Official Transcript of Proceedings

NUCLEAR REGULATORY COMMISSION

Title: 33rd Regulatory Information Conference
Technical Session - T9

Docket Number: (n/a)

Location: teleconference

Date: Tuesday, March 9, 2021

Work Order No.: NRC-1420 Pages 1-61

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

UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

+ + + + +

33RD REGULATORY INFORMATION CONFERENCE (RIC)

+ + + + +

TECHNICAL SESSION - T9

POWER REACTOR CYBER SECURITY:

THE PRESENT AND THE FUTURE

+ + + + +

TUESDAY,

MARCH 9, 2021

+ + + + +

The Commission met via Video Teleconference, at 10:45 a.m. EST, Jim Beardsley, Chief, Cyber Security Branch, Division of Physical and Cyber Security Policy, Office of Nuclear Security and Incident Response, presiding.

PRESENT:

JIM BEARDSLEY, Chief, Cyber Security Branch, Division of Physical and Cyber Security Policy, NSIR/NRC

PAUL SHANES, Professional Lead for Cyber Security and Superintending Inspector, United Kingdom Office of Nuclear Regulation

JUSTIN SIGETICH, Director, Systems Engineering Division, Canadiam Nuclear Safety Commission

BARRY KUEHNLE, Critical Infrastructure Protection Senior Advisor, Office of Electric Reliability, Federal Energy Regulatory Commission

DAN WARNER, IT Specialist, Cyber Security Branch, Division of Physical and Cyber Security Policy, NSIR/NRC

C-O-N-T-E-N-T-S

Introduction

Jim Beardsley.....4

Regulation of Cyber Security across the United Kingdom's Civil Nuclear Sector

Paul Shanes.....9

CNSC Cyber Security Program at Nuclear Power Plants: The Present and The Future

Justin Sigetich.....20

Barry Kuehnle.....29

Question and Answer Session.....35

P R O C E E D I N G S

10:45 a.m.

MR. BEARDSLEY: Good morning, ladies and gentlemen. Thank you for joining us for the Cyber Security 2021 RIC Session. Today's discussion is the latest in a series of RIC sessions on NRC's Cyber Security Oversight Program.

My name is Jim Beardsley, and I'm chief of the Cyber Security Branch in the NRC's Office of Nuclear Security and Incident Response. For today's session, I'll be joined by a group of international and interagency colleagues discussing the present and future of our respective cyber security oversight programs. We look forward to your questions as we proceed through the agenda.

The panel members include the following. Mr. Paul Shanes from the United Kingdom's Office of Nuclear Regulation. Paul is a professional lead for cyber security at ONR.

We had hoped to have Mr. Justin Sigetich from the Canadian Nuclear Safety Commission, but he has not been able to connect at this point. If he does, we'll add Justin to the agenda. Justin is the director of CNSC's Systems Engineering Division.

And last but not least, Mr. Barry Kuehnle from the US Federal Energy Regulatory Commission. Barry is a senior level energy infrastructure and cyber security advisor at FERC.

As we progress through the session, please feel free to enter questions into the session portal. Our team will queue up the questions for the panel following our remarks.

At this point, we'll transition into my presentation. I'll start out today's presentation with an update on the NRC's Cyber Security Oversight Program and then discuss the NRC's plans for the future of cyber security oversight at our power reactor licensees.

I'll go to Slide 1 in my presentation. If Slide 1 is up, I can't see it so -- okay, this slide shows the timeline for the power reactor cyber security program starting with Commission approval of our cyber security rule in 2009. The rule is 10 CFR 73.54.

Power reactor licensee's cyber security programs were implemented in two phases. The first phase, completed in 2012, was focused on cyber security program structure and securing the most

significant digital assets within the cyber security's infrastructure, the licensee's infrastructure.

The staff inspected those implementations from 2013 to 2015. Licensees completed the full cyber security implementation, so they went from the initial implementation to their full implementation in 2017. And the staff has been conducting inspections of the fully implemented programs for the past three years.

We've completed 53 inspections to date and are scheduled to complete the remaining five inspections in the first half of 2021. Over the course of the inspections, the staff has found, with reasonable assurance, that the licensees understand and have implemented the requirements of their cyber security programs.

In 2019 the staff conducted a self-assessment of the power reactor cyber security program. The assessment included all aspects of the program to include significant stakeholder input during multiple public meetings and other meetings with industry and internal NRC staff members.

As a result of the assessment and

feedback from the NRC Office of Inspector General Audit of the Cyber Security Inspection Program, staff developed an action plan to evaluate opportunities for program improvement in the future.

Next slide, please. The cyber action plan focuses on five high level areas as identified on this slide. In 2019 and 2020 the staff has focused our attention primarily on risk informing critical digital asset determination and also on the Cyber Security Inspection Oversight Program following full implementation. The other three elements will be addressed in the near future.

In the area of critical digital asset determination, the staff and industry initially focused on evaluation and protection on digital assets in the areas of emergency preparedness, balance of plant, as well as the evaluation of appropriate protections for safety related and important to safety systems.

During 2020 industry and staff evaluated risk informed guidance modifications for balance of plant, emergency preparedness, and the safety related, important to safety systems. Through a series of public meetings, the staff evaluated and

agreed to updated industry implementation guidance.

Today, the commercial nuclear fleet is starting to implement these revisions as part of their internal procedures. And the Nuclear Energy Institute, who maintains the guidance, is updating the overall guidance documents. Revisions are due to be submitted to the NRC staff for review and approval later this year.

The second step, oh, excuse me, the NRC staff is also working with industry at looking at updated guidance for physical security digital assets. We've conducted one public meeting and expect to provide feedback to industry on their proposed changes for guidance in that area in the near future.

In the area of inspection, the NRC staff have been developing a revision to the cyber security inspection procedure. The revision focuses on a shift from full implementation inspections which were primarily focused on verifying a wide variety of aspects of a licensee's implementation and, in detail, looking at how they have protected their digital assets.

And we intend to shift to reviewing the

ongoing program execution of the cyber security infrastructure to verify that the programs are, excuse me, to verify that their programs are being implemented in accordance with their cyber security commitments and their cyber security program.

