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

Interoperability, Automation and Sharing at Net Speed
Speaker: Dr. Peter Fonash, DHS

Introduction by Dr. Heidi Graham, LMI: So without further ado, I'd like to introduce Dr. Peter Fonash who is the Chief Technology Officer at the Office of Cybersecurity and Communications in DHS. Mr. Fonash has helped several other senior positions to include with the Federal Reserve Board and with the Defense and Other Systems Agency. Please welcome Dr. Fonash.

(Applause)

Dr. Peter Fonash, DHS: So, I'm not going to go over this slide very much [Reference to screen], there's too many people in the audience here that I recognize who could probably do this briefing slide as well as I can. So, I think I will avoid giving you a cybersecurity 101 on what we do. So, what I'm here to talk to you about is really setting up a framework so that we can get a much better cybersecurity then we have today. And what I'm going to do is setup the next few slides as the setup briefing and I say that we basically have problems today, and doing cybersecurity and the problems are getting worse and we haven't yet gotten yet to the Internet of Things. Now this is a chart that was taken from Evans when he was at Cisco. This was the original Internet of Things chart [Reference to screen]. Other people have done updated ones of this. It appears he was a little too optimistic in terms of the number of devices. The number of devices report 2020, I've seen newer numbers coming out that the numbers are lower. But still, it's an astronomically climbing curve. And so we're going to have billions of devices out there and all the hardware venders are really panting over this, they're very excited about this because they'll be selling a lot of hardware. Now, the challenge of this is going to be is that we're not doing a very good job of doing IT security on environments that are controlled by CIOs and CISOs and we're not doing a very good job of Industrial Control Systems Security where we actually have companies that are managing those Industrial Control Systems. Just think about this; where there's no one really in charge.

Now, there's really a Federal Register Notice, I don't know if everyone's aware of that, but that was put out by NTIA that's asking for comments on the Internet of Things. There's a series of questions that's a Federal Register Notice and you can just Google NTIA Federal Register Notice on Internet of Things. There's a series of 20, I think there's so many questions, and it's due back on the 24th of May. But the point of this slide is that there's enormous growth in the scope of the cybersecurity problem. And so, for example, think about this, and this is conceptual, is that I have a home, and in that home I have a refrigerator and a trash can, or recycling bin I should say by that point in time. And so what I do is I finish my last glass of milk and so my bottle is empty and I take it to recycling. Then the recycling bin says "Ah, he is throwing away a milk bottle. He's out of milk." So the next morning I go to work and then what happens is my car, which is connected to my refrigerator which is connected to my recycling bin; my recycle bin

tells the refrigerator “Hey, you’re out of milk, go order some more milk” and then my refrigerator gets in contact with my car and says “By the way, he can’t go home directly, we have to make a stop at the store to pick up milk.” So, I get notified when I get in my car in the afternoon that I’m going to go to grocery store and pick up milk. So, then I get home and I put the milk in the refrigerator. That is a plausible scenario in this future vision of things of the Internet of Things. Who managed the cybersecurity of all of that? No one. Alright? So, the attack surface is going to grow enormously and there’s efforts right now by IEEE there’s a big effort by Intel, MacAfee Security to do a big architecture on the Internet of Things in terms of the Security Architecture, but there’s just nascent efforts from the Federal Government in terms of we don’t even know who’s in charge of the Internet of Things. It’s probably like cybersecurity, it’s everyone’s problem and everyone’s responsibility. I can see NTIA having a role, the FTC has a role, and I think DHS has a role in the Internet of Things. So enormous increase in the surface area of potential attacks in cybersecurity and this covers the Internet of Things, not only covers home use, but also think about it, it impacts every critical structure. It impacts transportation, it impacts finance, and it impacts everything. So all the critical structures are going to be impacted by this as well as the private citizen.

