ICANN85 Mumbai | CF – SSAC Work Session: PIR Abuse Intervention Program
Tuesday, March 10, 2026 – 15:00 to 16:00 IST

KATHY SCHNITT

Hello, and welcome to the SSAC work session on PIR's Abuse Intervention Program. My name is Kathy, and I am the participation manager for this session. Please be advised that this session is being governed by the ICANN Expected Standards of Behavior, the ICANN Community Participant Code of Conduct, and the ICANN Community Anti-Harassment Policy.

Regarding participation today, this session is designed for the internal work and discussion of SSAC members. To join the speaking queue, SSAC members must be logged into the Zoom room and use the Raise Hand feature. When called upon, please state your name for the record.

For observers, please note that comments or questions in the Zoom chat will not be read aloud. However, the chair of the session may invite questions from the audience at their discretion and time permitting. And with that, I am happy to hand the floor back over to Ram Mohan.

RAM MOHAN

Thank you, Kathy. And before we get started, may I invite those of our community members who are in the audience to come join us at the table? We have space at the table, and that just makes it a

little bit easier to not think about who's behind our backs. So please come and join us at the table.

BRIAN CIMBOLIC: Check yourselves.

RAM MOHAN: And with that, I am so pleased to have our friends at PIR here to chat with us about the Abuse Intervention Program. Brian may not be known to all of you, but you know Brian is General Counsel at PIR, who is the steward of .org and several other very trusted top-level domains. Rick, of course, we know because he decided to throw in his lot with us in the SSAC. So with that, I'll hand it over to you, Brian.

BRIAN CIMBOLIC: Thank you, Ram. Hi, everyone. As Ram mentioned, I'm Brian Cimbolic with PIR. Today, Rick and I are going to chat about a new program that we're launching in April called the Abuse Intervention Program. Next slide. By the way, feel free to take-- we'll take questions as we go. It would be great if this was a little bit more conversation than presentation.

So first, just a little bit of intro as to who we are at PIR, how our abuse strategy has evolved over the years. The Abuse Intervention Program is really built on something called the Quality Performance Index. To really understand what we're doing with the AIP, Abuse Intervention Program, we want to briefly give you an

overview on our Quality Performance Index. While we'll take questions throughout, we are also happy to have any questions at the end. Next slide, please.

A little bit about PIR, Public Interest Registry. We are a U.S.-based 501(c)(3) nonprofit. We are proud to serve as the nonprofit registry operator for .org, but also a handful of other mission-driven TLDs such as .foundation, .charity, .ngo, and .ong, among others. There's others. One thing that is interesting about us is that we are a supporting organization to the Internet Society, which many of you in the audience are familiar with. More than 60 cents of every dollar that we take in goes to ISOC to fund its great work.

But we are also, as I mentioned, a nonprofit ourselves. Part of what we do, part of our mission fulfillment, is trying to improve the state of the domain name system. Next slide, I should say. First, just what is AIP in a nutshell? Then we can get into the weeds a little bit. And Rick, of course, please chime in anytime. The Abuse Intervention Program is a program that uses objective criteria to determine registrars with really outsized, egregious DNS abuse. When a registrar trips all three wires, we will ultimately turn off that registrar's ability to have new creates or inbound transfers. It doesn't affect existing registrants on the registrar's credential.

I want to be clear, though, this is all objective. There is no subjectivity here. We don't target any individual registrar. We let the data do the talking. Next slide, please. As I mentioned, part of our nonprofit mission is really to help improve the state of the DNS.

We try to be very thoughtful and deliberate, starting first with our own TLDs, the TLDs that we're lucky enough to be stewards of. We were one of the first registries to have a published anti-abuse policy. I believe we're still the only registry that has published anti-abuse principles, which is why we approach DNS abuse the way we do. It also includes why we deal with certain categories of website content abuse.

But we're also pretty active when it comes to trying to provide resources and tools for the community. We work with a number of trusted notifiers. Some of you are familiar, I'm sure, with the Internet Watch Foundation. We've worked with them for years now. They're an excellent partner that helps us deal with CSAM in our TLDs. But we also have a sort of novel sponsorship with them where, at first, any domain name registry could receive their services for free. There are more than 50 million domains now covered under that partnership just on the registry side.

As of this March, we have expanded that partnership so now any registrar can receive free anti-CSAM services for free. Speaking of free, it is free. We also created the NetBeacon Institute, which we've got Graeme and Rowena over there, that provides free tools to reporters, registries, and registrars. Obviously, we try and be pretty deliberate about our abuse thought process. That led us to creating the Quality Performance Index. Next slide, please.

