KATHY SCHNITT: Thank you. Hello, and welcome to our SSAC work session for the DNSAC operational considerations work party. My name is Kathy and I'm the participation manager for this session. Please note that this session is being recorded and is governed by the ICANN Expected Standards of Behavior and the ICANN Community Anti-Harassment Policy. Please be aware that this session is specifically designed for the internal work of the SSAC and is not structured for active engagement. Therefore, we will not be taking comments or questions from the audience during this time. I'm now happy to hand the floor over to Ram Mohan and Chaoyi Lu.

RAM MOHAN: Thank you, and Chaoyi Lu, welcome. I know it's remote for you. And if I heard you right, what you're suggesting is that we take the first 10 or 15 minutes of this work party meeting to go through the changes that you have made and then we re-engage. Is that what I heard you say?

CHAOYI LU: Yes, exactly. I made major edits, so it's kind of a brand-new outline.

RAM MOHAN Okay, great. So, can we get the edits up on the screen and let's have our members get on their screens, look at the document. Can you post a link to the document in the Zoom chat as well? And let's get going from there.

KATHY SCHNITT Ram, I removed it from the Zoom chat only because then it's public.

RAM MOHAN Ah, fair enough. So, send it to the list and we'll get it from the list. Thanks, Kathy.

KATHY SCHNITT Michael, I'll do that for you.

RAM MOHAN Thank you. I'm glad that was not on the microphone. Okay, so we're going to take--

CHAOYI LU I'm sharing my screen now. And can you all see the report being shared?

RAM MOHAN We can.

CHAOYI LU Okay, great.

RAM MOHAN Michael, I think you have to make it a little bit larger. My eyes are failing me from where I'm sitting. You should be able to link to it also from the SAC calendar.

STEVE CROCKER Am I live now?

RAM MOHAN You are.

STEVE CROCKER Yeah, but now I've got to take this off. So, one of the things that occurred to me after the last meeting was that there's a whole series of anecdotes of, or incident, anecdotes is a kind of dismissive term in a way, but of events where something went wrong and it was at least partially attributable, if not completely attributable, to DNSSEC. And a compendium of those is, I think, a useful thing to have and include for its own purposes as well as input to this report. I'm thinking of events like a zone was distributed, a signed zone was distributed, but it was broken partially. Germany, I think, somebody can remember better than I can about this.

Yeah, so that's enough for me to say there's some series of them. It's not hundreds, but it's not, I think, it's more than just the one or

two that we're talking about here. And each one of them had a dissection as to what the issue was, why it broke and what the consequence of that break was. And I think that would be an important part of the information that is included for the reader here, not just as there's issues and therefore, we have to do something, but more detail about all that as a primary section, not buried too deep.

And then, I'm sorry to be sort of clumsy about getting out my thoughts here, but so in my mind, a roster of those events that have happened in the past and then separately the kinds of things that we've talked about are included here about whether it's hesitation, for example, to implement DNSSEC or resistance and inputs and stories and postures is a different and also very useful. And I would rate that as deserving the same sort of first-class treatment to put all these things on the table and give us a richer position to work from in terms of seeing what the actual situation is about operational deployment.

RAM MOHAN Thanks, Steve. I'll come to you in just a moment. Geoff?

GEOFF HUSTON Hi, can you hear me?

RAM MOHAN We can.

GEOFF HUSTON Great. I think at some point, and I'm kind of thinking the introduction, but I'm not sure, there is the necessary observation that DNSSEC as a security solution is incomplete by design. The relevant quote is actually from RFC 2065, January '97, which noted that these extensions guaranteed the validity of resource records retrieved from the DNS. They do not magically solve other security problems.

For example, using secure DNS, you can have high confidence that the IP address you retrieve for a hostname, but this does not stop someone from substituting an unauthorized host at that address or capturing packets sent to that address and falsely responding with packets apparently from that address. Any reasonably complete security system will require the protection of many additional facets of the internet. And in looking at the tech so far, there's no acknowledgement that the original design was knowingly incomplete and was not a functionally adequate security solution right from the word go. Thank you.

RAM MOHAN Geoff, what text would you like to see added?

GEOFF HUSTON Well, I can put it in as a comment. I think that snippet directly quoted from RFC 2065 is about as good as it gets.

RAM MOHAN Then will you please add it in?

GEOFF HUSTON Yeah, okay, I'll do that.

RAM MOHAN Thank you. Chaoyi, what's your perspective on Crocker's suggestion to have what sounds to me like a somewhat comprehensive section on what I'm calling DNSSEC affected events on the internet over some time period? Do you have a perspective on that?

CHAOYI LU Oh, well, I'm thinking about adding a subsection in section two about that. Like when we discuss, after we provide educational and technical material about functional elements, and then we can provide some summary about some anecdotes. That's what I'm thinking.

RAM MOHAN So I heard Steve, at least my interpretation was Steve was saying we should do more than a few anecdotes. I heard it, at least to me, it sounded like we should have almost some kind of a compendium. Steve, you had your two fingers up?

STEVE CROCKER Yes. Let me ask a question. Warren is probably the most knowledgeable, but isn't there already a compendium somewhere, a list of these outages that have occurred because of provisioning problems or other things like that, operational errors?

WARREN KUMARI Let me just quickly get in the Zoom thing, and I will put a link to something. The Ionic site has a bunch of ones which are listed as partial. I'm unclear if you're asking just sort of DNSSEC, list of DNSSEC outages or ones where it was a partial outage?

STEVE CROCKER Well, my instinct is to say yes to everything. All of these implicate DNSSEC in one way or another.

WARREN KUMARI Careful what you ask for, because there are probably 100-ish or so on the Ionic's page.

STEVE CROCKER Well, that in fact is my point. Not that we should put each of those into our report, but at least refer to it and give some characterization that there's some range of experience that should be taken into account.

WARREN KUMARI

Also, probably we could highlight some of the, I'm not going to say more infamous ones, but things like nasa.gov or the Slack ones or things like that. We could have both sort of like, here's the list, but also here are ones which likely showed up in the press.

STEVE CROCKER

Let me expand that slightly. The noteworthy ones, yes, but also any common themes that come out of it, repetitions or are they 100 one-off events or are they 50 one-off events and a handful of repetitions?

RAM MOHAN

Joe?

JOE ABLEY

So, Steve, that's linked to what I was putting my fingers up for, which I think a lot of the large-scale problems that we've seen with DNSSEC over the past however many decades it is now have mainly been one-offs. I think when we've seen problems in signing TLDs or we've seen problems with prominent sites or we've seen in one case at least a TLD, ccTLD that did an algorithm roll over and exposed a difference of interpretation in the spec in Google public DNS.

