Information Sharing and Analysis Organization (ISAO) Standards Organization (SO) 3rd Public Meeting

Public Comment And Debate: Standards Working Group 6

Speaker: Mike Echols, Co-Chair, SWG6

Introduction by Dr. Heidi Graham, LMI: Alright next up, we are going to advance to work group 6 from Mike Echols. This is on government relations.

Mike Echols, SWG6: First of all I would like to thank all of you for being here. Making some serious advancement. I am sharing along with Dave Wienstein working group 6. We are the government relations working group. Something that is very important to understand is, when we set up the Standards Organization you guys will remember that we were initially holding these venues and having these meetings as DHS. Well we set up the cooperative agreement with the Standards Organization, they function fairly independently in cooperation with DHS. Therefore, there has to be a way or a mechanism to connect the Standards Organization to the government apparatus so that there is an alignment. There are activities going on all over the government that relate to ISAO's or that may in some way impinge upon or impede or potentially assist this process, and so there has to be some kind of alignment. So, we kind of help fulfill that responsibility.

Our document has two parts to it. The first part I will talk about, well let me just say the working group leaders, we have sub chairs because we have a full recognition that there is a federal component and there is a state local component, there is a law enforcement and intel component and the role of government. What is the role of government? And the international piece. So we set up sub-groups to make sure that we were looking across the work of all the other working groups as well as bringing to light some of the opportunities or questions or gaps that needed to be brought to life. Alright? So, we developed two separate documents within the working group. The first one is a little easier, its government programs and services that are relevant to an ISAO, and the goal here is to make sure that a standing ISAO or a potentially an Information Sharing and Analysis Organization that already exists has easy access to what is already available. What is your tax payer dollar are already paying for. The goal is not to recreate the wheel, it may be a situation where we are helping them stand up quicker. It may be a situation where we may be able to connect a service that they have or something that they are trying to do with an existing process, system or service. Or even just technical assistance. So that document, we organized it by programs and services and it's provided by various agencies. We are still doing our reach to make sure that we have touched as many agencies as possible that have potential services.

Part of the document aligns to the five cyber security framework functional lifecycle: Identify, Protect, Detect, Respond and Recover. The document is considered to be the starting point. Obviously it is a living documents. Some of those programs won't exist in the future, there will be new programs. And so, we will continue to work with our partners, and it was brought to our attention that recently that potentially there are some state resources or international resources that we need to also put to this document that we may not have considered.

The second document, it's the government relations considerations. So, I have to say that when we started going through this we started to, the goal was to assist ISAO's both new and existing with information relevant to their operations regarding relationships to federal state and local and tribal governments. So, that they had a heads up when they started as to those obligations, as I said hurdles and opportunities that might exists. Eyes wide open. Outlines the scope strategies and outputs concerning the roles of government addresses issues and considerations from the perspective of state and local government. Provides and overview of relevant of federal regulations and ISAO interactions and regulating entities. It is also in the scope of this working group we account for considerations for law enforcement and Intel. So, where law enforcement and intelligence organizations is didn't necessarily submit a part of this document. Clearly we want to make sure that those equities are met. Because part of what the executive order says we are not supposed to tread on treaties. We do not change the laws. Existing regulations still exist. We do not want anyone to have a misconception as they are starting down this process that any of that has changed.

So, part of what we do is not just this document this being created, it's the relationship management. So, NIST 800-150, that is a document on information sharing, there, in the second document, and they have it out for comment, it talks about ISAO's. So, it was really important that we connected the Standards Organizations with NIST, so we can work towards a definition and make sure that two entities weren't saying separate things. That we were saying common things. And then secondly SLTTGCC, so you heard of the 16 critical sectors under DHS infrastructure protection. They also have a group, government coordinating counsel for state and local tribal and territorial. And so, we have been working with them to make sure that there is an alignment. And one of the things that they looked at is regional monitoring. This idea that potentially state county local government entity that tis partnered with companies, entities, potentially providing services to those other counties localities around them or maybe the small business. Whatever it may be we want to understand what those requirements are for services that they might need. Again, it goes back to what was said earlier, there has to be a value proposition, so we are trying to understand the value proposition there. That also will feed into our document.