BARRY LEIBA And Brian, what does this cost?

BRIAN CIMBOLIC Oh, it's free, Barry. Thanks for asking.

BARRY LEIBA Thank you.

BRIAN CIMBOLIC So the Quality Performance Index. In 2019, you'll hear me refer to this as QPI. We sort of did a rethinking. First, what is QPI? QPI is an incentive scheme for registrars where they receive discounts if they have really healthy domain registration patterns. First and foremost, it is DNS abuse rates. If a registrar has too much DNS abuse, there are actually six criteria in QPI. But the one criteria that if the registrar fails, they're just totally ineligible, is DNS abuse.

QPI was a tool to both help reduce DNS abuse in .org and help create responsible growth. It's not just anti-abuse work; we're trying to grow the business. We're trying to grow .org registrations in a responsible manner. Next slide, please. QPI came about as we were sort of looking at our abuse standing. .org was never historically very abused, but we wanted to do better. QPI was a result of deliberate rethinking of our strategy. I want to give special kudos to SIDN, the ccTLD operator for .nl. They had a registrar scorecard out for some time which relied mostly on DNSSEC

enablement. We had a brainstorm with them and developed our own sort of flavor, which ultimately ended in QPI.

One of the other ways that we sort of rethought this was we started conducting more periodic DNS abuse sweeps. The method at the time for identifying DNS abuse was really reliant on catching domains in real time in new registration, but if they aged for a period of time, we were discovering we weren't catching them. We also implemented abuse sweeps. Next slide, please. The impact of QPI and these sweeps was pretty significant. We saw in the first year after implementing QPI and the sweeps a roughly 68% decline in DNS abuse. That is both in our own internal measurements and also verified by the Spamhaus badness index score.

At the time, we didn't yet have the NetBeacon Institute, so we couldn't look to NetBeacon map ratings. But by three years in, that was a 75% drop in DNS abuse cases that we saw by implementing those two measures. Next slide. Today, more than 80% of .org registrations pass through QPI-eligible registrars. This really gets to the point that yes, QPI is good for fighting DNS abuse or reducing DNS abuse, but it also really does help create responsible growth. We saw over 6% increase in our renewal rates. That is really helpful from a business perspective. Our .org continues to grow, our renewal rates are very high, and our abuse rates are low, in large part because of QPI.

RICK WILHELM

Go ahead, Rick, please. Success in business in a registry operation is frequently measured by your renewal rate for the domain. After someone goes and registers a name, the renewal rate is whether they go back and purchase that name again when it comes back up for renewal a year later. Oftentimes names are marketed so that the first year name price is $10. They might get that at a discount, but then on the renewal price, it might be $20 from the registrar.

The customer's decision to renew redwaterbottle.org is a much different decision than when they initially purchased it, because it might be a $20 or 20 euro decision rather than a $5 or 5 euro decision at the beginning. Whether or not they renew it depends on both what the price is, if they are using it, how they are feeling at the time, and how effective the registrar's marketing is.

This is not first-time renewal here that we have at 81%; this is all of the whole domain name base. For the renewal rates for the entire industry, I don't know what they are. Maybe Brian has that number off the top of his head, but they are not 81%. They are staggeringly lower. If you were a registry operator, this 81% is something almost every TLD wishes they had.

BRIAN CIMBOLIC

Yeah.

RICK WILHELM I mean, my understanding is basically the first year is a loss leader and the renewals by contract have to be at full price, and that's where all the money is.

BRIAN CIMBOLIC They don't have to be by contract at full price.

RICK WILHELM I thought the renewals had to be full price.

BRIAN CIMBOLIC The renewals do not have to be, not by contract. The first part of your statement was bang on. The first year generally is a loss leader for the registrars. Remember, the registries don't control retail pricing in most registries, setting aside vertically integrated ones. But the first year is typically a loss leader, and therefore you try to make it up on the renewal. Directionally, you're correct.

VIVEK GOYAL Thank you, Brian. My question is coming from the point that if I talk to another ccTLD or another registry, how do I convince them that doing good in terms of DNS helps you make money? If you can talk a little bit more about how QPI helps increase renewals, because the QPI program is an incentive for registrars to do well, whereas renewal decisions are made by individual customers.

BRIAN CIMBOLIC

It's a great question because you're right. This is not an incentive program where if you get higher renewal rates, you get more money. Ultimately, it all boils down to quality. But again, quality here also leads to good business because if you have a much less abusive registration base coming in, those names are always going to be much more likely to renew than a phishing domain. The renewal rates on phishing are very low.

