# Fast Flux PDP WG Teleconference
# TRANSCRIPTION
# Wednesday 29 July 2009 at 14:30 UTC

**Note:** The following is the output of transcribing from an audio recording of the Fast Flux PDP WG teleconference on Wednesday 29 July 2009, at 14:30 UTC. Although the transcription is largely accurate, in some cases it is incomplete or inaccurate due to inaudible passages or transcription errors. It is posted as an aid to understanding the proceedings at the meeting, but should not be treated as an authoritative record. The audio is also available at:
http://audio.icann.org/gnso/gnso-ff-20090729.mp3

On page:
http://gnso.icann.org/calendar/#july

**Present for the teleconference:**
James Bladel - GodaddyRRc - Working Group chair
Paul Diaz - Network Solutions
Mark Rodenbaugh - CBUC
Greg Aaron - Afilias Ry c.
Joe St Sauveur
Dave Piscitello (joined after roll call)

**Observers** (no constituency affiliation)
Randall Vaughn
Rod Rasmussen

**Staff:**
Marika Konings
Glen de Saint Gery
Gisella Gruber-White

**Apologies:**
Kal Fehrer (for all Wednesday calls)

Coordinator: This call is now being recorded. Please go ahead.

Gisella Gruber-White: Thank you good afternoon everyone. I'll do quick role call.

On today's call we have Joe St Sauver, Mike Rodenbaugh, Greg Aaron, James Bladel, Randal Vaughn, Paul Diaz, Rod Rasmussen. We have from staff Marika Konings, Glen DeSaintgery, myself, Gisella Gruber-White. And apologies for all Wednesday calls we have Kal Fehrer. Thank you.

James Bladel: Thank you, Gisella, and good morning everyone to the diehards that are getting this report finished and over the finish line. So we have a list of the final edits that Marika had posted to the mailing lists. Does everyone have that bulleted list?

Dave Piscitello: Yes, Dave joined by the way.

James Bladel: Oh, hi Dave. Okay. So if we can start there and Marika since I have a kind of a rough connection area here, maybe perhaps you could go through each of the lists and then I'll jump in for the items if we want to discuss some.

But I think, essentially, what we're looking for is broad, if not unanimous consent to these changes.

Marika Konings: Okay. And then just to point out the change that I listed in this email are the ones that I thought were more substantial. While they're more edits but they're more spelling or you know just minor corrections.

But if anyone else has found any other change that they would like to discuss, you know, suggest (that maybe do it) when we get through this list they raise them and we can consider those as well. So the first one on this list is line 332 to 334.

Mike Rodenbaugh: Marika, can you just step one - take one step back please. What email are you referring to?

Marika Konings: I sent an email on Monday, July 27 at 16:24 in which I basically outlined the changes that have been made between the previous version and this version based on comments submitted by Dave, James and Joe.

The facilitator review I highlighted those that made some - or not substantial change but made changes to the content or meaning of certain sections.

Mike Rodenbaugh: All right. I've got it front of me now.

Marika Konings: Yes, your fine then. (And) if there are any other items people would like to discuss or review I would propose it at the end of this list they bring those up as well.

So the first one is looking at Line 332 to 334, three lines have been added there stating that the fast flux working group does identify solutions that could result in policy development but the fast flux working group could not reach a consensus on whether these should be policy, best practices or industry solutions.

And if I remember correctly, I think (Dave) you suggested that this should be added, no?

Dave Piscitello: Just a minute. I'm actually looking at this. I don't think that's mine. Perhaps it is. I'd have to go back and look. I don't have any objection to it.

Marika Konings: Is there any objection to adding this to this section?

Paul Diaz: This is Paul. I'm just - perhaps a word-smithing request in 333. Instead of saying identify solutions that could result. How about something like responses or answers or something?

Solutions to me just means, you know, sort of like why don't you take this. It's - I guess I'm just hung-up on the word solutions. It seems like if I'm a third party reading this I'm wondering well if they have an answer why didn't they come to consensus on it.

Does anybody just share that? It seems that we say we identify solutions but then we go on to say yet we couldn't even identify it and it should be policy, practices or industry solutions. I'm not really...

James Bladel: Would you prefer the idea or the word ideas? Or...

Paul Diaz: Just some other word. Am I the only one? It just seems the word solutions is sort of, you know, it should be the end result and yet if we've identified it, it just begs the question why couldn't the group come to agreement on whether it should be policy or practices.

Man: Okay. I think I see what you're saying.

Paul Diaz: It might be a little thing.

Man: That's fair, I think.

Mike Rodenbaugh Maybe if we did either change the two ideas or some other word as you suggested or even put potential in front of the word solution.

Paul Diaz: Sure.

Man: While we're word-smithing, can we change "does identify" to "has identified?"

Man: I agree with that change. More active than...

Mike Rodenbaugh: Has identified potential solution?

Man: Yes.

Man: That work for everybody?

Man: Yes, that sounds good.

Man: Okay.

Marika Konings: So this is change them to the fast flux working group has identified potential solutions (but) good results. Everyone fine with that? Okay. Then the next one is a comment on Line 673, now let me just scroll down as well.

James Bladel: This was, I believe, Joe's comment that we should try to put this list in some sort of order either alphabetical or some such and I think that makes sense, so.

Marika Konings: Yes and he added as well the suggestion of maybe ordering it on the number of calls attended. I mean of course I would add another dimension to it because there are quite a number of names on this list that haven't participated or have only participated in a few calls.

Joe St Sauver: I should probably clarify that. That's actually for the second table, so in terms of this table at (4.1) last name.

But then for the final table on like the last page, that's the one I was saying it sort of seems like that's trying to report on the call frequency. And that's the one where I think it might make sense to have that one ordered by call frequency.

So this one obviously doesn't have call frequency, no need to screw with it in that regard, so. But just to kind of alphabetize it by last name.

James Bladel: Okay, does anyone have any objections reordering this table? Going once, okay.

Marika Konings: So alphabetize it on last name?

Joe St Sauveur: I think so.

Marika Konings: Okay.

Joe St Sauveur: Alphabetize that on last names and then if we look at the last table if we can.

Marika Konings: Yes, on call frequency. Okay, we'll do that because we will need to add as well of course this call to that list. So we need to change it anyways. Okay, has been noted.