And then thirdly, the regulatory groups. You heard Jeff Goldthorp this morning. Well, e have been working from the beginning and connecting with the Standards Organization and the Regulatory bodies to make sure, again, that there is some level of alignment, so that we are walking down this path together and there is no surprised on either end and we want to keep doing that. It is turning out to be a very good relationship.

Now, the last piece to this, and it is probably good that it is last because we need to sort of gather up all of this input and all of what the types of discussions that we have had. And it is the relationship with the NCCIC. The NCCIC in DHS (National Cybersecurity and Communications

Integration Center) it's the hub of information sharing for the government. And when we talk about CISA and limited liability protection and those types of things the NCCIC sits in a sweet spot. Of course that is if the entity wants to share information with the government. So, one of the next steps that we will do is that we have to align the Standards Organization work with how the NCCIC will carry out its business. How DHS will connect to those entities and what we should be doing though the Standards on the front end, to make sure that that connectivity actually works. So yesterday we had our working group session and it was pretty good. One of the things that came out of it that I want to sort of highlight here and have a discussion on were all the gaps that we determined. Some of them are just sort of, we don't have as much of an understanding that we need to have, and some of them were legitimate questions based on case studies that have not been created yet.

So one of the first topics was 'protections vary by state'. Each state needs proper mechanisms in place. And so in our current document we talk about how some states have come up with mechanisms to gather information that through that mechanism they don't have to release through FOIA. That is a concern of a lot of states. How are we going to overcome that? Than it came to our attention that apart of CISA allows for that protection. And so we need to clarify better in our document exactly what that means so when an entity at state and local level starts to look at it they at least understand where to go and what they should be looking form. The person that leads that subgroups, Isaac Janak. You want to come out for a minute and just talk about the topic. That is one for the bigger topics for at the state and local level, uh and as we discuss this in a few minutes I want to just make sure that you got it from the person that is leading that work.

Isaac Janak, SWG6: Good afternoon, yes there is something key for states, uh is being able to confidently share information with the private sector without it being released under FOIA. So until yesterday like Mike said that is was brought to our attention that CISA provides protections for states to be able to do that. We were thinking that drafting FOIA language, FOIA exemption language, to withhold that information from FOIA, (pause) FOIA release to public would benefit everyone. So um, yea so that is kind of where we are now.

Mike Echols, SWG6: So before I go on to the other topics you might as well hang around, before I go onto the other topics I want to just provide an opportunity for anyone that has any opinions on that. One of the questions was "guidelines, what we put in a document versus statute". Are we going to create a situation where somebody has a liability situation when they end up in court, or something that they end up having to release something. Is it clear enough that the states have that protection? Any comments or opinions on that? Alright. Thank you sir.

So the next area that we looked at having to also,

Michael Aisenburg, MITRE: With respect, the NCCIC is one of eight threat information sharing center including three that engage in private sector critical information sectors. One thing that has to be worked out post CISA is what is the role of U.S. government threat IS centers as the ISAO process advances? A commercial company doing business with both DOD and commercial business experience and exploit might be conflicted about how and where to share information.

Mike Echols, SWG6: So, I actually think from my presentation this morning from Matt, they are going to put out some guidelines that further clarify. So, you're absolutely correct Michael. There is that confusion because Matt [Shabat] and the guys on the team have heard that regularly and they are working on some clear guidance for ISAOs and ISACs and the sharing with the government.

Michael Aisenberg, MITRE: I have a little follow up to that if I may. Follow statute. This is what DOJ attorney general manual dictates. Follow statute. This is what DOJ attorney generals manual dictates.

