ICANN84 | AGM – Joint Meeting: GAC and ccNSO
Wednesday, October 29, 2025 – 10:30 to 12:00 IST

NICOLAS CABALLERO: Welcome, everyone. Please take your seats. We're about to start. I was going to say precisely that. Go ahead, please, Gulten. Thank you, Nico.

GULTEN TEPE: Welcome to the GAC Meeting with the ccNSO session on Wednesday, 29th of October at 10:30 UTC. Please note that this session is being recorded and is governed by the ICANN expected standards of behavior, ICANN Community Participant Code of Conduct, and the ICANN Community Anti-Harassment Policy. During this session, questions or comments will only be read aloud if submitted in the proper form in the Zoom chat pod. Interpretation for this session will include all six UN languages and Portuguese.

If you would like to speak during this session, please raise your hand in the Zoom room. And please remember to state your name for the record and the language you will be speaking in case speaking a language other than English. And please speak at a reasonable pace to allow for accurate interpretation. I will now hand the floor over to GAC Chair, Nicolas Caballero. Thank you.

NICOLAS CABALLERO: Thank you very much, Gulten. Welcome, everyone. I have the pleasure of introducing my colleagues from the ccNSO and the ccNSO Chair, Alejandra, right to my next, to my right, I'm sorry, right to my right hand. We're going to have a very interesting and, I would say, engaging session today, more or less the way the way we did in, was it Seattle or in Seattle? And the idea is to have active participation and ask questions and engage.

There's no wrong question, just in case. We're going to have different stations, so to say. Before we set the scene and we have a presentation on Cryptocurrency Investment Fraud Example that will be given by our colleague Gabe Andrews from the FBI, I'll give the floor to Alejandra for some housekeeping details as regarding the dynamics of the session today. Welcome, everyone. Alejandra, the floor is yours.

ALEJANDRA REYNOSO: Thank you, Nico. And it's always a pleasure to join the GAC and to do these different methodologies with you all. We believe it's very productive. Before going into the details of the active part, I think it would be best if we hear from Gabriel. And when he finishes, I will be more than delighted to tell you all about the next part. Thank you for inviting us.

NICOLAS CABALLERO: Thank you very much, Alejandra. So, now I'll give the floor to Gabe Andrews from the FBI. Gabe, the floor is yours. Please go ahead.

GABRIEL ANDREWS

Thank you, Nico. Thank you, Alejandra. Let's go ahead and go to the next slide to start. I'm going to be talking to you today about the top category of Internet crime that's reported to the FBI over the last several years. We're calling it Cryptocurrency Investment Fraud. In the media, it's also been called pig butchering. So, they're one and the same if you've heard that term. We're talking about this in the hopes that it can inform our ongoing DNS Abuse conversations.

This is a category of crime that was born out of COVID. It's one of the many bad things that we received in COVID years. What happened was there were Southeast Asian organized crime rings that were operating casino hotels in the region. When COVID hit, those hotels weren't making the money. So, they explored alternative means of making money.

One of those methods was to entice migrant workers to come and work for them. Once they came, they were held captive, turned into forced slave labor, and forced to target Westerners with fraud schemes. It's turned out that this has been very effective and the slave labor component is going to be very important for a reason that I'll come to in a moment.

So, we're going to quickly cover just some of the headlines that have been in the news in the last year. In May of this year, the UN released a report to highlight the importance of awareness of this ongoing scheme as a call to action to the world. We saw that in the

last seven days, the army of Myanmar raided one of these forced labor compounds. Next slide.

We saw that SpaceX in the last week has cut Starlink services to some of these Myanmar-based scam camps. And within the last week as well, my own Department of Justice in the U.S. seized more than $15 billion of Bitcoin currency from just one of these criminal scam rings. This was called the Prince Group.

I will note that this is the largest forfeiture action, the largest seizure ever done by the FBI, or not just FBI, by the U.S. for anything of all time. Let's go ahead and go to the next slide.

So, the way that this works is there's phishing that's conducted at the start of the scheme, but it's not done through email. Instead, you will typically see via one of your texting apps on your mobile device or through social media or sometimes through dating sites.

