CLAUDIA RUIZ: Good afternoon and good evening to you all. Welcome to the LACRALO Monthly call on Monday, April the 19th 2021 at 23:00 UTC.

On the call today, on the Spanish channel, we have Augusto Ho, Dr. Pablo Rodriguez, Harold Arcos, Vanda Scartezini, Adrian Carballo, Alberto Soto, Carlos Aguirre, Gerardo Martinez Hernandez, Hannah Frank, Jose Arce, Lito Ibarra, and Vanda Scartezini.

We have received apologies from Lillian Ivette De Luque, Dev Anand Teelucksingh, and Leon Sanchez.

We also have Gilberto Lara is just joining the call.

On behalf of the staff, we have Silva Vivanco, Heidi Ullrich; and myself, Claudia Ruiz, on call management.

Our interpreters today—we'll be working into Spanish, Portuguese, and French. We have Paula and Marina in Spanish. Bettina and Esperanza in Portuguese. And Claire and Isabelle in French.

Before starting, please let me remind you to say your name before taking the floor, and also to keep your mics muted to avoid any interferences. Without further ado, I will give the floor to Augusto.

AUGUSTO HO: Good evening to you all. Let me bring apologies from Sergio. He had an unexpected meeting that overlapped with this one, so it is my turn to take over. So, let me begin by thanking you all for joining the call on

time, and let's make the most of this monthly meeting. We have a lot of information to share with you.

So, now I'm going to give the floor to Harold so that he can go over the agenda for today's meeting. Go ahead, Harold.

HAROLD ARCOS: Thank you, Augusto. Greetings to you all in the region. We will start our agenda with a webinar on DNSSEC. This will be delivered by Pablo Rodriguez who is the Executive Vice President of PR top domain names and we will later on have a comment from the ALAC members, by Silvia Herlein. We will later on listen to the reports of the working group. We will start with the group on universal acceptance and IDNs. Then the Capacity Building Working Group, the WHOIS Working Group, and the Communications Working Group led by Marcelo Rodriguez.

Agenda item seven consists of a report from the Social Media Working Group. Lilian De Luque could not attend this meeting, so we will not have her with us today. Then we are going to have a regional update. We are going to talk about the virtual General Assembly, ICANN70, the LACRALO strategic plan, and LACRALO elections. If any of you would like to add any topic to the agenda, now is the time to raise it.

We would also like to say right now that we will be taking note of the topics that you want us to address between this meeting and the next meeting or that you would like to include in the agenda for the call next month, so that we can start sharing some information through our mailing list. So, I'm waiting to see if there are any hands raised or any

comments in the chat window. If you don't want to add any topics, then the agenda is adopted, so I give the floor back to Augusto.

AUGUSTO HO: Thank you, Harold. Okay, let's begin right now with the webinar. We are pleased to have with us Dr. Pablo Rodriguez, who is the Vice President of Puerto Rico top-level domain. His bio is quite long but I'm not going to read it all because it will take a few minutes. But he's talking about security for the domain name system. I understand that he is going to talk about DNSSEC.

Pablo Rodriguez is well-known by all of us, so I give the floor to you. Mr. Rodriguez, you have plenty of time for your presentation and we are going to leave a few minutes at the end of your presentation for a Q&A. We will have at least ten minutes for a Q&A. So, the floor is yours, Pablo. Go ahead.

CLAUDIA RUIZ: Pablo, I think you are muted.

DR. PABLO RODRIGUEZ: Good evening to you all. Thank you so much, Augusto. Greetings to all of you on this call. Greetings from Puerto Rico. I hope you can hear me well.

The purpose of this presentation is to provide information so that people who are not involved in our community to get familiar with DNSSEC.

Why is DNSSEC important in our life? I will try to convey an implement message to all the people who are part of our community about DNSSEC. Next slide, please.

So, in the beginning, an attempt was made by a group of graduate students from UCLA to send a comment—a [login comment]—to the Stanford Research Institute, a few miles away from UCLA.

They started with that attempt by connecting over the phone. So, they said we have sent the O for login, can you see it? And the other party would say, "Yes, we can see it." Now we are going to send you the O. So, they would send the command for O. Can you see the letter O? Yes, we can.

But when they tried to do the same with G the whole system went down. So they just had this [phrase] that was cut off. It was [LO]. It is like saying lo and behold, just look what we have here. So it was something like biblical. So this was the beginning of a new era and it started with that phrase made up of two letters: LO.