The staff has completed a draft of the new inspection procedure, and that draft was loaded into the Agency's document management system for public viewing yesterday. We will be hosting a public meeting in early April to discuss the draft procedure, and further information on accessing the procedure will be available as part of the public meeting announcement. The staff plans to have the new procedure in place to support cyber inspections, the next stage of cyber inspections which will start in January of 2022.

This completes my remarks, and I'll turn the virtual podium over to Paul Shanes.

MR. SHANES: Thank you, Jim. Let's start by thanking everybody for the opportunity to present today and for welcoming us along to your session. It's really informative. And it's a great opportunity to collaborate. And I thought I'd start by just talking around the regulation of cyber

security and how it's actually active within the United Kingdom's Civil Nuclear Sector.

So with that in mind, firstly to introduce myself, my name is Paul Shanes. I'm the professional lead for cyber security within ONR with the UK Statute Regulator across the Civil Nuclear Sector. And I oversee the specialist inspectors who look after cyber security and information assurance across the various duty holders, as we refer to them, within our regulatory terms.

Next slide, please. If we start by just looking at the trajectory we're on in terms of signed security regulation within the UK, what you'll hopefully see there, if it's not too small on the screen, is that we've gone through quite a radical transformation of late, and particularly over the last decade or so.

Starting back in 2007, we were a quite prescriptive regulator. We set out our expectations through something called the Technical Requirements Documents. This provided guidance on appropriate security standards, procedures, and arrangements.

It wasn't intentionally prescriptive, but licensees quite often referred heavily to the

documents and the expectations contained within them. And this led us, as an industry, down the inevitable path of prescription.

Back in 2012, we attempted to move away from this and started by setting some goals and high level objectives through the national objectives requirements or model standards in the regulatory framework.

Unfortunately, these were quite tactical and directive in tone. And the conditions just simply weren't right to move away from the culture prescription which had become embedded as a result of the initial approach back in 2007.

So in 2010, in 2012 we attempted to move to something rather more radical and really tried to embrace outcome-focused regulation. We did this with a new regulatory framework known as the Security Assessment Principles.

The Security Assessment Principles are high level and principle based. We don't give out model standards or model expectations but rather place great emphasis on strategic issues that may benefit security. We set out high level objectives and we asked duty holders to articulate to us your

claims arguments and evidence approach, how they intend to meet those objectives.

Below the Security Assessment Principles, we also have a suite of documentation aimed at our inspectors, technical assessment, and technical inspection guides. And those documents really aim to provide inspectors with a consistent framework from which to reach regulatory judgements.

Next slide, please. The topic of cyber security is covered in great detail within the Security Assessment Principles. We have ten fundamental principles within our expectations, and each of them tackles a different facet of security.

Within Fundamental Principle Number 7 there are five security deliverable principle areas that we expect our duty holders to achieve. Basically, you can't see them on the screen there. They revolve around effective cyber and information risk management, the exception of information through effective information security, protection of nuclear technology and operation with physical protection of information, and the preparation for and response to cyber security incidents.

And the key shift in our transition to

the Security Assessment Principles is an emphasis that duty holders must maintain effective cyber security information assurance arrangements that integrate technical and procedural controls. So as we say on the slide there, good cyber security is not simply about good cyber security.

And what do I mean by that? If we look at the next slide, what we often find when we're going out and doing our inspections and intervention activity is that when we identify cyber security vulnerabilities and issues, they don't solely relate to tactical or technical measures. More often than not, they can be drawn back through root cause analysis to more strategic enablers and high level facets of security.

So what you can see on the screen there are the ten fundamental principles that we, as a regulator, expect of duty holder community. On the left hand side, you'll see a series of five principles listed as strategic enablers. And on the right, those that are more distinct in tone, the secure operations.

So on the right, you have physical protection, cyber security, workforce trustworthiness, sometimes referred to as vetting,

policing and guarding, and emergency preparedness and response. These are all disciplined operations where we expect certain things of our duty holders.

But on the left hand side, you will see those higher level and more strategic enabling aspects of security which, as I mentioned earlier, are quite often at the root cause of regulatory challenges that we face.

And what we found in our transition to outcome-focused regulation is, by placing a greater onus on emphasis with our duty holders on ensuring that they have absolute clarity that they are responsible for the leadership, design, and implementation of effective security, that's required a tremendous amount of upscaling and a greater understanding of the risks that they face and the ways in which they need to mitigate against that.

So rather than, historically, ONR as the regulator simply setting out our expectations for security, we're now in a position where we set out high level expectations. And we require the duty holder community to understand and really get to grips with the challenges that they face and then articulate to us how they are going to deliver against those

expectations in an effective manner.

We'll quite often find, when we do our intervention activity, that those fundamental areas around effective leadership, the culture within an organization, or the competence of the staff undertaking the activities, are the areas where we really get most benefit in terms of regulatory engagement as opposed to that's where we were before, focusing on more technical and tactical matters on the coalface.

Next slide, please. So for me, the Security Assessment Principles really take us back to basics. We have a variety of overarching key security principles that govern everything we do, whether that's cyber security, personnel security, or physical security, terms you'll be familiar with around secure (audio interference) design and appropriate use of threat intelligence information, a graded approach to the way in which we operate, categorizing and classifying information and assets in order to prioritize the protection against them, and an overarching onus upon defense in depth arrangements.

So we'd expect our duty holders within

cyber security and information assurance arrangements to do exactly the same thing and follow the exact same process they do for other assets of security.

First and foremost, we expect them to categorize their assets. They can do this in one of two ways. And there's a significant amount of guidance available, but there simply isn't the time to go into detail today.

Firstly, they can classify information that they hold in line with the UK's government security classification scale. And that will give it a classification along with any other critical infrastructure in the UK. Alternatively, if we're talking about operational technology, then information is categorized. And it's categorized as either critical, major, significant, or minor, depending upon the impact of failure.

Once you categorize assets, when we want to determine an appropriate outcome, there's a methodology we follow within our Security Assessment Principles that articulates how to do that.

And the outcome will vary depending upon the categorization of the assets. So again, really using a graded approach as to whether we require

complete confidence in the arrangements to protect and safeguard information, all the assets involved, or whether it's simply a case of identifying that something untoward has happened.

Finally, an appropriate posture will be set. And that posture will again depend on a combination of the categorization of the assets and the required outcome. And that really enables a proportions approach to the way in which we regulate.

Next slide, please. So in a non-prescriptive world, we're often asked how do we identify what good looks like. And it's a really challenging question, particularly when you've been used to a very prescriptive approach in the past.