These are quality names. When the quality of a name is high, it is very likely directly predictive of whether that name is going to renew. By removing the junk that would have otherwise come in from those not-so-great registrars with higher abuse rates, it means that our renewal rate a year later really shot up.

VIVEK GOYAL

Did you see a decline in new registrations then along with this program?

BRIAN CIMBOLIC

Good question, and I'm going to get to that shortly. I want to point out that this was not just good business for us, but also for our registrars. Our registrars saw a much higher increase in renewal than non-participants in QPI. We have the data to show that it was successful for our registrars, but we also had behavioral proof. Can we move to the next slide, please?

This is a real-life example. This is a registrar. Remember, we implemented QPI in 2019, and this particular registrar, a medium

to large registrar, was having quite a lot of abuse in .org relative to its peers. The two lines that you see here—the green line is harder to see—the one that zigzags up and then flatlines is the abuse rate. In April of 2019, this registrar was observing roughly 6% of all of its new creates in .org were tied to abuse. We implemented QPI and informed the registrar that it did not qualify for QPI.

While they were very unhappy because they were not receiving discounts and their competitors were, their abuse fell off a cliff. You see that it basically goes to zero, with little blips here and there. But at the same time, you see that their growth in .org, which was steady state at the time they were abusive, went up as soon as they started qualifying for QPI. Their quality went up, the abuse went down, and it was good for business for the registrar too. Failing to qualify for QPI fundamentally changed this registrar's behavior. It fundamentally changed the way that they sold .org, and that was the real proof of concept for QPI.

RICK WILHELM Got a hand from Gabe.

GABRIEL ANDREWS Hi. This is Gabriel Andrews, SSAC. This is a question that's kind of out of left field, but I was wondering if you have any anecdotal feedback from some of the registrars that have had success with the QPI, that the steps they've taken in order to achieve those discounts and take that responsible behavior has also benefited

the observed abuse rates in other TLDs that you wouldn't have visibility into otherwise.

BRIAN CIMBOLIC

That's a great question. We don't have insight directly as far as what they did. I couldn't tell you if this registrar fundamentally changed the way they sold everything or if they just changed the way they sold .org. My hunch is it was just .org, but I'm not sure. We can see, and this is something that our NetBeacon friends can look at, abuse rates per TLD per registrar now. It would be interesting to see if this changes their behavior globally. Maybe they sell legacy TLDs more like they sell .org because that's easier, or is there no correlation?

RICK WILHELM

One of the things I can tell you from my time working at a registrar is that having this sort of data internally gives people information on how to do enabled testing. When they see it work in one TLD, it allows a registrar to consider knobs and dials to shift and where that balance lies. One of the things that I think is important, and we say this a lot at PIR: the right number for abuse is not zero.

Zero is not the target here. If you want to get to zero abuse, it's easy: you just stop selling names. Or you make everybody come apply at the window, like there is a big queue at the consulate. We could figure out a way that would solve all of our domain abuse problems at PIR if everyone just came to Reston, Virginia, and queued up

outside our door. The right number is not zero. It's about how to get that balance right.

GABRIEL ANDREWS: If I can just briefly add, you're financially incentivizing the training of some of these people to do better, more effective anti-abuse measures, and there's non-zero utility in that. So that's interesting. Thank you.

WARREN KUMARI: I mean, this all seems a little silly. Great on PIR for doing this; it's clearly made a difference. But what this illustrates is if there is some incentive for a registrar to do better, they will do better. Maybe we could solve this in a better way by having compliance actually do things if registrars are bad. You had evidence of a bad registrar, you did stuff, and they got better. We could solve a lot of this by having there be repercussions for people not doing the right thing.

RICK WILHELM: Actually, this is a great lead-in. Warren's playing the straight man. Let's keep going because I think that graduated sanctions are a big part of what we're going to talk about.

BRIAN CIMBOLIC: That brings us to AIP. That was the QPI lead-in, and thank you for indulging me, but I think it was important to understand how we got where we are. QPI works. It has changed registrar behavior, it

has grown the business responsibly, and it has done everything we want with one real exception. There are a handful of registrars that don't care about QPI. It seems as though it's too much for them. Their abuse rate is so far gone that to be compliant with QPI, they would really have to fundamentally change their business, and they haven't. This is me speculating, but I think it's a pretty fair guess.

Next slide, please. That led to the creation of the Abuse Intervention Program. For context, I want to give an example that points to NetBeacon friends again. The institute put out a blog in August of last year. Rowena put out a blog in which, in one month, there was a registrar that had less than 2% of market share for the entire DNS and had roughly 55% of all phishing for the entirety of the domain name system.