You'll see one of those accidental messages that come from someone that entice you just to start a conversation. They often will pose as someone who's interested in a friendship or a romantic relationship or business investment, what have you, but it starts slow. And what's really important about this is that the slave labor component enables the phishers to really take their time and build rapport.

Go ahead and go to the next slide. So, that by the time that they do actually turn the conversation to the potential to invest in some new and exciting cryptocurrency opportunity, it comes only after a

protracted rapport-building phase. This makes it very different than traditional phishing that we've seen in the past, where it would be just maybe one very well-crafted email.

Instead, this is a very slow phishing process that's built up over days or weeks that can only happen because these people are themselves being held captive and forced into the slave labor and turning the labor itself into a trivial expense for the bad guys.

Let's go ahead and go to the next slide. The domain component here, because I'm sure you're wondering, if it's not an email, then what is the actual domain name component that's involved? When the phish-hook is eventually set and the bad guys will say, oh, I just had this wonderful return on my investment. This is what happened. I'd love to share this opportunity with you and so forth.

What they'll provide via those chat messages is a link to their cryptocurrency exchange. It's a homoglyph domain usually that impersonates other legitimate exchanges. The bad guys, when they register these, will register them in bulk. When we talk about bulk or API access to bulk domain registrations, this is one of the ways criminals use bulk domain registrations.

They'll register hundreds or thousands at a time of domains that impersonate these cryptocurrency exchanges. Next slide, please. When they set up the infrastructure, and I apologize, this is a very small font slide. I took it from another presentation or press release on this game.

To explain it, what will happen is on the left side there in those rectangles that are pink and purple and yellow, they'll start off with a collection of those lookalike domains that they can just roll through. They're used no more than three months at a time.

If one of them gets burned, they quickly move to the next because they have so very many of them to choose from. But using a technique called CNAME forwarding or changing the canonical name settings in these domains, they will set the domain to route to the next domain and then to a next domain before finally reaching the cryptocurrency site at the end.

This is a trick that keeps the name of the lookalike domain in the browser, but goes through several hops of infrastructure before finally resolving. And so, I don't expect everyone to be familiar with CNAME settings, but for those who are in the audience that maybe are familiar and especially those that operate ccTLDs, I wanted you to be aware of this tactic.

So if you bump up into it, you'll recognize it for what it is. When the investigators go to investigate this, we find that it makes it harder for us to explore their infrastructure because of this tactic. So, they do it for those two reasons, to make it harder for investigators and to enable themselves to very rapidly cycle through those bulk registered domains, while keeping a much smaller number of protected infrastructure domains behind it.

So, to set the table for the ongoing discussions today, I wanted to raise the scheme for familiarity, but also to ask our partners and

our colleagues in the ccNSO, if this is something that they're seeing in their own space. I'm aware that in the gTLD space, .com, .top, .info were used, .net, but that's not something that I'm comfortable saying that we have perfect visibility into.

And there's very real chance that they're using the ccTLD space as well. And there's a number of different rings doing this kind of scheme now. So, different rings could be using different infrastructure. So one of the questions I hope to tee up for the conversation is, are you seeing abuse reports that involve this, that involve maybe bulk registrations of cryptocurrency sites, or that maybe involves CNAME forwarding that you're able to observe?

And then further, for the conversations that we'll have about the potential policymaking in the gTLD space with ICANN, when we're considering policy based around perhaps what we call an associated domain checks, when if you get an abuse report about one domain, that there would be a requirement to look at the other domains registered at the same time and see if they're involved in the scheme too. Or if we were to do a separate policy for controls on access to bulk registrations, such as through the APIs that enable them, we're wondering if the ccNSO has experiences that might inform our contemplation of such policy.

And so having set the table in that regard, I think I'm hitting my eight-minute clock and my timer. I want to thank you all for your attention on this. I feel it's a really big whole of world global response happening to the scheme right now. And I'm very happy

that you can be part of the conversation and addressing it. Thank you.

NICOLAS CABALLERO: Thank you so much, Gabe. Very interesting. And there you go. There we go. There we have the questions. And this is especially important for the ccTLD operators. Are you receiving abuse reports on this? That's on the one hand. Are you seeking bulk registrations plus CNAME forwarding on the other hand? And then you have some more questions there. But before we go any deeper, let me give the floor to Alejandra, who's going to walk us through the details and the nuances of how we will be operating for the next 75 minutes during the session with the ccNSO. So, over to you, Alejandra.