Mike Echols, SWG6: And I will do my best to make them follow the statute but, that is their intent. That is their intent, to follow the statute. Thank you Isaac. So, one of the next areas that came up was if we are talking about. It's a sort of a broader discussion. We were talking about the NCCIC and the sharing and we were talking about the fact that ISAOs are self-certify. However, if you are sharing with the NCCIC or any other government entity, almost surely you will have to at some point be, not necessarily certified but, qualified, to some extent. What does that look like? And if we can figure our working with the NCCIC what that looks like we can build it into the process with standards from the beginning for those that choose to share with the government. And so we need to get ahead of that. And a question that comes out of that is: what would be a disqualifying factor for ISAO's that operate [don't operate] according to the CISA guidance?

Kent Landfield, SWG3: So, isn't there today if you want to get a part of the AIS program, isn't there a process that you have to go through to actually become able to connect and use it?

Mike Echols, SWG6: Absolutely, there is a TOU agreement that you sign to become a sharing partner with AIS (automated information sharing). There is a CRADA agreement that is used for a relationship for like CISCP (cyber information sharing collaboration program). With an ISAO for instance, and this is a discussion that came up yesterday also, If we aren't certified and vetting an ISAO, the government is going to a relationship with that ISAO, does it than mean that we need to be looking who the members of the ISAO are and who owns that ISAO? So, each question leads to another question. Alright?

Frank Grimmelmann, SWG1: I think the disclosure of the members organizations could pose some barriers to their desire to engage, and again that is going to depend on the membership organization and the individual members but, requiring to disclose that information may have an adverse effect to what you are trying to achieve as opposed to sharing without attribution through the ISAO or the ISAC itself.

Isaac Janak, SWG6: I think if you're going to um the question is, is the government going to make that distinction, and if you are going to make that distinction of who is fit to share or trustworthy or whatever, when you get it wrong, is there liability to you? You know, so I am just wondering why would the government go down the road of certification beyond signing the interconnect agreement and kind of meeting at that level to participate?

Mike Echols, SWG6: It was a discussion. Kind of a supporting discussion to that was that many companies have multinational components. The idea was posed to have role of government listed. This is a different topic, to have role of government listed in an appendix, this discussion started in the morning yesterday with the leadership group and it lead to the afternoon, that as we are creating these documents, potentially the parts of this document that have a government connection may need to be in an appendix or separate document because a lot of companies are multinational companies and for that purpose, the understand of connecting with the U.S., they need that same understand with connecting with other nations. It is not just U.S. centric and there was the concern that in the way that we approach this, if we make the standards U.S. centric, that potentially we are somehow not empowering all the organizations. This idea that we want to make this ISAO concept open to different types of ISAO's.

Scott Algeiers, IT-ISAC: Seeking clarity, is Mike Echols, SWG6 saying that there will be a separate set of standards DHS will require ISAOs to have in order to share information with the government?

Mike Echols, SWG6: No. Actually, I'm saying that the Standards Organization, at this point, needs to coordinate with the NCCIC through the government relations working group, so that we can clearly understand that prior to putting out this document, and that in doing that, it may afford us some opportunities to develop some standards that makes it easy, up front, for some of the other working grops that we have, to give better guidance upfront to organizations that choose to share with the government.

Mike Echols, SWG6: So, another area for consideration, and it is sort of unique to other government relations working group, dispute resolution. What is the role of government in dispute resolution related to ISAOs? Is it all just going to be done in the courts? Is there some balance? Is there third party? Is there some mechanism? Is there some area that needs to be considered? Some way of doing this that we just hadn't thought about yet because we just got here?

Kent Landfield, SWG3: So what do you mean by dispute resolution? What kind of disputes are you envisioning that would need to be resolved?

[Audio Difficulty]

Mike Echols, SWG6: Not necessarily nefarious activities but, just it could be whatever the dispute is, not necessarily something that is alleged against, well one that might be alleged against another. Is there some third party validator somewhere? And I do not remember exactly how that conversation went.

Kent Landfield, SWG3: So ISAO versus ISAO or ISAO versus government?

Mike Echols, SWG6: ISAO versus ISAO.

Kent Landfield, SWG3: That is usually would be resolved in the courts and not something that would be of concern here, resolution aspects would either be accomplished by membership in trying to determine what they need to do or the board of directors of the ISAO or by the lawyers. And in all cases that is not something the responsibility of the government except for the judicial system in applying and executing the laws that we already have.