These things were actually quite widely talked about at the time. I think there's a danger in saying, look at all these incredibly high-profile problems that have happened and having that being

interpreted as DNSSEC is dangerous operationally. Whereas in fact, I think you could equally well present that list and say, here's a demonstration of how the tool chains have improved because we don't see repeats of the same kind of thing over again.

STEVE CROCKER Thank you. I would never have thought to leave blank the interpretation. I think we should supply the interpretation that we want on that, but also the raw data as I was suggesting.

WARREN KUMARI So actually, while we're doing this, I'm quickly going to see if I can find, like we've got on certain places, we have lists of outages. I can just go through and see. There are a number which do just repeat again and again and again. Some of them are ccTLDs. I think Morocco has done it a number of times, but let me try and make stats out of this.

RAM MOHAN Thanks, Peter.

PETER THOMASSEN Hello, it's Peter. So I agree it's useful to reference some sort of historic compilation of what went wrong, but as you're dealing with operational considerations, I think what's even more useful is to have a categorization of the sorts of failures that exist and then maybe reference examples of that if we want to do that. And I recall

that somebody, maybe John Kristof, was working on a DNSS failure mode categorization and I think it was presented in Seattle or the meeting before.

And that was quite useful, but it was incomplete at the time because he only considered certain failure modes and there are others which still need to be investigated. And I think he used sex spider for figuring out how frequently the specific failure mode happens. So I think that would be quite useful to organize the operational considerations. And there are examples from IANA, sorry, from IANX or whatever.

WARREN KUMARI This is only very initial data, but looking at a quick look, .mg apparently had 29 times, .mm 14 times, af.mail 11 times, and then like libraswan.org, just picking ones which we might all know, dnssec-tools.org has apparently shown up five times, army.mail. So like there are nohats.gov, sorry, nohats.ca four times. Yeah, Xfinity three times, Comcast a couple of times.

RAM MOHAN So, Chaoyi, I'll come to you in just a moment, Peter. On, again, finishing up on Crocker's proposal, where were you thinking of adding this? Because on 2, would it be a preamble before 2.1, starts? Would it be at the very top where we say, here is a set of issues that have been observed over the last little while, and we can characterize it. Maybe we take Christoph's work and what Peter

was suggesting, maybe we characterize it as, and it can be broadly classified or categorized into certain failure modes. And then after that, are we thinking that the failure modes are actually inside the dot points under 2?

CHAOYI LU: Yeah, again, I think we can mention something in the, before 2.1, of course, but not to elaborate on it, because we don't have much space before 2.1, I suppose. Then we can provide a classification or discussion or about the events. I'm suggesting somewhere like between 2.2 and 2.3. So, after we've introduced these functional elements, like we derived these from the design, and when we finish on that, we can then elaborate on the historic failures and classifications or whatever. How does that sound?

RAM MOHAN: I'm not sure that it fits in 3 at all, Chaoyi? The more I think about it, it feels like it perhaps fits somewhere in 3, because 3 is current state analysis, and it could be that it's a part of 3.1. Or just make it 3.1. Make it 3.1, yeah.

CHAOYI LU: Yes, it deserves some space.

PETER THOMASSEN Right. I think it would be better to make it 3.2, because then we first have an overview of what the deployment status is, then we have historic stuff, and then we have automation stuff.

RAM MOHAN Fair enough. Okay, so Michael, that's going to be the new 3.2. Okay, I think we've given everybody enough time to scroll through the document. Maarten?

MAARTEN AERTSEN So, maybe a final remark on the data gathering. I know Jaap has offered multiple times while this work party was being discussed before it was chartered, etc., that he has more than a decade, maybe two decades of monitoring data in perhaps an inconvenient format, because it's, I think, a mailbox or something. But if you want to have historical data, you should take Jaap up on his offer. And yeah, it will be probably some work to actually get it out. But I think he has offered multiple times on the mic. I think he hasn't been taken up on the offer. Just raising that.

RAM MOHAN I'm open to that. Chaoyi, do you have a perspective?

PETER THOMASSEN Look, I will just reach out to him and see what he has, and then we can see if it's useful. Okay.

RAM MOHAN So, the action on that comes to you and me, Chaoyi, to reach out to Jaap. But you can do it. Peter will do it. Okay. Michael, Peter has got the action. Okay. Shall we go through the document now? Chaoyi, you want to lead us?

CHAOYI LU Okay.

RAM MOHAN And you decide whether you want to go through the introduction part or whether you want to go to other sections. It's your call, where the bulk of our time here should be utilized.

CHAOYI LU All right. Let's just start with comments people leave in the introduction. I see one. Whoa, this is a long one.

JOE ABLEY That's the one that Geoff just talked about.

GEOFF HUSTON Steve Crocker wanted text. He's got text.

CHAOYI LU: Okay. So, we'll move on to the next one on signing. So, there was a suggestion changing signing into key management and then have a separate bullet on generation of signatures.

JOE ABLEY: This is Joe. So, that's my comment. I just think there's two different sets of things to talk about there. We definitely have examples of where signatures were not generated correctly. We definitely have examples where there were key management problems. Sometimes there were keys that were unavailable. We certainly had signatures that expired. I think there's two different sets of things there. So, I just suggest like break them out separately.

RAM MOHAN: Okay. Let's do that, Michael.

GEOFF HUSTON: I'll raise my hand at this point about signing. And I mentioned it later that maybe it comes in on the general point of signing here. There is a world of difference between pre-signing and online signing. It affects a whole bunch of things, including multiple operators, compact denial of existence, etc.

WARREN KUMARI: Yeah. I mean, a good example of that, and I'll put it in the link, is the differences of that, but also the bits where the key management

is unclear is the Randy Bush postmortem, which he posted for a bunch of TLDs. I can't remember how many it was, but the one that I had the link to was for .PT, yeah, PT as well, and Lebanon. And yeah, those were down for many hours or a couple of days, I think, in some cases. And that was exporting keys from one set of tooling and importing them into another set of tooling is a lot harder than it needs to be or should be, or at least it's very easy when doing something like that to shoot yourself in the foot.

MAARTEN AERTSEN So are you looking into doing some root cause analysis of what makes tools terrible? Because we were writing a FOSS report. I have some inklings of where you could go there because I don't have statistics, but I would be curious to see what percentage of people using these tools actually are somewhat involved with development, funding, whatever.

WARREN KUMARI I mean, I just actually put a link. Randy's got a fairly good write-up of how it went sideways. And reading through what all happened, if I had done it, it probably wasn't gone sideways in the same way for me. And part of this, I think, is we have a bunch of different signing software at the moment, and they all have different ways of storing their keys, exporting their keys, showing how the keys are being used. And in some cases, the level of documentation is definitely different, and some things could be lacking. But I don't really know what this helps, other than being like, turns out some

documentation sucks. And if you have a sharp and powerful tool, you can accidentally do bad things to yourself.

