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

Public Comment And Debate: Standards Working Group 1

Speaker: Frank Grimmelmann, Co-Chair, SWG1

Introduction by Dr. Heidi Graham, LMI: The chair of the public comment and debate on ISAO Creation, Mr. Frank Grimmelmann.

(applause)

Frank Grimmelmann, SWG1: Thank you very much. Appreciate it and welcome everybody. I wanted to start out by saying that in our leadership meetings we all concurred that we didn't want to create death by power point for anybody, and so consequently we won't be using any power point slides for summary. Instead, what we want to focus on is giving a high level overview and then allowing your questions to be answered on the assumption that you have had the opportunity to review the material that has been published in order to provide feedback. Should you not have had the opportunity to review that, there is a process for being able to submit comments that is going into place very rapidly that will give you the opportunity to provide your comments after the fact and allow us to have an opportunity to be able to respond to those comments and to adjudicate them as appropriate.

So, let me begin by giving a high level overview and then I'm going to open it up for questions and then we will, if time permits, invite some of our team leads on various topics to give a capsule summary. With regard to our approach, we are the ISAO Creation work group. So, what we are most concerned with is when you are performing an ISAO, what things do you need to think about to be able to be successful in the execution and implementation of your effort for information exchange, analysis and so forth. We looked at four major topics that we felt captured the essence of what was critical. The first of those is the strategic plan. What's the value proposition? Why are you doing this in the first place? The second major point that we looked at is governance. How do you have the interaction between and among the people for what policy perspective? Who's going to be at the table? How they are going to interact? How decisions are made and so on. The third is the operations, the finance, and the funding necessary to be able to support the effort and have it have sustainability into the future. And then finally, our last area is the marketing and communications. How do you outreach to people? How do you create membership opportunities? And how do you, essentially, bring those members to the table once they are targeted as the ones you wish to have at the table. Now, depending on the level of complexity in what you want to undertake, it could be as simple as an association of people informally working together or it could be as complex as some of the existing ISAOs in place that have full automation and everything else. We want to be able to capture all of those areas and provide you with the questions. So, the format we have taken for those of you who may be familiar with Turbo Tax is a very simple interactive question/answer that will ultimately be coupled with a tree diagram that will allow you to skip between what is important to you based on the answers to the questions. We are hoping in the longer term the

Standards Organization will actually computerize this where it would be an interactive online process that would allow for you to interact and be able to go down a simple question and answer, not prescriptive, focused on asking you to think about these subjects and think about how you want to implement it regardless of structure size or anything else. So, consequently, that is the direction we have taken. The first product to be published is a summary level document and that summary level document is giving you an outline of the questions we are going to be tweaking that with the feedback of our own assessments of the first drafts. Then we will be pushing out product with your comments coming back into us. So with that, I would like to take any questions you may have with regard to the product published or the conceptual overview if there are any you may have with this regard.

Q. **Patty Cray, SAE:** You mentioned about your first product, okay, the list of the questions. Do you have a timeline for that?

A. **Frank Grimmelmann, SWG1:** It's already out there as draft and it is on the website so any of the products that have been published you can download now directly from the SO website and that should give you the opportunity to review the detail. We would very much appreciate the commentary on any level. We are going to be refining that as I indicated. The biggest differentiator in first draft is the preliminary review for us. You'll notice in the governance section we had quite a bit of detail on things that were; how do you establish a corporate organization, for example? And since there are associations, so many different varieties, what we want to do is conform the governance section with the other sections which are all more ISAO specific focused and then going into the particular questions you would need to ask as it surrounds that. We will also be providing context because we have white papers underlying many of the individual questions and those are not, again, meant to be prescriptive but rather to provide a framework for you to be able to assess. Example, what type of services you may want to offer to your constituency or capabilities if you prefer to call it that. We also want to adopt common lexicon with the SO which would give us a uniform vocabulary used to cross the various product that are being published by the various work groups. Other questions?

Q. **Brad Howard, ISAO SO:** Frank, I have a question. This is for the creation of new ISAOs. Have you also folded in or considered existing ISAOs, how they might be able to use your products or your way ahead? Thank You.

