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

Cybersecurity Information Sharing Act 2015 Update
Speaker: Matthew Shabat, DHS

Introduction by Dr. Heidi Graham, LMI: I'd like to introduce Matthew Shabat, who is director of performance management with the DHS office of Cybersecurity and Communications. As the director of performance management Mr. Shabat contributes to strategic planning, he oversees program performance and he provides business process analysis across his organization. Of note, he led the DHS development of guidance and procedures required by Title I of the Cybersecurity Act of 2015. So please welcome Mr. Matthew Shabat.

(Applause)

Matthew Shabat, DHS: Thank you. Good morning, everyone. So I gave this presentation to the Information Sharing Working Group several weeks back. And they thought it made sense to re-present it here I've tried to tweak it a little bit so that those who have sat through it in either that forum or others will see something new and try to bring everyone up to speed on where we currently stand.

So in December of 2015, the Cybersecurity Act passed as part of the Omnibus spending bill. Title I of the Cybersecurity Act, is affectionately known as Cybersecurity Information Sharing Act (CISA). There were several titles, but I'm really only here to speak to Title I, which really focused on procedures, privacy protections and liability, and other legal protections associated with sharing cyber threat indicators and defensive measures. Title II is important, however, because, whereas Title I designates a capability within DHS, Title II identifies that capability to reside within the NCCIC, the National Cybersecurity and Communications Integration Center. There are several other critical aspects of the Cybersecurity Act, I'm not going to get into details on those today.

So, the easiest way, and it's really one to the more nuanced statutes I've read, and an easy way to think about Title I of the Cybersecurity Act is that it does several things; it authorizes sharing, it identifies permitted uses, with respect to cyber threat indicators and defensive measures, further authorizes monitoring, and it spells out the appropriate and acceptable monitoring, and then it establishes privacy protections. Really those are four key pieces of the act specifically within section 104.

So, it passed December 16th. It was a Friday. I remember because I was driving to the gym and I got a call that said "You're going to be working on implementing this." I hadn't really been paying attention to any of the timelines so I said "Great," and then I think it was a Saturday morning and I actually read through what had passed and I said "okay we have eight weeks to get four documents out, 90 days to also then have a capability in place that's certified."

So, we did and we worked with other agency partners, and it was a very quick timeline. Four documents came out. The first one, are guidelines for the government to share out, if you read it, it's all posted up on the www.us-cert.gov website. That's really a compendium of current activities across the inter-agency for sharing out of the government. The highlighted [reference to screen] one is the one I really wanted to focus on today. And that is guidance to companies and other non-federal entities in terms of how they should be sharing with the government and because of the direction and the statute I think that document has caused a lot of confusion and I'll get into some greater detail on that. The other two were interims. Interim operational procedures that's really speaking to the government and instructing government agencies on what they're supposed to do upon receipt of cyber threat indicators and defensive measures, and then privacy and civil liberties guidelines, which are also directed to federal agencies and the protections that they need to uphold.

So we issued those February 16th, and then a month later, we did have our capability in place. The Secretary of Homeland Security certified it and we've been moving out since then. Now, what's important to note here, obviously, are the last two documents [reference to screen], they're both interim. The finals are due June 15th and we're on track to deliver the final versions. But we all found, I don't want to say odd, but it was definitely glaring, was that the one that's highlighted in red, which was "guidance to companies and other non-federal entities," when we only had eight weeks to prepare it, didn't give us a lot of time to actually go out a solicit comments during the drafting phase.

There's no requirement that we re-issue that guidance, however, we and our co-authors at the department of Justice agreed, based on the feedback we've received the last few months, that we do need to re-issue them, so we're in the process of revising, so we can make some clarifications.

Probably the biggest comment that we heard back was that it didn't really speak to non-federal to non-federal sharing. Right. It was all about non-federal to government because that's what the statute required. So what we're going to have in there as well is more concrete information and guidance about non-federal to non-federal sharing and the protections associated with that. With respect to privacy and civil liberties interim guidelines, that's where you're also going to see the biggest set of changes. Our privacy folks from the department of Justice, and others, really spent a lot of time over the last several months with the privacy advocacy community, taking their feedback, and so you'll see adjustments to that document as well. So this is a summary of what the guidance to non-federal entities included. As I mentioned, you know, this is really the focus of what I want to talk about today. I think this is most relevant: as everyone's considering what an ISAO should look like, and what an ISAO might want to consider.

