ICANN81 | AGM – SSAC Briefing to the Community
Monday, November 11, 2024 – 10:45 to 12:00 TRT

RAM MOHAN: Good morning. This is the SSAC public meeting with the community. And I think we have a standard boilerplate to begin the meeting with for the recording, right?

[KATHY SCHNITT]: This session is now being recorded and is governed by the ICANN's expected state standards of behavior. Ram, back over to you.

RAM MOHAN: Thank you so much. My name is Ram Mohan. I'm the chair of the ICANN Security and Stability Committee. And we're pleased to be here with all of you here in the community to share a little bit about what the SAC is doing.

Next slide. So this is what we intend to cover in today's session. We'll have an update from SAC Vice-Chair Tara Whalen on what we've been doing this year, followed by an update from Duane on registrar name server management. The SSAC published a report on this earlier in the year. And following that, Peter, who is also an SSAC member, will provide an update on DNSSEC delegation signer automation, and we published a report on that as well. And after that, we will be open for questions and for an interaction with all of you in the community.

However, before we get the agenda started, I wanted to take a moment to or two even to recognize some of our beloved SSAC people who are making choices to graduate from the SSAC and who are also making choices to go forward in their own life's journey.

The very first person I want to recognize publicly and to thank is someone who has devoted a significant amount of his life at ICANN in dedication to the SSAC and to the work of the SSAC. This is someone who joined the ICANN organization as a staff member supporting the SSAC. I had the pleasure of interviewing him when he applied to the organization. And I was blown away by the ability and the capacity that Steve Sheng demonstrated at that time. The faith that we placed in Steve has been paid back multifold. And Steve, the SSAC is very grateful for your service, for your support, and for your guidance for the work that you have done because you have been much more than support for SSAC. You are one of the people who has made the SSAC what it is. You have been a pillar for the SSAC and you exemplify what we think is the kind of partnership that the SSAC, the community and folks from the ICANN Org ought to have. You are a shining star. You are setting out to a new journey in your life. We support you in that. We really appreciate everything that we've done.

And on behalf of all of the SSAC members, I would like to provide profound gratitude and thanks for you. We from the SSAC got together and we thought that we should not only publicly honor your work and your service, but we have a little gift for you. So please come on up and let's have you with that. And then let's have a standing ovation for Steve.

STEVE SHENG: Thank you, Ram and SSAC leadership. It's been a great journey for me. I personally learned so much from many of you, starting with Dr. Crocker, then with Patrik Faltstrom, with Rod, and then with Ram. So thank you. It's been an incredible journey supporting you. We did a lot of work collaborating together, 30-plus reports, but also seeing the institution being built through the collaboration between the community and the staff. So my best wishes and thank you very much.

RAM MOHAN: Thank you, Steve. Is there anyone else from the SSAC who would like to say a word?

JIM GALVIN: So, along with Ram, I had the pleasure of meeting Steve when he first came on board. He came on as a Fellow to ICANN, and in that assignment, he came to SSAC to work specifically for us. With his contribution and his technical work, he just uplifted our productivity and our ability to move along. It was just him at the time. It was Jamie Hedlund—Julie Hedlund. I got the wrong Hedlund. It was Julie Hedlund and Steve who came on board together, Julie as the administrative support. And Steve came on board as a technical writer. And as Ram said, I mean, with his contribution and his work over the years, just in terms of productivity, if you just look at documents that were published, he uplifted and more than doubled our rate of productivity in the SSAC and our ability to get work done and produce things. And he has risen to being leadership, manager of the entire team, that we

now have that supports SSAC. And it has truly been an honor and just unbelievable what he has done to raise our ability to function in this community and his relationship to the other parties and keeping SSAC to be a part of this community and on the straight and narrow.

So thank you, Steve. With great respect.

RAM MOHAN: Rod?

ROD RAMUSSEN: I want to offer my congratulations and deepest thanks to you, Steve. You and I have known each other for almost 20 years, I think, and I remember seeing you as a, I believe, PhD student and presenting at the APWG many years ago and helping you with your citizenship. And we've known each other for a very long time. It just means so much to me that you've made such an impact on not just the ICANN world but the overall cybersecurity world. Thank you for all your contributions. Not just us at SSAC, but the community at large is going to miss your contributions here. But I'm sure you're going to find great fulfillment and impact in your new career.

So thanks again and we're just going to miss you so much.

RAM MOHAN: I also want to take this opportunity to recognize two of our SSAC members who are deciding to step away from everyday work in the SSAC and graduate to become SSAC alumni. The first of them is sitting

right here: Jaap. Jaap, I remember, when the SSAC got started, you were right there at the very beginning. You're one of the charter members of the SSAC, and in your time here you have always been insightful, engaged, present and provided us just with a wealth of your knowledge and your expertise. We owe a huge debt of gratitude to you. Thank you for all of the service that you have done and thank you for everything that you will hopefully continue to contribute as you move forward in your career. Thank you so much.