Then the next one is change to Line 785. There - I think we initially had there an alternative viewpoint.

And I think, (Dave), this was again you that suggested taking that away as I think it linked with some other comments we made in changing it to members of the fast flux working group observe that artificially limiting TTLs via consensus policies we'll simply move the problem beyond the purview of ICANN. Any objections...

Greg Aaron: Well, it's actually more complicated than that. I don't think actually TTLs can be limited via ICANN consensus policy because it's an RFC issue. So it's an IETF thing. So I don't think this wording captures the situation.

Dave Piscitello: You know, Greg, I'm not sure it's an IETF issue because it's an operational practice and, you know, it would be - there hasn't been a (BCP) out of the IETF in since I had a full head of hair, so.

Greg Aaron: Well, I read about TTLs pretty extensively in the registry constituency comments. And the issue with TTLs is that there not set by - effective TTLs are not set by registries or usually even registrars. They're set by hosting providers and whoever controls and operates name servers.

So to effectively deal with the problem you have to basically change the way the RFCs work. If there was a consensus policy there's binding fund registries or registrars it wouldn't matter. It wouldn't actually solve the problem. And effect TTLs in a meaningful way.

James Bladel? So Greg and (Dave) and anyone else who wants to chime in. Is there a way without transforming this sentence into a couple paragraphs? Is there a way to save that (we're artificially eliminating) TTLs is not a - what I want to say - quick or silver-bullet-type solution.

Is there a way to save that without bringing in all the dependencies and all the different factors that play into that?

Dave Piscitello: Let me explain what I was trying to accomplish in one sentence because I think Greg is over reaching what my ambition was. We've been criticized in a number of (forums), you know, when we go and talk, we being the ICANN community, about why don't we just simply restrict TTLs.

There's also been, you know, a lame effort by someone in the IETF to do the same thing. The answer that I think is appropriate from the ICANN community that even if we did this, you know, it wouldn't have any effect.

So I'm really not ambivalent about how we say it. I just think it's important that we say, look we've listened to you and you've told us that we should do this. But if we did it, it would have no effect.

It's the same as telling people the speed limit is 55 and you can't drive over 55. Well you can't drive over 55 unless, you know, is an absolutely (unintelligible) kind of situation.
So we have the same situation in, you know, if we told registries and registrars they weren't allowed to put anything in the (zone file) that had a TTL (unintelligible).

So I really don't care how we say that. You know, and if other people feel strongly that we shouldn't say anything, that's fine too. I'm just trying to answer something that has been asked of us over and over and over again.

Man: Okay. So perhaps...

Greg Aaron: I think the answer there (Dave) is that - what I see is people are asking about TTLs they need to dig into actually how it works in the DNS.

Dave Piscitello: But that's not going to - yes, I understand...

Greg Aaron: And ICANN gets criticism...

((Crosstalk))

Greg Aaron: ...is not necessarily a compelling reason to respond to it if it's - it is in my opinion irrelevant because the registries and the registrars don't control the TTLs on these domains ultimately. I mean we have a note later in the paper at, let me see, 1110 that touches on it. But...

Marika Konings: Greg, if we would remove via consensus policies would that address some of your concerns? Because then we don't say that, you know, it would be ICANN doing it. It might been as well be through another means like IETF but would that be (unintelligible).

Greg Aaron: Well, (it'd be) -- there are two issues. (Dave) is I think - and correct me if I'm wrong, (Dave). You're trying to say that if ICANN gets policy then it would just move the problems of ccTLDs.

Dave Piscitello: It would move the problem to anyone actually. And you can hijack the zone and you can stick it on a bot and you can do whatever you want with it. I mean the problem isn't with - isn't solely our remit to solve is what I'm saying. And we, you know, yes.

Greg Aaron: Now I understand what you're trying to say. That was a good encapsulation. Think it - say the members of the fast flux working group observed that artificially limiting TTLs will one, be ineffective period.

Dave Piscitello: That's fine too, you know. I mean I'm happy with that. I just want to call attention to it. You know, and then if we want since Greg did a great job of writing in great detail in the registry constituency statement, we can just say that, you know, the reasons are amplified in the registry constituency statement and annex whatever it is.

James Bladel? That's a good idea, (Dave). If we can refer to, you know, something that expands upon why we feel it's ineffective. But I agree if we can shorten that to just that sentence and then diffuse some of that criticism because I've seen it too, (Dave).

Man: I have to just go ahead and say that ICANN does not control operational TTL values for the DNS.

Dave Piscitello That works too.

Man: My thoughts exactly.

Man: Yes.

Man: Yes.

Man: So members of the fast flux working group observe that artificially limiting TTLs will be ineffective as well - will be ineffective and...

Man: Ineffective period.

Man: Ineffective period, okay.

((Crosstalk))

Marika Konings: Can we just put it should be noted that ICANN does not control the operational TTLs values for the DNS. Was that the sentence?

Man: Right.

Marika Konings: Okay and then do we want to add then after the first sentence for further information please see registry constituency statement and annex whatever number it is? So people can find more information.

Man: I think that's a good idea.

Man: That's a good idea.

Man: Yes, that works. Thank you.

Marika Konings: Okay, I think I captured that all.

Man: Okay.

Marika Konings: Then the next - does anyone have any other further comments on this one or we can move to the next one.

The next one is a deletion at Line 884. There was a bullet point noting that - well the first one here the fast flux working groups offers the initial - the following initial working adds to the charter questions but would like to emphasize that continue work is required in the following areas.

And the bullet that has been deleted there is (a robust) technical and process definition of fast flux. And I think, again, I think, (Dave), you suggested this one.

Basically saying that we have - the working group has developed (a robust) definitions. So I think you state that you felt that this could be removed there. Am I correct?

Dave Piscitello: Yes.

Marika Konings: Are there any objections?

Dave Piscitello: My dog is emphatically excited about this.

Man: I think that's probably legacy language from the proprietor when we finished up the definition section. I remember - at least that was my take on it.

Marika Konings: Then on the next - in addition to Line 1111 to 1112, let me just set that one up. And there it's basically a reference again to the registry statement for further information that (unintelligible) and then the basic sentence has been added saying the fast flux working group finds the registry constituency statement sufficient and accurate for the purposes of this report.

Any comments? Okay, then we move to the next one which is a comment on Line 1483, moving down there, think I'm another one down because I actually don't have a comment here.