So, this is a reasonably updated slide [Reference to screen which talks about ransomware, where this is our attack surfaces where our attacks are increasing, but now companies are now are actually being attacked by ransomware. I went to a wedding up in Pennsylvania about six weeks ago, and I’m talking to a friend at the wedding he says, and he’s a systems guy, and he says, “by the way, we got attacked by ransomware.” And he starts telling me about how, what happen was is that they got this note about how they had to pay so much money, otherwise they had lost all their data. Well they decided that they were not going to go do the ransomware and they lost all their data and had to go back to two week ago tapes. I didn’t expect to be hearing about this at a wedding, but I did and so I think the types of attacks are also dramatically increasing and the number of attacks are also dramatically increasing. So we got surface area dramatically increasing, the types of attacks dramatically increasing so not a good picture so far.

Now, this is the latest from the Verizon Data Breach Investigations Report [Reference to screen], and I assume everyone is familiar with that report. And in that report there was one in 2013, there’s a curve. I think it was figure 17, I think it was in the 2013 report and what this curve does is it says that the blue line is our defenders, red line is the attackers and what the chart is showing you is that the probability of success, on average, of an adversary getting into a network, within 24 hours. Then the blue line is the probability of the defender actually identifying that attack in a day or less. Now what that shows is that, and this curve, and the dotted line is the actual points. So, you can see that back in 2005, the defenders were about 20 percent successful at detecting an attack and the adversaries were approximately 75 or about 72 percent successful in terms of launching an attack and being successful and getting out. So, they were doing better than we were doing in terms of defending back in 2005. The problem is

now, as you look at this curve, they're almost at 100 percent, and we're maybe only about 24 or 23 percent. So, the problem has gotten worse in terms of the adversary is being far more successful in launching attacks, getting in, getting out then we are at detecting those attacks in a day or less. This was true in the 2013 report, where we're about right here [Reference to screen, and now, this is actually 2015 data and the trend has not changed. We can actually see from the 2015 data point that we've actually gone down from up here in 2014. So we've actually gotten worse in the last year from that data point.

So, now I've said as the surface area, so let me say the last three slides, the surface area and potential attacks is going to grow enormously, types of attacks are growing enormously, and the number of attacks are growing enormously, and our success at defending ourselves from any individual attack is going down compared to the adversaries ability to launch attack and be successful. So, that to make says we need a paradigms shift of how we do cyber security. Our current methods and approaches are not working and we need to change some things.

So, what right now is, is that based on those charts [Reference to screen] the attacker starts an attack, gains network access and he achieves his objective and he gets out within 24 hours and he's gone. And the defender is somewhere and somewhere he figures out that just before the bad guy leaves and takes all the data with him that he's actually under attack and he starts the approach of identifying what the attack is and how to defend themselves and implement a COA, a course of action. So, it's great news is that they've implemented the course of action here [Reference to screen]. And all your data is stolen over here [Reference to screen], there's a timeline, that's where we are today.

So, these are our challenges and this is going to be a build slide. So, our first challenge is, is that, and I talked to all the, and in the federal government and talking to the industry and the large banks is that there's this large tool set, I shouldn't say set. There's a large number of tools, security tools on these large environments and they're multiple tool environments. Everyone has almost every tool set from every manufacturer or large vender and these tools don't work as tool sets. They're not integrated, and so what happens is, is that the CISO of the organization, but not he's only the CISO of the organization, but he's also the systems integrator for the tool set. So he has two jobs. He has the job of trying to get the tools to work together as well as trying to defend his network. And so what happens is, is that the tools don't inter-operate very well, and so that causes time delays, and also causes strain on the operators because the operators are trying to do two things, trying to integrate the tools as well as use them.

The next challenge is that the Internet of Things is greatly growing, and the adversaries are using automated tools. We're not using automated tools because we don't have inter-operability and the defender is not able to detect and respond to intrusions because he's not automated. And also because he's not automated, there's a workforce shortage problem because the workforce is spending most of their time doing mundane things like taking data from one tool and translating into data for another tool. So, right now the cybersecurity industry is awash in data, but have a dearth of good information that can be turned into an act

and actionable information in cyber-relevant time. I think that we at DHS have a wealth of data but we don't have as much actionable information as we need and I think that's true across the industry.