So, if you look here to the left on the screen, you will see the people on the UCLA campus that we are trying to communicate with SRI with the Stanford Research Institute and you can see the other two notes they had, UCSB—that is the University of California in Santa Barbara. And the other one in [Utah].

So, that was the beginning—the humble beginning—of what now is known as the Internet. It would have seemed impossible for many of our children and grandchildren to envisage a world without the Internet right now. So, basically, they were trying to establish a connection using

a protocol that had been designed by Professor Vint Cerf and Robert Kahn.

They had the ability to create, after many attempts, this protocol. So they established a relationship with [Bob Kahn] and they were able to develop a protocol that was called the transmission control protocol and the Internet protocol.

Many of us now working in the industry call it PCP/IP. In English, it is called PCP/IP. Eventually, that was the way in which they were able to start sending packets from point A to point B and making sure that the packet would get to their destination.

Nowadays, we use a different relationship. We associate a domain name. In those days, when they started working with this protocol, the protocol was comprised of numbers like the ones that you can see here on the screen—123.456.789.12—but it was impossible for anyone to remember such a long number. It is much easier to remember another type of name, like LACRALO.com.

So, if I can say instead of connecting with me using a number-based protocol, use a name like icann.org or domain.pr or nasa.gov and you will be able to remember the name much more easily.

We associate faces and names. That is easier than remembering just an address made up of numbers. So, nowadays, an association—a relationship is established between a domain name as an IP number that allows us to connect from our home to other points. We can visit a webpage and that can be done in different parts of the world. We do it so easily that, actually, we don't stop to think how we are doing it. We

just type in a domain name and we expect to reach that webpage without any problems. Next slide, please.

Unfortunately, at that time, when they were working on this development, their objective was to establish a connection between UCLA and the Stanford Research Institute. That was their only goal. They just wanted to have a communication designed to connect from point A to point B. That was it.

At that time, no one could imagine that it could be possible for somebody else to use that design, that architecture, to commit fraud. But that actually happened. So nobody thought at that time how they could establish a secure connection. They did not design any security modules to prevent fraud. Nobody was thinking about that possibility. It was a big breakthrough to be able to establish that connection between node A and node B. But they couldn't think at that time that someone would try to use that for criminal purposes or for fraud.

At that time, no one imagined that that this exercise they were implementing could turn into something that would be used for commercial purposes and that could also have [inaudible] for the national security of the country or for [inaudible].

Therefore, they were quite naïve at that time. They thought that they were going to use it for a good purpose and that no one was going to use that for committing crime. Next slide, please.

So, that was the end of innocence. The end of innocence started with Professor Bellovin. At that time, Professor Steve Bellovin discovered something, and this is very important because he was working in the

AT&T labs and already in the late 80s, early 90s he already had some suspicion that the DNS architecture had [inaudible] that could be taken advantage of.

However, he discovered this closely before the beginning of the Internet and probably only a few people knew at that time how they could take advantage of those vulnerabilities, so he remained silent and he didn't share that information almost for five years, and it was not until a conference was held in Utah in 1995 when he published an article that referred to the DNS vulnerabilities.

In that article, he said that it was possible to kidnap a website and redirect it somewhere else, that a person could pretend that he or she was somebody else and that probably nobody would notice that that was happening.

So, at that time, that was the beginning of discussion within the Internet Engineering Task Force (the IETF) among experts at that time. They started sharing and exchanging information to determine how they could address that problem because they had already identified that problem, so now they had to find a solution to that problem.

It is important to highlight that, [inaudible] usually happens, in this kind of situation, there are some important questions that need to be answered. Is it possible for someone to be able to take control over a website? Can someone pretend to be somebody else? And some people hesitated. They weren't sure that was possible.

But towards 2008, Dan Kaminsky succeeded physically in showing that it was possible to cause such an attack. He actually performed that attack

and he showed—he demonstrated—how that attack could be carried out. So that was the end of the argument for those who were still hesitant.

So, for the first time, they realized that something bad could really happen. Therefore, Dan Kaminsky started working with big companies such as Microsoft, among others, to look for ways to address this kind of problem.

By 2004-2005, there was already a DNSSEC version under development and discussions were starting to take place thanks to this discovery. So they started looking for ways to deal with this situation, to put a patch to this system to see how they could [inaudible] because it was like they had found a hole and that a criminal would take advantage of that hole in order to take advantage of that vulnerability and commit a crime.