Oh, sorry, I think this should be 1438. There's a comment from (Dave) on this sentence related to the port 53 (traffic) in which he notes the context is missing. Does this mean that ISP should not allow residential PCs to accept DNS queries? (Dave), do you have a suggestion on how to add the context or...

((Crosstalk))

Man: I'm asking a question. I don't understand, you know, I'm not certain what this is alluding to.

Man: Essentially what the deal there is is that a growing number of ISPs are going ahead and doing things like intercepting DNS query traffic that may be going to rogue DNS resolvers off network.

So if you think about things like DNS change their malware essentially what happens is those guys go ahead and hijack the DNS traffic by actually changing the resolvers that the customer uses.

So some ISPs have taken to blocking or intercepting and redirecting port-53 traffic that's going to odd places other than their servers. So that's kind of what's meant by managing port-53 traffic.

Man: Okay, so it's - I thought that what you were saying here was that broadband providers were not allowing customers to host main circuits and that you were referring to queries that were being directed out to a broadband - an IP address allocated to a broadband network.

Man: In this context, that is correct.

Man: Yes, so that was the context I was making. But then if no one else had a problem with that then we don't have to make the change.

Man: Do we need to change port-53 traffic to, you know, provide something that's a little more for both than what we said here?

Man: I mean you could change it to say forbid customers from hosting name servers on residential broadband hosts or something like that.

Man: I like the word managing better than forbid. But - so if managing DNS resolvers that exist on customer broadband networks. Any thoughts there?

Man: Yes, the part - I was asking a question on, you know, I think that'll work.

Man: No it's a good catch.

Marika Konings: So just to confirm, it would then read controlling that DNS traffic requires managing DNS resolvers that exist on customer broadband networks, locking external DNS queries (unintelligible) so on and on. So we just take out the port-53 traffic?

Man: Right.

Marika Konings: Okay. Just wanted to make sure I got that.

Man: We should probably remove managing port-53 traffic, all four words as it were.

Marika Konings: Okay.

Man: Do we lose a verb if we take out managing?

Marika Konings: Yes but managing DNS resolvers - that stays, no?

Man: And you get the (jeren) blocking in there, so it actually takes care of that. I knew that English class would in come in there somewhere, (jeren).

Man: Okay.

Man: That one class (we took).

Man: And I hated it, let me tell you.

Marika Konings: Okay, the next one is a comment on line 1497, just scrolling down. Another one from (Dave) asking whether it is appropriate to explain what a net flow slow flow is and how this would help trace back to traffic flow origins.

Man: And this was also part of what I put forth as well where I was saying are we talking about a category of tools are we naming products here because I'm not familiar with net flow or (s-flow).

And I'm thinking that perhaps we could - simply just - perhaps even a footnote, if someone can provide a URL that describes this particular tool, what it does, what its capabilities are, what its limitations are, something like that.

Joe St Sauver: My recollection is I sent in pointers to the two RFCs, could we just go ahead and use the RFCs to go ahead and kind of clarify what they are and what they do?

Man: An excellent idea, Joe.

Marika Konings: Joe, would you mind resending those to me? I'm sure I have them somewhere.

Man: I didn't see that.

Joe St Sauver: Okay.

Marika Konings: Okay, so I'll add those links then in the footnote to that specific issue. And then the next one is an additional line 1550, I think it relates to the previous discussion we had.

It's in addition to basically that the working group considered several possible options including governing time to live values and in between brackets, minimum (bounds) in TTLs within the scope of ICANN policy (end) agreement. I think, (Dave), this was again you, if I'm not mistaken.

(Dave): I'm sorry, can you repeat the line number? I'm missing that.

Marika Konings: It's 1550, 1-5-5-0.

Dave Piscitello: Thank you.

Man: Didn't we just say that limiting time to (live) values is not within ICANN's remit?

Man: Right, I think with the earlier changes, I'm wondering if that paragraph is even...

Man: Just drop it.

Man: ...required, yes.

(Dave): Actually that was supposed to read minimum bounds on TTLs is not within their scope of (unintelligible) remit.

Yes, I think this paragraph is actually legacy and we didn't - all we really need to say here is that we - this progress could summarize what we had the discussion earlier, can simply say the work group considered several possible options including governing time to (live) values.

And then eliminate most of this and say and concluded that establishing minimum bounds on TTLs was not within the scope of ICANN policy and remit.

Man: Maybe we can also reference it.

Dave Piscitello: And reference the registry constituency statement again because it's not true that we were - the last statement is in fact incorrect because the working group did reach consensus. I don't think any of us agree that or believe that, you know, we have any right to tinker with TTL value.

Marika Konings: So would it be sufficient then just to add to that sentence like (unintelligible) TTLs are not within the scope of ICANN policy and remit. See registry constituency statement for further details?

((Crosstalk))

Man: Yes, something like that, Marika, and borrowing heavily from the previous discussion on this earlier in the document.

Marika Konings: Okay. I'll make that change. Then the next one is 1567 - that's actually 1568, I think (unintelligible). So we got a comment from (Dave) right to the sentence mandating that multiple contacts must confirm DNS updates before they go into effect will be problematic.

And the comment from (Dave) reads, "I have to object to this claim on the basis that (ASAC) is making such a recommendation and (ASAC) 40 measures to protect registrations services against exportation or (misuse)."

The claim here suffers from the same tunnel vision that cause people to conclude that short TTLs indicate fast flux. If you couple strong verification measures, non refutable with the rule that multiple contacts must confirm DNS updates, you would reduce or mitigate the likely abuse by criminal suggestions in line 1707.

Man: Can I - I see what (Dave) is saying as it were - we're kind of being contradictory a little bit. But I'm wondering if the last sentence here is I think really the salient point of this paragraph is, you know, once we get into compromised domains and we're talking about hijacked domains and things like that, really anything goes as far as abusive behavior.

So I just - I want to be sure that we're not taking two steps down a slippery slope by trying to offer commentary or suggestions on that problem. But I'm wondering if this paragraph can be shortened or perhaps eliminated all together. I mean, it's something that we considered but, you know, it starts to open up a number of other issues.

Dave Piscitello: I think one thing that we could do is we can punt it to (ASAC) and we can say that, you know, mandating, you know - or we could just make mention that, you know, the security and (civil liberty) advisory committee is studying whether, you know, providing multiple contacts to confirm DNS updates would be an effective deterrent to certain, you know, aspects of malicious use of domain name.