Well, we turn to something called relevant good practice. And there are different standards of relevant good practice out there from a regulatory perspective.

There are defined standards that exist, so legislation, regulations, orders, and our overarching nuclear industry security regulations which really govern everything we do and give us the legal power to actually carry out our regulatory activity.

Those sets of good practice and expectations really hold the highest level of expectation. We even have established standards. These are typically internationally recognized codes of practices. They can be internal within our organization, so they could be our expectations within our own security and safety assessments principles. But equally, they could be expectations set out by national technical authorities or international standards organizations.

And then finally, where no such standards exist, we look to interpretive standards. And these are standards which are not published or available greatly across the flow but are examples of the performance needed to meet uncertain expectation.

And sometimes the industry will actually come together in working groups and forums to identify what it looks like, where it doesn't exist in a particular standard or arrangement.

Next slide, please. So what have we found in our time as we've transitioned from a more prescriptive to an outcome-focused approach? Well, both positive and challenging aspects, if we're honest.

In terms of benefits, we found we've got a far greater interaction now with our colleagues in safety. Our outcome-focused approach is now consistent with that that has already been in place with our very mature safety regulatory approach.

And we found that there's an enhanced senior level of understanding across the sector. It's much easier to articulate to a Board within a duty holder organization the challenges that are being faced, particularly when you've gone through a process of understanding and articulating the risk that exists.

The transfer of ownership from us as the regulator to our licensees or our duty holders has been something that's been particularly important. In a world where we set out a very prescriptive approach, we believe we carry a significant amount of risk in doing so.

The move to outcome-focused regulation really puts decision making in the hands of those that it should be invested in, which are the licensees, the operators, who should be best placed to make decisions around the adequacy of the arrangements that they have with oversight from the

process to regulator.

There's been significant amounts of upscaling and professionalization, particularly in terms of within ONR as the regulator. We've placed significant amounts of onus on ensuring that we have the right people in the right place to undertake our regulatory activity.

And it's now at a far greater level of flexibility and adaptiveness. We've been able to focus and target our regulatory activity where we perceive there to be greatest risk rather than historically where we actually just followed multi-trends across the sector and conducted the same work.

It hasn't all been perfect though. We've had a significant amount of challenges along the way. The span and complexity of the change has been significant. And we have had a culture of prescription, which has been embedded previously, which has been difficult to overcome.

It has been difficult to convey this change and the perceived benefits across the sector in an effective manner. And it has taken a fair bit of resource on engagement in order to do that but one which we feel has been justified.

Training and education's been absolutely key. I mentioned that we've upscaled our own staff, particularly around cyber security, in order to carry out effective regulation. But the journey for many of our duty holders has been ongoing and is one that we're having to support them with so that we don't end up with a complete imbalance between the regulated entities and the regulator.

And of course, as all of you will be familiar with on this call, cyber security scales remain in very short supply globally. And so it can be a real challenge to attract and maintain the right people within the organizations to drive this level of change through.

So I think I'll conclude with my remarks there on the final slide. And I'll take questions at the end during the panel session. Thank you very much for your attention. I'm now going to hand over, I believe he's joined, to Justin. Thank you.

MR. SIGETICH: Good morning, everyone. First I'd like to take the opportunity to thank you, to have the opportunity to speak today at this conference. I think this is an excellent opportunity to be able to share our experience from Canada with

you.

My name is Justin Sigetich, I'm the director of the Systems Engineering Division at the Canadian Nuclear Safety Commission, the CNSC. And I'll be talking with you this morning about the CNSC's regulation of cyber security at nuclear power plants.

Next slide, please. This slide provides an overview of the subjects I'll cover in this presentation. But instead of reviewing this, I'll jump right into it.

Next slide, please. Here's an overview of the main gate of the Canadian Nuclear Safety Commission for those of you who are not familiar with us. I will not delve into any detail here other than to state that the CNSC is Canada's nuclear regulator. And we regulate the use of nuclear energy and nuclear materials in Canada.

Next slide, please. The CNSC has a regulatory framework that provides us the legal authority to perform our regulatory work. The CNSC's regulatory framework consists of acts, regulations, licenses, and regulatory documents. Acts and regulations are passed by the Canadian Parliament and create overarching requirements for the CNSC and for

the nuclear industry.

Licenses and regulatory documents are issued by the CNSC and specify requirements and guidance for the industry and requirements and guidance for specific licensees. Please note that we refer to the organizations that operate licensed facilities as licensees.

Next slide, please. This slide outlines, in general, the relevant sections of the CNSC's regulatory framework that are applicable to cyber security. First, the general nuclear safety and control regulations require these licensees to take reasonable precautions to maintain the security of nuclear facilities and of nuclear substances.

Next, the nuclear security regulations provide requirements that are mostly specific to physical protection but have applicability to cyber security. These regulations are currently in the process of being updated to include specific cyber security requirements.

The CNSC regulatory document, REGDOC-2.5.2, which is entitled the Design of Reactor Facilities, Nuclear Power Plants, includes high level requirements and guidance for cyber security for the

design of nuclear power plants. This document applies to new reactor facilities, and it also provides guidance for existing nuclear power plants.

Finally, licenses and License Condition Handbooks, which we call LCHs, provide the most site-specific requirements and guidance to each licensee. The general purpose of these LCHs is for each licensed condition in the license to clarify the regulatory requirements by documenting specific compliance criteria and guidance.

The license condition that's applicable for cyber security for nuclear power plants is quite broad. It reads that the licensee shall implement and maintain a security program. And we interpret the phrase security program to include both a physical security program and a cyber security program. And that interpretation is clarified in each of the nuclear power plant's License Commission Handbook.

On the next slide, I'll talk about the history of the CNSC's regulation of cyber security. So we can go onto the next slide, please.

The CNSC officially began regulating cyber security in 2008. At that time, the CNSC sent a letter to all nuclear power plant licensees stating

our regulatory position and outlining our requirements and guidance for their cyber security programs.

The CNSC required all licensees to conduct a self-assessment, then develop and implement a comprehensive cyber security program. The expectations were based on international documents that were available at that time. For example, documents from the International Atomic Energy Agency, the IAEA, the Nuclear Energy Institute, and the US Nuclear Regulatory Commission were referenced. The CNSC inspections of these cyber security programs will be discussed in a future slide.