So, time went by and the protocol was created and strongly adopted by numerous pioneers, people who adopted also many other [competing] solutions.

I'm going to take the liberty to make a reference here. I apologize if you are too young to know this, but there was a moment—there was a time---when before the VHS was created—a bit cassette that you could use to record films—there were some other options competing against VHS and they had more or less the same function. They were quite similar and they were quite functional.

But at a given point, people started adopting VHS more than Betamax, the competing product. So, VHS turned into a standard. There were also

some other options available competing with DNSSEC, but over the years DNSSEC became a standard.

Approximately by the same time that Dan Kaminsky proved that it was possible to attack the system in 2008, as a result of that we started implementing and promoting the use of this technology. Next slide, please.

Let's see now what DNSSEC is. This is a protocol that performs two actions. It reinforces or strengthens the authentication in DNS based on digital signature on public key cryptography or KPI.

With DNSSEC, the DNS queries and the responses not only are cryptographically signed but the data itself are also signed cryptographically. The data that we are using here, we are using the keys to make sure two things happen. Next slide, please.

These are very significant features of the DNSSEC. The first is the authenticity of the data origin. In other words, when reached through a link because I wanted to join this meeting, my expectation is that I will be connected to the place where the LACRALO meeting will be held. Likewise, when you go to a website, your expectation is that the contact you have made is with the organization or the person with whom or with which you want to contact.

So, the authentication of the data origin allows the resolver to cryptographically verify that the data that you have received actually comes from the area, from the site, where you want it to come from. That is to say, if I look for information on LACRALO, I'm trying to contact LACRALO and it's not a third party that is conveying fake information.

When I contact my bank, I want to be sure that I am actually reaching my bank.

And the other feature that DNSSEC offers is that it protects the integrity. The data that I am receiving has not been changed. In other words, there is no third party who has intercepted this communication and the information that being received is fake. That is to say, data integrity protection allows the resolver or the receiver to know that the data hasn't been modified and that, from the moment when they left the origin, they haven't been intercepted and modified.

And this provides greater certainty, the fact that I know that I'm reaching the person or the site I want to reach and that the information I'm receiving is the appropriate information and I'm not receiving fake data.

Is there any other way we can make sure that I'm reaching the site I want to reach and that there is no third party manipulating all this and leading me to somewhere where I can become a victim of identity theft and many other crimes? Next slide, please. Next one, yes.

So, DNSSEC reduces the vulnerability to attacks. How does it do it? As we said in the previous slide, it uses this public key. When the resolver connects, it can check whether it is connecting the organization or the institution we want to connect or not.

Take a look at this slide. Without DNSSEC, we have someone who wants to reach the bank. That bank without DNSSEC can be a victim of a criminal who succeeds in sending a fake response to a resolver and has the resolver take the response as a good one and makes it the reply of that domain.

Let me explain it again. I go to my bank.pr. My bank.pr does not have DNSSEC. A criminal, when someone is making this attempt to contact this User A tries to reach the bank website to have access to his or her bank account and what happens, a criminal has taken their resolver and has sent a fake response to the bank. This is my bank.pr but the IP is different and that is called cache poisoning.

Why? Because the DNS architecture is designed so that it should work efficiency. And how can it be efficient? Well, based on an architecture that recalls and it recalls the first response given.

So, if a criminal sends a fake response to the resolver, that response is recorded and everyone who goes to that site is redirected to another website that might possibly be identical to the original bank, my bank.br, with the exception that there they have credentials. They are hijacking the credentials, usernames, passwords, etc. And with that information, they can go to the legitimate bank.pr and there steal money or, even worse, if it's not a bank, it's for the treasury department or the demographics registry, they could steal my personal data to commit other crimes.

So, it is extremely important for institutions with whom we do business or, let's say, government institutions with which we interact, such as the demographics department, the treasury, my bank, my hospital, they should have implemented this technology which protects me at least from this type of attack—cache poisoning—which enables or leads to many other attacks.

For example, identity theft attack does not happen with cache poisoning but it starts with cache poisoning. Why? Because it redirects me to a fake site where they are stealing information and capturing my credentials to commit other crimes. That's where the phishing starts. That's where identity theft starts. That's where fraud activity starts.

So, it's extremely important because it's a bigger gateway for other attacks which start with cache poisoning.