Mike Echols, SWG6: So, what if an organization is carrying out activities that are not necessarily criminal but, they are not necessarily what that ISAO says that they are doing or should be doing, is there role of government?

Kent Landfield, SWG3: As far as I am concerned, unless they are breaking the law, then no. It's up to the members of that ISAO. The community has shown in the past they they a pretty good mechanism for identifying those folks and making that public. Um, so if there is issues of, data poisoning or you know, various things that could be negative for the ecosystem, you know, I am quite confident that those around that organization, on external side, would be able to apply things one way or the other that would bring that to light.

Carlos Kizzee, SWG5: So, I really agree with Kent. I almost think that what that is teasing out is, rather than using the term government maybe the right term might be public sector, because you know what we are really saying, the relationship between private and public sector is you know we are going to maybe share information as partners, you know. We are maybe going to collaborate together as partners but, when government is exercising that sort of inherently government authority, to oversee, to regulate things like that, than that is possibly a different role that is not in the context in the sharing environment, right? So, I am going to deal with DHS as a partner and that's why I'm here. I'm going to deal with DOD as my regulator but, not necessarily as a partner. So, I am looking at DHS in the context of information sharing environment as a public sector partner, not necessarily as a government overseer.

Norma Krayem, HK Law: Just to add two pieces to that. One of the things we talked about whether it is within ISAOs or really the federal governments, potential issues and concern with sharing with an ISAOs, I mean a lot of ISACs already will run their membership through the OFAC (Office of Foreign Assets Control) list, sanctions list, I mean there are certain things, I mean they do go to you point about law but, it is about the membership issues within an ISAC or and ISAO for the members to consider but, they are basic things you want to look for. The other thing we talked a lot about in our group yesterday is whether or not and this is not some respect to the ISAOs first do you want a state owned enterprise company a member of your ISAO? Now and ISAO may say I do not care about that and I don't mind if they are Chinese SOESs that are in the ISAO that is one thing for them to consider. I think there are other security consideration for the federal government to consider if that ISAOs connecting to the NCCIC where I think there might be some national security considerations. I think it is a little bit of a messy middle on some of those issues but, those are some things to think about.

Kent Landfield, SWG3: Yeah. I understand but, I also believe that as part of the vetting process going through, that is something that can be vetted out as opposed when you're going through the normal process and trying to connect to the NCCIC and going through that, they have an established process today. I am not sure that it is the jurisdiction of this group to actually try to do some of that, those efforts, although I do understand the national security implications, I understand the 'no foreign' aspects some ISAOs might want to have but, it really comes down to, from the stand point of, again trust, partnership, if you really want to have, you know, a national level sharing program it's that's programs ability to say 'yes' or 'no' you can connect to me. It's like with any other ISAO.

Mike Echols, SWG6: So, you mentioned these mechanisms that exist? That is what we are trying to bring out. So, it is easy to say no government shouldn't do this, X, Y and Z but, if the process, we are not talking to ISAO to necessarily government because the government has a process, ISAO to ISAO. If this is undermined, than a lot of what we are doing, you just mentioned trust, a lot of what we are doing goes away. How do we, or is there… maybe there is no process maybe there is nothing we do but, is there something that should be done? Right, almost like I guess, an example was given of the Olympic doping. They have an organization that manages and everybody participants. Right? Is there a process? Is there something for ISAO to ISAO that will ensure that the process is not undermined?

Norma Krayem, HK Law: I'll just finish a thought and hand over the mic. I think we distinguish in the group, and let Mike opine on this, that the role of this group, that I am in as well, is to say, there is [are] some questions that ISAOs might want to consider thinking about when they are putting themselves together? Right? These are things in the structural component. The other piece that Mike is talking about, I think we were suggesting that if the federal government wants to come up with a different structure, a different vetting, a different something, that would be done potentially outside of this group completely and not to mix the two.

Mike Darling, SWG3: What she said.