Did you want us to take a minute?

JAAP AKKERHUSI: Just a minute or less. It's been a long journey. When SSAC was started, it was actually advisory committee from Stuart Lynn and it was called SAC, and the name started to catch some interesting nickname. So that's why it became SSAC and then became an official at a Board[-instigated] meeting. And yeah, I spent quite some time, and I hope that in future that the SSAC will live and prosper.

And there's one thing I actually want to tell about Steve Sheng: how dedicated he is to this work, which he once demonstrated while we are waiting on a taxi at a taxi stand. He fell asleep standing. He was so tired. That was in Singapore. So that tells something about how much time and effort he put in.

RAM MOHAN: Thank you, Jaap. The other departing SSAC member who I'd like to recognize is Doron. Doron Shikmoni is also stepping away from active

work in the SSAC and will graduate to our alumni group. And he is unfortunately unable to make this meeting either in person or online. Doron, too, along with you, Jaap, was a charter—

JAAP AKKERHUIS: Doron is online.

RAM MOHAN: Oh, he's online. I did not recognize that he was online. Doron was also, along with you, Jaap, one of the chartering members of the SSAC and has been there from the very start and has helped us chart a successful course.

Doron, so glad that you are online. Would you like to take a minute to also share your thoughts?

DORON SHIKMONI: Sure. Thanks, Ram. Just very briefly, it has been a long ride, over 22 years. I do remember the first phone call for recruiting me, and I was told that Steve Crocker was on the line. And the rest of it was blurry because there was no other possible response. But yes, sure, it was a privilege serving on this team. I got to work with some outstanding people. So it was, I mean, really a privilege. And I'd like to thank everyone. And good luck going forward with the committee, with all the future documents and work that the future holds. So thanks, everyone.

RAM MOHAN: Thank you, Doron. All right, the most fun part of this meeting is now done. We will now go to the work part of the meeting. Over to you, Tara.

TARA WHALEN: Apparently I get the non-fun part. Thank you, Ram. So a lot of this is looking back over the year. I guess for folks who have been listening to the changes here, it's been a year of change. We have obviously the change of our departing colleagues, but we are able to benefit from all the contributions that they gave. So we're in a good position. A lot of that is due to the work, I will say, of Doron and of Jaap and of Steve. So thank you for putting us in a good position to continue the work. So you depart, but there have been other changes in SSAC.

And I think one of the themes we looked at was sort of openness. One of those changes that we've had in our culture of SSAC was one of openness.

So next slide please. So here's a picture of us, or many of us, at our workshop in D.C., this past fall.

Next item. There we are. So here's some of the work that all of these happy people were working on. There were three major reports that came out in 2024. So you'll hear a bit more about two of those during this session. So if you want to hear more about the DNSSEC automation and registrar nameserver management reports, you'll get many details coming up. I will also mention the name collision analysis work, though, a substantial body of work that wrapped up this year ahead of the new gTLD round. So that was really important technical analysis work that got done. So that was a big accomplishment.

So if you look at our faces (and you'll see another slide later with the whole group), we had a large number of people join this year. We had an unprecedented number of nine new members this year. We had 27 applications come in from all around the world. So the people that we brought in … We have people now. We have a couple of members from Africa. We've expanded our representation from Asia-Pacific.

Also, the group continues to be one that has a core technical foundation and sort of core technical skills, but we also augment those with expertise from people's own backgrounds, professional skills, professional affiliation. So we have also expanded our representation from registries and registrars and some people that have policy background as well. So we're looking to deploy that as we write our advisories and strengthen those with those perspectives.

But we'll also note, because apparently this bears repeating, that we keep being told that it takes a while for the message to come in that the SSAC meetings are now for the most part open. So, here most of our meetings are open. It's not just the public meeting. So people are welcome to join the meetings and learn more about what SSAC is up to. And I believe that also has had benefits in terms of our recruiting for the membership as well. People are seeing more about SSAC and what it does and finding out how they can fit into the sort of the work that we do. And it also helps us disseminate our work in general because of course, we do write advisories, but it's also helpful for people to hear the distilled version and to be able to ask questions. And more familiarity, we feel, helps get the material out there.

We have a face-to-face workshop every year. And so this, as I mentioned, is where the photograph is from. And this year we had a number of presentations that were done, and we invited people from outside SSAC to give some presentations on a variety of technical topics. So there was also a presentation on AI and DNS abuse. Some of you may have also seen a synopsis, a shortened version of that presentation being given at this meeting. And we had a very interesting panel on quantum computing. So we're keeping abreast of developments in emerging technologies and similarly on DNS and blockchain, which again, we've had lots of questions on from members who want to know more about these technologies. So we're trying to provide some ways in which people can learn more. And again, we opened up these sessions so that more people than just the SSAC could benefit from this expertise.