Next slide, please. In 2012, the CSA Group was asked to develop a standard on cyber security on behalf of the nuclear industry in Canada. Representatives from the CNSC, from the nuclear power plant licensees, and from other stakeholders participated in developing CSA N290.7-14 which is entitled Cyber Security for Nuclear Power Plants and Small Reactor Facilities. This document was published in 2015.

The cyber security standard covers the cyber security of new and existing nuclear power

plants and small reactor facilities. This document states that, using the created approach, the requirements can be applied to other nuclear facilities.

For your reference, the use of a created approach means basically that the scope of actions necessary to comply with the requirements are commensurate with the relative risks and particular characteristics of the nuclear facility.

This CSA standard also specifies that cyber security controls are to be selected based on the classification of each cyber-essential asset in the facility after assessing the asset's safety significance and its vulnerability.

Now, that's another buzz word, so a cyber-essential asset is defined as basically an electronic device that has an impact on the functions important to nuclear safety, nuclear security, emergency preparedness, or safeguards functions.

The CNSC incorporated the CSA N290.7-14 standard into its regulatory framework and provided the nuclear power plant licensees with time to implement programs in accordance with this new standard. As of the end of 2020, all nuclear power

plant licensees had informed the CNSC that their cyber security programs are in accordance with their standard.

Next slide, please. As for our future plans, the CSA Group is in the process of updating N290.7 to incorporate the lessons learned by the CNSC and by the licensees over the past five years. The revision project will also take into consideration new best practices as suggested by recent documents published by the IAEA and other international bodies.

Further, the title of the standard may be changed to reflect an increased scope for the standard. Instead of referring to nuclear power plants and small reactor facilities, the new standard may be titled Cyber Security for Nuclear Power Plants and Nuclear Facilities.

This change in scope could help apply the Canadian cyber security requirements and guidance to nuclear facilities that do not house reactors. The current plan is to publish a new version of the cyber security standard in March of 2022.

Next slide, please. I will now talk about CNSC inspections. To conduct inspections at nuclear facilities, the CNSC uses approved inspection

guides. These inspection guides detail the specific checks and types of checks that inspectors are going to complete during the inspection to ensure that the program meets CNSC requirements, it meets licensee's program requirements, and that the program is consistent with industry best practices. The purpose of the guides are to ensure that CNSC inspectors conduct the inspection in a transparent and consistent manner for all licensees.

Next slide, please. Specific to cyber security, prior to 2021 the CNSC performed inspections for the cyber security programs at all nuclear power plants. These inspections were carried out by reviewing documents at our head office and by performing onsite verification activities. Based on these inspections, the CNSC staff concluded that all nuclear power plant licensees were in compliance with the regulatory requirements in force at that time.

As I mentioned earlier, all nuclear power plant licensees have informed us that they have fully implemented the CSA N290.7-14 standard and will be starting inspections to verify their compliance starting this year.

Next slide, please. In addition to the

update of the CSA N290.7 standard, and starting our CNSC inspections, we're also working on a number of other cyber security projects. First, as I mentioned earlier, the nuclear security regulations are being updated to include specific requirements for cyber security. We perform periodic updates to design basis threat analysis to reflect changes to the threat environment.

On the research front, the CNSC participates in a program called the Federal Nuclear Science and Technology Program which conducts research in nuclear science and technology. For cyber security, research is being conducted in areas such as supply chain protection, remote monitoring, and control of reactor systems.

The CNSC also meets with regulators and agencies from other governments to discuss cyber security issues, research, lessons learned, and best practices. And we have found that these discussions are particularly helpful to ensure that best practices and operating experience is effective and shared.

Next slide, please. In conclusion, the Canadian Nuclear Power Plants have all implemented

cyber security programs. The CNSC has conducted inspections at each nuclear power plant and determined that the nuclear power plants met the regulatory requirements that were in place at the time of those inspections.

The regulatory requirements have now been updated to incorporate the CSA standard and 290.7-14, and we have been informed that the licensee programs have been updated to implement this new standard.

Our compliance verification inspections based on the CSA standard will start in the coming months and start this year. In addition, we continue to update our regulatory framework, be involved in research projects, and engage with government agencies within Canada and outside of Canada, all with an aim to improve the safety of cyber assets.

Next slide, please. That concludes my presentation. If you have any questions, please feel free to submit them through the Q&A feature for the session. In addition, please feel free to visit the CNSC's webpage displayed on this page for any additional information. Thank you very much.

MR. BEARDSLEY: And now I'll introduce Barry Kuehnle from the Federal Energy Regulatory

Commission of the United States.

MR. KUEHNLE: Thank you, Jim. Good morning. I am Barry Kuehnle. I work for the Federal Energy Regulatory Commission in the Office of Electrical Reliability in the Division of Cyber Security, DCS.

Before I get started, I have to give our standard disclaimer to staff. I do not speak for the Commission, and my opinions are my own.

Just a little bit of background about FERC. I'm going to talk about our jurisdiction. Our jurisdiction, specifically for the bulk power system, is within the Unites States. And that excludes Alaska and Hawaii. It's approximately covering 100 kv and above, and we do not regulate nuclear. It also includes about 1,400 entities across the jurisdiction, again in the continental United States.

Where we get our authority at FERC, we get our authority through Section 215 of the Federal Power Act. And it gives FERC the authority to certify an electric reliability organization, called the ERO.

NERC, the North American Electric Reliability Corporation, has been named the ERO and is a non-governmental organization that is chartered

to develop and enforce mandatory reliability standards subject to Commission review and approval. It's important to note that the standards that the ERO is responsible for is actually written by industry.

As I mentioned, I work for the Division of Cyber Security, DCS. DCS is on a full life cycle of critical infrastructure protection standards from the development to the compliance aspect of those critical infrastructure and protection standards.

We oversee all aspects of cyber security related to the matters that affect the bulk power system. We monitor, and we participate in the development and the review of these standards, we oversee the compliance and enforcement with the approval of these standards. We observe and we perform audits related to the CIP standards, and we also assess and advise whether new standards should be modified or remanded. Currently, there are 12 enforceable standards.

In a little bit more detail, the critical infrastructure protection standards are required and do protect the bulk power system. They are very similar to the NIST standards, but they're written in

a way that's going to be applied specifically to the bulk electric system. But if you were to match the two of them up, if you're familiar with the NIST standards, they're very similar.