So, what are the capabilities that we stood up?

I think it's important to have a sense of what's available. So here's the automated indicator sharing capability that was called for [reference to screen]. We called it Automated Indicator Sharing (AIS) and AIS cuts across a number of our information sharing programs. It's really a tool that we set up, and as was previously discussed, the two information sharing standards that are relevant here, STIX and TAXII, are listed up there.

The idea was, that we created, and for folks that aren't familiar, if you take STIX and we're going to have a presentation on that later, but if you take STIX, you have potentially thousands of potential fields that a STIX file could include. Prior to the statute even passing, we, and others in the inner-agency had already gone through a process because we had already stood up a basic AIS capability and went through a process to narrow down those fields. Part of that was for privacy protection. The idea was, "let's figure out which fields are critical to sharing cyber-threat indicators and defensive measures, get rid of all the other fields, and cut down just the possibility that their fields could have free text put in.

We actually went to various operators across various agencies to say which of these fields are important to you. So we have what we call the AIS STIX profile. We actually had to update it after the statute passed because as folks have read the statutes, they expanded the definition of what we had of cyber-threat indicators and defensive measures.

So, we had to add a couple other fields just to make sure it was consistent with the statute, but now we have the AIS STIX profile and that's what we use with sharing over TAXII. The statute also required that we have two other options available; a web forum and an email option, recognizing obviously that they're going to be one-offs, and there are going to be plenty of people who may be interested in sharing and companies and state governments and federal agencies that want to share that just don't have either the sophistication to establish their own native TAXII capability or, for whatever reason, they're not going to be coming across the bulk of indicators that automated sharing is really designed for. So there's also a web form and email option that comes in. They still will be sent out through an automated means, but it's another ingest point for us.

Then, within the capabilities is actually an automated privacy scrub, and I'll get into that in a little bit of greater detail in a short while. So, this, I always thought was a very helpful graphic [reference to screen]. It was in the Guidance to non-federal entities. So, within the statutes there's the definition of cybersecurity information. Then there's the definitions for cyber threat indicators and defensive measures and those are a subset of cybersecurity information. You can find those within the statutes. What's important, though, is that that process of sharing, and what it means to share in accordance with the statute, is very important because that's when the protections attach. Just because an entity shares with another private entity, or with DHS, or with another federal agency, legal protections, or in the case of non-federal to non-federal, or non-federal to DHS, liability protections require that that sharing occur in accordance with the statutes. So, what does that mean? Well, what it really means when you get down to brass tacks, is you have to identify information within the cyber threat indicators and defensive measures and, as noted in the second box there [reference to screen], that the sharing entity has determined to be not directly related to the cyber-security threat, and they know that at the time of sharing.

It's essentially that they know that it relates to personal information. Now this has been a challenge with the documents that the statute itself doesn't define personal information but essentially what you have to do is carve out anything that's not related to the threat that as the time is known to relate to personal information. So, what you're left with is that sort of 'dome' over on the far right [reference to screen] and that's the information that can be shared under the statute.

So, liability protection. As you'll see in the re-issued document, we're going to make it much clearer that liability protection attaches to private to private or state to state or state to private is not just private sector sharing with DHS. Again, as long as the sharing is conducted in accordance with the statute; the act extends liability protection to private and other non-federal entities for sharing cyber threat indicators and defensive measures and that's whether this comes through the automated means, web form, or email.

The Act also extends liability protection, as I mentioned for sharing in between and among private sector entities and, I think, that that's something important to think about in the context of ISAO's.

We had this discussion within the inter-agency that it's important to make sure that the ISAO is not seen as a federal entity. I can't necessarily imagine where that would happen, but that is something to think about because then if a member shares with it and then that ISAO is actually a federal entity that means it's not sharing with DHS therefore the liability protection wouldn't apply. All the other legal protections would presumably still apply, but it's just one of those nuances in the statute that, whether the ISAO is private or not, will impact whether or not that sharing attaches the liability protections. So, I think we point to this URL (www.us-cert.gov/ais), obviously a few more weeks there will be the updated guidance included there. There have been a couple questions about section 106 which speaks to the liability protection, requires that it be shared with DHS and, if truly private to private sharing does receive liability protection, if you read, and the reading we have is, if you read it, it starts off saying that it will be protected and then there's the second piece of section 106 that I think is what's tripping people up is where it says if it's shared with the federal government then you must also do this, but that doesn't mean that you can't share private. I think that's pretty well spelled out in the new guidance that we will be putting out.