Next slide, please. So here is a picture of our current full membership. You can sort of see the different regions that we're from. So we feel like we've had a lot of progress in expanding the diversity of our membership in 2024 with the number of people that we have expanded in size. We really are looking to be able to handle the … It seems like there's a never-ending amount of work that needs to be done. This Internet and its security issues always seem to be expanding and becoming more complex. So there's no shortage of work. So we welcome our new members. Some of whom have shown up at this meeting. We've got to see them face-to-face, which has been wonderful. And so we're looking forward to working with them on our work in the upcoming years.

Next slide, please. So, because we have a large body of work, we also looked at how are we going to prioritize our work and how are we going to be more efficient and effective as we carry it out? I mean, we're a large volunteer organization. We're trying to do our best to get reports out, to get advisories to the community, to keep abreast of the concerns of other members of the community and to make sure that our own membership remains engaged, interested and continues to connect with work that they can contribute to in a substantial way and get fulfillment from that. So I won't go into details of all of these areas, but these are our highest goals, the core goals that the leadership team has set for the three-year term that we have that we've now nearly completed year one of. So some of those were inward-looking towards membership.

So you'll notice I mentioned about diversity, enhancing diversity of the SSAC membership, and also looking to connect ourselves. We have more representation into some of the other constituencies and have people responsible for those areas , being sure we develop those bridges and we find out what things are most relevant to those communities and ensure that we're connected and providing them with useful information.

And of course a lot of our responsibility is to be able to provide quality advice in a timely fashion. So we've been looking a lot at the ways in which we work together. We're trying to find ways to be sure that we get our reports out as quickly as we can, particularly as it's very useful for these things to come out. As I said, things change. You don't want your report to come out long after it was relevant. So we're looking at how

we can get our material out and as well looking at ways that we can talk to people, not just through the advisories (for example, we have short summaries of those reports that we want to put out there) to make it easier for people to digest and perhaps then dig further or do things through presentations, as I mentioned, or other forms of media so that everyone can more quickly get a snapshot and get the information that's useful to them.

Next slide, please. And so we do have a lot of topics that we cover. As I say, it's a complex base. But we also identified five topics that we were calling evergreen topics, these ones that are always coming up. They seem to be of importance on a recurring basis. So we're trying to find ways again of taking the work that we've done on this over the years, sort of clustering it around these sort of topic centers, so that you can find that more readily. This is where, for example, we're prioritizing getting summaries of our past work so that people, again, can dig in. When they want to know more, for example, about security and stability issues around new gTLDs, they can go straight to that material. As well, we're just being available as these questions come up, because, again, these are things that are coming up again and again. So we want to be in a position to be able to respond to these, to the community, when they have these questions.

So these are the five. Probably none of these are really of a surprise to people who are here: So, DNS abuse. Somehow we seem to have failed to have solved the problem of DNS abuse. Those security problems don't seem to go away. And DNS, again, is major system, so it's major source for abuse, for online abuse. So these phishing attacks still

happen. The malware distribution still happens. So we are there to try to provide what advice we can on getting ahead of these things and where we can identify mitigations for some of these problems.

Another major topic, a little bit timely right now, is around new gTLDs. So ahead of the next round, there are many issues coming up. I mentioned, for example, the Name Collision Analysis Project. So again, we're looking ahead of what security issues are coming up when there's an expansion of the namespace.

A third issue, again, is one of our significant DNS security technologies: DNSSEC. So this again is a significant technology. It's a core technology, it's a complex technology. So while it also expands its functionality, we also know that people sometimes have difficulty in deploying it correctly. And we want to be sure that as this rolls out, it is put forth in such a way that it delivers on the promise of the security. So we are providing information to help around that for, for example, things like automation, which you will hear a little more about today.

Another topic is on alternative namespaces. This probably came to some people's mind as the blockchain discussions were very active in recent years, where people were talking about deploying additional namespaces for dealing with things like cryptocurrency. But of course, this wasn't the first time that there have been discussions around naming systems that are not based on the DNS. They're a little older than that. And the discussion becomes, what does this mean for the DNS? How do these systems coexist, cooperate, work with one another? And the issues around the coexistence of those alternative namespaces continues to be active.

And finally, we look at issues around Internet governance, but specifically the security and stability issues there. So there are a lot of major issues involving the technological aspects in policy. So with the Internet being again a very large system, a very large global system, there are significant technological policy aspects there. And in our role as technologists, we want to be able to provide good advice for policymakers. People are making decisions on many of these technical policy issues, and we would like them to be grounded in good technical advice. So we're trying to find ways to also ensure that our advice is pitched in a way that can be accessible to someone who is trying to reason about it while they're making some sort of a policy decision.