I also don't know how we fix this other than somebody should provide more funding to people who write documentation. Yeah. And, or, I think we've already said this in the document, or at least outlined it. It would be nice if the tooling made it harder to accidentally shoot yourself in the foot. The trouble is, it's security tooling. And we've all seen a bunch of examples where somebody forgets to renew their TLS certificate, or forgets to renew their intermediate CA.

And, you know, large important sites fall off the internet. And if large important sites can't keep track of what certs they have, how do we expect anybody to be able to keep track of important keying material? The obvious solution to this is keying material should never expire. Okay, Russ was listening, I wasn't sure.

MAARTEN AERTSEN: No, I mean, but I think that is actually a useful step to make, because stopping at the tooling is bad is great, but also not super helpful, right? There's no, yeah.

WARREN KUMARI: I mean, something which I've never really understood in the DNSSEC world is, I can relatively easily sign up for a service, which will monitor all of my TLS certificates, and will send me whiny naggy emails if they're about to expire. It seems like there should

be a similar service for DNSSEC. And I've seen a couple of them kind of sort of, but they've never really worked. And I think many of them have gone away, but it shouldn't be possible. Ooh, is Peter going to say, I've got a cool tool that will do that?

JOE ABLEY Of course, you could always do the prudent thing and just go unsigned for a day.

WARREN KUMARI Been there, done that. I mean, actually, like, I guess we should mention a large TLD, ccTLD was like, rolling keys is kind of scary and kind of terrifying. When the IETF moved algorithms, it went unsigned. Nobody noticed. As far as I know, almost nobody noticed. When a lot of people move their system from one machine to another, or one algorithm to another, or one signing to another, they go unsigned because it's less scary. That may or may not be a good solution. I think it depends on a lot of your philosophical views.

CHAOYI LU Okay. I'm going to just summarize this quick. I think that the tooling that had been discussed earlier can become one of the bolts here. But since this is introduction, we won't be able to dig it in too far. I actually have a subsection in section four, a whole subsection about it to talk about tooling if we have things to elaborate on it. But in the intro, we can say that tooling is one of the additional

functional elements that people may need. Okay. I see one hand from Rick.

RICK WILHELM

Thank you, Rick Wilhelm. When Warren said the point about going unsigned, I just did a quick search in the document and we only have the word unsigned in there once, which was below my over under bet. I'm not sure what the over under line was for me, maybe four and a half or something like that. But it occurs to me that if we're going to talk about this one of the things that when you, when you go signed, you establish a user expectation that you're going to be signed and we might want to think about adding something in there about this topic.

So I'm not sure where in the outline it is, but the fact that a DNS, a DNS operational consideration is that once you go signed, you sort of establish a user expectation that you're going to be signed and then it, then just like the users in this, in a TLD or anything that when you're, if you're going to stop doing that, then how do you do that and announce it? If you're going to go unsigned for a period, how do you communicate that to users? But it just occurs to me that we're using it. The only spot in here that we've got, it is about, in the introduction about DNSSEC anecdotes.

And I think that the concept of it is an operational consideration, and I think we ought to give it consideration of being a stronger concept in the document somewhere. So I want to give Warren

some, some credit for highlighting that point. I think we need to chew on that a little bit. Thank you.

GEOFF HUSTON

I'd like to follow you up on that, Rick, and your comment about a user expectation once you go signed. What tangible difference in the look and feel in the UI of the screen I'm staring at, is there between the DNS resolution of an unsigned name and a successful resolution and validation of a signed name? I would argue nothing. The user actually has no visible indication whether a name is signed or unsigned, if everything is working. If DNSSEC is not working, the name disappears. It's serve fail. It's not a massively helpful diagnostic. There is no user level expectation being generated by having your name signed because there's no signal that it was signed in the first place. Nobody can tell.

RAM MOHAN

Peter than Warren.

PETER THOMASSEN

Thank you, Ram. Hi, Geoff. I think you are focusing too much on a specific type of user, right? I mean, you, you mentioned websites, browsers, whatever. But there are people who do use Dane authentication for email. For example, there's a few hundred thousand mail service. I think that, no, that's not true. A few million sites that use email service that are authenticated. That's right. That's what I wanted to say. And they might be relying on the fact

that they're like TLSA published certs or key material works, and then it can no longer be authenticated if it is insecure. And I'm not judging how large that problem is. I'm just saying that the thing you focus on is not the only thing, and it's nothing to do with what's on the screen.

WARREN KUMARI: And yes, sir, following on from that, I think it also comes down to what do you mean by user, right? Like I'm a user of a website, but I'm also a user of the .com and .net registry because I have domains in there. And so sometimes the user of a TLD is the registrant. Maybe customer would have been a better word. Of course, I'm not actually looking at the screen, so I'm not sure, but the screen is bouncing weirdly.

PETER THOMASSEN: Ram left. Rick.

RICK WILHELM: Since Ram's not here. I think that Peter and Warren are getting to the point, but I think I will agree with a point that Geoff said, which is completely agree that to an end user sitting in their browser, it might not make a bit of difference, which is also a thing I think that we should bring out in the paper in this point about user, whatever we mean by user, whether it's a Dane user, my auntie's sitting at sitting at her browser window or a monitoring user, or whatever it is, or whether it's YOPS monitoring, the stuff that goes into YOPS

email inbox or whatever it is. So I think that all of that deserves to get elaborated because those are all multiple perspectives on the same happening. Thank you.

RAM MOHAN Sorry, I missed what Peter and Warren, your response to Geoff was. So was there a resolution?

GEOFF HUSTON I can summarize if you want. Rick had said, once you sign, you create a user level expectation that the name will continue to be signed. And I was pointing out, at least from the perspective of the browser world, there is absolutely no visibility to an end user on the browser that names assigned, unsigned, validated, or anything else if it correctly validates, it looks the same as if it was never signed.

RAM MOHAN Right. I heard your part, Geoff. I missed out on what Peter and Warren's responses were.

GEOFF HUSTON Peter said there are many other users of DNSSEC validation, particularly around the email areas where that distinction is more obvious and Warren was saying there are many kinds of users, some are customers of other registries, and then the whole idea of what is a user changes context with those roles.

RAM MOHAN Thank you so much, Steve.

STEVE CROCKER Thanks, Geoff. Let me offer yet another way to look at the comparison that you're talking about. DNSSEC, as I know, you know full well, was motivated by cash poisoning experiences. So if you live in a world in which cash poisoning is a serious and ever-present threat, then your test case of whether or not the user would see anything different if for unsigned versus signed, it comes down to, yes, of course they would see something different, but they wouldn't be able to know that it was inappropriate or do anything about it.