But we also recognize the fact that cyber security threats are evolving, and they change really quickly, actually more quickly than standards could be developed. So as a result, we are continually looking at the changes to threats, to technologies, to resources, and how these CIP standards may change based on what's happening in the environment around them.

What needs to be done? As an example, in November of 2019 Chairman Chatterjee at the time introduced five focus areas to ensure that the CIP standards are keeping pace with the changing environments. And I'm going to cover those five topics at a high level. And then we'll leave the rest open for the panel discussion.

So the first one would be supply chain, insider threat, and third-party authorized access. We looked at that particular topic in the sense that typical cyber security defenses are wrapped around perimeter security.

We're looking at supply chain, insider threat, and the third-party authorized access which means that maybe a trusted partner, such as a vendor or a member company that you have a connection with, that is trusted, you potentially have the ability to maybe leapfrog those perimeter securities. So we're looking at ways to enhance the CIP standards to ensure that those type of threat factors, if you will, are addressed.

And the second one would be industry reactions to timely information on threats and vulnerabilities. And that would be information sharing, and not only within the electric sector but within other sectors as well, such as partners with the NRC we share information with and so on, and vice versa.

An example of that would be one of the CIP standards. CIP-00806 is required to report suspicious activity and events to FERC through the ERO and also to the Department of Homeland Security. And that information is shared in an anonymous way to ensure that the timely information is disseminated quickly.

The third one would be Cloud and its

security service providers. So we recognize the fact that Cloud is a technology that, if utilized properly, can be done securely and efficiently. And it helps with economies of scale by the way it's implemented. And we're looking at ways that possibly the electric sector can take advantage of those controls in the Cloud.

And the fourth one would be adequacy of security controls. And what we mean by that is currently the CIP standards, specifically, are rank facilities based on risk. And it would be high, medium, low impact ratings where the high and the medium, as you could expect, would probably have more, well, do have more security controls, where the low has minimal security controls, in my opinion.

So we're looking at ways to ensure that those low impact facilities do include also high and medium, but specifically low have the adequate security controls that would be justified for that risk.

And the last one would be internal network monitoring and detection. As I mentioned earlier, the CIP standards are very, in my opinion, are very similar to the NIST standards. If you

overlay them, the controls are very similar.

What we have concern about is internal movement with any trust zone, so just lateral movement if a machine is compromised. So we're looking potentially enhancing or ways that the internal network monitoring and detection can be done efficiently to ensure that any type of malicious activity is detected.

That's a very quick overview of some of the things we're doing here in DCS. Obviously, there's a lot more. But I'm looking forward to any questions that many have in the panel. Thank you very much.

MR. BEARDSLEY: Thank you, Barry. At this point, we'll go to the questions that have been submitted so far. We look forward to answering these and any other questions that the audience is interested in asking us.

So the first question goes to my presentation where I mentioned that the NRC's Office of Inspector General had conducted an audit of our Cyber Security Inspection Program. There were two findings as a result of that audit. The question was what were the findings.

So the answer is there were two findings. The first one had to do with staff, level of knowledge and also making sure we had enough staff so that we could account for retirements in staff. And the NRC staff is working on that process through our internal human resources activities.

The second finding had to do with introducing suitable performance measures into our inspection and oversight program. And as part of our new inspection procedure that we've drafted and we're working on implementing, we are looking at ways to include performance metrics and possibly performance testing and inputs to the staff's evaluation of a licensee's performance. That's the answer to the first question.

The second question was for Paul. And let me read it, and then we'll give Paul a chance to answer. With the UK's new approach, what are some of the steps taken to ensure the consistency of inspection and regulatory processes?

Also how does the outcome-driven approach ensure repeatability and scrutable regulatory process? Paul?

MR. SHANES: Thanks, Jim. And that's a

really key question actually, and one that's been a part of implementation about conflict regulation, I think firstly from a consistency perspective. And our security assessment really provide the backbone of a consistent regulatory methodology that enables consistent regulatory judgements. So our expectations are articulated within that document.

And underneath those, I think I briefly alluded to we have a number of technical inspection and technical assessment guides. And really, they serve to provide the backbone of the consistency from an inspector's perspective. They articulate the sort of things that the inspector should consider.

So from a consistency perspective, that suite of documentation, which we make fully available to duty holders, really provide that level of consistency.

In terms of repeatable processes, one of the fundamental principles that we have within ONR, in common with all regulators within the UK, is the principle of proportionality. And one of the things that we do is, whilst we wish to have a repeatable, and certainly one which may be evidence process for the way in which we regulate the industry, it is

proportionate. And it is based upon that identification of appropriate protection mechanisms up front.

So we don't necessarily follow the exact same schedule of interventions across all of our duty holders. We have varying regulatory attention levels. And that really guides the level of intervention activity that we undertake. However, there is consistency throughout, and that is based on the proportionality aspect that I mentioned there.

So in addition to that, occasionally we will also do thematic inspections whereby we will take a particular topic. If we wish to look at governance and leadership, or cyber security, for example, we may, as a thematic area, in consultation with government, look at doing that thematically across the sector and conducting consistent intervention activity.

But ordinarily, it is more targeted in our approach in order to achieve that preference for proportionality. I hope that answers the question. Thank you.

MR. BEARDSLEY: Thank you, Paul.

The next question, let me make sure I've

got it right here, was actually asked of the NRC, but I think it's a question that all of the licensees, or all of our panel members could speak to.

So let me read the question. Does the NRC distinguish between cyber security and physical security? If so, does the NRC view cyber/physical security approaches such as STPA, STPA Security, OCTAVE, or others?

So the NRC, from a regulatory point of view, starts our oversight with our cyber security rule. The rule then, we develop guidance for the rule which laid out the process for a licensee to develop and implement a cyber security plan.

The cyber security plans included a lot of structure that was related back to the National Institute Standards that Barry mentioned, the NIST standards. And so the controls that the licensees have to implement on their, not only in the manifestation of their program, but also in what they use to secure their digital assets, are laid out in their cyber security plans relatively explicitly.

And then they have industry guidance that they use to develop internal procedures to go determine which assets have to be protected and the

level of protection for those assets. So there are no other tools or models being used to break down the systems or the other areas that have to be protected, with the exception of the fact that the rule requires them to address cyber security for safety, security, and emergency preparedness systems.

