ICANN75 | AGM – Joint Session: ALAC and SSAC
Sunday, September 18, 2022 – 13:15 to 14:30 KUL

YESIM SAGLAM: Hello and welcome to joint ALAC and SSAC session. My name is Yesim Saglam, and I'm the remote participation manager for this session. Please note that this session is being recorded and is governed by the ICANN expected standards of behavior. During this session, questions or comments submitted in chat will be read aloud if put in the proper form, as noted in the chat. Taking part via audio, if you are remote, please wait until you are called upon and unmute your Zoom microphone. For those of you in the main room, please raise your hand in Zoom and when called upon, unmute your table microphone. For the benefit of other participants, please state your name for the record and speak at a reasonable pace. On-site participants may pick up a receiver and use their own headphones to listen to interpretation. However, please remember to take off your headsets when using the table microphones in order to avoid the interference. Virtual participants may access the interpretation via the Zoom toolbar.

With that, I will hand the floor over to Jonathan Zuck, ALAC Vice Chair. Thank you.

JONATHAN ZUCK: Hello, everyone. Welcome back from lunch, and welcome to one of our favorite interactions here between the At-Large community and the Security and Stability community. We often experience a lot of instability over in At-Large, so we always appreciate your stable presence in the room. It's a pleasure to have you here, and we have, I think, a real natural alliance given our remit to continue to try and advance the interests of everyday end users where a lot of security and stability issues come about. Do we know if Justine is on the—

UNIDENTIFIED MALE: Andrey.

JONATHAN ZUCK. Okay. The first topic on the agenda is related to the DNS abuse questions. There were questions that were generated by the GNSO small team on DNS abuse that basically amounted to, "What do you want us to do? As the GNSO, what is it you believe is in within the remit of the GNSO and straight up policy development processes?"

We responded with a number of different ideas and concepts, and they have just very recently, in the last two days constructed a preliminary response to those questions. What I'm going to do, though, is skip ahead to listen to the SSAC topic presentation first and retrieve my laptop so that I can dig up Justine's note about those specific reactions. What I would love to do if I haven't caught you off guard here, is hear from SSAC, and then I also want to have a little bit of the DNS abuse conversation with you, because Rod mentioned the idea of a DNS abuse roadmap potentially being in our future, and I think that's something we should work on together.

Without further ado, I'd love to pass the baton to you.

ROD RASMUSSEN: Thank you, Jonathan, and congratulations on your new role. Thank you to the ALAC for having us again. We really appreciate the time, and we know we have a lot of mutual interest in protecting the internet, and the users thereof, so it's always good to get together. I didn't know if Andrey wanted to say a few words, I believe he's online. Andrey. Would you like to say a few things before we get started here?

ANDREY KOLESNIKOV: Well, good afternoon. Good after lunch, everybody. Thank you, Rod, for giving me an open mic.

ROD RASMUSSEN: Not too open.

ANDREY KOLESNIKOV: Yes. I'd like to hear the agenda. Hello Jonathan, hello ALAC, hello SSAC. Nice to see you all. On the agenda, actually, we thought we would start with DNS abuse questions because it usually goes after the presentations of SSAC members and a lot of questions appeared, and usually we don't have time at the end of the meeting to answer all the questions. This is why the agenda looks like this. However, Jonathan thinks that we should start with presentations of the key topics of the SSAC. Then we can start this way. It's the traditional way, let me put it like this, but we live in the untraditional time. It's up to you guys to decide how to go with the agenda.

I'd like to hear the SSAC topics. W be the name collision, of course, with Jim and Matt. Routing security, last time this question actually was very popular, presented by Russ Mundy. Of course, there'll be SSAC new member outreach. It's a traditional topic. There'll be access to the data presented by Steve Crocker and then to the second one for the team, time permitting, led by Rod. Let's start, keep our time running. Thank you.

ROD RASMUSSEN: Thanks, Andrey, and great to see you. We'll try and move through this as quickly as we can. I know we already presented on routing. We've got some nice new, pretty pictures, though that really help explain it better, I think, than we did last time.

Turn it over to Matt Thomas to go give an update on NCAP and the DNS abuse thing is perfect, because I wanted to meld in the discussion, we had around a potential roadmap that Jonathan mentioned we talked about yesterday, so we'll try and get some good time for that. Matt, over to you for a quick update on the NCAP.

MATT THOMAS: Thanks Ron. Matt Thomas for the record, NCAP Co-Chair along with James Galvin. I just wanted to give a quick update today about the Name Collision Analysis Project. I know we had an opportunity with ALAC about a month ago to give a very detailed presentation about the work that's going on in Study Two of the NCAP. I just want to take that up maybe a level here, give a little bit more background and current status for the group.

As you all know, the NCAP has been going on for several years. The NCAP project was structured into three distinct phases. Study One, which was completed a couple of years ago, was the completion of a thorough reference of all name collision information and research to date. This then prompted a revised version of Study Two that we are conducting right now.

Study Two is specifically focused on two main objectives, the first of which is looking at providing some advice to the Board questions that were given to SSAC to answer around the name collision problems, as well as providing some advice on terms of the specific strings corp, home and mail from the 2012 round.

