Information Sharing and Analysis Organization (ISAO) Standards Organization (SO) 3rd Public Meeting
Anaheim, CA
May 19th 2016

Engagement between Regulator Forum and ISAO SO
Speaker: Mr. Jeffery Goldthorp, FCC

Introduction by Dr. Heidi Graham, LMI: The next speaker is Mr. Jeff Goldthorp who is the Associate Bureau Chief for Cybersecurity and Communications Reliability with FCC. In that role he is responsible for engaging communication providers and the development of a market driven cybersecurity risk management approach. Please welcome Mr. Goldthorp.

(Applause)

Mr. Jeffery Goldthorp, FCC: Thanks Heidi. Let me begin by just noting that it's alleged that folks here in the audience may not have the warmest attitude towards regulators. I've heard that, okay. And it just so happens that I had dinner with a friend last night and we went to an Asian restaurant and he got a fortune, by the way, and I did not. But he shared his with me, very kind, and I thought I'd share it with you. "Everywhere you choose to go, friendly faces will greet you." So, anyways with that, let me dive in. I'm here to talk about the inter-agency cybersecurity regulators forum. And that is a hard topic to talk about. There are a lot of federal regulators, who cover different sectors. Some of them are independent, some of them are affiliated with the administration, they have different stakeholder groups and different priorities, so what you see is regulators acting in different ways. They're not consistent. It's not even appropriate for them to collaborate and try to harmonize the policy. We don't do that, especially independent federal regulators, so that's something that's just a fact of life, but there are some things that are just true in the federal regulatory space and maybe regulation in general. And that is, first of all, that regulators tend to work in areas that result in rules. Not always, maybe even not most of the time and in this area, that we're going to be talking about today, we may not most of the time. But sometimes and because of that we have to adhere to certain guidance, not guidance, but certain laws. There's the Administrator's Procedures Act, and the Administrator's Procedures Act requires us, when we have an idea for a new set of rules, we have to seek comment on it. We do not have to authority to just declare what new rules will be. We have to see comments and in a lot of ways it's like the multi-say quarter process here. The outcome may be different but we see comment and we cannot just ignore the comments we receive. We can't act arbitrarily, we can't capriciously and if we do, we can be sued. And whatever we do as a consequence can be overturned in court and that happens, okay, I could tell you that. So, when it comes to regulators, we have constraints too, in addition to that, there are things like the Paperwork Reduction Act and other administrative procedures that constrain how we operate so that its transparent and there's participation. So, I wanted to assure you of that. The second thing that I wanted to assure you of is that we know that when it comes to high tech industries, and cyber in particular, there's a serious gap in expertise and the smartest people are not necessarily in DC. So, we know when it comes to proposals that we make, we have to

get input from the people who are actually practitioners, that are doing these things, and we'd be crazy if we did anything else.

So, hopefully the things that I talked to you about today, you will have some comfort that what we're doing in cyber and high tech more generally and when I say we, and I have to be a little careful, okay. Because there are going to be times where I talk to you today, where I am going to be talking to you as an employee of the FCC. And I can't speak on behalf of the FCC, but I have a lot of experience there and I can give you my opinion about what's happening there, and when I'm talking about that, I'll try to be specific I won't be trying to represent the views of the cyber-regulators forum, or any other regulator. There will be other times when I'm talking about the cyber-regulators forum so I'm going to have be as clear, as I can, when I'm putting one or the other's hats on. So, now let's talk for a minute about some issues that are important to the FCC and why it's important for regulators to play a role, even in a high-tech space, like say, communications alright. And here I'm talking about things that are relevant directly to what we do at the FCC.

911. Everyone cares about 911, when you have a medical emergency, a car accident, everyone wants their call to 911 to go through. So, that's not something you want to take a chance on, and there's something if there's a gap between something that's happening and the markets and, what the public need is sort of what the core need is, then maybe there is a need to seek comment and ask some questions about that need and say is there a need for an effort to close that gap somehow. So, 911 is one area where the FCC, while we don't have authority over 911 call centers themselves, the people that answer the calls, the 911 call center itself, we do have authority over the communications providers. And if you want to make sure those calls are going through, the fact that we're interested in that topic, constantly, is something you should care about, and the fact that 911 is going to an IP network and is subject to exploits, cyber exploits, is something that should concern you, and it's something that concerns us.

So, second example, relevant to the FCC is the Emergency Alerting System [EAS]. Something else that's sort of a core value is, everyone wants to know if something very serious is happening in the nation of in their region. So, you want the emergency alerting system to work. So, that's another one like 911, where 911 is an example of where there's not a whole lot of money to be made by 911 necessarily, maybe not a whole lot of money to be made in EAS, but it's important that both of those infrastructures work. And so, those are areas where a regulator may have a role and we've taken an interest in the past. EAS, just in the past 12 years, has been subject to cyber exploit. And there's one a couple of years ago that where the EAS in Montana was hacked and I think an emergency alert was issued, maybe you've all heard about this that zombies were rising from their graves. True story, okay? So, that was one, and that was a cyber hack it was just that the coders and the decoders and the broadcast stations had not been configured properly so they could be hacked, and they were. So, those are areas where a regulator, you probably would agree, should be interested. And we have been. Now, let me turn to what we have done over the years and as the FCC.