And so those are our five main topics. Some of our work will bridge between different areas. It may not stay in this. And of course there are some things that fit outside, but these are really our evergreen pillars. We have two new work parties that we've spun up for this year.

We have one on the free and open-source secure software and how it's used in the DNS technical infrastructure and what things were dependent on [it] and what that sort of means in terms of our of the reliability of the systems, the assumptions that people make about open source software, how true those may or may not be, the different dynamics, I guess, at play within open source, where you have large and small players with different amounts of reading resources, maybe differences in liability that may or may not be true. I know I have one of the two of the work party chairs who are welcome if they want to step to the mic. They may to add some meat to the bones or they can nod at me and we're good. All right.

And the other work party we have is on DNS blocking and filtering. So when there is content moderation going on in various kinds, often at a sort of government or regulatory level, where, for access to this content, sometimes the control of that is done through DNS. So it's using DNS for blocking of various types of content.

Now this is, again, not a new thing. It has been going on for some time, and SSAC wrote some guidance around this, but it's more than a decade old at this point. And since that time, both the regulatory political spheres have changed and also the underlying technologies have also evolved. So technologies like DNS over HTTPs, for example, mean that visibility of DNS queries are quite much reduced from what they used to be. And so the responses that are rolled out to try to do blocking have also changed. So we're looking at this again, looking at what has happened since we did that initial advice, and then looking at what we want to put forward in terms of guidance around what are the abilities for DNS blocking, what things it can do, what things it can't do, what unexpected side effects may happen, so that, if you're going to decide to deploy this as a technology, you have a better sense of what the outcome may be, should you choose to deploy that technology.

Next slide please. I'll pause before that to see if we have any questions before we dive into one of our overviews on SAC125.

RAM MOHAN: Yeah, if we could go back to the previous slide, then let's just stop for a moment and ask our community members if you have any questions or comments on this.

John, anything online? No? Okay. All right, let's go to the next slide then. And Duane, you're up.

DUANE WESSELS: All right, thanks, Ram. I'm Duane Wessel for the record. I'm not a full-time SSAC member, but I was invited to participate in this work party since I had been collaborating with KC Claffy and Gautam Akiwate prior to this being brought to SSAC. So this is about SAC125, the report on registrar name server management.

Next slide. Very briefly, the problem statement for this work party was due to the fact that when a domain name registration expires, the domain cannot be deleted if other domains depend on it. Specifically, that's due to a combination of advice from the EPP, RFCs and registry policies that prevent that simple deletion of domains with subordinate host objects within the same registry. So some registrars had been or have been bypassing these restrictions by issuing EPP rename commands for subordinate host objects to other names outside of the registry, which then allows the removal of an expired domain.

And what folks found was that renaming these host objects this way can create what the report calls unsafe sacrificial name servers, and then malicious actors can register those sacrificial name server names and take control or participate in DNS resolution of the domains that formerly depended on that host object.

Next slide. So you might be wondering, what, is this really a serious problem? And the paper from Gautam, KC, and others, which was published in 2021, titled Risky Business, found that there were nearly

half a million domains that were made vulnerable by this practice of unsafe sacrificial name servers. And of those half a million, nearly a third of them had actually experienced potential resolution hijacking due to the registration of some of those sacrificial names.

Next slide, please. So in the work party report, it explores the risks that emerged from this practice, from the expiration of domains that other domains relied on. It explored options for detection and remediation of domains that are presently exposed, as well as practices that could be put in place to prevent new exposures going forward for other domains.

And then for each of those options, the report talks about how the definite options might benefit different parties (registrars, registries and registrants), how it might burden those parties and if there are any residual risks to those parties or to others from implementing some of those options.

And I think the next slide has a table which talks about this a little bit more. This is pretty high-level, this table. There's a lot more detail in the report itself. But again, at a high-level view, registrants are the ones that are most incentivized to sort of solve this problem. They are the ones that experience the risk. The problem is that a lot of registrants are not of sufficient technical expertise or maybe even awareness to understand that the need for remediation or the need to solve this problem. So it has sort of a low success rate for that reason.

Registrars, on the other hand, are in a good position to make some of these changes since they have the ability to make changes to registries. But in some sense they have a misplaced incentive. It's not really in their

interests to take on this extra work and potential risks of doing that work. So we don't see that happening all that often, at least not yet.

Similarly, registries could have a big remediation impact, but generally registries tend not to initiate changes on their own, changes that don't come through registrars. So that also is sort of unlikely to happen.

And then in the case of registries and registrars, they generally would rely on third parties to identify lists of domains that are vulnerable. We could imagine that third parties could also implement defensive registrations. They could defensively register domains that are vulnerable, but that's also a misplaced incentive. And costs are not clear. And it's also not clear what the exit strategy would be for that. So that is also maybe not a great option.