The NCAP discussion group has been meeting regularly to discuss both of those items, as well as doing numerous other research studies in conjunction with the technical contractor hired through ICANN, who has been investigating the ICANN collision reports that were received from the 2012 round. So far, our work group has roughly about 25 members, including 14 SSAC Work Party members. We have a small, 23-set of community observers, and we're currently working through Study Two. Next slide, please.

There have been two main recent publications that have come out of the NCAP discussion group that went out for public comment, the first of which was a case study on the collision strings corp, home, mail, as well as internal, LAN and local. The three additional strings were added because at the time of the study those strings were receiving more than 100 million queries per day to A and J root servers. That study provided a time resolved longitudinal study of the DNS telemetry data seen at A and J root servers for those collision strings, and how they have evolved over time. That has provided some additional insights into the work that we have done, and some of our findings going forward, and it also has helped influence and understand how the alterations of the DNS ecosystem has changed over time due to fundamental things in the DNS protocol evolving.

The second study that went out was a prospective study of DNS queries for nonexistent top-level domains. This study was mainly focused on understanding the implications of where and how DNS telemetry data can be collected and assessed for name collision risk purposes. This purpose really allows us to get some insights into providing some heuristics going forward in terms of how such data measurements can be used to assess risk, and what appropriate guard rails need to be applied when looking at those types of measurements going forward. Next slide, please.

Some of our key findings include some of the items up here. The main one is that name collisions continue to be an increasing, difficult problem and the case studies clearly indicate that. As also seen by the case studies, the root cause of many of these name collision problems still stems from the original problems identified back in the 2012 round by Interisle JAS reports, where DNS service discovery protocols and suffix search lists are a main contributing factor to these problems.

We've also identified via this research a set of things that we have termed critical diagnostic measurements. These are simply a set of tools that quantitatively help assess the specific risk or harm that potential name collisions may pose based off o the telemetry data that we have seen. This is coupled with research in the prospective study that allows us to provide those guardrails for understanding the CDMs, or the critical diagnostic measurements, when looking at these particular vantage points in the DNS hierarchy, such as the root server system.

The main finding that we see in these CDS is that it is both a function of volume and diversity, and that as both of those vectors increase, the difficulty in addressing the risk and harm potentially posed by name collisions also increased. This research, in conjunction with other industry and community presentations has also identified some opportunities for existing measurement platforms, such as the ITHI platform, to be extended to help inform applicants a priori their application for the next round.

Getting the data to the applicants before they submit would be a big benefit to the community because it at least gives them insight before going into the application process about some preliminary findings on name collision risk for that string. Next slide, please.

Speaking a little bit more around these critical diagnostic measurements, for those of you that remember the 2012 Interisle JAS reports looking at risk and harm quantified for the particular applied-for string back then, these critical diagnostic measurements are very analogous to what was used back then, the first of which looks at simply query volume.

Now, well query volume is not a sole indicator of true risk or harm, it can be a leading indicator. The additional metrics, when looking at other properties of the telemetry, such as other versions of diversity, diversity across multiple dimensions, such as IP address diversity, network diversity, ASN diversity, the type of labels that are being queried, the type of queries that are being queried. All of those in combination assess a better way hopefully to quantitatively describe potential impact or harm that may be expressed by a particular collision string.

Of course, these quantitative measurements are not the entire picture. There is also a qualitative element to assessing name collisions, and those will have to be done on a bespoke basis per string. Next slide, please.

Where is the NCAP discussion group right now? We're really into the main development of the Study Two results. We are trying to establish a sustainable and repeatable workflow that provides a mechanism for the Board to assess name collisions going forward. This is along with the advice to the Board's questions and guidance on the corp, home and mail strings being culminated into the Study Two report right now. We are tentatively targeting for this initial report to go out for public comment in the fourth quarter of 2022. Next slide, please.

For those of you that would be interested in joining or contributing, there are the NCAP discussion group meetings. We typically meet on Wednesdays. There's also the discussion group mailing list that you're able to subscribe to and follow as well there. We would appreciate any of you to come along. We are near, hopefully, the end of getting a Study Two report out, but we'd always appreciate any additional feedback or commentary. Thank you.

JONATHAN ZUCK: Thanks, Matt, for your presentation on that. This is certainly an area that historically has been of interest to the At-Large community. Are there questions? We did have a great presentation before the CPWG on this report, but this may be new for some in this room. If anyone has questions, please raise them. Somebody tell me if there are questions in Zoom. I haven't been able to get into Zoom yet.

UNIDENTIFIED MALE: No.

JONATHAN ZUCK: Do you imagine that the net result of this will be a scoring system or something like that for calculation or risk, that will allow a ranking, or is it going to be a more complex set of risk assessments that are then used to put alongside proposed mitigation efforts or something like that? What do you think that's going to look like, ultimately?

MATT THOMAS: That's a great question. I think it's probably more towards the latter at this point. I think there is a fundamental component that the discussion group has come to, and that is that name collisions is a risk management problem, so understanding the risks and being able to profile them and treat them as such going forward is the best course of action for ICANN Board in terms of dealing with them. What we hope to do with the discussion group and the work product is to help provide some of those guardrails and context to help make that a sustainable, repeatable, and deterministic process for all strings.