There are registrars that when they get bad, they get real bad. These are the sorts of registrars that AIP is designed to protect .org from. We don't have huge abuse spikes even in these registrars relative to other TLDs, but they tend to still be the highest abuse registrars even in .org. We're creating the AIP to help protect .org, protect our registrants, and protect the trust in the name of .org. Next slide, please.

I want to be clear about what is and what isn't covered. We are specifically talking here about DNS abuse, specifically phishing, malware, and botnets where we have the information. Primarily we're talking about phishing and malware. I also want to be clear

that this only deals with malicious registration. Even if something is clearly a phish or clearly distributing malware, if it's on a compromised site, we don't count that. We're trying to get at registrar behavior, and a compromised site obviously isn't within the registrar's control. We want to be fair in AIP, so we don't seek to punish registrars for false positives or compromised sites. We're only measuring malicious registrations. Next slide, please.

What are the tripwires? I mentioned that there are three lines that ultimately, if you trip all three, you find yourself in an abuse intervention. First, the registrar has to be in the top 10 highest abuse rates just for .org, as measured by NetBeacon map data. I show you here the public information; the NetBeacon map data has a top 10 list, and they only name names in that top 10 list when a registrar is named four of the last six months. We thought that was a good methodology to replicate, so we're trying to target consistently high abuse: top 10 highest, four of six months in a row.

The second is a score that we created, which I'll get to shortly. Finally, a materiality requirement: the registrar has to have more than a set number of malicious registrations. Next slide, please. First, we use NetBeacon map data to identify the top 10 registrars each month. We look at those and get in contact with any registrar that is in the top 10. There are instances in which a registrar has an abuse spike but is otherwise a pretty good registrar. We're not trying to punish registrars for one-offs. We are trying to deal with consistent, egregious abuse levels. Next slide, please.

The second criteria really tries to get to the statistical significance of the abuse. We have a blended score that is basically half and half. We are very happy to use CleanDNS as our partner. We use a blend of real CleanDNS data for the .org domain names that we're suspending. We count those to keep track and see which registrar had how much. We take that and blend it with NetBeacon map data for .org and create a score. Each registrar is given a score each month. This is a metric that can change because it's based on standard deviations. We look at registrars that are two standard deviations above the mean for all registrars. That means you're already necessarily in the worst 2.5% of all registrars in .org. Next slide, please.

Finally, if you think about the first two criteria and take them to their natural conclusion, there's always going to be someone in the top 10 worst, even if they're pretty good. Similarly, with the abuse score, there's always going to be someone that is more than two standard deviations away. We're not trying to punish registrars; we're trying to drive behavior. That's why the materiality threshold comes in. If we're able to really change registrar behavior and they all get a lot better, there's always going to be someone in the top 10 and someone that's two standard deviations away.

We have to draw the line somewhere so that we don't end up punishing a registrar if it has six registrations and two of them are phishing. We want to instead reach out to them, get them in touch with NetBeacon, and try and figure out how to have less. We have a materiality threshold that we're not actually going to publicly

divulge because we don't want any sort of gaming or managing around a particular number. Did you have a question?

NABIL BENAMAR

Yes. It's related to some statistics that you have shown about malware and decreasing malware detection. For me, it's not necessarily showing that the organization is deploying a good solution to combat malware. Recent cybersecurity reports show clearly that there is a shift in malware detection because we are detecting malware-free attacks. The attacks' behavior is shifting from traditional malware to something based on identity. We are shifting from breaking in to logging into the systems. The stats might be misleading. Thanks.

RICK WILHELM

That's fair, Nabil. Right now, in the stats that we have, malware is not that big of a component. Most of it is dominated by phishing, as you probably know. As it becomes necessary to revise these based on the landscape changing, we'll take a look at that. But based on the data that we've been looking at over the past several years, these are the measurements that we have. Point taken. Thank you.

BRIAN CIMBOLIC

This gets to something that Warren was hinting at: the consequences. What happens when a registrar gets placed into an intervention? There are escalating sanctions. We want it to be almost a warning at first. To be clear, the registrar will have

received reports for six months in a row letting it know that it is in the top 10, so it won't be surprised.

We want to ramp up the pressure if the same registrar has the same egregious abuse levels. The first intervention, meaning the first time we actually step in and turn off the ability for new creates and transfers, is only two weeks. This is really trying to get the registrar's attention and inflict a little bit of pain so that they are incentivized to change their behavior.