ALEJANDRA REYNOSO: Thank you, Nico, and thank you, Gabriel, for the presentation. I know you had limited time. We'll take your questions and give you feedback afterwards. For the next activity, we will have, as we did before, a more interactive, literally on your feet experience to discuss several topics on DNS Abuse with people from the GAC and people from the ccNSO to understand different topics, such as in Station 1, we have the use of artificial intelligence in abuse detection and prevention.

In Station 2, we have challenges of bulk domain registrations, which is quite in tune to what we just heard. In Station 3, we have

investigating abuse with domain portfolios. Station 4, we have national frameworks for scam and fraud prevention. And in Station 5, we have trusted notifier arrangements.

So the way this is going to go is, taking your feedback from last time, you wanted us to have more rounds. But having more rounds means we have less time per round. So, this time, we will have three rounds. So, in each round, you can choose the station you want to go. When the time's up, you change stations to whichever you want to go. And yes, we have five stations.

You will have three opportunities to interact with them. But in the end, we will also include a summary wrap-up from each station, so you don't get devoid of not having gone to one of the stations.

And here we go. These are the stations. We will keep these up so you can move around. And how are we controlling the time? Bart? Oh, we will display a timer here? Okay. So, with that, Nico, shall we?

NICOLAS CABALLERO Thank you so very much for that. Alejandra, before we move on and before we start with the stations and the rounds, I just wanted to go back to Gabe's points and questions. I would like to get some feedback from the floor or those online.

In order to address the questions Gabe gave, let me allocate three or five minutes to that before we actually start with the rounds and the stations and the heavyweight DNS championship. So, the floor

is open. Any feedback, especially coming from the ccTLD operators on the topic of CNAME forwarding? And again, we don't expect everybody in the room to be an expert in DNS hoping or CNAME forwarding and those kinds of things. But Alejandra? Yeah, go ahead.

ALEJANDRA REYNOSO To kick start that conversation, I would like to address the question to the ccNSO in particular, whether we would consider developing a policy for this. And I just want to reiterate that the ccNSO has a very limited remit on where it can develop policies. And the policies are aimed to IANA to deal with how to manage the ccTLDs. Like, for example, retirement of ccTLDs, transfer, and all those operations in IANA.

So, we do not develop policy to tell ccTLDs how to do their work. Nevertheless, we do have a DNS Abuse standing committee, which was a huge part in arranging this session with all of you. And there we are collecting a repository of best practices to share with the world on how each ccTLD is dealing with that. And I believe that this activity that we are about to have may expand that conversation a bit further since I'm not seeing many hands up. Thank you.

NICOLAS CABALLERO Thank you so very much for that feedback, Alejandra. So, give me just one more minute in order to address the second question as

regarding the experiences that ccNSO operators might have, might or might not have that might inform such policy. And I see no hands in the room. No hands online. So, okay. So, back to you. Let's get to the thank you again, Gabe, if you're still online. Thank you so much. That's really important and certainly relevant to all GAC representatives. Thank you so much for that presentation. Alejandra, back to you.

ALEJANDRA REYNOSO Thank you. And we take these questions with us and we will come back to Gabriel with them. And thank you. So, with this, I invite you now to stand up and go to the station of your preference. I'll keep the timer here. And for this first round, we will have 18 minutes. So, your time starts now.

Hello, everybody. Time's up. So, please finish your conversation and change stations. Thank you. We will start the clock in one minute.

Quick reminder, we are going to start the second round. So please change your station and move to your next station. Can we please restart the timer? Thank you.

Hi, everyone. This is a two-minute warning. Two minutes.

All right, time's up. Wrap it up and change stations for the third round. We will start the timer in one minute. Thank you.

All right, I hope you have reached your third destination. We will start the timer now. Thank you.

This is the two-minute warning. Two minutes.

Time's up. Thank you all. Please return to your seats and to the hosts and scribes, please stay in your stations so we're ready for the summaries. Everyone else, thank you for participating and come back to your seats so we can summarize the activity.

Okay, ten more seconds to go back to your seats so we can start with the summaries.

So, I think we're ready. We will have a rolling mic going station to station for the summary. May I start with station number one, use of Artificial Intelligence in abuse detection and prevention. Please, Nico.