JONATHAN ZUCK: If you were a betting man, do you imagine that corp or home is ever going to be sufficiently mitigated to be delegated?

MATT THOMAS: I'll defer my opinion and encourage you to go look at the corp/home/mail case study yourself, and you can make your own judgment.

JONATHAN ZUCK: Thank you. Other questions? Anything, Yesim, in Zoom? Okay. Back to you, Rod.

ROD RASMUSSEN: I'll take that bet and I'll say no. Next slide, please.

This is the routing, which we talked about before, but now we have, I think, a much nicer presentation with some more details on it. Russ, if you could run through that. Russ is remote. Please take it away Russ and take us on through this.

RUSS MUNDY: Hello, everybody. I hope everyone had a good lunch there in KL, and everybody else, wherever you may be, welcome to this little presentation on SAC121. As Rod said, we did have an overview of it as nearly published at the last meeting. In fact, it was published during the meeting itself, but thanks to our wonderful support staff we now have a much more thorough set of slides that helps describe the content of the document. Hopefully some of the people may have actually looked at it and read through it, but if not, this is intended to give everybody a good, high-level summary of it. I've got the Zoom on here, of course, that's how I'm getting to you all. Raise your hands or just speak up if I don't stop. I'd love to have any questions at any point during the presentation.

The overview is there. It's really five main sets of things. Let's go on to the next slide, please.

This particular picture is right out of the document itself. It is a description that bears a little bit of time just to walk through things, because it does have an illustration that is hopefully understandable to folks, about an example where someone, Client C, looking like maybe a cell phone there, asks the question, "Where is www.example.net," and that query, that initial question, as a DNS question, goes to his DNS resolver. The way it gets to his DNS resolver is by passing through the bubble you see down at the bottom, AS1, AS2, AS3, to actually get to Resolver D. Resolver D then does what's known as recursion in the DNS. It goes and asks however many authoritative DNS servers it needs to ask to get the answer to that question.

In this case the DNS Resolver D goes to the authoritative DNS Server A, and he gets there by packets passing through Autonomous System 3 and Autonomous System 6. Those, again, the bottom part of the line is an indication of how the packets are flowing, and the upper part, above the line is really an illustration of the DNS protocol itself.

The answer that authoritative DNS Server A sends back passes through AS6, AS3, gets back to Recursive Resolver D, who then sends it back to Client C who asked the original question, and that passes through AS3, AS2, AS1 to get to the client.

This is an example, if one spends a few minutes thinking about, it’s quite astounding how fast all this happens. This happens with every DNS query, packets replying all over the place and they are not only involved in DNS servers, but they are also moved by way of the routing that occurs down the ASs. Let’s go to the next slide, please.

Now, this is [inaudible] of attack. In this case the attack is occurring at AS1. When Client C sends his request to get to Resolver D, it actually doesn’t get to Resolver D, or if it does, he gets a faster answer from the malicious DNS Resolver M at the bottom of the page. This is done by way of a routing hijack. If you look at the red return address that Client C gets, it is a different address than what would be coming from the actual, legitimate, authoritative server. If we go back just one slide, and then look at that same box, you can see the address is different. This is the result of the routing hijack. Next slide, please.

Are there any questions that anybody would like to ask on either of these two? These are quite important concepts to understand. Okay. This is not the only way that a routing hijack can affect the DNS, but it is one good example of how it in fact has been done in the past. Next slide, please.

The potentially most well-known routing hijack that resulted in some very impactful results is what's sometimes called the MyEtherWallet/Route53 hijack. In this case it was a group of criminals, don't know who. As far as I know they've never been identified. What they were able to do was a hijack that was very similar to what we had on the previous slide. What they did to hijack the route was inject what's called a more specific route information into the routing service, and the Route53 DNS service is operated by Google. What they did was they inserted more specific routes for the MyEtherWallet DNS services, and then they, with their malicious DNS machinery, which is what the more specific route pointed the requesters to, were able to steal $150,000, roughly, in about two hours.

The other impact, when the bad guys figured out ways to take money by doing routing attacks, I consider it a waterfall event, because other bad guys are going to try to do the same thing. In addition to the money they stole, which was an impressive amount, $150,000 in two hours. That's a pretty good return for your investment. They also, because of this hijack, essentially put all the other users of Route53 DNS service out of function. What they did was for any DNS query except for the MyEtherWallet, they returned a cert fail. People that were using the Route53 DNS service essentially couldn't get DNS answers.

I see we have a question. Yes, please go ahead, Hadia.

HADIA ELMINIAWI: Thank you. My question here is, would the BGP hijacking attack be identified as a network attack or a DNS abuse incident? How would you call it?

RUSS MUNDY: I would call it both because both of the main protocols were involved. The fundamental first attack was on the routing system, was on BGP, but to make it effective they also had to essentially give malicious, incorrect DNS answers. The giving queries incorrect answers has been a problem with the DNS for many, many years, and if people are not using DNS sec, they are completely vulnerable to attacks like that, that can be done in a number of different ways. This was probably foremost a BGP attack, but also a DNS attack. Is that a clear, understandable response?