Stewart Gerson, EBG Law: The whole point is not to resolve disputes in court that can be avoided. The statement that was just made concerning the government's authority is incorrect. I was once the attorney general and can validate my statement. Litigation is public, time consuming and expensive and an ADR (alternative dispute resolution) mechanism is often attractive.

Carlos Kizzee, SWG5: I think that this is an area where, you know, if we have organizations and we do that have actually been actively engage, you know, in partnership with each other and in partnership with the government, maybe that is a good forum to kind of tee that question up. Before we are sort of pulling new people in and, you know, kind of giving them information, this might be one to go back to PCIS (Partnership for Critical Infrastructure Security), National Council of ISACs and kind of some of the sector coordinating councils and that have been around for a long time and tee that up and see if there is any value or interest in a different role for government in the context of that. I think you will probably get the same answers you are getting from Kent If you did that but, I would strongly recommend looking for a role in that place that would probably be a good place to go to kind of ask those questions.

Mike Echols, SWG6: And then one of the major questions, getting towards the end here, one of the major questions is, what do you need from the government? What role does the government play? I mean if I listen I hear you know in a way people saying the government doesn't play a role. That is an impossibility. Right? This is a partnership. And we have to remember what the basis all of this is for, is to create that net across the country where people can protect themselves. Right? The government has resources, the government has access, so the question becomes, what is the role of government? Because we need for this organization, and we need for the private sector to weigh in, to sort of help build those requirements.

Carlos Kizzee, SWG5: And I don't think I have heard that there is no role, or no desired role for government. At least if that was stated I do not think that was intended from anybody. I think the perspective is, and you nailed it Mike at the end where you were saying that our interaction as partners is going to define asset of requirement. We are in a position to refine a set of requirements for things that will enhance and allow us to enhance or to do what we all want us to do better. Some of those requirements are things that the government, as our public sector partner might like of us, and so capture those requirement, publish those requirements, and let's talk about it. And then some of those might be requirements that industry has that would enhance our ability and do what we are doing better, that are requirements that we would present. I think, what I committed to a few minutes ago, when I was up there [at DHS], I do not think I did a good job at listing those requirements, as good as I could have done. I think you are doing a better job at it than I did and that your time at DHS. So I think more of that is really really helpful. I think that it is a requirements drill, is what it is. What do we need that government is uniquely positioned and qualified to do, and likewise.

Mike Darling, SWG3: So, I think you need to caveat that question in understanding that the government is not monolithic. So, in your working group you got feds, you got state and locals in that sort of thing and so you need to think about it in that way you know? In my mind there are kind of three big umbrellas of what the government does. One is the oversight the regulatory, just making sure American works. There is a law enforcement piece, there is this role in protection in information sharing, and you know, I think you need to parse those things out a little bit because there are different roles in each of those. Um, and you know, if you are just talking about information sharing, just putting my plug in, declassified information. Something that is actionable. Something that has context around it. Context is what matters. Right? Because what we are, if we go back to why we are here, we are here to enable organizations to take actions that will make themselves more secure. You cannot make risk informed decision, you cannot make risk management decisions without the context of what is going on, and that comes with declassification. So, that's my plug on just the information sharing piece.

Bruce Bakis, MITRE: Do you believe that the ISAO constructs can be used introspectively within the government, and by that I mean, can there be an intra-government ISAO? Government to government?

Mike Echols, SWG6: I don't think we need that. I think with… Are you saying within the U.S. government? I don't think we need that. I think the U.S. government just needs to communicate better between agencies, which is different than setting up an ISAO to do that. We are already have that construct. We already have, and now with CISA it tells us that we have to share information so theoretically, the design has been set with these new legislations that tell government to share information better and who shares to who and when and how they share. So we sort of almost created an ISAO in the government.

Michael Aisenberg, MITRE: One core problem in this is the reality of this continuum between infrastructure protection and counter terrorism.

Boris Krutos: Why does the government not mandate information sharing with cleared industry, or not, as part of their contracting process?