If it happens again, then they go to a 30-day intervention. Third and subsequent interventions are 180 days. .org is a pretty sizable domain. We're roughly number four at the moment with roughly 11.8 million names. Registrars, generally speaking, want to sell .org. Turning off that ability to sell .org is hopefully going to drive registrar behavior, certainly for .org. Otherwise, they will find themselves no longer able to sell us. Next slide, please. Go ahead, Rick.

RICK WILHELM Warren looks like he's chewing on the inside of his cheek.

WARREN KUMARI Warren is, because we all know that there are some registrars who are clearly bad. I'm sure fairly much everybody in this room can list easily 10 or 12 of them who appear to be primarily there just for abuse. NetBeacon has some great stats. You have some great stats. You're actually doing some good things here. I don't understand

why we're in this weird Whac-A-Mole thing. ICANN spends a huge amount of time talking about DNS abuse and solving it. PIR is doing it without much work. This seems like it should clearly scale. We could solve this globally by saying we all know these ones suck; let's fix them.

BRIAN CIMBOLIC

It's a good point, and I understand the frustration. But I do want to point out that one of the benefits of the DNS Abuse Amendments was concentrating bad activity in handfuls of registrars and handfuls of TLDs. That actually makes it a lot easier for ICANN contractual compliance, because if the same level of abuse is spread over 100 registrars, it is harder, but when you concentrate that down to six or seven, it actually becomes a lot easier.

To Compliance's credit, the breach notices for registries and registrars are public. If you look at the breach notices that Compliance has sent for abuse, it involves many of the registrars and TLDs that are named in the NetBeacon reporting. The way the ICANN contractual compliance process works, for them to get to a public breach notice, there are many interim steps where that registrar had an off-ramp to not find itself in breach.

It's probably fair to say that there are actions that Compliance is taking behind the scenes that are just not public yet. But the ones that are public show a meaningful effort to enforce the new amendments. Maybe I'm optimistic, but I actually think they've got a hard job, and the public results speak to looking at those

registrars with really outsized abuse footprints. We'll see if they end up terminating a credential. I can't opine to that, but it seems at this point they're taking some real meaningful steps in the right direction.

I wanted to introduce a concept: the NetBeacon map 4-of-6 is six months, and the abuse score is a rolling six-month score. We wanted to make sure that we weren't being unfair. If a registrar fails AIP, us turning off that registrar's ability to have new creates or transfers in for two weeks isn't going to meaningfully change that score. Fourteen days goes by and you're going to have basically the exact same score. You're going to basically be in the same position for NetBeacon map data.

In that spirit of trying to be fair, we have cooling-off periods so that the registrar won't be eligible for a second intervention for 90 days. The idea is to let the data catch up. The registrar gets its 14-day intervention, and the next time it can't be placed into an intervention until a minimum of 90 days. Next slide, please.

This is something I've hinted at, but I just want to call out specifically. With AIP, we really have a no-surprises policy. We announced AIP ahead of the ICANN meeting in Dublin, knowing that it wouldn't actually start to go live until April. We've officially sent out the notice; it will go live April 01st. For the last five months, we have been behind the scenes sending out notices to the registrars that would be tripping those wires saying, "This program

is not yet live, but if it were, you would find yourself in danger of an abuse intervention."

The registrars that could end up being affected are already very much on notice. Registrars that have not received those notices are not in danger of AIP. The question we get most about AIP is from registrars asking if they are on it. If you haven't heard from us, you're not on it. Next slide, please. I think we can open up to Q&A.

RICK WILHELM

One thing I would say is no one's doing anything like this in the G space, and we don't know of anybody doing anything like this in the ccTLD space, although I'll admit that our knowledge isn't perfect there. As a gTLD registry operator, we don't have a choice in who our customers are; we have to take anybody that is ICANN accredited.

The idea is that we're basically saying to someone in the bar that we're not going to serve you drinks because you're not well-behaved. To translate it into something the ICANN crowd can understand: you're in the bar, but we're not going to serve you drinks because you're being unruly. In the 25 years of ICANN, that is not something the bartender has ever done. In our big, large pub that says .org behind the bar, we are saying we're not serving you because you're unruly. We're going to make a run at it to see if we can achieve the ends that Brian talked about.

BRIAN CIMBOLIC

I did want to flag one more thing. The reception so far, particularly among registrars, has been really positive. We were curious how this would go over, and by and large, registrars have been really positive about this. Obviously, maybe not the ones that might be affected, but there's a real sense I get from a lot of the registrars that are here at ICANN—the ones that aren't named in the top 10 most abused—that they oftentimes get painted with the same brush as those registrars with super high abuse concentrations.