WARREN KUMARI I actually, I think I disagree with that. If we didn't have DNSSEC and there was cash poisoning attacks, users would see the same thing that they do now. In fact, I think they would see something more helpful. Currently with DNSSEC, probably the way it ends poorly is the name does not resolve or it doesn't work properly in the resolution phase. If you send a user somewhere else now, what they get is a big TLS warning saying the site you are trying to get to is not the site that you wanted to go to. TLS is providing, sadly, most of the protection here.

STEVE CROCKER So that's a critical point to bring into view that DNSSEC was invented as the protection against that. And the certificate folks said, oh, we got you here. That's a non-trivial.

WARREN KUMARI Yeah. I mean, I think that at the moment, TLS is providing the majority of protection because it doesn't just do name resolution failures, it's man in the middle. It's any other sense of along the way path. And yeah, if there wasn't TLS, DNSSEC would be like absolute requirement for everything, I think. But because at the moment, all of the internet runs over the web, as far as most users are concerned.

STEVE CROCKER I'll allow myself just a little bit of leeway here to say something that need not be said. I hate certificates. And it pains me a lot to suggest that TLS is a good substitution for DNSSEC. Geoff, it's entirely different when it's signing, when it's encryption.

RAM MOHAN Joe.

JOE ABLEY I wonder if it's useful to look at this slightly differently. I think Geoff is right. And I think Rick is right. And the reason they can both be right, but apparently say different things, is that there are some uses of DNSSEC, which are the kind that Geoff implied, where a user

doesn't care, it's invisible as to whether it's validation was possible or not possible, whether something was signed or not signed.

There are other uses of DNSSEC, which rely on the fact that there are signatures and a validation chain, like Dane, like other things that try to use DNSSEC as a PKI. And those things obviously do require D and there is an expectation for users of those protocols, probably indirectly, because they've never heard of DNSSEC, that DNSSEC signatures are validatable and present.

So there's two different classes there of relying parties on DNSSEC. One of them very reasonably doesn't care. And in the in the case of like Geoff's example, it's very reasonable to take a TLD unsigned because the risk profile suggests that's the safest way of doing it. But we also perhaps need to acknowledge that there are other uses of DNSSEC where there is an expectation that once signed, something will remain signed because the protocols perhaps don't anticipate something going unsigned and mail having to fall back on other checks or mail having to be queued and not delivered or something.

RAM MOHAN

So I'm actually just wondering, I mean, this is important. I'm wondering where it fits in because I don't see a place in the document right now, the way we've structured it or this fits in easily.

GEOFF HUSTON That long comment in the introduction that I added said that.

RAM MOHAN Yeah, but that's the introduction. If you want to explicate it, Geoff, and we want to take on what Rick was saying.

GEOFF HUSTON The point was at the time of cache poisoning, which was mid-90s, the ITF DNS folk came up with this secure framework for DNS, which has become DNSSEC. But already then I pointed out the references RFC 2065 pointed out that it wasn't a complete solution and that any reasonably complete security system will require the protection of many additional facets. And the commentary is at the same time, Netscape brought out SSL to 2.0. That was 95 that actually answered a subtly different but more useful connection question. Am I connecting to the named thing that can demonstrate that it is that name? Doesn't matter what the DNS said, doesn't matter which address you're going to. Is this connection authentic?

And that was where SSL was aiming at. And you see that two subtly different questions is the DNS line or is my connection to the wrong thing? And history has proved that the bulk of the market, the second question, the authenticity of a connection was way more important economically, practically, operationally than the first question. And so DNSSEC kind of disappeared in importance and became a niche solution looking for a question. Now, to my mind,

that's introductory material. It's kind of, we knew this then, we know it now. This is not a new finding.

RICK WILHELM

As far as where to put this kind of thing, what if we added something in section 2 where we talked about observable impacts or observable indicators of DNSSEC deployment, where we included the things that are both observable, which would include the things that Geoff was talking about, the things that Warren was talking about, the things that Peter was talking about, as well as then if it started and stopped the things that happen, and have a section in there not sure where, but like what you observe when DNSSEC is deployed, what you see right at the different layers, layers in the architecture is not really the right term, but at the different portions of the ecosystem, something like that.

And not really focusing on the why, because 2.3 is, is more about the why. 2.4 is about forces impacting. 2.1 is about the functional elements about how you do it. But this would probably, functional elements about how you do it. And 2.2 is about functional elements of validation, but maybe this is, but be like between 2.2 and 2.3, which is about what you see when DNSSEC is out there. Shrugged shoulders offers that up. And then they're under 2. Somewhere between, not 2.2 and a half, but a new, in between 2.2 and 2.3, a new section, deployed DNSSEC observed or observable impacts or something like that. So.

RAM MOHAN Okay. So that's a proposal, a new 2.3 DNSSEC observable impacts. Steve?

STEVE CROCKER The interplay, my play here about the success of DNSSEC versus the success of TLS and how all that's played out, seems to me to lead inescapably to the big question of is DNSSEC necessary at all, is it just simply an extra and redundant mechanism that is not providing any incremental thing?

RAM MOHAN I mean, that will be the follow-up after we finish this paper. I don't think we do it in this paper. And what I've been thinking about and I spoke about this with Gautam and with briefly with Warren was maybe that's a thing that we go to the IAB and say, that's something the IAB should be looking at.

STEVE CROCKER Perhaps, but I don't think that saying that it's a separate thing, we should take that up is okay. But the fact that that's coming, I think has to be mentioned and acknowledged sort of as, as one of the outcomes. Not strong enough in my view.

RAM MOHAN

But it's implied, isn't it? I mean, if you take what Geoff has written, what Geoff has put in his comment, it's pretty explicit in what he's saying. He ends it with DNSSEC may not be useful.

STEVE CROCKER

So do we want to say-- I'll shut up after this, do we want to say something about the fact that we're going to take that up further and include this as part of the framing of this paper?

RAM MOHAN

I don't think that comes in the paper we write. I think that that's in the scoping part, but not in the paper we write. My, my opinion, three hands here. So you guys decide who go.

WARREN KUMARI

This is where I finally make friends with Peter again. I think that DNSSEC is still needed. I think that it is a decision that the user should make the end user, whether or not, when I say the end user, like the insight should make whether or not they want to use it. But I think it's important for TLDs to provide it. I think it's important for the root to provide it because it provides the layer that other people can choose to build onto or not. There's also things like zone checksum. The reason that I can download the entire root zone and put it in my local resolver and trust it is honestly somewhat because it comes over TLS these days, but also because the entire zone is signed as a blob with DNSSEC.

Some mail people are using it to do validation, like validation of should this domain www or I guess kumari.net be able to actually use Google's mail servers. Like I have something signing the image record saying, yes, those are my right mail, but I think the thing is if you run a web server, like my personal web server Kumari.net, nobody looks at it. Nobody cares about it. There is basically zero threat of somebody doing important, scary DNS things and moving my web, like my web content somewhere else. It's not a threat that I care about. I might, however, care about the additional faff and work and stuff. Kumari.net? If you have a website at this point, you fairly much have to have a certificate. So I have a set. Yep. Yep. That is the bit that actually keeps my site more. Oh, wow. More hands. I should leave now because they get excitable.