A. **Frank Grimmelmann, SWG1:** I think it folds directly into the questions and answers. You have many existing corporations that could be for example for profit, non-profit, you have informal information sharing exchange groups of people who are trusted in the community and simply come together and any of those organizations in what we would perceive as the ultimate Question and Answer, can come in. They would already have many of the foundation elements in place. So, if you are talking a major corporate entity, they already know how they operate, they already know how they are funded. So, those questions simply aren't applicable. Questions that would be applicable to them are do they fit the definition of what an ISAO is,

which as Dr. White had indicated, is extremely broad, meaning information exchange for the purpose of protecting cyber security, exposed assets is really the name of the game and virtually anything that is creative or otherwise, would allow you to come together to achieve that objective by definition today is an ISAO. So, it becomes that question of how do we incorporate that and do we as an organization want to fit into that definition with whatever responsibilities and/or opportunities may accrue to it as we continue to go along the curve? Other questions?

Let me call on a couple of our chairs since there don't appear to be [questions] and we have a few minutes. We form committees, originally those committees were collapsed and we created Team Leads, so what I'd like to do cause it's such an important opening stone, invite Tim Evans, who heads our strategic team to come up and share a few words on his perspective on how we are approaching the strategic planning and value propositions.

Q. **Mike Echols, DHS:** My question is, you mentioned value propositions. On the document you talk about the organization. I understand your problem you're trying to solve. So, is that the thesis or the basis for the formation of an ISAO? Is that the thing that's going to make it conceivably viable? Is the idea, that we are actually solving problems and that's one of the first steps?

A. **Frank Grimmelmann, SWG1:** Absolutely, I think it goes without saying that you don't come together to meet just to meet. Unless there's a value which is to find, regardless of the type of entity whether it be government, private sector, etc., fundamentally you are not going to keep coming back to the table, so in order to have value you need to define what is the problem we are trying to solve, how does this align with that problem and why is it we are coming together in the first place? Structure and everything else simply follow. It's a question of, given the value proposition, how you decide to approach it, [and] what structure do you need in place to accomplish that and actually execute against it.

Q: **Tim Evans, SWG 1:** The value proposition is a good question. So, people say, well, what exactly does an ISAO have to do? The bottom line is the market. The market is going to determine whether they succeed in the long run anyway. We had great conversation yesterday. Rick Simon from Intel did an awesome job of commenting on, while we were going through the value proposition, establishing that trust and sharing model, collaboration, are all important things just to think about. Nobody is going to put any determination of whether your value proposition is the right one, the market is going to do that and that's what is kind of the beautiful thing for the ISAOs and that's why it has gone from the public sector only I think to the private sector as well and we are trying to, I know DHS is doing a great job of trying to encourage that, because maybe we all haven't thought of everything that needs to be shared and how it needs to be shared. So, it's going to be a good thing. That's really all I had. I would love to hear everyone's comments on if we have not thought of something we should be thinking about it as you go through it. The strategic planning is upfront, have I thought about

most of the factors that I need to think about? We tried to make it not too long and intensive but enough depth so that you are thinking about what am I going to share, who am I going to share it with, how many people are doing the same thing? You know, those are important things for the market as well.

Q. **Mike Vermilye, JHUAPL:** I just have a question, maybe this is more of the standards organization itself. As these products get developed and delivered and looking at automation to make it easier for people to maneuver through the information in those documents, its maybe taking the questionnaire that you have from the initial document then as the questions gets answered, [seeing that] these capabilities might fulfill the answer to the questions. So kind of integrate the documents and the material and the information going down the road just to make it easier for both organizations that are starting up, plus ones that maybe want to branch out in different directions.

A. **Frank Grimmelmann, SWG1:** Yeah, let me address that because that was a major topic in our leadership meeting yesterday. The working tool that you'll see online when you download it we developed was adapted by the SO to go across to all of the work groups and you'll actually see we've taken, with their permission, we have taken information, for example, from work group 3 and some of the other groups which are dealing with things like privacy and/or information exchange and actually incorporated those already as a tracking mechanism because of the overlap between what you need to think about in creating. Also, organizations coming into play may elect to have capabilities that are very advanced from day one. Even if it's only two or three people, if they have STIX TAXII or other means available to automate efficiently, they could be making contributions on a machine to machine basis from day one. [On] the same token, we do not view anything along the lines of maturity as being important. The question is, what do you need to be able to do to effectively share the information given what you've said was the strategic plan targeting those who you want at the table? So, it may be that informal association with no capabilities beyond communications when you're together or email suffice permanently. So, we are trying in that and that gets us to where decision tree is, to be able to address those types of capabilities whether you are wanting to just start out and figure how to get into it or going up the curve with more capabilities for your members.