HADIA ELMINIAWI: Thank you, yes.

ROD RASMUSSEN: There's a question in the chat, too, Russ.

RUSS MUNDY: Thank you, Rod. I did not see it. Previous diagram, [inaudible]. Yes, the AS4 is also involved in the attack itself, probably. It's not an absolute certainty, but it probably is. The routing system itself is designed to be a set of information that some people have described as rumors that are passed around between people that might trust each other, but maybe shouldn't. We get into some of the things that are needed to improve the security of BGP in the document, but the BGP vulnerabilities have been around for, also, many years. Is that a sufficient answer to the chatroom question?

ROD RASMUSSEN: We also have Sander with a question in the queue. Go ahead, Sander.

SANDER STEFFANN: Hi. You said that it returned a cert fail for all other queries. Did that affect how long it took for the hijack to be noticed? I could imagine that if they actually served proper data for all their other domains it might have taken much longer to detect, maybe.

RUSS MUNDY: I think you are probably correct. These are speculations, but in actuality, if you are doing this type of attack, if you make yourself less visible, then usually it's going to take longer to identify just what's going on. Probably, yes. Any others at this point? Okay, let's go on to the—

JONATHAN ZUCK: Doesn't look like it. Go ahead.

RUSS MUNDY: Thanks, Jonathan. Let's go on to the next slide, please. Here is a set of more textually intense couple of slides here, but what we have identified here and in the document itself, is how there are a number of places where these interactions can occur, and a number of reasons why many of the vulnerabilities that indeed are out there could be improved, if they had all of the security mechanisms in place. For instance, there are mechanisms to identify the actual server that is providing a response to a query. Very few resolvers make use of that. DNS sec is a very strong provisions that would prevent this, effectively DNS poisoning, but end clients, most of them, still don't do DNS sec validation. In the illustration that we have in the document the query wouldn't get to the actual recursive resolver, so that's where the DNS sec evaluation is done for most users that are doing it.

You can see that there are a number of places where pieces can be put in place to strengthen security, and the technology in many cases is available, but it's just actually not there and not in use today. Any questions on this slide itself and any of the content here? Okay. Next slide, please.

With the sequence of this particular attack, one of the reasons that we chose this particular attack to be the example of what the bad guys are doing in the real world is it allows you to see the sequence of events fairly clearly. The result, you can see in the consequences portion, is a big theft that was successful by somebody, and a whole lot of folks that were using Route53 DNS were essentially having no DNS servers for a couple of hours. Next slide, please.

The part of the document that talks about how things can be done to improve the security of the routing system, one of the things that we looked at as the work party went through the effort to put this together and we got good support from the main SSAC and a good number of questions and improvements there that went through out internal process, is that routing security is more than just the technical pieces. The thing that people hear about the most is BGP security, which is good in as much as there are quite a few weaknesses and there are many hundreds of attacks every day.

Now, is something an attack or is it a mistake? If somebody went, "Oops, I shouldn't have done that," or, "That was a fat finger," the reality is, in most cases you're not able to tell if it was intentional or unintentional. The only, and it's a very subtle, subjective indicator, is how quickly the problem is fixed once it's identified and the people who are causing the problem. If it was a fat finger, and a mistake, they'll go, "Oh no," and fix it right away, or as fast as they can. If it's an aggressive attack itself, the people will just disappear and not even acknowledge that they did it. You can't really tell the difference because the results, in almost all cases, look the same to the rest of the internet.

The other aspects that are really important in enhancing routing security are having an accurate routing policy for your operation. If your operation is primarily an ISP operation, then routing is a huge part of that. If you're primarily a DNS centric operation you're probably still doing some routing, or you have service providers that are doing routing for you. You need to understand what the routing policy requirements are and make sure that they are accurate and stay in place.

The other really important aspect of enhancing routing security is operational robustness, and there are a number of things that we talk about in the document. One of the things that we point to in there, some of you may have heard of. It's a group of operators that got together and created a thing called MANRS. It's housed in the Internet Society, and they promote and foster it and so forth. It has a lot of sound principles in it and monitoring as well as good operational security.

Those three aspects are the real cornerstones, and improvements in those areas, in all of those areas, are what's needed to improve the robustness of the routing system. Next, please.

One of the things for the technical routing part, the BGP routing part, is what are known as routing registries. These are essentially databases that provide a mechanism for operators to both place their information in and share it with others, and to get information out of it for use in their system. They have a number of limitations. There are a number of routing registries. It's pretty common to have conflicting information between the routing registries. They don't have a lot of robustness and strengths themselves. Next slide, please.

The Resource Public Key Infrastructure is really an attempt to have a cryptographically verifiable mechanism that permits the receivers of routing information to know if those that originated the routing update were permitted to originate that routing update or not.

JONATHAN ZUCK: Please, keep going, Russ.

RUSS MUNDY: Next slide, please, unless we have questions here. I'll go through this fairly quickly. It is somewhat a different way to illustrate what was on the enhanced operational security. Here's the more detailed approach. The bottom line is operators of infrastructure, whether it's DNS infrastructure, routing infrastructure, need to do monitoring both internal to their system and external to their system. They need to do coordination with other operators. They need to have established cooperation in place and know who to call if they see something go wrong. Also, following the MANRS principles is highly suggested. Next slide, please.