RAM MOHAN All right. Russ and then Joe.

RUSS HOUSLEY So DNSSEC is the only integrity mechanism for distributing the root.

WARREN KUMARI Nope.

RUSS HOUSLEY If it is. If you go back before signatures, the integrity came from the fact that you had 13 collaborating parties to watching each other,

that's where the integrity came from then and now. So the collaboration of the root servers was the integrity mechanism in the beginning, and now it's the signature. If we're going to, maintain the gains in integrity that we got with signing, we have to at least at the top of the tree, keep it.

JOE ABLEY

So I think any blanket statement that anybody makes about whether DNSSEC is useful or not is useless. I think the statement means nothing. I think, that irony was not lost on me. So for example, if you say that in a particular context, DNSSEC doesn't help. So, therefore DNSSEC is useless, you could also say that TLS is useless, you could say firewalls are useless, you could say every individual protection that might not apply in a particular case is useless, and none of those statements are helpful, they don't help anything. The important thing, I think, is that people have the option of incorporating DNSSEC into whatever their mitigations to the risk profile they've identified for their service or their user or their device or their infrastructure.

It's important that it's available. Unless we are 100% confident that there isn't a single person in the world who thinks that. And I don't think we can think that. I think we have lots of data points to the contrary, where lots of people do use DNSSEC. And for them, in their expert opinion about their own situation, it does have some use, either on its own or in combination with other things.

So this leads on to some other comments I put in the document, which is about adoption, and I think it's related, so I'll mention it now, which is I think we fall into a trap often of talking about adoption as something that can be measured by a metric of how many people who could be using it are using it. And if that number is low, we think adoption has failed. But in fact, there are lots of people who have a reasonable option for DNSSEC, might decide not to use it, that doesn't mean that DNSSEC has failed. The fact that it's there and present, available as an option, allows it potentially to be incorporated where it's useful. It doesn't have to be universally useful to have succeeded.

So I think we need to separate those concepts. I think, for example, having DNSSEC in the root zone is important, in TLDs is important, because it gives the option of people to use DNSSEC further down the namespace that otherwise is cumbersome and difficult to do, because you have to implement your own key distribution and you don't have the benefit of a parent providing a chain of trust. But I think all these things are linked. I think we could usefully say something that we think the way that DNSSEC is promoted could bear changing, because the way that we measure success perhaps would be better done in a different way. Those are useful things that we could say. I don't think it's useful in any way for us to make any claims about whether DNSSEC in general is useful or whether it has succeeded or failed.

RAM MOHAN Thank you, Warren?

WARREN KUMARI Yeah, largely what Joe said, I think for a while we've been doing like people should do DNSSEC because it's good and people should do DNSSEC because it's good and leaving out the people should do DNSSEC because it has these benefits, but it also has these operational costs and potential to shoot yourself in the foot badly. If you would like these sets of benefits, go ahead and do DNSSEC. If you are concerned about these cons, here's how you can mitigate some of the cons so that maybe you do want to do DNSSEC.

I think that some of our cheerleading or advocacy has actually hurt some of the deployment, looking through like for example the list of failures, one of the places where you see a substantial amount of failures is in the .gov zone, and there was an early push that .gov should be signed and there was I think actually a federal requirement, you will sign these things, and that pushed people who weren't initially ready for it into doing it. They did stuff and it went bad and now it's sort of the once bitten twice shy, they don't want to try it again.

And I think if we did more of a here is why we think DNSSEC gets you some protection, keep in mind these are the sharp pointy bits as with any tool circular saw can do really good things for cutting a 2x4, it also cuts your arm off, understand do these bits, not those bits, I think we would be, would have more deployment if we'd.

RAM MOHAN Thanks Warren, Rick, and then Steve.

RICK WILHELM I really want to agree with the stuff that Joe said and with Warren. I think that when it comes time for us to write the introduction to this thing, I think we should go back to the transcript. I think that was really well summarized. So whatever coffee you had at the break really nailed it. And so I think that, I mean, that's exactly the tone I think we want to strike. And I think we should really try and mine that vibe, right? SSAC really doesn't do vibes, but I think we should try and capture that vibe for the intro. Thank you.

RAM MOHAN And I think, Rick, it goes beyond the introduction. I think that's probably, perhaps for even in, I can see a recommendation come through that encapsulates what the three of you have said, Warren, Russ, and Joe. One of it might be it is a useful tool that should continue to be deployed at the root zone, at the TLD level, etc. So there's some value there. Steve, and then Robert.

STEVE CROCKER Thank you. I listened as carefully as I could to both Joe and to Warren. And while there was a certain amount of commonality, there was some differences that I want to highlight here. I don't have any problem with the idea that not everybody needs to use

DNSSEC for all the time. But stopping at the point of saying DNSSEC might be useful, and we ought to provide the ability for people to use it, and then not saying the next thing of what is it good for, or what are the positive experiences, or what kind of advice to give, is sort of too laid back in a way. And so that may be uncomfortable.

But then Warren talked about, and here's the things that it's good for. And here are the warnings that you ought to adhere to. And here's the thing to pay attention to. A related but maybe separate comment about .gov, and as a standout of how not to do things, in a way. The question of who makes the decision, and what are they trying to accomplish, may be an important thing to include in the overall picture here. Because, and I guess this was a point that you were making Joe, that the person who makes the decision to use DNSSEC needs to have a picture of how that's going to affect the community that they're trying to serve, and so forth. And they have to know enough to be able to put all that together.

The .gov case, as best I can recall, I'll just say there was a resource issue in that there was not enough clue included in the process. That is, the people who were assigned to do it didn't know what they were doing, and there was no management and oversight process that said, wait a minute here, let's get this right. Which they could have done, putting in my own opinion. And so we can separate that out a little bit. That was just sad, in a way, as opposed to instructive.

RAM MOHAN Joe? Sorry, Robert, and then Joe.

ROBERT GUERRA Yeah, I just wanted to echo some of the comments in regards to Warren and Joe's comments, but particularly Warren's, in terms of thinking ahead, in terms of how when this hits the community, or we get the feedback, in terms of what to put in, because the community's heard a lot about DNSSEC. But having that angle that kind of Warren mentioned, in terms of, I think would just help with the community. I think that's something that we need to think about. It's not only the text itself, but just having like, what's the teaser sort of at the beginning.