Now, the next one is limited automated authentication, and so where actual identity ecosystems steering working group and we're actually NSTIC (National Strategy for Trusted Identities in Cyberspace) is working this issue and I think it's going to be worked form a technical basis. But the challenge is not just technical. The other part of the problem is the fact that we don't have trust. [Reference to screen] So, trust is going to be an issue and what we need to do is, we not only need to have the technical infrastructure to support trust but we have to have the partnerships and relationships and the actual trust that you give me a piece of information and I will act on that information and not verify it before I act on it. So, once you have inter-operability you can have automation, because you need operability to do automation. Once you have automation inter-operability, then you can put that trust infrastructure into place both the technical piece and the personal piece. Then you can actually get to the point where there's information sharing. So, if you don't have these, above, you're going to have a very hard time doing information sharing in a cyber-relevant time. Then, on top of that is you have to make sure you have a communications mechanism, a secure, reliable security mechanism. One of the assumptions that's has the whole cyber industry, and when we do cyber exercises, we always make the assumptions of [that] communications is available. I don't necessarily think that that could be true. I think that as you go forward, and it's happening already is that when you go to an all IP based infrastructure it's the data is mixed with the control plane and so you're going to be able to attack the control plane and then attack the infrastructure and actually disrupt communications. So, there has to be mechanisms that give you some form of communications so that you can coordinate the response. [Reference to screen]

So, our purposed mechanisms for those solutions, and there better ways of doing it were opened for discussions, but what we believe is that we need to get a common data model so that the tools, so that we get inter-operability. How do we get inter-operability? And I'm going to use the dirty word standards and I don't mean standards in the traditional sense, we're going to do a standards, it's going to take us five years to get it done. I'm talking about the STIX TAXII model where we actually worked with industry and got something done within a couple years. That's what we need to do and we need to get these mechanisms in place so that we now have automation that allows for the analysts to be much more effective and much more productive. The work force problem goes away. We also can now respond in the same cycle time as the attacker can because we're both automated. But we also now have the advantage that we can do automated sharing and we can actually protect ourselves with information we garner from our partners.

I get harassed on this slide lots of times by industry [Reference to screen] and I'm not proposing that this is the only architecture or that this is the only one implementation. The idea is that this is an infrastructure to enable protection as well as to enable information sharing. So, if I

start over on the right here, this is the enterprise level and that security environment is either virtual or real, or actually physically there, so it could be in the cloud. So this could be a cloud implementation. It has connections to the outside perimeter and I'm stealing thunder from my NSA buddies, so these are the things that you do and the processes you go through when you do cybersecurity; Sensing, Sense-Making, Decision-Making and Acting. In other words you sense something, you make sense out of it. What's actually going on? Based on that information you make a decision and then you take an action or course of action. And so what we want to do is we want to get to the point where, through automation at this level, the human is no longer always 'in the loop', but he's mostly 'on a loop'. And what I mean by today he's 'in the loop' is they're busy processing the data from one pool to the other pool. What we want is we want to analyst to be 'on the loop' where he's observing what's going on. If the machine cannot detect something, you know, it doesn't know what to do it will alert the human, and the human has situational awareness of what's going on and says, "Ah, I know. Let me investigate this, this is something that we haven't seen before." But for the most part, we're hoping that the automation and the knowledge base included in this will be able to handle most of the events and take an automated course of action.

Now, we've been working with the NSA for the last couple of years on something called Integrated Adaptive Defense at Johns Hopkins Physics Lab, and those concepts that we presented to you on a previous slide about automation, we've actually implemented them at Johns Hopkins on a partial lab environment, partial real environment of about 300 people and so what we've done is, using orchestration, and we use multiple different tool sets for tools from multiple different venders. We've actually achieved a high level of automation where we actually automated the process so much that we can handle several orders of magnitude higher in terms of events we can look at with the same staffing. We have orders of magnitude increase in speed in terms of detecting and coming up with a course of action, orders of magnitude change. We've also gotten to the ability where we can actually share that information out to a diversity of environments, automated, and automated courses of action that says this is our recommended course of action.