Today, there are routing anomalies happening all the time, literally every day, hundreds usually. Sometimes thousands in a day. To improve the robustness of routing security, this takes really the work of the whole community in multiple ways. Yes, people operating ISPs have the biggest part of it, but others also can contribute, especially if they understand more, to do the things that are needed to improve it. I think you can see the other two bullets are the same there.

We have a question at the top with, gee, it looks like a tree and a ladder. Please, go ahead.

SHIVA MUTHUSAMY: The slide shows that the organization should monitor the roots. Instead, is there a process by MANRS to monitor rogue roots? You might call it by whatever name. Or to identify compromised ASNs or malignant ASNs and take suitable action to streamline the roots, is there an overall design to monitor the entire routing that takes place on the internet and streamline it by some process? Is there a process?

ROSS MUNDY: There is not. There's not a single process, there's not a single monitoring system. There are many monitoring systems. Every operator who has built a system, whether they're doing primarily DNS things or primarily routing things, they need to tailor their monitoring so that they get the insight that they want and need to know if their system is being abused either externally or internally. The operator-to-operator coordination is really the response part. You know you can know, or find out, who to talk to. That's how things are corrected, but the internet routing system, the routing that's done on the internet is massive, involves thousands of activities, and there's no likelihood, at least in my opinion, that there's going to be ever a single, ubiquitous monitoring system.

SHIVA MUTHUSAMY: If I may respond, very briefly, different operators, different ASNs have different levels of expertise. While some may have the intention to secure their routing, a few others may not have the expertise or may not have a clue as to how to fix it, which is why a body like MANRS has to play a role, has to monitor the overall routing, and identify, help them fix the issue or take them out if they're malignant. That's what I was trying to suggest. Thank you.

RUSS MUNDY: There are many open-source capabilities that exist, and you don't have to spend huge amounts of money, although if you have the money to spend you can get better monitoring. It becomes a tradeoff, and oftentimes a business decision. One of the things that we do have as far as recommendations, and we don't have any recommendations for the Board in the document, but for operators, that they have or acquire the knowledge that they need to be able to effectively monitor and respond to routing attacks, and hopefully prevent them. If they happen, it involves your infrastructure, you need to be able to respond.

One thing I would also like to say, this document has an appendix, probably the most extensive list of references of additional material related to routing security of any document I've ever seen or am knowledgeable about. There's lots of information, lots of pointers available in the appendix to the document that will also help people learn more, dig deeper, find answers for themselves.

I think that's the last slide.

JONATHAN ZUCK: Thanks, Russ. This is an interesting document from the standpoint of where its intersection is with either ICANN as an organization, or the community from a policy development standpoint. Does anything come to the surface here as something that we should be trying to think about actively or get on, or is it largely a community-based issue, and we ought to be thinking about trying to use the communication channels we have to get this out as just a resource document to the operator community? Is there something we ought to be doing, either as ICANN, or as the ICANN community, to mitigate any of these risks?

ROD RASMUSSEN: We're going to be briefing the board on this in our session on Tuesday, I think it is. I think that one of the things we'd like to see is ICANN Org getting behind this and disseminating this out to the broader operator community. It's mainly in the DNS space, would be where the issues are. Folks who are doing large scale routing know this stuff, so there's plenty of knowledge for those who show up at the RIRs and the like, but I think that it would be useful for folks that are in the DNS community who may not be paying as much attention to this, as we saw with some of the incidents that have occurred, to have that. Octo and the like have been doing capacity building in this area, so I think this adds to the capabilities and the story that they can tell. That's a discussion that we want to have with the communications team, et cetera, with ICANN Org. Why we bring it here, too, is you have some influence and some ability to disseminate information as well, and I think that as Russ said, we've put together, if nothing else, a compendium that is probably unmatched as far as bringing all these things together.

JONATHAN ZUCK: If you want to read more after reading this, there's plenty to read, is what you're saying. Yes, that sounds thrilling. Let's jump into Julie's presentation quickly so we can get back to DNS abuse.

ROD RASMUSSEN: Yes, I'm going to go ahead and call in audible here. We're going to give Julie just a 30 second blurb. Steve Crocker will be set for a minute or so to talk about the SSAD, and then we're going to skip this stuff on 114. I'm not even sure why we included that. We've already talked about it.

Then we can concentrate on the topic that we wanted to talk about. Julie, I'll give you a brief blurb there, please.

JULIE HAMMER: Thanks, Rod. Next slide, please. As most of you are aware we have a skills survey that defines the types of skillsets we're seeking in a second, that many of our members have. We use that for a variety of purposes, including new member self-assessment and ongoing member updates. Next slide, please. We also use it to identify gaps in skills areas where we'd like to seek new members. We particularly want to share with you these gaps that we're currently looking for new members who might be able to come to the SSAC with some of these skills. We're also trying to increase our diversity in a number of areas, particularly our geographic diversity, with new members from Africa, Latin America and Asia/Pacific, and potentially also new members that might have an academic background and bring with them analytical skills. Next slide, please.