And think of also the wider audience, because I think it ends up being sort of like education. I think maybe that piece hasn't been there. Because I know I've recently done some training related to this, and people didn't know the value, and then it's just hard. And it's not people who would implement it, but just kind of like, oh, your websites, you can tell whether they've been captured or not. It's like, oh, I had no idea this existed. And so popularizing it a little bit, and it may not be the scope for this group, but just like in terms of making it simple at the beginning, I think could be helpful along the larger path.

JOE ABLEY

Yeah, so I just had a brief comment after your comments about .gov. I don't know what standing we might have to say anything about the decisions of the US government 15 years ago or something. I don't know how useful that would be. But I do think around the same time, around 2010 or so, 2010 is when we signed the root zone. And around that time, I was ICANN staff, and there was a big push amongst global stakeholder engagement or whatever they were called back in 2010, to encourage ccTLDs to be signed.

And there were a lot of resources pushed towards ccTLDs being signed and there was a lot of pressure put on ccTLDs that felt a bit like you're not doing your job unless you deploy DNSSEC. I think actually I heard at the time, and this is apocryphal, but the then CEO actually may have been measured in some sense by how many of the ccTLDs were signed because this was somehow some measure of his performance as the president of ICANN.

So I saw that from the other side because I was also volunteering with NSRC doing workshops with ccTLDs and doing direct engineering engagement and our message to ccTLDs was unless your physical security is good, unless you've solved the problem of all your engineers running off to France and the UK for jobs after six months, unless you've got continuity in the personnel, unless you've got-- We had name servers that were running desktop versions of Ubuntu, running Mozilla, like Firefox is running on the server and running X and there's no firewall setup. Sort all these things out first before you even think about doing DNSSEC, which

was the opposite message that these ccTLD managers at the time were receiving from ICANN.

So I think .gov is, I believe you, it's probably a good example of a mandate that was you're required to follow it even if you don't understand or care about it and that caused problems. But we have examples that are much closer to home, and I think we can influence ICANN's message towards ccTLDs and parts of the community, and actually give a better message that will encourage better security.

STEVE CROCKER I'm not suggesting that we should make a comment about .gov or and so forth in here, but we know, you, I and various other people lived through that period, that it was a pretty messy period with DHS following a presidential level mandate that DNSSEC will go and Department of Commerce listening to a different set of input saying, oh, this is problematic, we won't do this and they were butting heads. Well, the net of it was it just caused a lot of delay and partial, nobody took the complete picture as you're saying and pick up pieces of-- anyway, we can agree on that.

RAM MOHAN Just to let you know, I'm adding a Section 4 findings or 5, I guess it should be findings and 6 for recommendations. I'm just writing some text that is very roughly trying to capture what we're talking about here.

GEOFF HUSTON

I think in your findings or somewhere around here, if you're trying to balance things out, there are a few fundamental observations and the first is adding keying material to DNS answers increases the size of DNS answers, and the overriding assumption of the economics of the DNS is that UDP works because anything else is horrendously more expensive. The problem is that very large answers don't and even though we might say ECDSA will save our bacon for a year or two, as soon as the first post quantum crypto algorithm pokes its ugly little nose through the door, say goodbye to small answers and at that point you get back into the whole issue of are the niche benefits of DNSSEC worth sacrificing the entire DNS for?

Because DNSSEC is not for everyone and that's the first kind of question about when you've got a technology like this where, if you will, everything has to make it has to be there in order for even the most niches of applications to actually be viable. That's a tough call. Who makes that call? The market. No one's in charge. So that's kind of the first issue here around this stuff is hard because we're stretching the DNS well beyond its safe point and it's not safe to sort of send massive responses around the net. It doesn't work.

Secondly, validation is as bad today as it was 30 years ago. We spend obsessive amounts of time trying to make every other part of the internet go faster and validation is just crap. The extended queries, waiting for answers, do another query, wait for answers to

validate stuff, really is an horrendous imposition. What killed Dane? The cost of validation. No one else has ever tried validating down in the stub resolver in the end client. We do validation in recursives because that's about the only place where it can work with effective caching. If you've ever tried to run it down in the stub, you don't live long enough to get answers.

Again, this is a real fundamental problem. You could get rid of query-based validation if you could allow massive answers, chained DNSSEC validation answers, but then the answer gets big and you're back to problem number one. DNS was not designed for big answers. And it's those kind of fundamental contradictions that sort of sit behind DNSSEC, which are the elephants in this room, because we're pushing the DNS in both response time and time beyond what's reasonable out there in the internet. And no one's willing to either cut us a bigger check so we spend more money and convert the DNS to TCP. I don't know what else is the options here. If you want to make DNSSEC work, someone's got to pay a much bigger price than they're currently paying.

PETER THOMASSEN Just for curiosity, do you have an answer to any of the questions you've raised? I mean, it's a serious question.

GEOFF HUSTON I remember Peter Spacek did a DNSOARC presentation some years back that pointed out that if the DNS was running over TCP, the

effective throughput of servers would drop by 60%. In other words, we'd need to triple the money in current infrastructure to maintain current query answer capacity. It's not clear who's going to pay that cost. There were efforts by routers, Paul routers, to try and push for chained DNSSEC validation answers to actually give the validation chain together with the response so you didn't have to go down iterative query hell.

It's written up as an RFC. I've forgotten the number. It's been ignored for about 10 years. Again, part of the problem is you can do chain DNSSEC validation answers, but you're shoveling a few kilobytes of data through and the DNS itself, as soon as you get beyond 1500, it all just goes to pot pretty quickly. So those are the only two answers I've seen around those areas.

RAM MOHAN Joe.

JOE ABLEY Joe, so I think what Geoff says is pretty accurate. There's one thing that you didn't mention, Geoff, which is use of DOH, DOT, those kinds of transport protocols where we do demonstrably have a server side that can handle big responses because it's the same way that we serve the web.

GEOFF HUSTON: You're right, Joe, but the deployment numbers are almost microscopic at this point [CROSSTALK].

JOE ABLEY: I'm not suggesting it's widespread, but I'm saying that we can separate DNSSEC as a means of providing authentic answers from the transport. The fact that it doesn't work with the common transports today is definitively a challenge for the use of DNSSEC today. But for example, if we saw a resurgence of the ideas around, I think people called it zero RTT DNS, the idea of interleaving DNS responses in HTTPS bundles that are otherwise serving regular MIME objects, which opens the door to sort of delivering DNS responses out of the hot path because you can predict what names might be needed for the next click, as is often done with predictive cache pushes through CDNs like Cloudflare.

I mean, you could imagine an answer there where the validation overhead is not actually causing a change in page load time, but is sitting there in the browser ahead of time. You have validated answers ready for someone to click, and then you could do validation in the stub. So I'm not saying this is likely, but it's the kind of thing that if one big CDN or a couple of big CDNs said, yes, this could actually become quite prevalent. It's not necessarily something that requires enormous truck roll across a large number of applications. So again, I'm not disagreeing with what you said about the world today, but I'm saying that doesn't necessarily mean that there isn't a future in which this is different.