Next slide please. This slide here shows the options that the report talks about for preventing new exposure of vulnerable domains. The first here is that registries could relax their requirements and allow deletion of host objects for expired domains. And there's currently an Internet draft in the Regex Working Group that talks a lot more about this and takes a step to actually make that happen. I believe that draft is nearing the end of its time as an Internet draft and is very likely to become an RFC in the coming months or so.

Along the same lines, the report talks about the same thing, deleting host objects, but also with some kind of notification. And this would be kind of a heavy lift because no such system exists today for making notifications, especially between registries and registrants. But the idea is that if a depending domain was deleted, a registrant would be

notified that that change had been made and then they would be made aware that they need to change something on their own to avoid the risk of resolution hijack.

An option explored was to use a specific domain, EMPTY.AS112.ARPA, as a sacrificial namespace. So registrars would create random nameservers under this. And as112arpa is a sort of a special domain that gets distributed among a large sort of cooperative party. And this would make those domains unavailable to registrants. But it also, at the same time, it does actually create new risks and it distributes these unwanted queries to other parties.

The next option was that each registrar could create their own non-registerable sacrificial namespace for sinkhole domains. And there are benefits and burdens and risks to that. There could be a global non-registrable namespace that registrars and other providers could leverage along the same lines. Again, the idea here is to have a namespace where somebody could not come in and register that and then take over operation of a dependent domain.

And lastly, the report talks about possibly some reserved TLDs or special-use domain names. I think specific ones mentioned are dot-invalid or dot-alt, but we would look to ICANN to advise on specific strings if that was to be a viable approach.

Next slide. So these are the recommendations from SAC125. First is that ICANN registrar and registry communities should collaborate to develop a code of conduct to mitigate these risks that were identified specifically with creating unsafe sacrificial name servers. Number two

is that ICANN. Org should develop and publish statistics around this problem so that we can keep an eye on the scope of the problem, but also understand if any remediation efforts are effective. And then lastly, ICANN Org should engage with registries and registrars to assist in mitigation and prevention efforts as identified by the report and from recommendation two.

And that's the last slide on this topic. Do we have time for questions?

RAM MOHAN: Yes, any questions for Duane? Looks like you get off easy.

DUANE WESSELS: All right, well, thank you very much.

RAM MOHAN: Thank you. Let's go to our next slide. And over to you, Peter.

PETER THOMASSEN: Hi. So this topic might be quite repetitive for those who attend SSAC sessions regularly, but of course this presentation is for those who haven't heard about it. So there's a new SSAC report. It took quite a while to get it out—I think one and a half years, roughly. It was published this August. And it is on the problem of the automation of provisioning DS records in the context of DNSSEC.

So as a starter, if you have signed your zone, in order for a resolver to be able to validate it, it needs to have trust in the key that is used for

validation, and that key is endorsed by the parent domain. So if I have existed example.org with some key, then.org has a cryptographic link to example.org for example, and so that's achieved by putting a DS record into the parent domain. And we're dealing with how that works. Exactly.

“Next slide” is what I was going to say. So when the registrar and the DNS operator of the child zone are the same entity, then this provisioning is an internal operation and it's pretty easy. But that's not always the case. And if those are different entities, then the DNS operator of the child zone in general has no way to talk to the registrar because essentially it has no relation, no authorization, no credentials.

So what happens today is what we call the registrant-centric approach, where the registrant fetches the key details from the DNS operator and relays them to the parent level, which is in this case the registrar, or, for a ccTLD, sometimes the registry. And there's different kinds of formats for this. So there's the key format actually, and then there is a hashed format and there's different fields in it and they have numbers or sometimes instead of numbers they have mnemonics. And it's quite diverse how it could be implemented. And it's done differently at different registrars and different registries. And it's actually quite confusing if you don't know the technical background for this stuff. In addition, you might in fact have to talk to your reseller and not to the registrar, depending on what the business relationships are. And there is a paper that has shown that about 40% of registrants who attempt this procedure do not succeed in actually getting things completed. So that's a problem and that's why the SSAC got together to look into this

problem and consider how automation could improve it. And in fact, there is some automation already and there is some standards. And so I'll tell you some more about it.

Next slide. Yeah, I guess we can skip this one. So next one. Next slide. Yeah, so instead of the registrant talking to the DNS operator, which is what I just explained as the registrant-centric approach, it would be more direct if the registrar would talk to the DNS operator or their servers directly somehow. That would have to be authenticated, of course. And that way, the burden of coordinating this arrangement could be taken off the shoulders of the registrant. So as you can see, the intermediate layer here is completely gone in this approach. That's called the pull-based approach because the registrar pulls the information from the parent and then forwards it to the registry through EPP.