Man: Someone else was trying to get in there as well?

Man: I was just going to say that, you know, I'm not sure that we're really seeing people hijacking domain names to go ahead and use those fast flux. They just go ahead and buy them.

So if they've bought them, presumably they'd be able to supply the multiple contacts that might be required.

I just don't see it being an effective measure. I mean the multiple contacts thing is really more designed to ensure that eBay doesn't get pointed to some random location in, you know, South America right?

Man: Correct.

Man: Sure, this particular measure or deterrent would be - is to protect more about - more of the legitimate organization that has an account compromised than somebody, you know, somebody maliciously alters their domain server.

So you probably - I imagine that the incident where fast flux factors would, you know, malicious fast flux factors would be doing that would be small because it's not a straightforward to pass, you're right.

Man: Okay, so (Dave), you know, we've got a couple of options here to shorten this paragraph or to throw it overboard as maybe it was a side topic that really didn’t take us in any new direction. What are your thoughts on that?

Dave Piscitello: Yes, I think the original reason why all these bullet items were here was to - was for the working group, you know, to have acknowledge the suggestions made in (stack) 25.

So if you - I understand now what Joe was saying and maybe the right thing to do is to rewrite that sentence saying that this would not really be effective or not really be an effective deterrent in the fast flux case because such, you know, or domains used by fast flux typically, you know, newly registered as opposed to comprised registration.

Well that would certainly satisfy my comment and I think it would be, you know, an accurate summary of what Joe aptly described as the typical case as opposed to the (unintelligible) case.

Man: So something is...

Man: I would not throw this paragraph out. I mean, at least the concept because it has been raised as a potential solution in some sectors as a way of doing this, so we need to acknowledge it and limitations that come with it.

Man: Okay, so something along the lines of managing the multiple contacts - mandating the multiple contacts, you must confirm DNS updates before they go into effect is not a viable solution as they would - this - as fast flux - domains used in fast-flux are not necessarily compromised domains?

Man: Not typically compromised domains but newly registered domain.

Man: Right and then the second sentence also solving for hijacked domains is (unintelligible) outside the scope of this working group. Is that too clumsy or does that work?

Man: It's fine for me.

Man: Works for me.

Man: I can live with it.

Man: Marika, we went over that pretty fast.

Marika Konings: I think I got the first sentence but do we want to take out the sentence on such a validation process, did I get...

Man: Yes.

Marika Konings: So we take that out on...

Man: I think we want to take out...

Marika Konings: Okay, so then just to confirm read, mandating that multiple contacts must confirm DNS updates before they go into effect is not a viable solution as domain names used in fast flux are not necessarily hijacked domains. Also solving for hijacked domains is a separate problem outside the scope of this working group. Correct?

Man: Yes.

Man: I like it.

Man: Yes.

Marika Konings: Okay. Then we move on to 2119, I think we're getting now to the conclusions section.

So 2119 there is a - let me just read it, there was a proposed addition deleted, (unintelligible) but I think it actually was deleted in the previous review, following comments from Joe St Sauver who strongly disagrees with the proposed language as criminal fast flux involves hosting on comprised broadband connected host while legitimate (agile) hosting does not.

I think the problem is that you cannot actually see the little deletion anymore.

Man: And what line number were we on again?

Marika Konings: This is 2119.

Man: So this particular change is 2116 is where that - couple lines above, correct?

Marika Konings: Yes, there was a section there that was deleted but because I accepted all the changes between the previous version and this one, cannot - actually not see what was deleted.

Joe St Sauver: I think my point simply was that where was a lot of kind of dithery language at the start of the section and it really kind of reflected more of the old, earlier philosophy and not sort of where we are at currently I think.

Marika Konings: I can look back where the deletion was but if I recall, I don't think it was a big thing. And so then the next one is 2132, am I right?

Or no, wait because I actually didn't list this one, the one that I wanted to go to was actually the one in - I think back to list 2119, that related to the sentence, the fast flux working group understands that many types of organizations can potentially be involved in fast flux use including registries, registrars, IFCs, hosting firms and other online businesses.

And Joe's made a comment there saying strongly disagree, this assertion (conflates) various (address) agile methods with true fast flux. With only rare exception, legitimate organizations will not knowingly be participating in fast flux hosting methods exposing bottled hosts. Legitimate organizations may be abused by fast fluxers but that is a different issue.

Man: Yes, I think we need some word-smithing here. I mean involved in fast flux use, I'm not sure what that means. It sounds pretty...

Man: I think I was the original person behind that sentence and my purpose or point was just to kind of say that, you know, there's not one single bottleneck that we can - or one single type of organization that sits at the crossroads of everything that someone would need that can mitigate the abuse of fast flux just by controlling that particular type of organization.

I think it goes back to what we were saying earlier that the problem just moves somewhere else. So, you know, if there's a better way of saying that instead of...

Marika Konings: Can we say effective - affected instead of involved?

Man: Be affected by fast flux use, that would be - I think that would be fine.

Man: Except a lot of them aren't really affected by it. They may be potentially unknowingly involved but they're not really affected by it. So I think if you were to add potentially unknowingly involved that could go ahead and take care of the issue.

Man: Okay. And putting those two adverbs together, could we say parentheses and unknowingly or can potentially - how about potentially be involved in fast flux use without their knowledge or without their consent?

Man: You could use exploited - no, sorry.

Man: I guess the point is that they may be involved but they're involved either peripherally or they're involved without their intentional ascent, I mean it's something where they're kind of roped into it, where they may not even know they're involved.

Man: You could get rid of potentially and say unintentionally involved.

Man: Okay because we've already captured potentially with the word can.

Man: Yes.

Man: I would agree.

Man: Okay. So...

Marika Konings: So the consensus, the fast flux (unintelligible) understands that many types of organizations can be unintentionally involved in fast flux use.

Man: Beauty.

Man: Yes.

Marika Konings: Correct, okay. And the next one is 2132 and we have a comment from Joe related to this - the sentence, additionally measures could be adopted to help ensure that parties reporting fast flux activity are trustworthy and uncompromised.