That reputationally impacts registrars. The registrars that are not in that boat are like, "This is great." The feedback honestly we've got is that we should be publishing and naming who these registrars are. At this point, our status quo is that we're not yet, but this could be an iterative process. We've made adjustments to QPI over the years. The fundamentals have always been the same, but you learn and you adjust. It may be that some future iteration of AIP includes that, but the status quo is that we're not going to name those names.

RAM MOHAN

Thanks, Brian. Danielle, you're managing the queue, right?

DANIELLE RUTHERFORD

Yeah, happy to. Right now we've only got one hand up. Billy, go ahead.

BILLY: Can we get back to the slide with the graph of the good citizen registrar? Thank you. Does anybody have any data on other TLDs for this registrar? Is it possible that they focused on your TLDs and dropped the ball for other TLDs?

BRIAN CIMBOLIC: It's a great question. We didn't have it at the time, but NetBeacon MAP has data per registrar, per TLD. You could now look at how a registrar in QPI sells for abuse. How abusive are they for our TLDs versus other TLDs where there's not an incentive scheme or the incentive scheme is just "grow, grow, grow" without any sort of guardrail? We have not done that comparison. Graeme and Rowena, do you want to come to the mic regarding the availability of the data for other registries?

RICK WILHELM: One quick one. We would have comparative data in the latter period. The exciting left-hand part of this graph lacks cross-TLD data. NetBeacon MAP has data going back to 2022.

GRAEME BUNTON: We have data going back to 2022, but we don't have the ability to do this work at the TLD registrar level going further back than 2024.

DANIELLE RUTHERFORD: We do now.

RICK WILHELM I think the gist of Billy's question was during the left-hand part of the graph where it's exciting. We don't have that ability.

ROWENA SCHOO This is Rowena schoo from the NetBeacon Institute. The point we're trying to get across is that QPI started before MAP started. For the 2019 part, we don't have the data, but we would from May 2022. We haven't looked at it, though.

BILLY I was asking because whenever any registrar makes any success or any registry implements new cool tactics, we should have a holistic view on the entire landscape. When abuse just migrates from one point to another, we're not making it better for humanity. Thank you.

RICK WILHELM That's a very fair point, Billy. When we implemented this stuff, we were not trying to clean the entire ocean; we were trying to clean our bay. Thank you.

PETER THOMASSEN Hello. I think it helps cleaning the bay. The abuse might move elsewhere, but if that model were adopted by other registries broadly, then abusers would have a harder time. The question I

really wanted to ask: when did you put the intervention program in effect?

RICK WILHELM: It goes live in April. No registrar has yet received an intervention. You're getting the sneak preview before it goes live.

PETER THOMASSEN: Cool. Nice. Appreciate it. I was wondering because the first criterion was four out of six months. I'm not a registrar expert at all, but I believe there are some companies who operate under several IANA IDs. You could rotate and be abusive in three out of six months.

RICK WILHELM: That's a great question. That's something that we're keen on: avoiding gamesmanship. In our program terms, we write in the ability to look at registrars holistically at the family level, so that if they are fine getting one credential turned off, they can't just dump all the junk in another one. We reserve the right to look at the registrar at the family level.

GRAEME BUNTON: To be clear, ICANN does not have a concept of families. That's not an ICANN concept. That's something that is more loosely defined. We have a mechanism.

PETER THOMASSEN I can imagine that people would play games with different jurisdictions. You might identify that as a family, and they might say it's not a family and take you to court because you shut them down.

RICK WILHELM I appreciate that, but it's a risk tolerance thing. This is one of the things that you hear often in ICANN and other fora with registrars and TLDs: "Well, if we do that, we might get sued." We are very aggressive when it comes to DNS abuse. We are pretty aggressive when it comes to limited forms of website content abuse that violates our policies, like CSAM or distribution of opioids.

BRIAN CIMBOLIC I find the liability argument to be a rhetorical crutch from actors that don't want to do more. We have been operating this way for a long time and have not received a single credible threat of litigation. As long as your policy is clear and you operate under it, I really don't think there's a lot of liability risk. But we're just one TLD. Other registries or registrars might validly have those concerns, but we don't share them.

JOHN LEVINE I was going to ask if you got much pushback from the registrars, but you just answered that. Looking at your registrar agreement, it looks pretty well crafted to me. Going back to statistics across all registrars and all TLDs, Spamhaus does still publish stuff every

month. I believe it was most recently updated on the ninth. I presume you're looking at that.