Mike Echols, SWG6: So, the whole goal of this is 'voluntary'. We figured out that over a long period of time, that we can accomplish more if we bring more players to the team and they come willingly. And, so in response to that question, yes there are some agencies might just say DOD does require that but, that is not typically the goal across the government because we are going to get a handle on this better by coming up with standards that we all work towards and we all, sort of, determine to do.

Carlos Kizzee, SWG5: I think that is a good answer. I am glad that question is asked because it forces us to think what we are talking about. Information sharing is not an end. It doesn't do or solve anything. Information sharing is an enabler of something. So, when DOD is asking the DIB (Defense Industrial Base) to provide certain types of information, it is to enable enterprise security because it protects national security information and data. Right? It isn't just to make more information sharing. So, the reason that the government can't and shouldn't mandate information sharing because information sharing is not an end. So, the government is acting prudently to get us to do things, to partner together and to enhance what we need to do for a specific purpose, and I think it is good to spend a lot of time on considering what we are here to do. What is that purpose?

Kent Landfield, SWG3: And I want to sort of tag onto that. I think we need to look at information sharing as outcome based. You know what are the things we want to get out of the information that we are getting? If you are an organization there has to be a value to that information, otherwise you are wasting your time and your infrastructure, and other people's resources. You need to be able to apply it. So, when we talk about sharing we can't talk about sharing as an end, as the end all be all, we have to talk about really how we make that information useful and actionable.

Mike Echols, SWG6: So, let me through this last thing out there. That is, if you have an ISAO and that ISAO Is, let's take the government out of this. You have and ISAO and that ISAO is doing nefarious activity again, not necessarily criminal, what do you guys think, is there a marketplace, is there going to be like a Yelp? Does the marketplace sort of saying, don't go to that group that is a bad group, they are doing things, they're not living up to a certain standard, and how does that happen? And that is one of those overarching questions that we have to think through, we are thinking about the work that we are doing, each of these working groups. There are a couple overarching questions and that is one of them. And that is the type of question that government would be concerned about. Right? Because our goal is to protect our citizens. So, how does that work? Any ideas?

Carlos Kizzee, SWG5: Kent and I are probably doing to say the same thing, you know. I went to Morton's last night because steaks at Morton's are really good. I didn't need the government to tell me.

Mike Echols, SWG6: No we took the government out of this. This has nothing to do with the government. This has to do with 200, 300 ISAOs across the country.

Carlos Kizzee, SWG5: Right. So we are smart people. We do market research and we figure it out. I mean if we kind of forget that, than we have become kind of a sheep that are doing what someone else is telling us to do. I think that we are empowering people to make informed decisions, we talked about mentor registry, we talked about also of setting up tools and capabilities. Let the market place kind of work.

Mire Darling, SWG3: I mean I think you see a number of places where things like this, the private sector comes around and does a number of things to, in different places too, that you know give people something to think about how good or bad, you know, in a given thing is. There are bond ratings that tell you know that give you some sense of the risk associated with them, and those bonds are priced differently. The lower the risk the less the return. I think, you know, for me it fundamentally comes back to are you actually providing something of value? I agree with Carlos, I went to Morton's too, and nobody told me but, who I work with told me I need to go there. Um, its, I think it has to start with the data. You know, I probably sound like a broken record but, is the data actually useful? Do you have an organization that routinely gives you good data? That sort of thing. And I think there is a coalescing that will happen naturally that is not necessarily, and that will adjust in a way that the government will not. It goes back to those roles of government, you know, there is little bit of a conflict of interests, across a lot of different industries, you have this oversight role and then we are going to tell you how good they are as well. Um, so that's my thoughts.