Q. **Brandon Workentin, Energy ISAC:** On the list of questions, some of them will have consistent answers across ISAOs like government, does the government require anything to share and receive information? I think it may be more beneficial to instead of post the question, to actually provide that information. Are there any plans to do that?

A. **Frank Grimmelmann, SWG1:** Presently, under the existing executive order, the opportunity to share with government and for government to share are available but not mandated, everything is voluntary. So, consequently, it's up to you whom you wish to share with whether it's just those in your trusted group, ISAO to ISAO. If you remember Dr. White's slide, he listed out all the ways you can share, and again that's all voluntary. You can share with whom you

want, the question is where do you get the value and that's what should be driving the decision.

Q. **Brandon Workentin, Energy ISAC, Cont.:** I don't think I worded it to get what I was thinking. My point was, if my organization goes and researches a question like that, we are going to get the same answer but I put my time into researching and if there are 100 different organizations there are 100 people putting that time in, maybe it would be more beneficial to do that once and provide that information. Does that make more sense? That's kind of what I was going at.

A. **Norma Krayem, SWG1:** Thank you. It's a good question and we have talked about it both in this committee and on governance. But we are also doing this in the privacy and security committee. We have our co-chairs here and what we are doing here is, for privacy and security, what we talk about, if you are going to share with the federal government, some of the system issues are citing to what ISAOs would need to have in place and consider. We talked about having an appendix of sorts of other documents and things that you can cite too. I think that's what you are asking about.

Q. **Roger Callahan, FS ISAC:** In a decision tree type thing model one of the areas I'm curious about is the creation of ISAOs, that's sort of the overall goal. How about encouraging them to join other ISAOs and maybe we could include that in the model. In other words, here is an example, FS ISAC. If people are going to start forming a financial ISAO, are you going to say, Woah, excuse me, there happens to be an FS ISAC or there may be other cases where there's threat analysis group. I'm wondering if there is a discouragement decision tree.

A. **Frank Grimmelmann, SWG1:** I think that it's very simple, as we go through the questions, implicitly in that is what I would call a make vs buy decision meaning, do you want to form your own, do you want to effectively leverage what else may be out there. A lot of times if the real focal point is the sharing of information and you have confidence and trust, it does not make sense to create corporations, to create partnerships, whatever form you would need and if you're talking about an informal exchange it may be good to draw on the capabilities of what's already out there. So as we take people through that "decision tree" part of the process is to get them to think, what in fact is needed to be successful and then the question that is implicit in that is do you do it yourself, you don't have to do it all yourself, or do you draw and establish ISACs, ISAOs, or others for that service, including for profit companies given the way that the executive order is presented.

Q. **Roger Callahan, FS ISAC, Cont.:** If they are going through the questionnaire, it implies that they don't know what the answer is. And so, I'm curious to whether they say look I need to start thinking about, I'm using this as an example, forming a financial ISAC. If they are going through that, they don't know it exists. How are you going to help them know what exists?

A. **Rick Lipsey, ISAO SO:** So, to address the question directly, it's the intent of the Standards Organization to publicize the existence of existing ISACs and other information sharing organizations and to encourage those who are looking for support in this realm, to look to

those organizations first as a means to address their information sharing and analysis requirements. And, if after that exploration, they discover there is not an organization in existence that meets their needs then of course we want to provide them with the information to consider establishing their own organization.

A. **Frank Grimmelmann, SWG1:** I've got a very short answer for that. One of our questions specifically asks who else is providing this information presently and would you potentially be competing with in trying to attract members. So, the question itself doesn't, the resource is through the SO and/or direct websites.