And then within those systems they determine which assets have to be protected and then subsequently what protections are appropriate for the assets.

So I hope that answers the question. And I'll turn it over to the other panel members if they have any thoughts.

MR. SHANES: So, Jim, just to complement that from an ONR perspective, everything really hinges around a duty holder having a site security plan or an equivalent if they're a transportation provider, for example. And within that site security plan, would come all the facets of security. And we're really looking for an integrated model and one which, you know, covers all aspects of security.

So do we distinguish between cyber and physical? Yes, we do. But we very much follow a graded approach and a defense in depth principle

whereby actually, you know, we see the intrinsic link between all of the different facets of security.

And we expect our duty holders really to manage security holistically and to consider mitigation measures and security arrangements across the board rather than just focus purely on a dedicated cyber security plan that, for example, stood completely alone from other security expectations.

MR. BEARDSLEY: Thank you, Paul.

MR. KUEHNLE: This is Barry with FERC. So from a physical perspective, the CIP standards include both physical and cyber. So specifically CIP 14, one of the standards within this suite, specifically addresses physical security. And also, physical security is kind of sprinkled throughout the standards as well, you know, such as protection of the data centers and the control systems, and that type of thing.

MR. SIGETICH: From a CNSC perspective, I would echo what my colleagues on this panel have said already. It's really that from a holistic perspective we're looking at both the integration of security aspect and cyber security, the physical security plus cyber security.

So really, we're looking to have licensees have an integrated approach to looking at all of the systems together. And we don't prescribe the type of models that they're using. We have overarching requirements for their -- that they need to come up with methods to have a security plan and a cyber security program. And they're the ones who propose the different methodologies that they use to meet the requirements. Thank you.

MR. BEARDSLEY: Thank you, Justin. So the next question was for Paul in particular. Power plants are subject to a range of cyber regimes, nuclear, electric, reliability, et cetera.

Do you feel the approach in the UK, high level expectations, in parentheses, allows entities to implement an enterprise-wide cyber program versus separate cyber programs designated to be very specific regulatory requirements by each regulatory body?

MR. SHANES: Yes, another really good question and something that has actually been at the heart of the implementation at CyOps again. Because one of the requests that we had from our duty holder community during extensive consultation was really to

empower them to not have a mandated approach to cyber security, or security more widely, but rather to allow them to offer up evidence of arrangements that could be from other expectations, whether that's regulatory or certification expectations from other bodies, et cetera.

And the duty holders that we regulate are regulated in the round by numerous other organizations as well. But we have the sole responsibility from a nuclear perspective. You know, clearly there are expectations of our duty holders around data protection arrangements.

We regulate the civil nuclear constabulary, and they have expectations on them as a policing organization. And likewise our carriers, in terms of road, rail, and air, are often subject to maritime, air, or road regulations in terms of the way in which they operate.

So, you know, I'm a firm believer that actually the outcome-focused approach really does empower duty holders to put forward a suite of evidence which may come from satisfying any other regulatory expectation.

And provided that, you know, it justifies

the claims that are being made by our duty holders, we are open to receiving that. And so we actually strongly encourage that. And we see it as a huge cost benefit to those that we regulate, that they can re-utilize evidence from other aspects of their business operation. Thank you.

MR. BEARDSLEY: Thank you, Paul. Does anyone else on the panel have any thoughts on that question? Or we can move onto the next.

MR. SIGETICH: Looking ahead, a bit of perspective from the CNSC that the CNSC's approach has always been to create higher level objectives as opposed to very specific, prescriptive requirements. We do have some level of prescriptive requirements, but we do not specify in detail exactly all of the methods that licensees are required to follow.

We instead provide them with the overarching requirements, and they have flexibility in the way that they meet those requirements, as long as they can provide us with documented safety analysis to detail exactly why what they're proposing to do, if it doesn't meet our guidance, is acceptable.

So we have valued this approach of some regulatory flexibility, since it allows our licensees

to be able to come up with better methods than had been thought. So anyway, this has been the CNSC approach.

But for us in this particular area, we have found that we have specified that licensees are to have comprehensive cyber security programs, that they are required to come up with one program for their facility. And that is to ensure that they are having a comprehensive management system that encompasses all of the various program systems and including, like, a comprehensive cyber security program as well.

So we're looking at them to have a comprehensive system, as part of our comprehensive system, for them to be able to ensure that they have all of the requirements they need and well documented governance.

MR. BEARDSLEY: Thank you, Justin. So let me move on to the next question. This is a question for all the panel members. Are there any operators or regulators that are studying the potential for blockchain technology as an integrated layer for securing records management?

And I'll take the first crack at this

one, and then we can move on. The NRC staff has monitored the potential use of blockchain technology in multiple different areas. But we don't mandate to the licensees how they maintain their record systems or how they maintain their supply chain.

We understand that blockchain technology could be used for managing and securing multiple different elements of the supply chain. So we understand the technology, and we're watching it. But it's really up to our licensees to elect to implement that type of technology or any technology. And then they would basically, through inspection, we would observe how it is implemented and make sure that it meets the regulatory requirements.

And I'll turn the question over to the rest of the panel.

MR. SIGETICH: From the CNSC perspective -- oh, sorry, Paul.

MR. SHANES: Go ahead, please, Justin.

MR. SIGETICH: Oh, okay. From the CNSC perspective, I would echo what, Jim, you just said, that I have not heard of any specific use of blockchain.

But we would not be prescriptive in the

methods that licensees use to protect their record systems other than our high level requirements that they need to ensure that their records are protected, and especially with any, what we call prescribed information that's held digitally. They would need to ensure that that information is protected from any potential cyber risk.

MR. SHANES: And quite similarly from the UK's perspective, you know, again it's not something that we would mandate in one way or another. The sector as a whole commissions a reasonable amount of research and development on an ongoing basis.

We support quite a bit of that, you know, in order to understand the regulatory aspects, and the sector obviously, to look at potential future uses of technology. But it's not something specifically that we would necessarily have an immediate view on without a duty holder proposing it.

MR. KUEHNLE: And this is Barry with FERC. I would echo the same thing. We do require the protection of documentation in a supply chain. Obviously, we do not specifically recommend any type of technology that would ensure that those risks are mitigated.