And DNSSEC, actually, it stops such criminal activity. When there is DNSSEC implemented, the resolver also sends the public key so that it can be compared—you can compare the public key that is being used in that zone, and if they are not equivalent, the resolver returns an error. It says 403, which means the page does not exist. But it doesn't redirect anyone else, unlike when there is no DNSSEC implemented and the person is redirected somewhere else.

On the slide, you can see at a very high level how DNSSEC have vulnerabilities with and without DNSSEC, but certainly this is much more complex and much more intricate than what I'm explaining.

The purpose of this presentation is for us to understand what DNSSEC is about, how it protects us, and how it can help our community—this community—to be more robust, resilient, and protected. Next slide, please.

DNSSEC also offers innovation promotion and it does it so because new protocols have been recently developed based on DNSSEC and leveraging the important features that we have already

discussed—authentication and its ability to ensure the validation of the information.

There are other technologies, other protocols such as the DANE protocol. The DANE protocol is an example. It allows the publication of security keys at the transfer layer security level (TLS). So, at the transport-layer security, DANE offers protection as well.

It provides a way to verify the authenticity of those keys, and this is very relevant because we have to highlight that DNSSEC is not the only solution. It is not a silver bullet, as it goes. This is not a magic solution [inaudible] or potential vulnerabilities that can be exploited by criminals. Therefore, we must have several solutions for many things that, all together, help us ensure again and again that we are safe—that the users are safe—as well as the organizations.

So, here DANE is an example. It's a protocol that operates well only in DNSSEC-signed zones. You cannot use DANE in zones that are not signed. So this is another benefit of having the zones signed by DNSSEC because those who have implemented DNSSEC will be able to implement other technologies that add to the security of that ecosystem. Next, please.

Now, echoing or along the lines of what I have said before, DNSSEC is not a silver bullet. It doesn't solve all problems. For example, a problem that it doesn't solve is the DDoS attack, which is the acronym for Denial of Service. This is an attack that is using several terminals to attack with questions, with queries, coming from many places at the same time and going for a server that is incapable of replying, giving a reply to all those

queries, it cannot reply effectively and the result is that it is taken out of service. That is why it is called Distributed Denial of Service (DDoS). It is the service that has been denied in a distributed manner through several terminals that are attacking from different places.

Again, it is important for us to make sure that our infrastructure is implementing all available security solutions to make sure that these vulnerabilities that can be exploited are not there.

We can also mention that, with every solution we implement, we are also bringing a problem and that is typical of all complex problems. Complex problems are not the same as complicated problems. Complex and complicated is not the same thing. A complicated problem is that problem that requires experts and resources to be solved, which could also be complex.

We want to send a spaceship to Mars. What do we need for that? Well, as you know, we need many electrical and electronic engineers, systems engineers, chemical engineers to talk about fuel, [inaudible], astronauts. We need people from the medical field, people who have made research on how the body works with zero gravity. So there are many things that we need because they have already been defined. Or for instance, how do we build a computer? Each computer component has been already defined. They are very many, they are complicated but they have been defined. And definitions do not change.

On the other hand, complex problems are not easy to define. They are not easy to define because we do not necessarily know how they work every time we implement a solution for that.

Let me take this chance to make a caveat. An example that I always give about this difference on the characteristics of a complex problem was, that year when the winter was very harsh in the US and the forest keepers decided that it would be a good idea to give food to deer who couldn't go deep into the snow to eat the little grass that was there, so they started feeding the deer and the deer started eating up the bark of the tree, so the population of animals expanded with this new footsteps they were having and these trees were the trees used by beavers to create their pools and their water reservoirs with the dams where they have the little houses and can have their offspring. So the beavers in this area and they left and they left far away.

So, what happened? When the summer comes, they start looking for where the beavers lived, because in those pools that are built because of the dams built by the beavers they can nest there. They can lay their eggs there. So as they didn't have these pools, the [inaudible] laid their eggs as they always did and they left. But a year later, next year, the population of [inaudible] was much smaller, to such an extent that millions of dollars were lost in business [inaudible] business.

So, who would have envisaged or been able to say two years ago? Giving, feeding the deer is going to create this problem that we will not have [inaudible] to eat in two years' time.

So this characteristic, the distinctive feature of the complex problem, is that we're unable to see in the long term for many years ahead how this solution that we are implementing today could become a problem in the future, so much so that the majority of both the organizational and personal problems we face today are the result in many cases of

solutions that were adopted with restrictions we've made thinking it was the best solution at the time. So that is what a complex problem is and how it can be compared with a complicated problem.