A. **Natalie Sjeline, ISAO SO Support:** Just to add on to that Roger, Yes. We will have those things posted, but in addition to that as the support mechanism one of the first things we will do is ask the questions so if an emerging ISAO comes to us, the first thing we do is take them through a step by step process of "what is it that you really want?" that way we can determine whether they really are looking to become and ISAO or if they really are just looking for that support or to be a part of that information network.

Q. **Azzar Nadvi, DHS:** First of all, thank you both. I really appreciated the path you guys took creating this document. My question is, do you view some of the ISAO startup topics as more critical than others. If so, do you have some sort of plan to maybe mark them as critical, medium/low, 1/2/3, or something of that nature?

A. **Frank Grimmelmann, SWG1:** I think in the breadth of the way we are addressing the topic, it is most critical because it is taking you through a checklist, if you will, of wanting to become an ISAO whether you're an established corporation or not. So everybody has to, at some point, make that decision that they want to essentially engage under the executive order and under the processes that are emerging as the standards in being an ISAO for exchange. So, consequently I think it's core to it, there is overlap with the other work groups that you will be hearing from and I don't want to cut in to any of their topics but we are trying to integrate as part of the total picture we are trying to bring it all together not just you know separately talk about everything involved because every one of the work groups with a lot more depth and there is some areas of expertise in the subject matter are contributing to the overall questions and product.

I would like to then draw, if we could, on our finance operations and funding group because again that foundation that the outset is very important and maybe you would like to share a little bit of overview of your team and what you have been looking on, I see Meeta Sidhu is going to be responding to that again trying to stimulate additional dialogue.

Q. **Meeta Sidhu, SWG1:** I think in the aspect of finance and operations I think there is two kind of components we have been considering from a funding model perspective where the option is whether it be a non-for-profit or profit organizations and from that stand point, what does your membership model look like? Second to that is the cost drivers. It's something that we

also had a good discussion yesterday in terms of trying to be not too prescriptive but enough information to understand that if you are in the instance or the case where you want to set up an ISAO, what are the drivers? Is it cost of promotion, Infrastructure, technology, and those types of things? So kind of giving a checklist, guide, spreadsheet, an assessment tool, so to speak, kind of give those folks whether you are really creating something from the ground up, enough information to kind of guide them through.

A. **Frank Grimmelmann, SWG1:** So, what I would like to do, again if there are any questions feel free to jump in, is to leave you with a key thought. In terms of information exchange, the most important part of the equation is people and people are what, in working together, creates trust. And without trust, there is no exchange regardless of the infrastructure or anything else. So, I would challenge each of you as you are thinking of becoming an ISAO whether established or in a formative stage, that you really put the people that you want to attract to the table first and realize that each of them individually and collectively have the power of one to change the world and the equation of cyber security in this country. And if we forget that, then we forget the essence of what is driving this whole process and that trust needs to extend beyond just private sector, we need to get rid of the silos. It's got to include government. It's got to include, ultimately, law enforcement and intelligence to neutralize the threat at the source. But the decision, and this is your opportunity to make it vs. having it made for you, is for you voluntarily to decide who you trust who you are willing to share with and what is the appropriate infrastructure whether simple or more complex it needs to be wrapped around that to achieve the outcome and objective. I leave you with that challenge and I thank you very much. Are there any last questions? Last opportunity.

Q. **Rick Lipsey, ISAO SO:** First of all, I'd like to say thanks very much to you and Deb for the leadership you've provided. You've come a long way from a dead start in January so my hats off to you. I'm going to toss something that may be helpful as we step through each of the groups and that's to talk about some interdependencies. So, I think as most of the people in this room know, the Standards Organization snapped a chalk line and released a set of documents that are in progress as of May 3rd so they weren't intended to be at any particular state of maturity but to provide an opportunity for the public to take a look at what we have been doing so far and how the groups are progressing and to be asking questions. We still have work to do in terms of integrating those products and coordinating and resolving those interdependencies between the groups and so frank I would like you to address, if you would, please. What do you see as your core principle dependencies on things that you might still be looking for from other groups and what are things that you think your group might be developing that you see as potential influencers to other groups?