Should you be out and about, or know of people, or be someone that might have skills in those areas, please do approach is. We're going to be looking at doing outreach over the next several months, up until about March and April, and around about that timeframe we look at all of the applicants that might have approached SSAC with an expression of interest. We process those applications as a batch. Please do have a look at the skillset. It's on our website. Point people with the relevant skills in that direction. Next slide, please. Anyone who is interested, please contact Rod, myself, or any member of our wonderful SSAC support staff. Thank you.

ROD RASMUSSEN: Thank you, Julie. Any questions, please feel free to forward them on over to us. We're going to keep moving in the interest of time. Steve Crocker, are you available to chat a bit about where things stand with the SSAD and probably the pilot program, or the pilot system?

STEVE CROCKER: Always ready, Rod. I think we just have the one slide here, right?

ROD RASMUSSEN: Correct.

STEVE CROCKER: Let me give a slightly broader picture. As I think everyone knows, ICANN has been wrestling with the WHOIS problem, or the data directory registration problem for a long time. The current state of play is that there's a lightweight version of SSAD called WHOIS Disclosure. That org is committed to or appears to be committed to trying to build and deploy as rapidly as possible. It is a lightweight ticketing system that forwards requests to registrars. There's very little content in it in the sense of describing what requests will be satisfied or how registrars will handle it.

There's a different part of the whole ball of wax in which the GNSO Expedited Policy Development working group has been engaged in trying to define what the revision to the temp spec is. A huge amount of effort, but carefully avoiding any specification as to what the rules are going to be for getting access to non-public data. There's a massive effect of kicking the can down the road, because when all of the stuff is done, we'll still have the problem of who are the users, what do they need, and how are they going to get that data. Those discussions have been carefully pushed away and we're sitting in an awkward position.

That's my summary of where we stand.

ROD RASMUSSEN: Excellent. Any questions for Steve, me, or other SSAC members from the ALAC on where we are on this one?

JONATHAN ZUCK: Are we anywhere, is the question, I guess.

STEVE CROCKER: Kicking the can down the road.

JONATHAN ZUCK: Yes, kicking the can down the road. If I may, I'd like to put Justine on the spot. Oh, Alan, sorry. Alan Greenberg. I didn't see your name before. Go ahead.

ALAN GREENBERG: Thank you very much. Just one brief comment. I'd like to thank the SSAC and Steve. Steve has been doing a yeoman's job of trying to force the groups, various groups, to actually focus on the real issues, often not very successfully. I certainly appreciate the effort and what he's been putting into this. Thank you to Steve and the SSAC. Thank you.

STEVE CROCKER: Thank you, Alan. Let me say, I think it would be timely and helpful for ALAC to take a strong view as to what's needed overall. No question, Alan has been very active participating, and each of the little working groups has its own rules, but the bigger picture is that this whole thing is not coming together in a useful way. ALAC is one of the primary organizations that represent the people who presumably need the data and can speak on the side of the people who need the data. The people who have the data are the contracted parties, ICANN, the registries, and the registrars. They have no trouble getting organized. Without trying to say anything particularly negative about them, they are understandably focused on how to minimize their risk and how to minimize their expense. Not included in their natural posture is how to provide data to the people who actually need it for legitimate purposes. They'll do it, but they're not spending much time trying to think through those issues and trying to help organize and specify how that can all come together in a nice way.

ROD RASMUSSEN: That is Steve's personal opinion on that.

ALAN GREENBERG: Yes, fair enough.

ROD RASMUSSEN: Not an official SSAC position. However, if you corner some of us in the hallway, we may have some interesting parallel opinions. In all fairness, I think there's a lot of effort going on, but as Steve points out, there are opposing interests, and whenever you have opposing interests, you're going to end up with having to come together for solutions. Right now, I think that we've been pretty clear that access to the data by security practitioners is one of the most important things that we're focused on, and it's just not happening at this point. We all need to come together to figure out how to make that work. We're going to continue with that angle, and I'm sure you will too. We'll keep doing that.

JONATHAN ZUCK: That's been our mantra, yes.

ROD RASMUSSEN: Yes. I think that segues us into the DNS abuse issue.

JONATHAN ZUCK: That's right. Here to give us a short summary of what the response is of the GNSO small team— I'm sorry, I'm just looking for hands in the Zoom, my friend. Go ahead Sebastien.

SEBASTIEN BACHOLLET: Thank you. Steve, I want to come back to this topic, here. One of the reasons I would like to come back is that it's fair enough to ask all the participants in the ICANN community to participate, and I hope that could be a position of the SSAC and not just of Steve. One of the problems, I feel, with that, is if we don't solve the issue of a natural person and an organization, we, as end users, we are in trouble because, I am talking as a European, I don't understand why. It's clearly indicated in the GDPR what's needed to be, either it's data for personal people and not for the organization, therefore we can try to solve by another way this issue, but I don't see how one user will ask to have access to data that needs naturally to be accessible. Thank you.

JONATHAN ZUCK: Thanks, Sebastien. That's definitely an ongoing discussion, and unfortunately the GDPR is worded, permits the differentiation but doesn't demand it. That's part of what's going on at NCS, too, and elsewhere. Those conversations are ongoing. Yes, please.