So, privacy protections. So, this has been very important to us and this is something that DHS has embedded in its culture. Our federal inter-agency partners as well. So we were very cognizant of the concerns when it comes to information sharing and privacy. So we've built it in, both to the STIX profiles, right, we tried to limit the number of profiles that we had. We also tried to limit the number of potential free text fields because, if you know what you're going to be receiving generally, it can be a lot easier to watch out for things that could trip a privacy concern. Essentially, what we do then, as indictors come in to the automated systems we have an automated capability that will screen and eliminate anything that flashes as potentially personal information. At the same time, if it can't process it through the automated process, it'll actually kick it to an analyst to look at it and this is when it kicks to the analyst. It's also important to note we can't actually use the cyber-threat indicator. It's not actually one of the analysts that could be either sharing it further or putting it into an intrusion detection system that we have, it's actually a separate sort of analyst who actually has to go through and clear it before it can move on into operations and before we can share it out to the other federal agencies.

Now, the beauty of STIX is that there's a versioning feature in STIX and what happens is a STIX file comes in, something flags for human review, all the fields that didn't get flagged can continue on and they'll move in machine speed. And then you use the versioning feature, once they clear that field or whatever fields did flag, it catches up, and the STIX file is updated with the version feature. So, the hope would be that some of the more actionable information; domain names, IP address, malware hashes, that that's the fairly standard form. That the automated check is going to know where is or isn't, and it's going to keep moving through very quickly.

So this sort of gets into the details of the privacy scrub. Now, again, built in multiple layers, plus we have a series of audit checks to make sure the analysts are actually doing the scrub that nothing is making it through. So, for federal agencies, and there's a concept in the statutes of what they call the appropriate federal agencies, and there are seven named agencies in there, those agencies are essentially taking DHS as the conduit in for automatic indicators sharing, and, assuming we are actually conducting the scrub, so that they don't have to then do it. So, we're taking the scrub piece of this very seriously because, otherwise, each of those other agencies would have to invest resources in conducting their own scrubs in accordance with the privacy guidelines.

Although I'm not talking about it in great detail today, one of the other documents which the operational procedures essentially established something that's very important. Under the statute, when indicators and defensive measures come into us, we're not allowed to modify them or delay them, before we send them out to the other six appropriate federal entities which are Department of Energy, Department of Treasury, Office of the Director of National Intelligence, Department of Defense, Commerce, and the Department of Justice.

So, we're not allowed to modify or delay, except for those situations where we've all pre-agreed to those modifications or delays, and that's actually captured in those operational procedures. The only modifications or delays that we have currently all agreed on is the privacy scrubs. So we can modify the cyber threat indicators and delay some of those fields for purposes of the privacy scrub.

So, this is just a graphical depiction [reference to screen], you know, it's obviously probably more complicated than this, but essentially you can see the maroon arrow over on the far right from various partners, which shows how the STIX indicator files with the flow into the TAXII server that we have, then it comes into our automated process, then the next red arrow pushes out anything that can be machine sanitized in real-time.

Anything else that comes to the analysts would then come catch up to it, would push back out to the blue arrow, at the same time, we're obviously taking, we see indicators from multiple sources so if we can provide any enhancements. And so, for example, automated indicator sharing is really designed for quick and bulk sharing and whatever gets shared in, we want to get it out, right?

We've been told by a number of our partners, you know, "don't worry about analyzing it, and get it to us as quickly as you can." There's lots of sophisticated companies that have capabilities, they want to see the indicators and then they'll run their own analytics on them. So we're trying to move them quickly, the challenge obviously is someone could put in an indicator that may have been horribly malicious in the past, it's not being seen as actively in the wild anymore; we would like to be able to then add a score to that, to say, "look you're getting this, you then as a recipient can assess, okay based on the score associated with it." I'm going to then funnel it in for certain actions and say it was scored one to ten, you may, based on your risk profile and if you understand the algorithm we're using to score it, then you could say, one to five, I'm not going to worry about those; six to seven, six to eight I'm going to put in an intrusion detection system, I may funnel nines or tens over to look at intrusion prevention.