GEOFF HUSTON For the record, I agree with you, Joe. That's an accurate observation. The future might change, yes.

RAM MOHAN Okay. I have Peter, then I have Rick, Warren, and Steve. You took it down. Okay, Rick.

RICK WILHELM I'd like to agree with the point that Geoff made and further, no pun intended, amplify it since Geoff was talking about load. But Geoff kind of talked about server load. When I was learning about DNS capacity in some way that I was taught to keep a very much closer eye on network capacity about bandwidth attacks, because I learned that DDoS attack or bandwidth attacks primarily, and that normally you'll exhaust the bandwidth, especially when you're talking about hitting TCP and stuff. So yes, and to what Geoff said, but also in addition to server capacity, it's network capacity. It'd be very quickly exhausted if everything went TCP. So at least that's what we used to worry about. Thanks.

RAM MOHAN Thanks, Warren.

WARREN KUMARI So I wasn't going to open this can of worms, but seeing as Geoff and--

GEOFF HUSTON Go there, Warren, go there.

WARREN KUMARI Others have. One could make a fairly good argument that Doe and Dot and similar end up replacing the need for DNSSEC. Yep. I knew I was going to get the funny look from Russ. So currently what happens is if I'm using a validating resolver, my laptop connects to 8.8.8.8 or something and says, please give me the answer. And what I get back is I get back an answer from 8.8.8.8 or 1.1.1.1, and there's a bit that is set saying, don't worry, I did this check-in for you.

What that bit is sort of in theory kind of protecting against is somebody along the path having fiddled with things kind of maybe sort of. The actual, like the majority, you end up largely trusting that your resolver has done the right thing, right? You're trusting that your resolver has set this bit correctly. If you're doing Doe or others, what you are potentially doing is having a trusted connection to this resolver and you're just trusting what the resolver sends you anyway. If you have a trusted connection from the recursive resolver to the authoritative because it's done over some encrypted thing, then potentially what you're doing is you're just trusting that connection as well.

I don't necessarily agree with this, but if the concern was things like cash poisoning and you can validate where you're getting the data from because you have a way to trust that and you can trust your connection to the resolver and you've been trusting the resolver anyway up until now, you're just sort of have layers of trust instead. The thing where this all goes sideways and I think where DNSSEC went sideways is you're not actually validating the answer yourself. You're trusting the resolver to have done it. You're trusting the person who did the signing to have done stuff correctly. By moving to an encrypted transport, you no longer have to worry about somebody on the path making a set of changes. You have changed your trust model to be endpoint to endpoint and sort of ignoring, no.

PETER THOMASSEN Hello, Warren.

RAM MOHAN Actually, Steve had his hand before you. Sorry.

STEVE CROCKER So two things. First of all, with apologies, I'm going to bolt just after this comment. I am increasingly concerned about trying to draw a line about the scope of this report versus the bigger question. I worry about how you're going to, even if you complete the report, put the things in it, what impact it's going to have on the community? What are we going to, how are we going to

communicate it and what effect are we going to try to achieve? So my sense is that we may want to step back a bit and say, don't we have to include the considerations that we're talking about, about where DNSSEC fits and what the trust models look like and the technology and all of that?

RAM MOHAN I've tried to make a go of it in Section 5 findings, and we may have to do more there, Steve, but I've tried to, at least on number two, for example, I've tried to go there.

STEVE CROCKER And that's reflected, I haven't been paying as close attention to the text there, but does the introduction cover that as well?

RAM MOHAN Well, I think we'll have to get to that. I mean, the way I'm looking at it is we get the content in and then we make sure that the introduction.

STEVE CROCKER You don't have to answer me. I just raised the question here. Thank you all very much.

RAM MOHAN Thanks, Steve. Could you turn the mic off? Peter and then Russ.

PETER THOMASSEN Hello, Warren. Do you know MyEtherWallet.com? MyEtherWallet.com. Okay, so you know that incident that happened with them? So what happened is that they used Route 53 and there was a B2B hijack on the Route 53 IP address space and attackers set up fake name servers and send fake responses. And if the site had used DNSSEC, then that would have been caught. I mean, not the hijack, but the responses wouldn't have been accepted. So there would have been no fake page. And without DNSSEC and DOE or DOT instead, how would that have helped?

WARREN KUMARI So presumably, when I make the connection to Route 53, there would be a TLS connection, right? DOT, DOH. I'm saying you need the authoritative part of this as well. It's clearly not just the recursive. You need authoritative DOE. You need authoritative DOT. Basically, potentially where we're heading with DELEG and stuff.

PETER THOMASSEN I see. I thought you were focusing on the client-reserve.

WARREN KUMARI Oh, no, no, no. You need this all the way down. Otherwise, all you've done is you've taken an untrusted bit and you've stuck it in a sort of tunnel. But yeah, you need to have all the things. And I

don't really think that I'm necessarily supporting this as a good argument because I think it is useful to be able to get the root zone as a trusted blob and validate the signature through some other manner. You could make the argument that if you get the root zone directly from IANA and it is signed with the TLS certificate for IANA, that's why you should trust the root zone. In fact, there are some of the local host, sorry, local root instances, which actually get the DNS zone information over HTTPS and trust it because of the server.

STEVE CROCKER You two just made the point that I was going to make, which is you're really doing hop by hop security.

RAM MOHAN Okay. We have just about 10 minutes left. So this has been a good discussion. We will not have time to go through all the rest of the comments. Chaoyi, what do you think we should be doing here? We set up a work party call in two weeks' time and we then start to go through the comments step by step. This has been a productive conversation.

CHAOYI LU Yeah, I agree with that.

RAM MOHAN

Well, I propose two weeks because I'll be unavailable that week. Chaoyi will have to run the work party. Just joking. The one question that I did not find a place to resolve or a place to necessarily put in was what Rick was talking about and Rick was proposing, which had to do with user considerations or the user experience. And I don't know what to do with it. So I wonder if you guys have any thoughts, Rick? Yeah.

RICK WILHELM

While we were discussing, I think we made some progress. I think Michael's scrolling the screen. Is that right? Who's scrolling the screen? Michael is. Yeah. Okay. So 2.3 got put in there and there's been a bit of-- I scribbled some junk in there and Michael tarted it up and rewrote it. And so there's some stuff in there that deserves, could get updated. There's a spot in there for folks to improve upon it. And so, yeah, as it says over there on the right, please improve these sub bullets. So we've kind of put something in there. And so please go in and add your own special sauce.