Now, I've got my FCC hat on now, I'm not speaking about the cyber regulators forum or any other regulators. So, what we have done over the years to deal with communications reliability and security at the FCC? Well, let's go back all the way to 1991. In '91, there was a situation that came about, that was shortly after divestiture, so now instead of having one company administrating a whole nations wide of communication network that was AT&T. Now we had seven, administrating seven companies and having to operate a nationwide network. Well, at the same time that that was happening, or shortly after it happened, we introduced a new signaling network, the signaling system seven network. A new nationwide network, a new technology, packet switching protocol and a new protocol and transport technology and we also introduced new, multiple venders, so it was a perfect storm. More than one vender, so there was AT&T, telecomm and other switch venders and STP [Signal Transfer Points] venders and multiple service providers and new technologies and there was an outage. And it wasn't just a local outage, it was an outage that effected DC, it affected New York, it effected the west coast. And now, you might think that as the FCC, first we've heard about this very quickly, despite the fact that the phones weren't working folks found a way to get the word to us that there was a problem and we needed to do something about it, or what were we doing about it? And what we did was we established a public private partnership that was at that time called the Network Reliability and Interoperability Council, NRIC and NRIC was a group that met. It was practitioners, experts based, that met and made recommendations to the commission on what could be done to keep this thing from happening again. The recommendations they made to us were voluntary. We have not enacted rules that would require anybody to do any of those things. And NRIC and subsequent to that, CSRIC, have been meeting since 1991 and making best practice recommendations to us. So, I know there's a concern and again I can't speak for what might happen in other agencies or in other sectors, I can't even speak for what might happen at the FCC eventually, but I can say what has happened in the past. And our approach has always been, in high tech sector's regarding reliability and security, to rely on the expertise of industry and make recommendations to us and then trust that expertise. It just made sense and it's worked. We haven't had an outage, an SS7 outage, like that since 1991, and we have a way of knowing what the condition of the infrastructure is, so we have some assurances about what's happening in the network and that's what allows us to keep doing what we're doing, without doing any more than what we're doing.

So, it's important that in addition to this voluntary based approach, which is flexible, that there be some transparency that the regulator be aware of what's happening in the network. So, that's what's been happening with NRIC, CSRIC and now moving into cyber, what we've done is we've gone back to CSRIC [Communications Security, Reliability and Interoperability Council's], so instead of doing anything unusual or different then what we've been doing, we've asked CSRIC to come to us, and this has been a couple of years since we asked them this question,

come to us with recommendations on how different segments in the communications sector should implement the NIST cybersecurity framework. And they did. They came to us with those recommendations and, it's been about a year now, and the recommendations were that we go to industry, meet with industry, when I say meet individually, that's impossible, we meet with companies individually, so we meet with individual service providers and talk to them, have a dialogue with them about what they're doing in cyber, what their cyber risk management practices are. The whole approach is to be risk-management based, and it's intended to be a dialogue. So, that's the path we're on with cyber. Very similar to what we've done in communications reliability and I'm telling you all this to give you some confidence that at least one regulator, and probably more than one, is taking an approach to this, but I think that this is very similar to what you're doing here, you have the same goals in mind and even our approaches to achieving those goals, those outcomes isn't that much different. And what's important, one of the things that's important, is that we stay in contact with what we're doing today, that we stay in touch, that we know what you're doing, you know what we're doing and the fact that what you're here is exactly the kind of thing to give us confidence to use what you're doing as a way forward. Right? So if you're looking to avoid the FCC or any other regulator acting in a way different from what we've done in the past this is it, what you're doing here.

Now, let's talk for a minute about the Cyber Regulator's Forum. The Cyber Regulator's Forum was formed a couple of years ago, it was after the NIST framework came out, and the purpose was to convene a group and provide a forum for where communications regulators could meet and dialogue and share ideas to the extent possible, avoid discontinuities, in other words, unintentional either duplication or disconnect and so that's a useful thing to do. What we can't do is harmonize regulation, but we can talk about what we're doing and we do that. And we've had workshops on cyber-risk management and we've had a workshop on cyber-information sharing. One of the things we've done at that workshop was to issue or draft a set of recommendation so the ISAO's Standards Organization. So I'll talk a little bit about that today. But let me first talk about the form itself, and it's composed of not only independent regulators, but also regulators that are affiliated with the administration. I mean some of the stuff, I haven't memorized it, but I will tell you that the Nuclear Regulatory Commission sharing the form right now, the FCC is obviously on it. The FTA and Federal Reserve Board, the Securities and Exchange Commission and the Federal Trade Commission, the Federal Energy Reliability Commission. Those are all members of the forum and there are others, those aren't the only ones.