Different recipients can use it in different ways, but that's just a filtering option that we would like to start building in, we could also filter, obviously by sector we anonymize it as it comes through. But what sector submitted could still be included, maybe different ISAOs or ISACSs that want to be able to filter by sector, there are certainly sector specific agencies within the government that are probably going to want to get the whole feed. That then will also want to see what type of productivity and defensive measures are generally being reported by members of their sector.

So, these are just some details on how to sign up for it [reference to screen]. We had, or we still have, a program in place that requires a signature of a cooperative research and development agreement (CRADA), and that can take a little while. It's a very lengthy document and we received a lot of feedback that we need something lighter weight, and the National Cybersecurity Act of 2015 actually required we come up with a lighter weight information sharing agreement. So we still use CRADAs for those, it's really for a program that develops strong analyst to analyst exchange, but for signing up for AIS we came up with a Terms of Use, I believe its three or four pages long, it's very lightweight.

These are the processes [Reference to screen]. Federal agencies come in through something different; the multi-lateral information sharing agreement, terms of use however is what we're using for non-federal entities. Then there's obviously setting up a TAXII client or a TAXII server. TAXII client is open source, so you really just need something to put the software on. There's also commercial solutions that use TAXII and a number of solutions that have native TAXII and STIX capabilities that are out on the market. Signing an Interconnection Security Agreement and then exchanging certificates and understanding the IP's, so that we can make sure that we have a trust relationship. There’s going to be lots of indicators coming in, we don’t want indicators coming in from untrusted sources.

So, these are the folks to reach out to if you’re looking for the actual documents [reference to screen]. If you want to access the web form, the email option, you can go to www.us-cert.gov/ais. For additional questions, you know our external affairs team is always available, but if you go to the AIS website, there’s also the TAXII administrator for any entities interested in getting the terms of use and starting the discussion to sign on.

You know, we’re starting relatively small and I think we’ve started to onboard both public and private sector entities and as, you know, we ramp up, we want to make sure that everything scales. And you know we see ISAOs as a very interesting solution and in the guidance to non-federal entities, one of the challenges was that we were focused on explaining how to share with the federal government, so there was a section in there that said private sector companies can share with an ISAO which can share with DHS. And that’s true, and in many cases, that may be the most efficient way to drive sharing, but that doesn’t mean that the company couldn’t share directly with DHS and I do want to point out, you know, companies, ISAOs can share with other federal agencies and they still get a bunch of legal protections. They don’t get the liability protection but there’s protections against federal disclosure laws, there’s prohibition on regulatory use by federal government, by state government. There’s protection against state disclosure laws for private to private. Obviously FOIA (Freedom of Information Act) isn’t a concern, but anti-trust exemption [is], so there’s a number of other legal protections.

I think that part of the reason that’s there is, and I think that everyone whose interested in ISAO understands this; it’s all about trust, right; you share with everyone whom you trust. Overtime you may build other trust relationships and then share there and we don’t want to chill sharing so I don’t think there was any interest in saying you can only share with DHS. There may be entities that have very strong relationships with a sector specific agency; healthcare provider with HHS; they may feel more comfortable sharing there.

They still get a whole number of legal protections, they just don’t get the liability protection and what’s written into the statute and it’s something we are constantly reminding our federal partners is when you receive, as a federal agency, indicators under the act, you’re actually required to share with those seven appropriate federal entities as soon as operationally practical. Then they will get into the system of eventually of who’s the first, what’s the in-door, and ISAO’s making a lot of sense; especially based on who the membership would potentially be, that ISAO will understand how the sharing relationship will best work for their membership. So, very excited to be here, happy to take questions either now or during breaks.

Q&A

Q: **Isaac Janak, Commonwealth of Virginia:** for the preemption of state FOIA, does that only apply if that state funnels it up to DHS?

A: **Matthew Shabat, DHS:** No. That would apply for any non-federal to non-federal sharing so private sector companies share with the state partner or state shares with the state partner. It's a broad protection for states, or for state sharing.