Next slide. This is very similar. It's also a pull-based approach, but instead of the registrar having the hat on for taking the risk responsibility, it's in this case the registry. This is what some ccTLDs do. We're just laying out the solution space. Conceptually, it's not a judgment on which is better. But if the registry gets active, of course, then the registrar's information might not always be up to date when the registry made a change to the DNSSEC configuration. So after making the actual change, there is the last step of the registry informing the registrar that the change has happened. That has its own implications. Not every registrar has a support for receiving such information. So the devil's in detail, as usual.

Next slide. So, on a much higher level, there is the registrant-based approach, which is manual. There is the pull-based approach which I just showed you in the two previous slides. There are IETF standards available for this. There's also conceptually the push- based approach, where the child DNS operator (so the DNS operator for example.org) would somehow contact the parent and tell them, “Look, we have a new set of DS parameters. Can you please publish them?” The question then is, of course, how does the parent know that this thing that they are receiving is actually trustworthy or authentic? So this approach needs credential provisioning. So it needs another kind of exchange between the child and the parent before it actually works. And it kind of is a circular thing, at least it seems, because then instead of DS provisioning, you have a credential provisioning problem. And so IETF standards for this are not available. That's not to say that it couldn't be done, but it hasn't been done so far.

What might bring the best of both together would be a hybrid approach. It mainly solves one downside of the pull-based approach, which is that when the parent wants to fetch stuff from the child operator, they never know when to do that. Like, how does the parent know that there is an update actually for the DS parameters? So they could look daily, for example, and they would have to scan all the domains daily. If you have a large registry or registrar, that's quite a lot of work. And it's also inefficient because most of the time nothing changes. And a hybrid approach would be if one uses the push-based approach to notify the parent that there is a change but not actually have anything sensitive in it, not have the key material itself, and then the parent uses that as an opportunity to perform a pull essentially. So this would be a

combination of notify and then fetch. It's actually a quite small extension of the pull-based approach because also a notify mechanism is used in the DNS for other reasons and it can be reused. And IETF standardization of this is underway, but not yet finished.

Next slide. Yeah, so this is mainly if you want to look at it later or compare things. So on the lefthand column, there's the four different approaches manual and the three conceptual automation things. And it essentially summarizes what I've just told you.

Next slide. So this one has the recommendations from the SSAC report. There's three recommendations. The first one is that if a registry or registrar wants to implement DS automation today for domains that have a DNS operator that is not the registrar itself, then the currently standardized recommended and already in some places deployed method is the pull-based method using CDS and CDNSKEY records. That means that the child domain publishes a set of tentative DS records that are not in the parent yet, but they want to be in the parent. And so then the parent can see that and essentially copy the CDS record as the DS record into the parent after some validation and stuff like that. And as I said before, there's limitations. For example, it's not very efficient, but it works and it might be improved. And if people want to use it, that should be okay.

The second recommendation is that ICANN Org should actually support registries and registrars who want to do this. So some say that this kind of automation is a new registry feature that needs an RCEP process. It would be very nice if this could be just done once as a kind of template thing and then others could use it, reuse it, in the fast-track manner. So

the SSAC recommends that ICANN Org helps with that and makes this possible and not more difficult for parent actors that want to use this than would be necessary.

And the third recommendation is about these shortcomings that I mentioned. I already said that the recommended method today usually is done by daily scanning, which is not very efficient. There's other implications or other questions which are actually not dependent on how the automation is done, not dependent on which method is picked, but the general automation complexity. For example, what do you do if there is a registry lock on the domain? Do you continue with DS maintenance or do you not continue with it? And what about registrar locks, for example? So that's a question that needs to be solved. Another one is what's good TTLs for the DS records after they have been changed? Because the longer the TTL for a DS record, the longer is your rollback period if you mess up. Then there is questions about, if for some reason the update fails, who should receive a notification or error report, if anyone? And do you also report success?

Yeah, so there's all kinds of things and it would be very nice if those aspects could be treated consistently across TLDs so that folks who have several registrations under several suffixes can expect comparable performance. And because of this, it would be nice to have some kind of operational guidance document. So we're planning to work (I don't mean the SSAC, but people in the community) on this. And ICANN Org would be very welcome to be part of this effort so that the result actually is to everyone's liking. We also presented this to the CPH TechOps group and we will, I guess, continue inviting folks to read

whatever the guidance drafts are and come to consensus about how it should be done.

That's all I got. I don't know if there's questions.

RAM MOHAN: Questions for Peter?

PETER THOMASSEN: So maybe the last sentence. The hope is that this will make DNS easier for registrants and reduce the error rate and reduce the number of outages. And that in turn hopefully would make DNSSEC a more realistic technology to use.

RAM MOHAN: Ok, so that brings us to the conclusion of our scheduled presentations. We have a little bit of time available, so. So if members of the community have any comments or questions, we do have a separate open mic session, but this is really our briefing to the community. So if members of the community online or here present in person, if you have questions on what we are doing on the work that is going on, we welcome you to ask or to speak to that.