ROD RASMUSSEN: One quick point on that. From a technical perspective this is an initiative. It's easily solvable. That's all a legal and interpretations issue. It gets outside of the remit that SSAC really feels comfortable talking to. However, we're very comfortable saying, "Technically, this is very solvable. Figure out the law."

JONATHAN ZUCK: Go ahead. We really want to get to the DNS abuse issue.

HADIA ELMINIAWI: Yes, it's just a quick comment about the technical part because we were always told during the EPDP that we're not making this differentiation because of fears of having mistakes, because technical solutions to that are still risky. They're not guaranteed.

ROD RASMUSSEN: Yes, when I mean technical, I mean about storing the data, preserving the data, et cetera, not having some machine figure out whether you're a legal person or a natural person. Let me clarify that because that's, I think, what you're talking about.

JONATHAN ZUCK: Yes, and there are data validity issues and everything like that as well. All right, thank you. We're circling back to the top of our agenda, and while Justine has dutifully passed on to me the results of the GNSO small team on DNS abuse, I thought I'd rather hear it from our liaison, since she happened to wander into the room. Justine, please give us a little bit of description of what you think the outcome of those questions has been.

JUSTINE CHEW: Since you put me on the spot, thank you Jonathan. I don't know which hat I'm wearing now, so don't mind me. In terms of the outcome of the GNSO Council small team on DNS abuse, there was a session earlier this morning, I think it was, no, yesterday. Yesterday, sorry. The report is probably in its final stages. It's still a draft, but they need to do a little bit of cleanup. Essentially there are four recommendations that are being put forward. The four recommendations, in my opinion, speak to high level goals. Again, when we have the meeting with GNSO I would really like input from people to see whether it is specific enough, whether it's satisfactory. I wanted to say that in an earlier GNSO working session where Rod and Julie were there you brought up the possibility of working together. This was something that I was going to bring up in the next session when we do the ALAC policy update.

The way I see it is from the angle of subsequent procedures. You know that subsequent procedures had a recommendation to basically kick it down the line and make it a holistic, community-wide effort, but what has happened, I suppose naturally as well, is we have pockets of effort everywhere. That's what you have identified as well, earlier today, with GNSO. We have different components of the community doing different things. Not necessarily bad things, they're doing good things, but they're working in silos, and that has always been a problem with ICANN. We're all working in silos. The offer that you made to GNSO today to try and work out a framework or lead the development of a framework where we can all work together and piece the pieces together, piece every component's efforts together, I would strongly invite you to invite the ALAC to join that effort. I think ALAC would be wholeheartedly behind it as well.

JONATHAN ZUCK: Yes, thanks. I feel like the GNSO small team response to questions was high level in its current form and involved shuffling the conversation out to others as opposed to doing anything concrete like, "Let's start a PDP," or something like that. That again suggests the need, as you've mentioned over the past couple of days, Rod, of the idea of a kind of roadmap that really lays out the steps that need to take place. I think we'd be very interested in participating in that type of effort.

ROD RASMUSSEN: If I may, let me bring the rest of the folks in the ALAC here up to speed. You and I had the conversation yesterday with the fellow chairs of the other SOACs. Actually, it's interesting. My observation on ICANN right now is there's really good communication at the very top, where the chairs and all that are. We have a lot of coordination, but you can only do so much there when all the work is going on in various subcommittees and the like. The Board is a little bit hands of and not touching the policy side. When you just mentioned the silos et cetera, what we're going to be discussing with the Board is inspiration from their question to all of us around, "What are the things we need to coordinate?" Looking to put together a roadmap, an overview, a plan, et cetera, a strategic plan for taking the high-level goals around DNS abuse, which are already codified, and turning that into a community wide, "Here's how we're going to do this," thing and bring together those efforts. We briefed the GNSO about that today as well, and there was definitely a lot of head nodding and agreement that something like that, especially with the small team report coming out and it sounds like they're pushing things out, "Fine, then let's coordinate what pushing that out means." Our goal would be to help work with the Board and all the rest of the constituencies to put together, from a project/building a product framework, a plan which includes what are the things we're going to tackle. What are the different aspects of the problem throughout there?

It also forces us all to get in some sort of alignment as to what it is we're trying to tackle, what we're going to decide is within the remit of this community to do. One of the points we want to make is for those things that we decide are not within our remit, not just say they're not our problem. Figure out who's problem they are and push that over to them and do it somewhat aggressively if possible. If there's nobody standing out there to take that problem on, maybe we need to reconsider whether or not it's our problem, so to speak. Just a thought. That's a personal observation on that last bit. That's what we're talking about tomorrow or the next day with the Board, with our session. That's already been pre-released, so to speak, to some of the Board, and I know they're like, "It sounds like a good idea. We need to talk about it." We'll see, but I definitely would like to coordinate with the work you guys are doing, the work that GAC is doing, PSWG. There are all kinds of different efforts within the GNSO, various constituencies. There's a lot of work that the contractor parties are doing that's really good work, and we want to coordinate and bring that all together. Let's agree as a community on what the plan is.