NICOLAS CABALLERO Thank you very much. We had in station one, as regarding the use of Artificial Intelligence and machine learning, in the first place, we explained with Christian from the .nl, we had a fantastic three-round mini-session on AI and ML, and we explained the differences, what is AI, what is ML, what is deep learning, what is generative AI, the difference between ChatGPT and so on and so forth, and how the algorithms are actually used to detect DNS threats and all that kind of stuff, and DNS traffic and a whole bunch of other things are actually used that are not necessarily related to LLMs or generative AI and the differences and so on and so forth.

And the measures in this case, Netherlands and the team from the Netherlands are implementing in order to combat DNS Abuse, many good questions, good and intelligent questions, not only about the technology itself, but the implementation, the internal mechanics, and how the whole thing actually works at an internal level, what happens under the hood, so to say.

So, very interesting. I liked it very much, and I hope that the participants also liked it. And so, thank you very much again to Chris and the .nl team over there. So, that's my short super mini-report from Station 1. Back to you.

ALEJANDRA REYNOSO Thank you very much, Nico. Moving along to Station 2, challenges of bulk domain registrations with Peter Koch and Martina Barbero.

PETER KOCH Yeah, thank you. So, we talked about bulk registrations, and don't worry, we did not come up with a definition what a bulk registration is, but we discussed for some time why that is a challenge on one side, but on the other hand, not so important.

We also discussed automated registration, and we differentiated between the communication between the registrar and the registry versus automated registration support for others, and found out where that is potentially something to look into. And I'll hand over the microphone to Martina for more details of the results. Thank you.

MARTINA BARBERO

Thank you very much. And it was also a very interesting discussion with a lot of good questions, but in a nutshell what we discussed about in terms of how to address concerns related to bulk registration, we discussed about the tension between identification with the ability to understand the intent of the bulk registrations, as some of these use cases for bulk registration, like brands registering multiple domains, are legitimate.

So, which kind of friction do you put, and how do you address the identification without discouraging the legitimate use cases? And in that respect, when we spoke about identification, we mentioned the difference between identifying organizations and identifying individuals, which requires different practices and approaches.

We also touched upon many different practices from the ccTLD space, with some registries that do look at behaviors that are suspicious after delegation and recognize those and try to address those when linked to bulk registration, and some other registries that are addressing those kinds of suspicious behaviors before delegation itself.

And in general, we spoke about the importance of being conscious of the amount of damages that can be done in very little time with the phishing campaigns, as we heard from our colleague Gabe earlier. And therefore, the reactivity and the time that you need to address ill-intentioned behavior needs to be speedy, which of course is a limitation and needs to be taken into account when we

speak about remedies. Unfortunately, we did not have a lot of brilliant ideas on how to solve this on the spot, but I hope this was already helpful.

ALEJANDRA REYNOSO: Thank you so much. Moving along to station number three that I have here at the table, we have Investigating Abuse Within Domain Portfolios with Crystal Peterson and Susan Chalmers.

SUSAN CHALMERS: Thank you so much. Susan Chalmers from the United States and NTIA, which is the policy authority for the .US Country Code Top-Level Domain, joined by Crystal Peterson here from Registry Services, who administers the .US ccTLD. I'll just share a few overarching points and then turn it to Crystal. But our corner was looking at what would be looked at in the policy development, upcoming policy development process for associated domain checks, and that is when an abuse report is received.

The U.S. TLD registry is actually the authoritative source for registrant information in the .US zone, so that is rather unique. Also, I should note that the U.S. TLD prohibits, as a matter of policy, the use of privacy and proxy services. So, all of the registrant data that is in the database is real registrant data, which puts us in a unique position to be able to mitigate abuse based upon input that is received. And Crystal may I turn it to you.

CRYSTAL PETERSON Sure. Thank you, Susan. So, in our review that we had during our three sessions, we were reviewing how do we, as a registry, detect Associated Domains and Domain Portfolios, which I also know comes back to one of the questions that Gabe had at the beginning of our session with his cryptocurrency policy as well.

So, as Susan mentioned, the fact that .US is unique in its policies of no Privacy Proxy and the fact that we also have who is accuracy verifications, we are looking at, from a registry perspective, of being able to help support in the abuse mitigation efforts of the community to be able to identify associated domains through registrant contact data.