Online, there was a question from Wataru Ohgai who asked, “Are there some web pages that can read about the ongoing work party discussions?” I responded online that we do not have such a page that provides an ongoing status update. However, at this ICANN meeting, on the two work parties at we have, there are meetings of the work parties.

One of them has already concluded (the DNS filtering one), but, Maarten, I think the other one is scheduled. Right, John?

[JOHN LEVINE]: It's tomorrow, I believe.

[MAARTEN AERTSEN]: Yeah, the Open Source Software Work Party meeting is scheduled for tomorrow in slot [B], 10:30 to noon, local time. And for those of you present here, it's 3B01, and the Zoom link will be in the schedule as well.

[JOHN LEVINE] Yeah, and what we're going to be mostly doing there is fleshing out the starting of the document, getting ideas of what's going into the documents. The work party is just getting started. So this should be a particularly interesting time to observe it and let us know if we're going in right direction there.

RAM MOHAN: Okay. I do not see any questions online. Oh, there's a question here in the audience. Please come to the microphone, introduce yourself and please ask your question.

PAUL FOODY: Hi. Thanks. Paul Foody for the record. Gentlemen, I think what you do is amazing. It's way beyond me. I'm a user and I'm also a registrant. What you do is incredible. The safety and security of our world depends

on you. I, as I say, am a registrant. I use webnames.ca. I have a domain name, foody.com ,which is registered that I don't use but accept for email. Last week I received a 10k email which I read and it was interesting so I saved it as a PDF to my hard drive and then because I was in my guest user (and when you log out of your guest user, everything disappears), I transferred it to a hard drive, an external hard drive. When I transferred it, I noticed it was 67.1 megs. I wrote to webname.ca.. I got the response, "We don't know what's happened. We suggest you change your password." I changed my password, but now I'm terrified. If I send emails, how do I know that, whatever was attached to this 10k email that I received, I'm not then spreading that? Who do I report that to? Because I've tried finding out even here. The only person that has given me any real help is Dave Knight of Vercara. And he suggested I email him. I send the email to him, but I don't want to do that while I'm in Turkey. Who do I report this sort of thing to? I've been to Apple. I've been to the other electronic vendors in Vancouver. Nobody wanted to know. "Oh, just doesn't matter." But 67.1 megs. And I checked back. I got the same email or a very similar email from the same people a month ago. Again, it was 67.1 when I've saved it. Who do I go to with this? Because as a user I'm totally lost.

[BARRY LEIBA]: And generally there's not much of an answer to that. There's a lot of garbage email going around. There's a lot of malware being transmitted through email. PDFs are basically programs, and when you create a PDF, it's sucking down something else from the web that's not part of the email.

PAUL FOODY: But there was no paperclip. There was no attachment. It was a 10k email. So I saved it and I—

[BARRY LEIBA]: Right, but there links in the email that it's following and sucking them down. And there's really no place to report this stuff to.

PAUL FOODY: So how do I know that any other email isn't doing the same thing?

[BARRY LEIBA]: You don't. That's part of the problem with … So one of the biggest problems with email is that the design of it allows people who you don't know to send you things. We want that, but that's one of the downsides of it, that you don't know what they're going to send you. And it's a battle. We're trying to put in place filters that find this stuff and block it, but the bad guys are just as good as we are and get them through.

PAUL FOODY: But doesn't Webnames have a responsibility as a registrar to accept … Because I said, look, I'll send this email to you because it was sent to one email account I have, which automatically sends it to another email account, which is sort of like a trash email account—

[BARRY LEIBA]: The people who are running your email service are doing the best they can to try to block this stuff. [If it] calls for making them legally liable for what they send you, if that were ever to happen, you would just stop getting email because they wouldn't be willing to take that responsibility.

[BARRY LEIBA]: Just real quick, we have a queue going.

PAUL FOODY: Sorry.

[BARRY LEIBA]: No, no, no.

PAUL FOODY: Thank you very much, gentlemen.

[BARRY LEIBA]: No, to answer your question. we have Rod, Robert and then Jothan.

ROD RASMUSSEN: Okay, so anything like that, like file or something that shows up like that, I report to something called VirusTotal. That is the ubiquitous place for any researcher, but anybody from the public can upload a file that they suspect is malicious to that and it'll run out against all the antivirus engines and let you know whether or not that people think it's

malicious or not. So if you're looking for peace of mind whether or not you've been infected with something, that's probably your first step.

The other great thing about using VirusTotal is that most of the security vendors get reports from it. So if you report there, it's likely to be examined and have research done on it, and people probably will figure out whether or not it's bad or not and block it, or send information to your email service provider who would then block it in the future.