And Joe states that the existence of objective tools for assessing fast (fluxness) such as a (unintelligible) formula means that reporting party reputation is effectively irrelevant. A site is not fast flux because I say it is but because the data confirms that it is. Trustworthiness has nothing to do with whether or not a given qualified domain name is fluxing or not.

Man: Well I'll go ahead and throw the simplest solution out there, what if we drop the sentence beginning with additionally?

Man: That would suit me.

Man: I mean, was the concern here that someone would compromise - that bad actors would compromise that reporting system?

Man: I think traditionally it kind of comes out of the phishing world where people are concerned that someone's going to go ahead and have like a false positive, that they're going to report a legitimate site as phishing, get it taken down and then somebody's going to go ahead and end up suing them.

But in this case fast flux is something that's able to be objectively assessed so, you know, the trustworthiness of the reporter really doesn't matter.

Man: Well let me ask you a question, Joe. How does somebody know when - are you suggesting that any time somebody reports fast flux activity, that a registrar will always ask to see the data before they take action?

Joe St Sauver: I think there should be data supporting an assertion that someone is fast flux, yes.

Man: So I think that's part of what, you know, I think removing the sentence doesn't quite accomplish what you're suggesting because I think what you're suggesting is that, you know, parties reporting fast flux activity, you know, will typically be required to present, you know, sufficient data to support the claim.

Joe St Sauver: No, they wouldn't need to support - or they wouldn't need to provide the data because you wouldn't have any way of verifying that their data's accurate. You'd need to basically go ahead and accumulate your own data as, you know, oversight entity.

Man: Additionally - I'm sorry - additionally measures can be adopted to ensure that reports of fast flux activity are verifiable because I think we've pretty well established that we can make fairly good judgments about that.

Man: I think that's - yes that's more accurate than deleting this or, you know, making modifications.

Man: Okay, so we would just remove trustworthy and uncompromised and put verifiable in its place.

Man: That reports are verifiable.

Man: Correct.

Man: Fine with me.

Man: Excuse me.

Marika Konings: All right. Could you repeat then where the verifiable (unintelligible) additional measures could be adopted to help ensure that parties reporting fast flux activity are verifiable?

Man: You could just say fast flux activity reports are verifiable.

Marika Konings: Okay, so...

Man: Well, we're still using the noun of parties, so I would suggest that we strike parties and then we'd say additionally measures could be adopted to help ensure that reports of fast flux activity are verifiable.

Man: Yes.

Man: Fine.

Marika Konings: Okay, got that. And the next one is on line 2137. I think it's again Joe (unintelligible) sentence, those domains will still require some form of mitigation in order to end or prevent the undesired activity. And Joe notes, yes. Mitigation would involve holding or suspending a domain involved with fast flux.

Joe St Sauver: My point there is just being that, you know, we kind of seem like we dance around the issue which is essentially at some point these domains need to get dealt with. And the way they get dealt with is pretty straight-forward I think.

Man: That's true.

Man: Okay. And then the suggested language I just wanted to point out that the same potentially be involved phrase is here that we addressed earlier. But that's totally a separate issue.

Joe St Sauver: My point I guess is just that the sentence kind of makes it sound like there's going to be a gee wiz R&D effort required to figure out what to do here. And it's really a pretty straight-forward process. It's (reflecting), you know, and (unintelligible) should go ahead and (get held).

Man: Okay. So locking or suspending...

Man: Yes. My suggestion would be - would still require suspension of the domains in order to end or prevent the undesired activity.

Man: That would be fine.

Man: That's - it doesn't reflect reality though. I mean a lot of people delete, a lot of people point them to other places. So suspension is...

Man: Well it's, yes, I mean that's...

Man: (Pretty general).

Man: True. That's not the only way you can do it. I mean it's very - unless the domain's in grace period, registrars usually don't delete them. But sometimes they catch these early. So suspension, yes, it would be suspension, deletion or...

Marika Konings: Redirection.

Man: ...sinkholing - sinkholing actually. Does that work for you, Rod?

Rod Rasmussen: Yes. That's fine.

Marika Konings: There will be, there's a major (unintelligible) required suspension, deletion or...

Man: Sinkholing. Sinkhole is one word.

Marika Konings: Sinkholing of the domain.

Man: Yes.

Marika Konings: Okay.

Man: (Is that) spellchecker?

Marika Konings: Yes. I'm sure it won't recognize it. I think I'll have to Google it probably to make sure I get it right.

Man: I think spellchecker went ahead and got spamvertising everywhere I notice too.

Marika Konings: Yes. It didn't like that word either. So the next one is (unintelligible) 2139. This next sentence (unintelligible) from a domain registry or registrar to DNS or hosting service providers.

Another comment from Joe stating that, "Only the domain, registry or registrar can suspend the domain and thus they are the only ones who can ultimately stop a fast (fluxing) domain."

Joe St Sauver: And the reason for my saying that is, you know, if they have a DNS service provider that's not being as cooperative as they like they just change their DNS, you know. And in terms of hosting providers this is the fast flux.

There is no hosting provider. They're on a compromised broadband, you know, host. So I think the DNS or hosting services provider term should be removed.

Man: I think that those are there because, you know, they actually are involved. (In other words) I think your point is quite important that they're involved, but they can't actually directly affect the final outcome for it - for the domain.

Marika Konings: So should there be any changes to this line or we leave it as is?

Man: I would say go ahead and remove to DNS or hosting service providers.

Man: I would disagree with that.

Man: Yes. I would disagree as well. You know, you can say...

Man: ...it's a problem with the entire sentence. It's just because we said it for...

Man: I mean what hosting service provider would be involved?

Man: Yes.

Man: You've got a whole context here around detection and identification, et cetera. You know, they're involved. (Unintelligible) they're being exploited typically.

Man: There you go.

Man: But no, I mean because the hosting service providers aren't in the loop at all because this is being done on broadband, you know, compromise host unlike the DNS guys. The DNS guys may be involved, but only until they do something and then they get replaced.

Man: Right. And ISPs might be better than hosting service providers.

James Bladel: Can we say other hosting - other service providers instead of DNS or hosting?

Man: I can live with that.

Man: Yes.

Marika Konings: Could you repeat that, James?

James Bladel: It would say from a domain registry or registrar, comma, or other service providers.

Marika Konings: Okay. That's noted. And then the last one is a comment on 2211 (unintelligible).