MR. BEARDSLEY: Thanks, Barry. The next question is actually for you. So we'll keep you up on the screen here. Are additional CIP standards directed at CIP low impact site controls coming out?

MR. KUEHNLE: Obviously, I can't speak to anything that's happening internal to the Commission right now. However, the Commission has recently released the Cyber Security Incentive Program specifically for transmission where there is the opportunity for a transmission owner to enhance their cyber security controls, and many of those would be the low impact, and have financial benefit by doing that.

I know that, within the standard drafting teams, low impact is routinely discussed because of the security controls that are wrapped around those low impact. But as far as anything specific coming out, I can't speak to anything along those lines. Thank you.

MR. BEARDSLEY: Thanks, Barry. The next question is for all the panel members. Is a quantitative risk assessment approach used to establish cyber security defenses, and what documents are used to assess cyber security risk?

So from a US point of view, each licensee has an approved cyber security plan. And within the cyber security plan, they have elements that may have systems they have to analyze. They have to decide which digital assets in those systems have to be protected. And then there's a series of protections that have to be assessed for each digital asset that's included.

Beyond that structure, it's really up to the licensees to determine the assessments and figuring out, well, in the level of protection of those assets have to, you know, have to be put in place for those assets.

The staff has reviewed and accepted for use a number of industry guidance documents that provide a structure for risk assessing different levels of assets in different systems and then agreeing with a somewhat lower set of controls that we placed on those assets.

But there is no particular model that's been used to date for assessing the risk of systems or assets and then what systems, what controls would be appropriate for those.

And with that, I'll turn the next

question over to Paul.

MR. SHANES: Yes. So as you might expect, a similar answer, I think in terms of mandates within the CyOps, you know, the closest thing we would kind of go as far as mandating the categorization and classification of assets and associated postulate results from that.

Within our security delivery principles, affected information in cyber risk management is up there. And, you know, we set out some expectations for our duty holders but didn't go as far as mandating a particular approach. And so really it is for duty holders to put forward to us how they're going to effectively identify, categorize, and then manage any risks that result.

MR. SIGETICH: Similar for the Canadian approach, that we do not specify a particular model that they would need to use to be able to assess the risk of their cyber essential assets. So they have different methods that they use, but we do not specify any particular method that they use.

MR. KUEHNLE: And from a FERC perspective, the CIP standards in CIP-002, they have a method to determine your high, medium, and low

impact. And you could wrap risk around those high, medium, and low impact.

MR. BEARDSLEY: Thank you. The very next question is for you again. So let's see, DHS did, let me just take out the acronym, the U.S. Department of Homeland Security did a cross-walk of the NIST 2.0 and electric sector requirements a year ago.

The questioner says, "I think." And 2.0 included supply chain, but how do the NIST and electric requirements address insider threat, trusted partner access, and third party authorizations? It's a good question.

MR. KUEHNLE: Excellent. So I'm going to speak specifically to the CIP standards, not the NIST standards. So the CIP standards, they include background checks, they include security awareness training. They include controls wrapped around the personnel that are in those high trust zones, if you will, from the CIP standards perspective. So that addresses your insider threats and your security awareness of just personnel in general.

From a trusted partner perspective, we're looking at technical controls as well. There are technical controls right now within the CIP standards

that require, you know, justification reports and services and, you know, controls wrapped around monitoring of those connections that exist within the CIP standards to address those requirements.

But I think we all know, and I think SolarWinds is a really good example, of what just recently happened specifically with supply chain that kind of highlights the need to ensure that we need this type of security controls that are wrapped around supply chain and insiders, because I kind of lumped the two together.

It should be reviewed and ensure that they are robust enough to at least mitigate any type of event like a SolarWinds in the future. And I'm not saying we're going to be able to prevent it, but earlier detection is obviously better than later. Thank you.

MR. BEARDSLEY: I can actually jump in and just give some perspective from the NRC point of view on supply chain in particular and then the insider threat.

From a supply chain point of view, we do have high level supply chain requirements that the licensees have committed to on their cyber security

plans. There's not a specific or prescriptive process for the supply controls or system and services acquisition which is what the section is actually titled.

The U.S. NRC is working within the larger U.S. government with Department of Homeland Security and Department of Energy looking at methods to secure the electrical and subsequently the nuclear supply chain. That's a large problem. And I think that most people would recognize that it's going to take a lot of work.

But our licensees do have requirements for their purchasing. They do have requirements for testing of their systems. And they also have requirements for defense in depth so that if, for instance, a system or a component did get installed that had some level of malware or something like that in it, that they should be able to identify that as part of their overall system and take mitigative actions. So that's sort of the high level.

The other question had to do with insiders. The U.S. NRC does have insider mitigation regulations and requirements for all the licensees. Those are inspected as a separate part of our

regulatory oversight, not part of cyber security. But we do rely on that to manage any potential cyber security insider activity.

That's the U.S. point of view, I don't know if Justin or Paul have any thoughts.

MR. SHANES: Yes, I'll be happy to kick off. So again, quite similar in terms of the expectations. We do set out high level expectations or effective supply chain management, effective contract security, and contract monitoring.

Our safety colleagues, from a supply chain perspective, also look at quality assurance expectations which, as you know, are making sure that, you know, assets are appropriately governed throughout the life cycle of the development and into operation.

In terms of insider threat once again, you know, we would again pick that up. Again it wouldn't necessarily be specifically within the cyber security team, because that probably is part of our workforce trust worthiness measures, and perhaps assessment of the cultural aspects within the organization as well, so a kind of broader aspect of security that we do set high expectations with.

MR. SIGETICH: I don't have much to add.

Everyone has really addressed many of the same points that Canada has in its programs.

So for the supply chain, we are certainly very interested in ensuring that we are addressing any issues in the supply chain. We have research ongoing in this area to ensure that the supply chain is protected. And certainly the insider threat is one of the threats that's assessed in any of the analyses that are part of any security plan.

MR. BEARDSLEY: Thank you. The next question was actually targeted towards the NRC, so I will answer it. And then we can move on.

So the question is are we going to see force on force exercise start to look at cyber attacks as part of their exercises?

In the US, we do have a robust force on force testing program at all of our commercial power licensees. At this time, we have focused on the licensees implementing their programs. That's been the primary focus of our inspection and oversight.