Now, one of the problems with the courses of action is a lot of the times it depends on the environment, and to make sure there's no un-intended consequences. But we've demonstrated that you can do this using some standards based solutions and also using what's called 'orchestration'. Orchestration is just a tool that actually Command and Controls this process so it's really the management of this process. That's what an orchestrator really is. We've achieved dramatic results in that and hopefully we'll be able to incorporate that into future versions of our programs as we go forward. Now, so what's going on here is that there's a lot of information that being contained internally, but it's also through STIX and TAXII and other mechanisms sharing this up to what we call the weather map. That's going to be a DHS implementation, but from your perspective, there's no reason none of your organizations can't have the same capabilities. And what this does, is it does a couple of functions. It takes all these

sources of data, it also has commercial feeds from its partners, all this information that it does analytics on and does that analytics and shares that information out to our partners. This would be our vision of what Phyllis Schneck calls the cyber-web map and with our partners out here we share that information out. We also have a visualization of that. We have a visualization of what we think is actually going on in the infrastructure. But, this could also be the model, or a potential model, for an ISAO or an ISAC, to do these same functions. This would be the different members of that ISAO, this would be some type of capabilities that an ISAO would have, and in particular for its partners and participants in this and then it would share that information out. So, we're not saying that this is just one implementation. This is basically an architecture model view of how DHS is going to do it, but I think its serves as a model for how everyone can do it.

So, [Reference to screen] the whole idea is, that what we do is, we're here [Reference to screen], but what we want to do is, we believe that through the technology that we have helped develop, we can actually get to the left of 'boom' and turn that Verizon chart around. We've demonstrated in the lab and we're actually, potentially going go look at doing some pilots with some prototypes with some sectors in terms of that technology.

So, [Reference to screen] what we want to do with a global point of view, is this is where the endpoint is [Reference to screen], this is where we want to be. This is a maturation process. What I purposed before is going to take years to get industry to come up with an agreement of standards. What we've done is we first of all, we had a request for information and in January 2015, we sent out a request for information. Then had a round table of what we thought were industry and academic experts in terms of what to do. The industry and academic experts told us "Hey government, you go out and don't tell us what the answer is and facilitate us developing the answer."

We've been spending a lot of time with industry with what the answer should be. We've been talking to the major companies. We've also been talking with NSA on an open C2 and open C2 being command and control standard, or really more of a specification. And that's really the command language for an orchestrator, so, in other words, say for example it would be the nouns and verbs an orchestrator would use to take actions so block port X would be an example of the, the verb would be 'block' the noun would be 'port X'. So we're actually working with that and we also, Juan Gonzalez is sitting here, has started an effort with NSA to identify a data model for orchestration for end points and also for network devices. We're going to take that specification, this summer, to the IETF, the SACM at the IETF.

So, those are the things we've got done. So, we've started the journey, and this is hopefully where we'll fully end up in that journey. In terms of at the enterprise level, people are able to defend themselves in a cyber-relevant time. They can also have the ability in an automated fashion to work among the sectors, can work among themselves, and at the national level, cross sector at that level so they can provide them an overview of what's going on that then informs people below and organizations below the big picture of what's going on.

Q/A

Q: **Evan Wolff, Crowell Moring:** When you were talking earlier about the sort of unknown regulatory authority / who's in charge of the IOT, would that, if we asked a question about the industrial Internet of Things meaning SCADA and ICS would your question answer be slightly different. Can you talk about that?

A: **Dr. Peter Fonash, DHS:** So, the answer to the distinguished gentleman's question was that how that relate to industrial systems and the answer, to my point of view, was that we're not dealing with the power grid, and you could argue at some point in time that our smart devices are on the power grid and smart meters are they a part of the IOT or are they part of the SCADA system of a utility. So that gets to gray area, but I'm thinking of like, for example, the Telemax and the car where somebody can download some malware to your car to then causes it to crash for example, or another example is going back to the power grid and the smart meters, if I could overload, if I could start closing harmonics in your thermostats, for an example, on the power grid, I could actually cause instability in the power grid because I'm actually changing the load so quickly I could actually disable the power grid. Now, I don't think the thermostat is part of the power grid, or turning off and on the refrigerators compressor is part of the power grid or the air conditioning system, but that can but an enormous load difference on the power grid and that can cause, the power grid is basically unstable. And so you spend a lot of effort keeping it stable but you can actually introduce instability into that through the internet of things. But that SCADA system that's controlling that power grid, is a SCADA system that's well defined and can be regulated by the electric utility regulators, but nobody is regulating the thermostat or the air conditioning system in that persons home.

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