Man: That was just a reaction to the comment that, you know, we really can't do anything because if we go ahead and fix this one there's going to be something else bad that they're going to find to exploit. Well that may be true, but that doesn't mean that we should go ahead and let them have fast flux as a freebie without any attempt to control or fix it.

Marika Konings: So the thing you guys are talking about a comment on the same page (unintelligible) addition that you proposed.

Man: (We're on 59). Sorry if we weren't there yet.

Marika Konings: Yes. Okay.

Man: Which - I'm sorry, what line number are we on, Marika?

Marika Konings: (Unintelligible) my lines have moved slightly because of course I'm adding text.

Man: Okay.

Marika Konings: I think it's further down on this page. I guess it must be 2158, there's an addition proposed by Joe, despite availability of a portfolio of exploitable approaches it does not justify feeding fast flux or any other criminally exploitable technique to the miscreants for their unfettered use and abuse.

Man: All I can say it's just a reaction to the preceding sentence.

Man: I like that addition.

Man: Yes. I think I don't have any problems with that idea. But is miscreants the word we want? Do we want bad actors, criminals?

Man: I like criminals.

Man: I don't know what the right word is.

Man: Miscreants is kind of a team (unintelligible) term, but, you know, (unintelligible) to do it.

Marika Konings: So change to criminals?

Man: Sure.

Marika Konings: Okay. And then there's a last comment on line 2211 from (Dave) (unintelligible) the findings of such audits should then be communicated to the broader community.

And (Dave) adds a comment here saying one possible (corollary) addition to this recommendation would be to recommend that ICANN study ways in which it could provide acknowledgments, (trust sales), as far as a (SSL), a monetary incentives for registrars and registries that voluntarily submit to an audit that measures the implementation of best practices.

In the (SSL) world (traits), VeriSign and other certificate authorities operate trusted mark programs. A merchant can implement all the criterion for satisfying the program (unintelligible) party with the ability to indicate so through a trust mark.

This is similar to ICANN's accreditations seal. Studies demonstrate that customers choose merchants who earn its seals over competitors. It's reasonable to assume that they would choose among registries and registrars in this manner as well.

Man: I like that addition.

James Bladel: I don't necessarily - this is James - I don't necessarily have any critique of that particular addition. I just have some questions. One, is this really a new recommendation? And if so, do we want to capture it as such?

And two, this idea of a seal, if we're talking about criminals, if I'm looking to set up or use some sort of a service provider to conduct fast flux exploit, wouldn't I avoid those types of trusted seals?

I'm just trying to explore this idea a little bit because I understand the program of some sort of a seal of approval or just logo that can be displayed. But I'm just wondering if it's a new idea that hasn't fully been thought of.

Man: We certainly knew it was in the context of this working group. So I think it would have...

Man: Well actually, I mean I will (confess) to having been doing three things at once, one of which was working on an SBAC document where we talked about this. And this was sort of a stream of consciousness observation.

It is new here. It is something that will be in (unintelligible). It will probably be studied elsewhere. It's not absolutely necessary to include it here if, you know, if we're going to add a significant amount of discussion and possibly create some point of dissension. So I'm comfortable.

Man: I like the first sentence there, (Dave), if you just get rid of the seal. (Unintelligible) provide acknowledgment or incentives. I'd probably get rid of monetary. But (if there's) a way to state that briefly, I do like the idea. But, you know...

((Crosstalk))

Man: Personally I would remove the word submit to an audit and I would just say registries and registrars that voluntarily implement the best practices.

Man: That's a reasonable - yes, that's a reasonable point here because going - yes, mentioning the word audit is a sensitive issue when we actually talk about it in much more detail in the SBAC report. So that's probably a reasonable modification.

Man: Okay. So Marika...

Marika Konings: So then it would read after the word community one possible addition to this recommendation would be to recommend that ICANN study ways in which it could provide acknowledgments and (unintelligible) for registrars and registries that voluntarily implement best practices, correct?

Man: Acknowledgment or incentives.

Marika Konings: Okay, (unintelligible).

Man: I'm fine with that, but I think ICANN might have trouble with that because there's only one way to incent registries and registrars.

Man: Well, you know what - I mean right now that would probably - there is no way to incent registrars because the agreements are the agreement and the contract to the contract. But in future contracts there might be clauses that basically set, you know, set from, you know, some measures and, you know, and it's, you know...

Man: That's a way to...

((Crosstalk))

Man: That's a way to obligate registries and registrars. I thought (we were) incentives.

Man: No, I mean the incentive would be that it's as an example, you know, your per-domain fee is reduced by some percent if you meet the best practices in a measurable manner.

There's also disincentives which would say if you are a total screw-up and you're not doing this then we charge you more because you're making trouble for everybody else.

It's not necessarily, you know, meaning to registrar services, you know, registration services. It would be something that, you know, lots of companies could do that tend to get bogged down in the details of measurement because that's where all the wiggle room is.

Man: Okay. So, James, in the next sentence I would suggest dropping (unintelligible) and VeriSign, just have it say certificate authorities because basically they're both the same company. What about all the other CAs that are out there? We don't to be showing any favoritism.

Marika Konings: Are we adding that because I...

((Crosstalk))

Man: No, I think that whole thought is actually going away.

Man: That's going away? Okay, just...

Marika Konings: So, it's just a comment then. All the comments will be removed, but just added that one sentence there to (defection).

Man: Great.

Marika Konings: And I think that covers it for all the major changes. I don't know if we're - if anyone else has any other items they would like to raise or discuss...

Man: (Unintelligible).

Marika Konings: ...in the last two minutes.

Man: Yes. And actually I would say that - I would like to propose to the group that, you know, we treat this as kind of, you know, we're already in extra innings in a lot of different ways with this particular report and project.

But I think that this was really good information that we wanted to capture and plush up some of these thoughts and comments. The next steps would be I think if we can post that revision, Marika, in the next couple of days and maybe keep it open not for weeks and weeks, but just for a few more days, give folks an opportunity to see it in its total finished form.

And then also to comment on the draft motion that I posted at about 2:00 o'clock this morning and particularly focusing on the results section because I really was, you know, shooting from the hip in that particular section of the motion.

Marika Konings: If I can add one thing to that is something I discussed with James in (raising) of the motion, something that the group could consider as well recommending to the Council is organizing a workshop or meeting in (the fall) to discuss the report and especially the ideas that have been proposed for next steps.