David Turetsky, SWG4: Mike, I think some of these are good questions and I think people have different views but, I think sometimes we are not being careful about just how hard the questions are that you are asking because um you know we can talk about ISAO's and who their members are, in state owned enterprises and the like but, in order for that to work there needs to be information and all the members need the information, and there would have to be transparency. Because no market place works without information and transparency. And frankly, when it comes to security threats and state owned enterprises, it's incredibly hard to get real transparency, because when you think about it, when there is an acquisition that may involve a national security issue you have an whole CIFUS (Committee on Foreign Investment in the United States) process that comes into play and investigates and investigates and investigates with multiple agencies to try to figure out whether there is a threat or not and then how to mitigate it. And the notion that your garden variety of ISAO or ISAC, for that matter, is you know, able to have clear rules about state owned enterprises or maybe not state owned but majority owned, or partly owned, and that members are going to understand this and understand who their partners are in an ISAO or ISAC and that they have the kind of information available to them in making that assessment that the government gathers through intelligence and through other means... You know, that is a real stretch. And so I do think this is, I don't have an answer but, I do think this is a very complex issue and I especially understand if the government is going to be sharing with an ISAO or an ISAC, which an ISAO or ISAC doesn't have to share with the government but, I can certainly understand, you know, with all of the access to information the government has, that the commercial sector doesn't necessarily have, that the government would be concerned about, you know, telling entities that may affiliating in some sense with drug operations or with nation states or who knows what. You know everything we have seen in terms of attack vectors you know and which threat indicators we have discovered and characterized that way and the rest, so I don't have an answer but, I think we are being a little over simplistic to talk about the ISAOs and the members just controlling this because it assumes a tremendous amount of insight and information that I don't think is, obvious to me, how they are going to get.

Frank Grimmelmann, SWG1: I wanted to follow up on the earlier foundation comment about identification of member organizations because I think this kind of builds on the same token that might identify a solution. It takes on a big responsibility if you are vetting everybody down on a member level and possibly saying what type of members do you have might address that issue where the ISAO itself certifies to who set the table. As you are aware, we are primarily CIKR (Critical Infrastructure and Key Resources), the question there is fairly simple one, it may be more complex as you get further involved. But on the question to who to share with, there are two, there is one area we chose to share with you, with various programs and that is on the foundation and basis of trust that those that you're sharing with, and in turn sharing with, are a trusted group that you in fact have vetted. The second sharing comes directly with other ISAOs and ISACs and that comes on the foundation of trust with those individual organizations. And they may also be sharing with you but, none the less, we have chosen to share directly at various levels of information. So, I think if we take it as a trust of trust model, that if you trust the ISAOs you are contracting with to effectively choose the members appropriately it is going to allow you to have a much more rapid rollout. Much more effective in getting this in place needing to address an enemy that is not waiting for us to get our act together. And would allow you to leverage, as a force multiplier, the existing ISACs and ISAOS already in place and those you choose to have added in the future.

Kent Landfield, SWG3: And I totally get your point in the stand point of a nefarious types of activities in an ISAO because you can bet that the bad guys are going to use this, like they do every other thing that the put in place, to their advantage. But, at the same time we are really sort of more concerned I think and maybe I am just generalizing things but, more concerned with the automation aspects with sharing between ISAOs where they can actually have some affect outside of the direct membership of the ones that they are trying to work with. We, as was mentioned this morning, have a mechanism that has, it sort of not that new but is one that has been working, it is a matter of now it needs to be a bit more automated, and that's a level of more confidence on the data that you are getting. Sources, honestly, if we are talking about a mesh environment where we are really starting to have ISAOs communicating with other ISAOs at scale, there is going to have to be a way to grade them. To make sure that we can trust them, um and that trust is more electronic in the stand point that I have a real confidence that the data I am getting is something that it can use and I think in a lot of respects we are going to filter out a lot of those bad actor kind of organizations. Maybe not as quickly as we want but we will be filtering out of the system and identifying them rather quickly but, once we get to the point where we have that kind of automated capability and yes it is still years down the road but once we have that kind of ecosystem, um we will be able to than propagate that as an information item to other ISAOs that we participate with and you end up with something like an RBL (real-time blacklist) list where you have a blacklist of email like we used to use in the past or the early days where you didn't want spammers sending you junk so you blacklist'em. So, I think in some respects, we will whitelist'em in the other way. Those ISAOs we trust because they always produce quality will be acceptable to share with. Those that we have any question what's so ever why bother?

Boris Krutos: There is a need for a centralized sharing portal that is aggregated across the industry as a central repository for threat data. I see many non-converged portals.

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