We have evaluated the potential to include cyber security as part of the force on force program and have elected not to do that at this time. There's a couple of reasons for that. One, based on

the successful implementation of the licensee's programs, we believe there would be limited ability of a cyber attack to impact the physical security programs and thus be an active part of a force on force test.

And the other side of it is, you know, we're looking at overall licensee programs. And within the cyber security program, licensee's do conduct their own internal exercises of their cyber security response which we believe adequately covers the same type of information you would gain from a force on force exam. So we don't know, at this time, that there would be a significant amount of information we would gain.

The next question is for everyone on the panel, so let me just read it out. And I know we're starting to run out of time, but I think we have enough time for this one.

There seems to be a pattern on the question of retirement or low staff supply to meet demand. What are the individual regulators doing and planning to do to sort out new talent and address the issue of cyber security professionals?

I'll take that first from the NRC

perspective. We recognize that the level of cyber security knowledge worldwide, if not just in the United States, is extremely competitive. The U.S. government does have, actually, has implemented direct-hire authority for a number of agencies to directly hire cyber security professionals without having to go through a competitive process.

We evaluate the use of that, and we look at how we maintain our staffing. We also have staffing tools in our human resources programs that look at our overall staffing, what we need for the future. So we're looking five to ten years in the future, trying to factor in retirements and training for the staff.

At the NRC, we maintain the majority of cyber security expertise at our headquarters. And then we consult and assist the inspectors in the field with their cyber security inspections. And then by doing that we can centralize our training and the other assets we use to maintain our cyber security knowledge base.

I'll turn the question over to Justin to answer from a Canadian point of view.

MR. SIGETICH: Yes, from the Canadian

perspective, I would say that cyber security is certainly one of the areas. But I think I would say that the aging workforce in the nuclear industry is certainly one aspect overall that is a concern.

And just to answer that in general, I'd say that the CNSC has the ability to hire staff directly across the board. So what we have is plans for succession, some succession plans looking for, like, a five-year and a ten-year plan, looking down the road.

We have talent management programs, we have training programs, and we're coming up with new training programs to ensure that any new hires would be able to take on their roles for the next few years and come in to use some of the new roles that would be open when people are looking at retirement in the next few years.

We're also developing and improving the current coaching and mentoring programs. And we're conducting targeted hiring for the areas where we know we'll have some weaknesses. When we have experts who have been in the industry for decades, when those people start to retire, we know that we need to make sure that we're hiring people with significant

experience, and background, and trying to find ways of replacing that kind of experience.

But there are certainly challenges, but we're putting in place programs to be able to make sure that we can maintain the knowledge and skill to continue to effectively regulate the industry.

MR. BEARDSLEY: Paul?

MR. SHANES: Thanks, Jim. So I think in line with yourselves, we identify this as a real challenge. And it's certainly one of the things I picked up in the presentation. Trying to recruit and then retain appropriately qualified and experienced staff is a real challenge.

And it's not something that we, as a regulator, are suffering alone, nor as an industry actually. There is a huge amount of effort across the UK, led in part by government and in part by the National Technical Authority, our National Cyber Security Centre, to encourage and promote careers in cyber security. So I guess on a national footing, that is happening.

And also within the UK is the formation of a new Cyber Security Council, a professional body dedicated to cyber, which is undergoing work at the

moment and really a lot of effort, I know, that's being placed nationally to encourage people to get into the field.

That doesn't necessarily immediately solve the problem within the nuclear sector. We do struggle, like many sectors, to attract and retain the right people. And we're really using a whole myriad of mechanisms to address that.

We're working really closely with industry to attempt to ensure that both we, as the regulator, but also duty holders have the right people. We're working with government on the formation of their next cyber security strategy for the sector.

And certainly training and retention of skills is featuring heavily in those conversations around how that might be taken forward jointly between government, industry, and the regulator. Because it's in all of our interests to get the right people.

Slightly close to time, within the regulator we have embarked on cyber security graduate programs and joined forces with industry to attract people into the sector without routinely sponsoring the graduates at apprenticeship placements that

rotate across the sector to bring in the next cadre of future inspectors.

And we blend that with cross-training and joint working internally so that we work closely with colleagues in disciplines that are linked in places to ours, such as emergency preparedness and response, control and instrumentation expertise, for example.

And we work closely to cross-skill where it's appropriate, and to work jointly to really pass our skills and experience on. But it is something that is definitely a challenge. And I think it will remain a challenge for a while and one, I think, that we're not suffering alone. So all ideas welcome, please.

MR. BEARDSLEY: Barry?

MR. KUEHNLE: Yes, thank you. So I'm just going to echo what Jim said earlier related to the federal government. FERC pretty much follows the same model.

But I'd like to add from a utility perspective, I know the utilities really struggle with being able to find qualified staff in a cyber security perspective that not only understand cyber security but also understands the control systems,

which is a unique environment to begin with, and how that cyber security relates to the need for real time communications within that industrial control system environment.

So from a utility perspective, some of the things that we're hearing from the utilities is what they do is they train within, they go to recruit at colleges. They do as much as they can to try to grow people from the ground up to get into that cyber security environment since it is so unique.

They're having a lot of success, from what I'm hearing and what I'm seeing from the audits that we're on as well, that people actually are growing within the organization that may have a desire to learn it, are kind of filling those roles in addition to, you know, your standard pathways of going through colleges and recruiting, and community colleges as well, and so on. Thank you.

MR. BEARDSLEY: Thank you, Barry. Well, that brings us to pretty much the end of our session. I don't know that we're going to have time to answer any more questions.

At this point, I'd like to thank all of the panelists. I think we covered a lot of ground

today, a lot of different perspectives. Although what you might find is, although we are coming from different perspectives and regulating different levels of industries, I think the approaches we're taking are relatively similar. And we're all very, very interested in making sure that our respective licensees have the appropriate cyber security controls in place.

Again, thank you to the panelists. I'd like to thank the RIC support staff. The background of running this RIC digitally has been a challenge, but I think they did a great job.

And I'd also like to thank Yuris Guantrans (phonetic) and Dan Warner of my staff who helped us organize the questions, reached out to the panelists about 1,000 times to make sure everyone understood what we were doing to get logged in and get ready for the RIC.

Thank you very much. And I hope you enjoy the rest of the program.

(Whereupon, the above-entitled matter went off the record at 11:59 a.m.)