RAM MOHAN

Got it, thanks. The other part that I didn't know what to do with was what Warren was saying. He was saying, Warren, that in the finding section where we have a piece that says, and there's links to what Joe was saying, but it's a link topic number three on findings, mandates to implement DNSSEC should be tempered by the knowledge that not all TLDs and ccTLDs are ready to deploy DNSSEC. But Warren, you were saying something about those who

deploy should know the pros and cons while they deploy or before they deploy. I don't know what we're trying to say there.

WARREN KUMARI

I also don't really know how we'd say it, but I also wonder at this point if number 3 is actually OBE, because we've already mandated that all gTLDs have to do it. And I can't see us undoing that. But basically, all ccTLDs have already. So I think it's more not just mandating gTLDs or others, but that strongly suggesting that people need to do this or otherwise they're bad people should be tempered by making sure that they're not going to shoot themselves in the foot.

RAM MOHAN

Gotcha. Still doesn't address my question, Warren, which is, what do we say about pros and cons? Should we actually have a section? Or is a document in total, when people read it, is going to come up with, they'll be able to summarize and say, here are the pros and cons? Joe.

JOE ABLEY

Joe? So I don't necessarily know that we should try and make an exhaustive list of pros and cons, because pros and cons are going to be different from every perspective. Everyone has different risk profile. I don't know that that's useful. We can maybe give some examples of case studies and illustrate the ways of thinking about this other than just, is it good? Is it bad? Which is probably not

helpful. I think that the more important thing is to frame the thing in terms of your own decisions about your own risk profile, and point out that sometimes it's applicable to incorporate this into your security approach, sometimes it isn't. And that there are costs of doing it, just like everything. I think we could usefully make the point that framing it like that is the right way to think about it, and not say that if you're not adopting it, you're behind the curve or you're insecure, which is the inference that I think a lot of the ICANN messaging has given.

RAM MOHAN Thanks. And just before I come to you, Warren, I think that part should be a recommendation that we make to ICANN, that they should consider changing their messaging.

JOE ABLEY I mean, I will say I'm not current on what ICANN's advice is. So I think we should obviously check and make sure that their current advice also hasn't matured on its own. But I mean, if there are gaps between what we think and the way that they're currently approaching this, I think we could ask them. I don't know that we should be in the business of telling staff what to do, but I think we could certainly suggest that they incorporate this thinking into the way that they do it.

RAM MOHAN Thanks. Waren?

WARREN KUMARI Yeah. I mean, the one sort of sticky bit in all of this is, if one looks at like the top hundred TLDs in terms of usage and stuff, they, the majority of them, and I would assume all of them, have done some hard thinking about whether they want to sign or not. And at the moment for the top hundred, the signature number is only a hundred, sorry, only 6%. Mission accomplished. So like the top hundred TLDs are probably the least signed out of everything. If you look at the top million.

PETER THOMASSEN I don't understand what you mean. Like you mean the second level names are 6% or what?

WARREN KUMARI So of the top hundred domains on the internet measured by the ITHI index, which is like number of queries and blah, blah, blah. Yes. Did I say TLD? Yeah. Okay. Sorry. The top hundred names, not top hundred TLDs, only 6% are signed. And then the numbers go up from that, right? 6%, then like 17%, 10% for the top thousand to 10,000, 7% for the top 10,000 to a hundred thousand. And then it drops back down when you get into the millions number.

So I don't know what message to take away from that, other than people who've sat and thought about how to minimize their

opportunity for downtime made a decision. And it's not the whole signing on the fly thing. Like a while back, the answer was it's too hard to sign on the fly. That's not why, as far as I know, that's not why very much any of the top hundred people aren't signing. Signing on the fly is relatively trivial, especially because these days, many of the large sites are just a small number of IPs and they're just any cost, but that's a separate rant.

RAM MOHAN Thanks. Joe?

JOE ABLEY Well, your conclusion there is interesting because I was about to say the opposite. So I realize I don't have any good data, so I'm not disagreeing with you, but there certainly was a time when most or all of those top Alexa something, which was the list that I used to look at, didn't do their own DNS. They used external providers to do their DNS. This is going back in the day. So they used Dyn, they used other people, and it just was not an option. If you wanted the stupid DNS tricks that your DNS company would provide, then DNSSEC was not an option because they did not at that time have an option of doing online signing and doing the special DNS tricks at response time and generating a signature to cover. I certainly obviously know that it's possible because Cloudflare does it.

WARREN KUMARI I mean, that's an interesting thought. I hadn't thought of that. I mean, I'm viewing it through the, where I happen to work, we all do our own DNS and Google has not currently signed.

GEOFF HUSTON I have put in the chat, Joe and Warren, current data from Cloudflare's 1.1.1.1 recursive resolver service. Of the names that it gets queried, 3. 7% of those names are DNSSEC signed, the other 96 point whatever percent are unsigned.

JOE ABLEY So, I mean, that doesn't sound very surprising. I think there is a difference between there are people who are not in the position to make a decision about whether to sign because their DNS enterprise, DNS provider doesn't give them the option and people who've made an informed decision not to sign or other people who just didn't think about it. So, I don't know how to distinguish between those.

WARREN KUMARI And I mean, I do think that the data that Geoff put in here is fascinating because a lot of the metrics we've been doing is we count the number of signed domains and those go up and to the right. But that is working on the assumption that domain names have equal value. And no matter how much I try and pretend otherwise, www.kamari.net is not nearly as interesting as www.tiktok or insert other or whatever. Not as many people care

about my thing as they do about Taylor Swift. I don't understand why. I mean, obviously, I'm more awesome than Taylor Swift in every conceivable manner.

MICHAEL PUCKETT Rick, I see your hand up.

RICK WILHELM Yep, thank you. So, I put a comment in the document that Ram didn't understand. And so, that got him to call me, which is an amazing thing to do. Love you, Ram. So, one of the things I noticed in comment three, in finding number three, is that we say mandates implement DNSSEC, blah, blah, blah. It occurs to me that our comment here should be broadened because Steve brought up the mandate to implement DNSSEC inside the U.S. Government. And our comment here should, I think, be more expansive because mandates could be implemented by a variety of entities.

And our guidance here should not only be to ICANN or TLD operators, but it should be to very large enterprises, to government entities, and things like this. Because people without clue, I think that word appears in the transcript at least once or twice, that sort of issue these broad sweeping edicts, thou shalt, and then those things go down into the masses, and poor people are faced with whatever.

Joe gave the example of when these things happen in and around the ICANN, but we've all seen it happen in and around governments. It happens also inside of very large enterprises where these kind of-- I've seen that happen inside of enterprises, too, not so much with DNSSEC, but with other technologies. So, you need to upgrade to the latest version of this or do that. So, I think that we should rewrite this to be a little bit more expansive. Thank you. Take a look at what I wrote.

RAM MOHAN

Okay. So, we are out of time. We will schedule the next call. This has been very helpful, very useful. We've made progress. Thanks, everyone. This session is concluded.

[END OF TRANSCRIPTION]