Q: **Roger Callahan, FS-ISAC:** Matt, is there an unintended consequence potentially as a result of the CISA?, And what I mean by that is it encourages sharing of the defensive measures, if their wrong in other words, likely maybe folks don't have to do as much due-diligence now in thinking about defensive measures because they can share it and then protect it from liability. So, might that be an unintended consequence?

A: **Matthew Shabat, DHS:** I think the implementation of defensive measures. I think that everyone has to go in with their eyes wide open. There's an initiative underway right now, I believe it's called the Open C2 group, that's looking at how to automate the defensive measures. So you would want to have a comfort level around a defensive measure before you implement. In some ways though, you know, for example, at US Cert or ICS-Cert or any number of government and private sector organizations, they'll put out mitigation strategies for various things and you still wouldn't want to blindly implement mitigation strategies, you'd want to understand potential consequences and your own environment, but I think that that's a good point. Everyone still needs to understand that these defensive measures are being offered, that they may not be wholly appropriate. They may have been appropriate for whoever shared them or developed them. They may not be appropriate in the environment that they're being received.

Q: **Brian Engle, ISAO SO:** So, CISA describes the liability protection and the private to private and private to government as entities and then we have the Executive Order defining ISAOs, in the prediction for the future do you see any coalescence of the ISAO or how it relates to an independent defined activity that entities as they exist versus how an ISAO might be adapted in that.

A: **Matthew Shabat, DHS:** Are you asking whether we envision the ISAO as a potential entity under CISA.

Q: **Brian Engle, Cont.:** Obviously I think it does but do you think there's anything you see that happens in the future that distinguishes the characteristics of an ISAO versus just no, this just generally applies to entities at large and that sill affords that same protection?

A: **Matthew Shabat, DHS:** From everything I've seen I don't see anything changing. Obviously as we start to implement and as this process keeps moving forward, I think it's going to be interesting to watch and see if anything pops up because we can intercede as necessary or, at least, understand things as designed for one purpose or bumping up against something we hadn't anticipated.

Q: **David Turetsky, Akin Gump:** I co-lead, for the standards organization, the privacy and security working group. I just wanted to get some clarification about what additional guidance may be coming in the final documents. I gather that those are for the June 15th an active area of discussion among some folks yesterday was for private to private sharing. A company sharing with an ISAC or an ISAO in order to get liability protection and who does it attach to? Would the ISAC or ISAO have to do any level of screening itself on privacy or could it just depend on a requirement that it would issue that members screen before they give, in order to get that liability protection.

A: **Matthew Shabat, DHS:** I'd want to look back at the guidance on this especially if this is one of the pieces that's changed. My sense is that the recipient's screen function only applies to federally agencies receiving. Obviously the sharing screen applies to anyone that shares, now if the ISAO received and then further shared there would be an expectation again of that privacy screening.

Q: **David Turetski, Cont.:** Shared with its members or shared with the government?

A: **Matthew Shabat, DHS:** Both. That's my read because it's each instance of sharing.

Q: **Stuart Gerson, EBG Law:** What if a government agency is in the ISAO? Does that make the ISAO a government agency itself?

A: **Matthew Shabat, DHS:** I think that's a good question, I saw that on one of the earlier slides that an ISAO could be private, members could be public, it could be a combination of the two. I think that's something that needs to be assessed. Whether the fact that the government agency is in the ISAO does that make the ISAO a federal entity such that it's not being shared anymore with DHS liability and protection. I think that's a good question and that's partly, probably, goes to how the ISAO is formed and established.

Q: **Jeremy Feigelson, Debevoise & Plimpton:** So, the portal's [DHS AIS portal] been open for a while. Is there anything you can tell us about the experience you've had so far

A: **Matthew Shabat, DHS:** We would like more entities sharing in and we understand the number of at least on the private sector side, the number of entities that are waiting for the June 15th final deliverable to come out, just to see what the privacy guidance especially looks like. We've been putting, I think we've put out a few thousand indicators through the portal ourselves to folks who have signed up so it is definitely open and the system is working. So, we're really just waiting for others to just turn on the taps and our hope is that ISACs may be some of first ones doing it because they're already serving as that trusted intermediary with their partners.

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