Now, I want to step through some of the recommendations that the Regulator's Forum had made to the ISAO Standards Organization. I'm not going to go through all of these, I'm happy to provide these to the organization, okay? But one of them is that DHS and the ISAO organization should provide further clarification on the freedom of information act. Now I think we've

already heard from somebody that FOIA is believed to apply, and I think that this is the question really, does it just apply to government entities or to what extent is an ISAO a government entity that is subject to FOIA. At the FCC we are a government entity, obviously, so some of the processes we have generate the information that is presumptively confidential and we get FOIA requests that we have to address, to deal with and if it's presumptively confidential, there's a process you go through to either deny the request or not. The ISAO community is going to have to have a clear idea of what obligations their under with respect to FOIA. The ISAO Standards Organization is responsible for defining all ISAO obligations, so this is a making sure that the CISA obligations are clear and that the ISAOs are aware of them. There's a role for ISAOs, possibly, and I'm sort of saying as if it was true and I don't know that for sure, but I think it's worth asserting. There's a role for ISAO's in incident response. Once something has been shared, is there a role for the ISAO after the fact? And that's a fact that we think the ISAO Standards Organization should help to address. The ISAO Standards Organization should consider explaining the link between ISAOs and ISACs and I think we heard a little about that today.

So there's a number of these kids of recommendations here. And I really don't want to kind of stand here and just kind of read you these things and so what I'm going to do here instead is that I'm going to make them available to you and you can use them to the extent that they are helpful to you. But I do want to say, just in closing, that I came today representing the Cyber Regulator's Forum, to help you understand, and to help me understand too, but help me to understand how we tend to look at things as I can't claim to know how all of us do these things, but I can however say how the FCC tends to look at things and to learn about what you're doing here, because that will help us to know what the right things to do in our agencies. So, I'm really encouraging us to open a dialogue, we want to get more involved in what you're doing here and we want to encourage you to continue it because this is exactly, just like NRIC and CSRIC have been over the years, been exactly the kind of multi-stakeholder voluntary effort that gives the regulatory kind of community the assurances that industry is acting to deal with these issues that are hard to deal with and need to be dealt with. And so I'll close there and see if there are questions.

Q: **Carl Anderson, HiTRUST:** Thank you [this is from Carl Anderson]. Did you state, sir, that the FDA was part of the Cyber Regulators Forum?

A: **Jeffery Goldthorp, FCC:** I think I did, but I will look. I'm pretty sure I did and I think that they are. But if you want I will send you a complete list of members that you can put up on the website with the other information that I've stated with this event.

Dr. Heidi Graham, LMI: Thank you, any other questions?

Q: **Cathy Petrozzino, Mitre:** I'm interested in understanding a little bit better the products coming out of the regulator forum, the artifacts, what exactly do those look like? Or is it mainly a discussion forum?

A: **Jeffery Goldthorp, FCC:** First of all, before I answer your question, yes, I did say that the FDA is a member. So let me check on that to make sure but I think that they are. To answer your question, and you're asking what are the products of the regulator's forum and you're asking if it's mainly a discussion forum? It is. We do meet and we have discussions, we have workshops where we invite folks to come in and speak to us and address specific topics. We had one on cyber-risk management, we had one on information sharing and we had one on voluntary methods and obviously the principles meet. The principles are the leaders of the organizations that make up the forum, and the group will come to agreement on certain issues like with cyber-risk management we came to agreement on talking points that we had talked about and agreed to, but as far as formal work products, deliverables, there's less of that. Now, there is this set of recommendations for the ISAO Standards Committee that we will share.

Dr. Heidi Graham, LMI: We have a question in the back

Q: **David Turestsky, Akin Gump:** I just have a question about the independent regulator's forum. The questions, or recommendations, that were given to the ISAO standards organization, were those related to the work products, the drafts that were generated that were being commented on, or were those sort of prepared separately as subjects or questions that we should address? And, do you know if the independent forum is likely, if it wasn't addressing the drafts, is likely to review the drafts and offer any comments?

A: **Jeffery Goldthorp, FCC:** I don't think the recommendations that I was talking about, they were prepared, like, before the drafts for the standards were released or were available, so we didn't have those when we wrote the recommendations. I don't know yet, whether or not, we're going to be making comments on the draft standards.

Q: **Mike Echols, DHS:** Hi Jeff. When you guys were going to present to agency leadership, the members of the regulators forum, were there any guidance provided to the forum from leadership of the various agencies regarding ISAOs or what's going on with voluntary formations of ISAOs?

A: **Jeffery Goldthorp, FCC:** I don't recall seeing that, Mike. Is there something in particular that, when we present at the agency leadership, is there a particular meeting that you're thinking of?

Q: **Mike Echols, DHS, Cont.:** I know that you guys at some point shared those recommendations that you're going to send to the standards organization with the member of the councils.

A: **Jeffery Goldthorp, FCC:** Well, yes, obviously we got feedback from the various members of the council and to the extent that they were knowledgeable about what's happening here, that

was reflected about their feedback. Right? So that all sort of flowed through, and made it's way to the final recommendations.

Dr. Heidi Graham, LMI: Thank you Mr. Goldthorp.

Jeffery Goldthorp, FCC: Thanks Heidi

ISAO SO Note: This transcript contains edits from the original recording for presentation in written format.