So, our session was really good in the fact that we were able to review how is it we define associated domains and what is it that we're looking at from a mitigation perspective for that point, and had some great questions for that.

ALEJANDRA REYNOSO Thank you very much. Moving to station number four, National Frameworks for Scam and Fraud Prevention, we have Bruce Tonkin and Ian Sheldon.

IAN SHELDON Thank you. Over here. Station four, we had a fantastic discussion on National Anti-Scams Frameworks. Bruce took us through a couple of different steps required to tackle scams at a national level, needing governance, prevention, detection, disruption,

response, and reference of referring information back to the relevant parties.

So, here in Australia, we have a National Anti-Scams Centre that's been set up to tackle this challenge, and it acts as a front door for the Australian population to come and report their scams and work out how to get remediation for their challenges. They work very closely with .au ccTLD operator, who takes a lot of quite responsive actions when they're alerted of a scam.

There's some good discussion about how much scams are a cybersecurity issue and how much they're a consumer protection problem. In Australia, our National Anti-Scam Centre sits within our competition and consumer commission, and so it's largely regarded as a consumer protection problem, but there's good interaction between our cybersecurity authorities and the consumer protection parts of our government.

There's also some discussion about measures that ATA takes to ensure our consumers are protected as well, with a lot of really good discussion around the nexus requirement and how much that really works to cut down a lot of these problems, but doesn't eliminate them completely, given there's a lot of behavior happening around stolen credentials, and so even if you do have that nexus requirement, those identity credentials are stolen and used in a lot of scams as well.

Anything else you wanted to add to that conversation, Bruce? I think that's about it from us. Thank you.

ALEJANDRA REYNOSO Thank you very much, and moving to the last station, Station 5, Trusted Notifier Arrangements, with Jake Vincet and Tomonori Miyamoto.

JAKE VINCET Thank you. I'll keep it brief because I know time is against us. So, we talked about the Trusted Notifier Arrangements we have in place with .UK and the different tiers, and we also spent a long time talking about some of the risks and rewards of having Trusted Notifier Arrangements in place.

I think what became clear from the groups that came to visit was that A, Trusted Notifiers don't seem to be that popular and widespread, and B, some of the challenges that you might have with foreign jurisdictions, how do you verify those reporters as being accurate, but I think overall people see the benefits of the type of arrangements Nominet and .UK has in place. Would you like to add anything else? That's us. Thank you.

ALEJANDRA REYNOSO Thank you very much, everyone. While I'll start wrapping up this session, please join us in Mentimeter to rate this session. We would like your feedback on this one. If the summary you think was not enough information for you, don't worry. We will send back a

summary with what was discussed in all of these stations to the GAC to be distributed so you can keep all information ready and handy. With that, I'll turn it over to you, Nico.

NICOLAS CABALLERO

Thank you very much. Thank you, Alejandra. Thank you to the ccNSO. This has been a fantastic session, one of my favorites, to tell the truth, with all due respect to all other advisory committees and constituencies. I really think we should do more sessions like this with the other constituencies as well, very engaging, very interactive, so to say.

So, thank you, thank you again very much to the ccNSO. It is very important for you to actually complete the take, I don't know, two minutes, 45 seconds to complete the Mentimeter because it helps us decide if, for example, if the time allocated to the rounds is enough, too short, too long, should be 18 minutes, should be 15 minutes, should we allocate more time for the wrap-up and so on and so forth, right?

So, thank you so very much for that. This is the end of the session. As a matter of fact, sorry for going four minutes over time. Just a very quick housekeeping detail. We're going to have lunch now, and this is good news for you, you'll have 15 extra minutes because we have a GAC leadership meeting, so you need to be back in the room at 1:30 instead of 1.15.

GULTEN TEPE	13:45, Nico.
NICOLAS CABALLERO	Sorry, sorry, even better, even better. 13:45. Any strong feelings against that? Anybody against? This is the right time to speak. So, thank you so very much. This session is adjourned. Please be back at 13:45. Thank you so much, and a big round of applause to our colleagues from the ccNSO.
ALEJANDRA REYNOSO	Thank you very much.

[END OF TRANSCRIPTION]