And, you know, have some feedback maybe from the broader community where people feel, you know, would be a reasonable way to move forward or, you know, what would be the best thing to focus on where there's (unintelligible) community support. (Can we see) if that's something that this group (think) would be helpful as a, you know, next step in this whole process.

Mike Rodenbach: I personally think it might be more harmful than good to wait and put that into the process. I mean the Council could take this report now and, you know, start acting on it well before. So I don't see what good a public workshop (in the fall) is going to do.

Marika Konings: It does not - I mean, Mike, (unintelligible), I don't mean as much before the Council decides, but as a way as well to - because I presume the Council will look at these next steps and decide to take them forward.

And (the fall) meeting could then be a way as well to already involve the community and get some feedback on those next steps and how to take them forward. That was more my thinking.

Mike Rodenbach: Yes, okay. I hear you. But that's also, you know, three months from now. And a lot can be accomplished in the meanwhile to get things moving. And I feel like if we make that recommendation to the Council then the Council will do nothing until after that workshop happens.

And frankly I don't see what good is going to come out of that workshop. Can we put the report out for public comment? Doesn't that normally happen with the final report anyway?

Marika Konings: I don't think so. I think it normally goes after the - if there are any recommendations that go to the Board then I think there's normally a public comment period after the Council adopts the recommendations and before they go to the Board.

But is there no recommendations for consensus policies? I don't think normally there's a public comment period, but I presume the Council could decide to have a public comment period if you would like to.

Mike Rodenbach: That's right. Or we can just decide to take some of the next steps anyway without further public input because obviously we've had public input throughout this process of a working group.

I don't know. I'm pretty heavily against recommending that we do a workshop on this. I frankly just don't find workshops very useful most of the time at ICANN meetings anyway. And I don't see what we're hoping to get out of this one...

Marika Konings: Well my question would be - because a lot of the ideas for next steps are very basic and not very detailed. What would be - what do you think would be the likely scenario for how to take this further because...

Mike RodenbaughFor example I think that the Council should be recommending to the (RAP) working group that they consider that recommendation that we've made that, you know, they look at solutions that would help remedy fast flux exploits as well as all the other registration abuses that that group is looking at.

Plus one thing I think the Council could do right away is don't need any further public input on that. I'll have to look at the other recommendations really quick. But I don't know. I mean can you justify what would come out of a public forum on this in three months that we need to wait for?

Marika Konings: No. It's more, you know, because (unintelligible). I think some of the discussions, like for example the data reporting system or, you know, ICANN as a best practices facilitator and as well involving other stakeholders.

Those are maybe questions that, you know, would benefit from some (unintelligible) discussion as to how those things should look or how they can be taken further.

Man: Well I think I understand part of what Mike is suggesting because while we've been struggling with the same kind of issue in terms of recommendations in SBAC, one of the requests from the Board of Directors was that when, you know, SOs and ACs have, you know, make recommendations, especially if some of them result in recommendations that percolate up to the Board, that they be very specific and actionable.

And so I interpret what Mike is saying more like we've got a specific recommendation for the (RAP) group. We should tell the Council forward this recommendation to the (RAP) group.

If we have a specific recommendation for SBAC to do something we should, you know, write the recommendation specifically (unintelligible) SBAC or, you know, as opposed to bringing it up for more discussion which might be enlightening to some people who haven't been involved in the process for the past year.

But it is probably not going to result in that much more, you know, constructive thinking and it's probably not going to result in refining the recommendations. Did I capture what you were saying, Mike?

Mike Rodenbach: Pretty much. I mean this report is done. It's not going to be reopened because of the public workshop for one thing.

Marika Konings: No, no, no. I mean I wouldn't question that. But it's more like who will be the people taking these different recommendations forward? I mean, yes, on the (RAP) one, that one is obvious. But on the other ones...

Man: Marika...

Man: (Unintelligible) could pass something along to ICANN. If we're going to actually talk about, you know, ICANN in some way, shape or form either helping set best practices or recognizing, you know, recognizing best practices and measuring them, that's ICANN's staff shoulders at that point.

And it either falls into the compliance world or into, you know, policy, security, compliance, multi-departmental activities.

James Bladel: And, Marika, this is James. I think that, you know, and maybe I agree with Mike although maybe for slightly different reasons. I don't necessarily want to put a workshop out there just because it gives the impression that we're somehow unfinished.

I think we have some packaged recommendations. And, you know, each one is directed at whether it's directed at staff or interested stakeholders or, you know, future (PVP)s or successor (PVP)s, et cetera.

And I think that, you know, those could involve workshops or whatever types of involvement. I guess we're leaving it somewhat open-ended and that's not necessarily a bad thing.

So I think I agree that, you know, mentioning a specific means to get community involvement and stakeholder involvement and staff involvement and all that stuff is maybe secondary to just recommending that it's happened and then leaving it at that.

Marika Konings: Okay.

Man: I would also say that the meeting in Asia is going to be more likely attended by folks interested in fast flux issues than it would be if it was somewhere easier to reach or more inexpensive to reach.

Mike Rodenbach: That's the problem I have with workshops in general is they tend to get way too much weight from staff and others based on the very few people that tend to participate and come to the ICANN meetings.

You know, this has been out for public comment. The working group was wide open to anybody to participate. I just don't feel like, you know, a workshop is going to add anything.

Marika Konings: And again, my idea wasn't to, you know, question or, you know, anything about what's in the report. That's, you know, once this is done, it's done. But there's more looking ahead and, you know, how to move forward with those recommendations in an efficient manner.

That was more of the thinking. But if everyone feels that all of these can be taken forward just by Council action then that's fine.

Man: Yes. I think that, you know, I felt bad enough writing the results clauses that we're meeting with somewhat still open-ended with loose threads. And I'd just hate to introduce even more, so.

Man: So one of the things that we might want to do is schedule a (unintelligible) or schedule, you know, with some opportunity to, you know, to summarize, you know, the report for the community.

But I think that's different than a workshop and it could be part of the whole e-crimes or abuse of DNS workshops that we've sort of, you know, run over the past several meetings or it was something (unintelligible).

But I think it would be useful to, you know, to try to help, you know, crystallize some of the information that is in this (350) page report and especially from, you know, one of the objectives I would hope we would try to do is help people understand the difference between a fast flux attack network and, you know, our production use of volatile networking.