BRIAN CIMBOLIC: You're absolutely right. The issue we run into is historical data. It's not just per TLD or per registrar; it's the registrar in each specific TLD. So it's both. The question is, was registrar A really abusive in other TLDs and not in .org?

JOHN LEVINE: Spamhaus probably has that information. I could ask and see if they were willing to share it with you.

BRIAN CIMBOLIC: It might be of some interest, but I think we're at the point now where we might be able to with the NetBeacon map data as well. It certainly would be of interest to see if this particular registrar changed its behavior or if QPI changed its behavior in .org. It's a good question.

DANIELLE RUTHERFORD: All right. Next up, we have a question from Vivek Goyal.

VIVEK GOYAL: Thank you. When there was a question of family of registrars, I thought I would love to see the data once you put this into place and when we meet again in June or October. Abusers are not loyal

to a family of registrars. They will register a domain for abuse wherever they are getting the cheapest and least pushback. The idea that a registrar might be trying to put all the bad domains to a small company, I would like to see the data before I make that assumption or that assumption is verified. Thank you. Let's look forward to it.

BRIAN CIMBOLIC

It's an interesting thing. You can imagine this was pretty complicated to come up with. We debated in a healthy way whether criteria one should be this or that. One of the questions we debated was whether this will shift the abuse that was going to happen in .org to other TLDs. When we look at the abuse from these particular registrars, they're not pretending to phish as nonprofits. It's just garbage stuff. I really don't think that we're going to make anything worse; it's just not going to be in .org.

WARREN KUMARI

It's not going to be in .org, but it's still going to be somewhere. I think the only way to fix this is if we have a more global solution. I realize I'm beating a dead horse at this point, but it needs to be solved at a global level. We all know who the bad folk are. We have data. I don't see how any TLD can solve the global problem. It needs to be solved at the regulator.

BRIAN CIMBOLIC

I agree with the sentiment, but we have to move in achievable steps. We're hoping that if we do this, and other big registries did the exact same thing, the moment these registrars are feeling that pain and are really disincentivized from doing this in multiple spots, that's what's going to change their behavior. Maybe these registrars are totally unaffected and just find themselves in a constant loop of AIPs or interventions. But if they had to do that with different TLDs, that's not sustainable.

The other thing I would say is the corralling of DNS abuse. Graeme mentioned taking what was spread out DNS abuse and pushing it to the edges in concentrated ways, which becomes a much more manageable problem. If it moves to a handful of TLDs, we can make it easier for compliance to go after those actors. I think we are seeing progress. The public breach notices that are out right now suggest that ICANN is looking at these registrars and TLDs with extreme levels of abuse.

DANIELLE RUTHERFORD

All righty. Next up, we have a hand from Maarten Botterman.

MAARTEN BOTTERMAN

Hi. Maarten Botterman. Excellent work. I'm impressed and proud to have been part of this family for a long while and leading by example. Two things. First, .org is in an excellent position because registrars want to sell .org. I can see it may be more difficult for other registries to follow the example. It doesn't take away the

value, but it's just a thought: how can we bring it wider? Second, I hear you about the top 10 abusers and cutting off with a certain number that you don't disclose. What made you choose that instead of a defined bottom line so people know if we stay beyond that, we're good?

BRIAN CIMBOLIC

It's a good question, Maarten. We wanted this to be fluid. If we just set a number or a percentage, the incentive is to manage your numbers to be just below that, making everything to the left of that acceptable. We thought that if we set a firm number or percentage, then it would just be managed to that. The fluid nature of standard deviations means as registrars collectively get better at this, if you don't change your practices, you're just going to fall behind. Fluidity is a feature and not a bug.

To your first point, you're right. .org is big, and AIP might not be all that scary for your registrars. But you should think about implementing QPI, or some version of QPI that works for you. We have six dials; you might have two. Something that incentivizes quality growth in your TLDs sets you up for success in the future.

DANIELLE RUTHERFORD

All right. The gentleman on my side of the U, go ahead.

SAIIDNAJIB SAIDISLOMZODA

Saiidnajib for the record. I'm the ICANN Fellow. Thank you for this presentation. I have a couple of questions. First, does this system

operate with other domain names than .org, such as .charity or .foundation?

RICK WILHELM: Let's just go one by one because my short-term memory is not my strong suit.

BRIAN CIMBOLIC: Good question. Obviously .org by volume is our largest by a lot, and we are using it as the flagship to drive the behavior. We're measuring in .org, but if a registrar essentially fails and gets placed into an intervention, it's for all of our TLDs at the same time.

SAIIDNAJIB SAIDISLOMZODA: Are there other types of threats like phishing, malware, and botnets?

