solution that will be put forth would be something that we don't have here in the guidance.

01:26:27.020 --> 01:26:27.830

So Like I said, we welcome comments. We are saying that everyone must for every instance implement every control.

01:26:35.610 --> 01:26:37.760

OK, but you need to know your facility what you're protecting and why and then choose the appropriate controls. We don't do the controls based on the regulator.

01:26:49.520 --> 01:27:11.030

Because the attacker did as I said the attacker doesn't care that it's a critical digital asset. It doesn't care that the vulnerability is 20 years old, and you just implemented the plan 2 years ago, it will use the 20 year old attack that still works on the vulnerability. So my point is you. You know that's for better or worse for security.

01:27:11.810 --> 01:27:42.040

We have to have the right sufficiently sized toolbox to do things but it will be the applicants are licensees responsibility to know their facility to understand the equipment they're putting that facility that will perform a SSP functions and then have a plan that will adequately implement that the protections and that's what we're trying to give the guidance for in this document no ones going to implement I believe a complete version of 5.71.

01:27:43.410 --> 01:27:48.590

But we're going give them the information they need to implement or appropriately tailored cybersecurity plan for their facility.

01:27:52.570 --> 01:27:53.380

That is our goal.

01:27:57.360 --> 01:28:00.570

OK are there any other comments or questions?

01:28:07.450 --> 01:28:09.630

Please once again one more.

01:28:09.810 --> 01:28:11.960

With Laurie.

01:28:13.730 --> 01:28:14.390

Please speak.

01:28:17.620 --> 01:28:20.490

And identify yourself with your organization you're with please.

01:28:25.320 --> 01:28:33.720

So I had a lot of comments that are submitted, but I I just had a couple of high level ones related to document layout and a couple on definitions.

01:28:34.440 --> 01:28:59.860

I found it very confusing that the section C of the Red Guide had sections that were numbered starting with C and appendix. C also uses the same but then, when you get to the cybersecurity plan template and appendix. A It drops. The C designation when it refers back to the body of the red guide. It seems like it'd be like cleaner to just eliminate the see numbering in section C.

01:29:01.740 --> 01:29:31.210

And then also in in the template you know at the beginning of the template. It basically refers back to say you're going to do everything in section 33 of the body of the red guide. And if you go through the other sections. Sometimes it repeats the language that's in the body and sometimes it refers back to other sections and I just think that would make it very difficult to try to read through the cybersecurity plan and figure out what it's actually telling you need to do because you're going to have to always have a copy of The Reg guide with you to refer back to it just seems like it would be a lot cleaner to.

01:29:31.380 --> 01:29:37.620

Integrate all of that into the template so that the cybersecurity plan actually states everything that you're doing for your program.

01:29:43.070 --> 01:30:13.280

And then as far as definitions. I just wanted to point out a couple of things. It seemed like the definition for CDA was incomplete and doesn't really align with Alpha 313 because it would it kind of implies that any digital device in a critical system would be CDA. And when we look at our critical systems. We look at all. The functions those systems perform, and if any of those functions or SSP functions. We call it a critical system. But if you had a standalone digital device performing one of the functions.

01:30:13.400 --> 01:30:18.610

Of the system that was not an SSP function, it wouldn't necessarily need to be a CDA.

01:30:19.580 --> 01:30:48.110

And then lastly I was just going to point out that there are definitions for attack pathway and attack vector and it seems that what it's defining as attack pathway is what is defined as a threat or attack vector in the NRC approved NEI 10.04. So I just think we need to ensure we, we work through that and clarify that otherwise we could end up causing a lot of confusion and discussions between the energy and industry and what we mean that was all I had.

01:30:48.840 --> 01:30:58.500

OK, as I said, please do submit your comments formally in regulations.gov and will address each one individually.

01:30:59.510 --> 01:31:01.240

OK, thank you.

01:31:04.850 --> 01:31:06.790

Are there any other questions?

01:31:18.480 --> 01:31:24.270

First of all I want to thank Jim Beardsley.

01:31:25.090 --> 01:31:55.640

And all my teammates here at the NRC. I always say whenever we give a presentation on the cybersecurity program that it is not just one person doing it. You know that it's really a team and everyone has been incredibly supportive, giving comments giving feedback so I can't say enough about the cyber security branch. Here, the NRC. Thank you very much so and thank you to the stakeholders.

01:31:55.710 --> 01:32:02.900

Everyone who's giving us comments we look forward to addressing them to make the document useful for people who will be using in the future for the new applicants and licensees so. Thank you very much for the comments. Thank you for the feedback today and we look forward to getting all your comments.

01:32:15.490 --> 01:32:16.170

Thank you for joining us today.

01:32:19.920 --> 01:32:21.850

The meeting is adjourned.