I think that that is a very, very important, you know, distinguishing effort that we need to be involved in because we're probably, you know, among the few people that have actually had to tackle both sides of it.

And, you know, if I were to struggle to try to, you know, come to agreement and appreciation for both and get both of the communities to actually appreciate that we've made that effort, worked so hard and long we might save a lot of other people a lot of, you know, a lot of (frustrating cycles).

Man: Well we're over our time here by a little bit, but I think the consensus is, Marika, that, you know, there's some recommendations here that we've tried to translate into action, not necessarily a punt, but more as a if you choose X then, you know, this is this the Y approach, but not to be met at a limiting fashion.

And if any of the other groups want to take up this report as a part of their agenda, you know, I think we certainly are open and encouraging of that without necessarily making a separate and dedicated fast flux event at any future meetings.

So - but can we say that we want to put this draft of motion on the list here and that if we can close off any comment on this by, you know, let's say by Friday, Saturday timeframe. It's not a very long document.

And I know that everybody's busy, but I really would like to get at least this part of it flushed out in a matter of days rather than waiting too long into next week. Does that seem reasonable?

Mike Rodenbach: I think so. I have one issue maybe quickly covered. The results paragraph, it says to consider the inclusion of other stakeholders from within and outside ICANN for any thoughts of - any future thoughts policy development efforts.

What are we talking about there? That makes it seem like, you know, for some reason we weren't as open as we need to be or something.

Man: Yes. I think that, Mike, going back to the recommendations I think - and forgive me I did this at 2:00 am, but there's something in the recommendations towards the end about exploring the possibilities to involve other stakeholders.

And then it lists just a laundry list of all the different groups and law enforcement agencies and all those types of things that we're trying to maybe clumsily to encapsulate that into within and without the ICANN community, so.

Marika Konings: I mean just to note as well in the report itself it does say the fast flux program was open to anyone, had representation from the (APWG) and (ASAC) and that several members of some of these other organizations.

But the working group recognized however that ICANN policy development is not a familiar or accessible activity for many organizations and the fast flux working group encourages further outreach to achieve a broader group.

((Crosstalk))

Marika Konings: And in the actual report that is, you know, captured, that it was open and there was participation, but maybe not broad enough.

Man: And, Mike, if there's a better way to say that without listing all of those groups, I mean - and all those acronyms, I mean I'm all for it. I just...

Mike Rodenbach: I'll word-smith it probably just with another phrase. Something like wow, the working group was open and has broad representation, comma, and then the rest of it.

Man: Okay. Okay.

((Crosstalk))

Man: Before we call an end to things, can I just inject one quick thing? On Annex 6 went ahead and actually had a WHOIS substitution there that capitalized WHOIS throughout the whole document including Annex 6.

And that's going to go ahead and actually break like the WHOIS examples that are in there because WHOIS is a Unix command. It's all lower case. So can the WHOIS's that were changed in Annex 6 be unchanged?

Marika Konings: Okay.

Man: And then the other thing that's kind of weird about that is the formatting because originally it was (monospaced) and then it's in a proportional font. Some of the stuff comes out looking pretty junky.

So can that either be changed back to (monospaced) font for the stuff that's currently looking kind of ragged or can that go ahead and be lined up with tabs?

Marika Konings: Which - is (it all) the same annex you're referring to?

Man: Right. Like on Page 114, there's an example of like WHOIS from Google. And in the original WHOIS it all kind of lines up because it was done (monospaced) in the output, but now kind of junky looking because it's...

Marika Konings: Okay.

Man: ...all proportional spaced.

Marika Konings: Okay. I get what you mean.

Man: There's, you know, other examples where the same sort of thing farther down, but...

Man: The other thing is I'm wondering if we have any issues including things like live email addresses in there. I didn't think about that until I happened to go ahead and see them underlined as well.

Man: Yes, I think if there's any, you know, we should sanitize that to make sure that they're not putting any specific data in there, either x-ing it out or even changing the entire thing to example.com.

Man: Well that kind of makes it impossible to actually have the honest-to-God data there, but...

Man: Yes, understood.

Man: For things like email addresses or phone numbers...

Man: Yes.

Man: ...maybe we can just X those out like they're done on the comments form, Marika.

Marika Konings: Just - you mean in the WHOIS records - (is what) we're talking about in the same annex.

Man: Right.

Marika Konings: So phone numbers and emails, fax numbers as well?

Man: I guess so.

Marika Konings: And address?

Man: I mean, it's all public data I guess at this point. But, you know, the question is whether or not that should go ahead and receive sort of permanent placement, if you see what I mean.

Man: Right.

Marika Konings: Well to be perfectly honest of course I have the many versions of this report that are posted and have the data as well.

Man: Yes. I was going to say that, yes, the ship's sailed on this.

Man: Yes. Let's close the barn doors before the horses get back in.

Man: All right.

Man: Just thought I'd mention it.

Man: That's a good point. It's a good point. Okay. Well let's, you know, belatedly bring this call to a close. And I guess the next steps are we'll be looking for an updated report. I see that Joe has already sent some the IETF links for (unintelligible). So thank you for that.

And, Mike, you said you were going to take another look at the results section and maybe word-smith some of my late night language in there. And then if we can put some hard expiration, you know, non-negotiable, iron-clad expiration dates on when we can get changes in and get this submitted to Council I think that would be helping it - all of us could get behind at this point.

So I was thinking for the motion if we could close off comments by the end of this week. And then for the final version of the report, once Marika has it, maybe we could (give) four or five days, certainly not much longer than a week and then we call that complete and polished. Sound good?

Man: Cool.

((Crosstalk))

Man: Thanks very much for everyone for - and thanks to Marika. She's the one that's probably bearing a lot of the burden on this and some of these changes.

Marika Konings: Thanks all of you.

Man: So, you know, so thanks to Marika and staff and thanks for everyone helping, you know, it was an hour and 14 minutes here on the call. And I think it probably saved a day if not longer on the list. So thank you very much for coming in today and to clear up some of these last minute comments and we'll see you on the list.

Man: Very good.

Man: Okay. Bye.

Man: Bye guys.

Man: Bye.

Coordinator: Thanks for participating in today's conference call. You may now disconnect.

Marika Konings: Thank you.

END