A. **Frank Grimmelmann, SWG1:** I think again, as I indicated earlier, the overlaps are fairly significant as we talk about what you need to create and ISAO, privacy comes to the top of my list and willingness to share. Trust comes to the top of the list. The culture you create. So the interdependencies among the groups are total. What we talked about at length in the

leadership conference yesterday was how do we adjudicate and bring together and avoid that overlap in a cohesive document that has consistency. So what we are looking for as a group and what we are requesting is that the SO consider and evaluate writing an umbrella document that incorporates from the bottom up the work groups effort and in turn shares that doc and think of it as an executive summary that effectively lists its comments of the total picture so you're not just looking at one side of the elephant or the other, but the whole animal and being able to evaluate and judge, with that then to push those comments back to the work groups so the work groups have the ability to conform to the feedback that is there and then again have it reflected with the correct language within the summary documents. So I think once we move into this, the adjudication process given the interrelationship of all the work groups needs to be there and we think that should be a responsibility of the SO and allowing the comment which keeps the control at the decentralize level but doesn't have a replication of the work from each independent work group. One thing I finally get to correct, Rick Lipsey, which is a good feeling, I appreciate and on behalf of Deborah, who is at a family reunion this week or would be here, is a phenomenal co-chair, the compliment but truly, our work group as you have seen our team leads is very decentralized and we are composited of a phenomenal group of people who have come together with the right intention of changing the equation to protect critical infrastructure and national security interest and our assets through exchange and it were not for the work group we would not have the work product so I just want to tip my hat to all of our members and thank the core development team, leadership, as well as our general membership. Again, please download the document. We are looking for comments, we are not trying to be prescriptive, we want your feedback. Thank you.

Rick Lipsey, ISAO SO: Thank you very much Frank. I just want to state for the record that the Standards Organization has agreed to adopt the approach that he eluded to. So we will be developing that umbrella executive summary document that serves to help align the work of the various working groups.

Q. **Jamie Clark, OASIS:** In a framework that requires voluntary systems, your guidance will need both a) to help nascent ISAOs discover the existence of other ISAOs, which include ISACs, but also b) to help nascent ISAOs with how to decide on their own whether an existing ISAO or ISAC is fit for purpose for their needs. Contrary to Rick's comment, I have not yet sure that there should be guidance from this group recommending that new projects always should air on the side of joining on the side of a sharing group. One unexplored question is what this group would recommend that existing ISACs and ISAOs should do to, if anything, share with other ISAOs. There are some unresolved issues about how to incentivize inter-ISAO sharing and de-incentivize hoarding when hoarding is not appropriate.

A. **Frank Grimmelmann, SWG1:** I think that's a number of questions and complex issues and given the time I'm going to be as concise as I can be. One of our guiding principles from the first moment was allowing creativity where we are not trying to replicate necessarily what's in the past or foster the imitations by accepting only joining existing organizations, but rather to decide what your objectives are and how you can best meet them; that's the critical element. You always have two options. You either build your own or you rely on something that is already in place, allowing you, if it makes sense if the value proposition is right, to be able to exchange data without having to worry about the overhead considerations. So, our objective is to make sure that there is nothing prescriptive, rather the focus is on what do you need to do and how do you wish to do it. We are simply walking people through the questions they need to ask to come to an informed decision on that with regard to either existing ISAOs or new. And at this point in time what I would direct you to for guidance in that is to publish statement of a definition, a working definition, of what an ISAO is. It appears on the main web page of the ISAOs standards board organization and would allow you to see that it is a very general, very broad, applicability and then you are able to make those decisions.

The other implicit question that was asked is capabilities and those capabilities might include for example, fully automated exchange. On the other hand, if your objective is informal exchange, that's another matter. We think actionable intelligence that is timely is has to drive the equation but as to how you share that, what you share, the format, whether you decide to go with the standard definitions, standard data sets, standard transmissions protocols, use proprietary APIs, that's totally up to you. So, again, the decision is in your hands we simply want to give the roadmap or guidance asking the right questions to assist in making the right decision.

Rick Lipsey, ISAO SO: I'll follow up on the comment that the participant put in writing a more accurate articulation of what I was trying to convey verbally. So, we are not necessarily saying that we want to provide guidance that expresses some explicit indorsement of existing organization over a new organization that might be formed that might be formed that might fit more appropriately for the purpose. We are simply saying that we want to make that information available and encourage people to explore those options.

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