BRIAN CIMBOLIC: It's a good question and it gets to the question of what is DNS abuse. We follow the ICANN definition in the ICANN agreements: phishing, pharming, malware, botnets, and spam. But we also act on abuse that is outside of that definition. We have limited categories of website content abuse in our policy. There's a document called The Framework to Address Abuse, and it sets forth categories of website content abuses that are so egregious that certain registries and registrars take action. We try to be appropriate and avoid collateral damage, but those real egregious

	harms like CSAM and selling narcotics online, we will take action on those domains too.
SAIIDNAJIB SAIDISLOMZODA	What risks does this program create for registrars?
BRIAN CIMBOLIC	The risk is the inability to sell .org and our TLDs. It's a threat to future business registrations in our top-level domains.
SAIIDNAJIB SAIDISLOMZODA	How could this affect the DNS system in the future?
BRIAN CIMBOLIC	I think that if other registries were to implement a similar system, it would push the abuse to the edges. Rather than having it spread, you can push it to the edges in the TLDs or the registrars that everyone knows have an abuse problem. This then gets you to the point where it might be easier for contractual compliance to act upon those actors. Thank you very much.
DANIELLE RUTHERFORD	We've got about five minutes left in this session. Sourena, go ahead.

SOURENA MAROOFI: Hi. Thank you for the presentation. I think QPI is a good program, mostly in terms of incentives and discounts for registrars. But personally, based on my experience, I think it doesn't work for reducing DNS abuse for all TLDs. Maybe it works for .org because you didn't have that much domain abuse even before that program. Probably it works because registrars you are working with didn't have much malicious registration and you didn't have that many campaigns. In the past 10 years, you didn't have even one major phishing campaign, right?

RICK WILHELM: I'm certain we did.

SOURENA MAROOFI: We are talking about those campaigns registering thousands of domain names per day.

BRIAN CIMBOLIC: With the Winter Fuel campaign, for example, there was a handful of .org domains. What we see is that it's not concentrated in our TLD, but we will get included in a broader campaign that spans across TLDs.

SOURENA MAROOFI: For the Winter Fuel campaign, I guess you were the smallest chunk. Why I think it doesn't work for all TLDs and registrars is that some of those registrars that register malicious domains own their own

TLD. They are registering domain names under their own TLD. It means that the registry should punish the registrar, which are the same thing. Or another TLD that is very malicious: there are only three registrars registering more than 80% of the domain names, and you can barely find benign domains in that TLD. If they remove those registrars, there is no one else to register domains in that TLD. How can this program work for all these cases?

RICK WILHELM

Neither QPI nor AIP is intended to solve everything. It's intended as a damper and a mechanism to help improve abuse management. These are commercial and contractual measures that complement and supplement operational approaches to abuse control. Both of these programs are interesting because they are commercial approaches, so they attack the problem from a different side.

While it's true that .org has not been a hotbed or cesspool, .org has managed to grow a lot since 2019 while having decreasing rates of abuse, which is counterintuitive. It's a tool in the toolbox. It might not be suitable for all domains, but it's helped .org. We're here to share these things in hopes that they might help other registries design commercial tools to supplement their operational tools.

BRIAN CIMBOLIC

I know we're pressed for time. We're putting it out there: any registry that wants to do QPI or AIP, have at it. We're happy to help you talk about what might work for you. This isn't proprietary; we

want other people to do it. We think that if other registries were to implement these programs, it could really have a meaningful impact.

DANIELLE RUTHERFORD: We're actually at time. Ram, do you want to take the last question from the SSAC member? All right. Billy, go ahead.

BILLY: You mentioned content-based abuse. I wanted to ask whether you distinguish actual sale of narcotics versus promises to sell narcotics and not deliver them.

BRIAN CIMBOLIC: No, because we figure if there was buyheroinonline.org and we acted on that domain, it was claiming to sell heroin. Either it sold and shipped heroin or it defrauded people. Either one, we're not good with, so we still suspended it.

BILLY: In the second case, it would not be reported. I'm asking because I often see these kinds of domains with portfolios which include other non-delivery scams like logistics or heating wood.

BRIAN CIMBOLIC: It's going to be super fact-dependent in each case, so it's hard to answer broadly, but that's a specific example in which we didn't

	know but we didn't care. Thank you for having us. We appreciate the opportunity to chat about this. If you see me in the hallway and have any further questions, I'm happy to take them.
RAM MOHAN	Great. Thank you so much. This session is adjourned.
KATHY SCHNITT	Recording stopped.

[END OF TRANSCRIPTION]