So there's this ecosystem set up where you can report things, and VirusTotal is number 1. There's other ones out there. You can just do a Google search for reporting suspicious files. There's several services out there. A lot of the antivirus vendors will take them directly as well. So there are resources out there to actually report these things to. If you get something like a phishing email, you can send that over to the Anti-Phishing Working Group or PhishTank or a couple of other places. So if you think that somebody's trying to fool you into exposing your login credentials and things like that, there are plenty of community resources that you can use to push that over.

For the most part, as Barry said, your email service provider, your hosting providers, et cetera, are taking steps in the back end to try and prevent things. However, as just a regular consumer of one of millions of customers, you're very unlikely to get any special attention if you try and report it directly to them, just because of the amount of things that are out there. If you have a smaller provider, you might get attention because you're one customer in a smaller batch. Or, just like anybody else, if you're the big customer, you get more service, unfortunately. But there are lots of community resources out there and there are places

online you can go as well and find a list of sources as well. So there are places to go. I don't want to take a whole hour to talk about it. There's tons out there, but you just got to do a little bit of research. Thanks.

PAUL FOODY: Thank you.

ROBERT GUERRA: Yeah, so this is Robert Guerra from the SSAC, but I'm also from Canada as well, too. And so this for me triggers a couple thoughts to share, both with you, but also with the SSAC and the community here as well. This is a very typical type of comment that you'll get from a registrant or from an Internet user: where to go. You got a problem, but you want to help and you want to contribute. So I think one of the things that we may want to do is the SSAC is the work that we're doing with the ALAC in regard to cyber hygiene and stuff like that. That is something that really needs to get out there.

I think for you, the suggestion that I would make too, is that while you're here in Istanbul, though you can access a lot of resources and experts that are here, one group you should talk to is CIRA So the people that run dot-ca are actually here. Some of their people are here. There are resources. They have of their own as well, too. They also have settings that you can change on your devices that run through their kind of DNS and stuff like that to try to prevent some of the things. And so I would connect with the Canadian resources, the folks that are here as well. I can follow up with you after this as well. In terms of folks that are here, one of the outgoing, I think, SSAC members, Jacques, should be here,

who's the CTO of CIRA. So he should be here. And stuff like that. So take advantage of it as well, too. But it also raises for me, for the SSAC, that this is a very common type of question and [a] way that we can push out so that it's not just a person that's here that asks a question that gets an answer, but a way that we can push that out so it's known to more people as well, too. They don't have to come to an ICANN meeting in Istanbul to get this answer.

[JOHN LEVINE]: Jothan?

JOTHAN FRAKES: Thank you. Paul, it's great to see you. It's been a while. I'm here with a registrar hat on and I think one of the parts of your question was would webname.ca have some responsibility to you to address this for you? And, candidly, registrars receive reports of varying types and qualities and amounts of data or evidence to help with this. If there was some evidence of phishing or things that would be provided in headers, often they will help you. Many registrars though will just say that's not something we can help you with, that's related to content, or that's not part of the Contracted Party House definition of abuse.

What we're really trying to do is take a radical empathy approach to how confusing it can be as to where to report it. And so often we may say as a registrar, in response to an inquiry such as that, are we providing that mail service? Or maybe you need to talk to the people who are providing that mail service that that originated from because they could troubleshoot it a bit more.

I think you heard some fantastic suggestions from Rod, but in addition to that, for registrars, often the person who's asking the question, I think there's an educational hurdle with respect to understanding these because they can get very complicated very quickly as to troubleshooting or knowing where to route it. And so what we've been trying to do is include, in addition to "Hey, it's not us," saying things like, "You can also try these things in order to help people," so that there's not sort of a dismissive message or a negative customer experience in order to help that process. And it sounds like you still kind of ended up a little perplexed as to where to talk, but I hope you've been armed with some good ideas as part of this responses you're getting today. Thanks, Paul.

PAUL FOODY: Thanks very much, Jothan. I think what I expected from Webnames was to say, "We've never seen this before," which is what a lot of people have told me—"Can you send it to us or can you somehow get it to us?"—so that they can look at it themselves because if I'm getting this today and so many people seem never to have heard of it, then other people are going to be getting it in the future. And there were a couple of people here who said they'd never heard of it and it sounds like a very new type of virus because it didn't come with the paperclip. There was no indication that there was anything attached. It just said 10k. And that was what I … I figured that this was something that could be dissected by people who know what they're doing and maybe find out how it has happened because if I have to go through every email that I receive and treat it like it's got an attachment, then I'm already wasting

too much time on spam. Thank you. Thank you, gentlemen. But once again, it's amazing what you do. Thank you.

[JOHN LEVINE]: And that's it for the current queue. Do we have any other questions from the audience? Any IT issues they can't solve, that they want solved immediately? Now's your chance.

RAM MOHAN: Okay. All right. Thank you so much. That concludes this public session. Thank you for coming. And have a good rest of the day.

[END OF TRANSCRIPTION]