The other big benefit of doing that is actually showing that the ICANN community at large, no pun intended, is actually addressing this issue with a plan, metrics and deliverables, because out in the world right now there are a lot of people talking about how ICANN can't solve this problem. "They're not doing anything." There's a lot going on, work gets done a lot, but you can't show results if you don't have a story to tell. Let's put together the story, the plan, and the metrics so we can share that and execute against it. That's the thought. Sorry, I'll get off the soapbox.

JONATHAN ZUCK: No, thanks Rod. This is all about soapboxing, completely, and which one to climb aboard. It's interesting, the Contracted Party House has been doing a lot of work, for sure, and so has the DNS Abuse Institute that sprung out of the Contracted Party House. In fact, the Contracted Party House's subgroup on DNS abuse is having their public meeting right now. Unfortunately, it's very difficult to figure out how to schedule your own meetings so that you're represented at those as well.

I will say that the net-net result of a lot of those efforts has been to try and harden the narrow definition of what constitutes DNS abuse in the context of ICANN's remit. That's something we need to be very cognizant of and make sure that we get on that train willingly. To some extent it has been the At-Large position that we don't need to define it in order to improve it, that even if we accept your definition, your narrow definition right now, there's still plenty to do, and then we can talk about definition. At the same time, that definition is getting hardened, so we need to be careful about what we're seeding. I think that's part of the conversation.

The other part of the conversation is the data itself. There's the business community generating data through Interisle and things like that, and then there's ICANN itself that has DAAR and through blacklists is generating a type of data that's interesting to track. Now the DNS Abuse Institute has just come out with its own measure of DNS abuse, and I will tell you that it really does focus in on maliciously registered domain names. In other words, the idea of hijacked domain names is very quietly being shuffled off to being outside of ICANN's remit, and for our point we need to figure out who that's being shuffled off to, because in theory who it's being shuffled off to are hosting providers. There's a huge overlap between registrars and hosting providers. There's also this community of resellers, so that a wholesaler like Tucows is selling most of their domains through people like Squarespace and Wix and things like that.

Those host providers may very well be the best able to handle a hijacked domain, but the question is, do we just say that's not our problem. Do we need more of those people to be brought in? Is there enough influence among the registrars to make that a community within ICANN? I feel like there are some questions, to your point, about if we pass the ball and it just goes off into space because there's nobody there to catch it, have we really tackled the problem effectively or not.

I want to see if there's anybody that wants to speak up on any of that. I don't see cards in the room, and I don't see hands in the Zoom room. I encourage you all to take a look at the draft report coming out of the GNSO small team on DNS abuse. They did specifically address this issue, again, maliciously registered domains. There's a focus in on that. Honestly, we've focused on that in our response to the questions, but our perspective on that was, "Sure, let's focus on that and address that." It wasn't meant to be at the exclusion of other issues, but some things that we talked about did get through, such as bulk registration and some of the issues associated with operating in volume like that.

I think there was some responsiveness to some of the things that we raised, and we need to make sure and acknowledge that response. I think we definitely would work together with you guys on some kind of a roadmap. Any other questions? Gabriel Andrews, please go ahead.

GABRIEL ANDREWS: Hi, thank for that, Jonathan. I'm not so sure whether I'm asking this question of you or of the SSAC colleagues in the room, but when you mention things like the complexity of the reseller market and the relationship between the wholesaler, registrars and other commercial interests, and then you add in the fact that some are hosts, some might provide email services, some might provide privacy or proxy services, I'm left wondering to what extent there exists a good lay of the land map of all of this. Whether or not the systems that were set up in the first place to track roles and responsibilities way back decades ago is still valid, or whether that itself has been updated elsewhere or if it's in need of updating. Just curious what other folks' thoughts on that are.

ROD RASMUSSEN: Yes, talking about a market map if you will, or a map of infrastructure. I don't know if ICANN has ever done anything like that, necessarily. It gets complex pretty quickly in that you need to understand what type of compromise versus a malicious thing. That's very important and that means these providers are involved with these roles. It becomes a decision tree type of thing, where depending on this knowledge bit then you go a different path, down the way, to deal with the abuse issue, whatever it is.

There are people who've got those kinds of mappings out there. It might be interesting. That might be a great Octo type project if they haven't done something like that already, to say, “Hey, can we have a decision mapping thing around dealing with abuse?” Call it whatever you want, just abuse. Who do you go to for these kinds of things? That’s an academic type of thing, and there are already resources out there that have done that. That might be an interesting thing to do to help inform that planning and coordination effort, because I think that there are still some fundamental misunderstandings for various people who may be in the room trying to make decisions around these things about who all is involved and why.

JONATHAN ZUCK: That’s right. I think we have to face the fact that there does need to be a boundary over what can be considered ICANN’s remit and that it can’t be boundless.

I’ve been given the hook here by staff. We’re a little bit over time. Please join me in thanking the SSAC for joining us here and presenting on these issues.

ROD RASMUSSEN: Thank you for having us.

JONATHAN ZUCK: We’ll keep the conversation going. We’ve got a lot to work on together.

[END OF TRANSCRIPTION]