DNSSEC is a complex problem. Each solution with DNSSEC has caused a new problem. You might have seen that there was a step. We have DNSSEC. Now we have DNSSEC 3 and research still goes on to make sure that when the new problem comes up, we'll be ready to mitigate those risks.

Another problem—and I'm going back to the slide—another thing that DNSSEC does not do is to maintain the confidentiality of the data we are sending. What it does is it says this data comes from this side. This data has not been forged, so it is not fake, but they are open. Anyone can see them. So we should find ways to guarantee the privacy, the data confidentiality. Then we are talking about other solutions, DoH, DNS Over HTTP, DNS Over TLS. But those solutions are not the point of our discussion today.

DNSSEC does not protect the server either. The server that is valuable to other attacks which we should also be ready to make sure that all the server vulnerabilities have been taken into consideration, so that they will not happen.

Okay, just bear with me for a minute. Next slide, please. Next slide.

Over the years, in 1995, there were already discussions on DNSSEC that later on—ten years later—became a standard. It became adopted by many TLDs by many organizations, but anyway DNSSEC still faces some challenges—big challenges.

For instance, the adoption and implementation of DNSSEC by ccTLDs, ISPs, and other institutions is still very low in Latin America and Africa, for instance. Some studies have identified financial challenges associated with implementation of DNSSEC, and once again financial challenges means the following.

In order to implement DNSSEC, I need to hire new staff. If the answer is yes because you want to do that in house, if you want to do it in your own organization, you don't want to outsource these services—probably you will have to recruit new personnel.

So, DNSSEC is not so easy. Bigger [inaudible] are being made in order to offer webinars and workshops and training and more information on how to implement DNSSEC, but it is still quite expensive because if you need to recruit more staff, your headcount will increase and you have to find a way to produce more.

In addition to this, perhaps I hire qualified person, but probably that person will require also special training on DNSSEC and other related solutions in order to make sure that that person can not only help implement DNSSEC in their organization but also maintain it. And this requires additional training and that usually implies traveling to another country. Even within the same continent in South America or in Latin America, there are some costs involved in that travel. And in addition to that, you need to consider other expenses for accommodation, meals, so it may end up being quite expensive. So these are some of the financial challenges associated with DNSSEC implement. That is why there have been some resistance. Next slide.

For those of you who are wondering whether your bank has DNSSEC, how can you check whether a certain organization has DNSSEC implemented or not?

Well, you can take a picture of this slide or I'm sure that you will have this presentation available after the meeting. So you can type in the domain name and you can check whether they have DNSSEC. You can try doing that with my name that is my domain name and you can see what the appearance is when DNSSEC is implemented and when it is not.

And then you need to have good protection measures in place. You need to make sure not to use publicly available computers. Make sure that you are communicating with the right person. Try to install antivirus programs that protect you from spyware. Next slide, please.

How can I make sure who is writing to me? This is an example of a bank, a well-known bank in Puerto Rico. The site is Popular.com, but you can see that I used a sign to indicate that it is different from Popular.com. But that is not actually an O, it is a zero. So the letter "O" and the number "0" are sometimes used to commit fraud. When you don't pay careful attention, you think that it is the same character, but actually they are not. So try to make sure that you are talking to the right person.

These are some of the ways that you can protect your information. You can also disseminate this information to other people and you can become an ambassador for security. You can talk to the organizations you transact with in order to make sure that they can implement DNSSEC to protect themselves and their users.

Thank you so much for giving me this opportunity to give this talk. I am very pleased to be with all of you here this evening.

AUGUSTO HO: Thank you, Dr. Rodriguez. Once again, he is the Vice President of Puerto Rico top-level domain and he is a well-experienced person with a lot of expertise in this field.

So now I'm going to ask Harold to let m know whether there are any questions in the chat. Harold, go ahead.

HAROLD ARCOS: I have just checked, and for the time being, there are no questions, but there are some participants asking for the floor. Alejandro Pisanty has his hand up, so I am going to give the floor to him and we will let you know if there are more questions.

ALEJANDRO PISANTY: Thank you so much for this wonderful presentation. It is true that not all potential attacks were considered when designing the DNS. As I was saying, not all potential attacks were prevented when the DNS was created. But I think it is [excessive] to speak about innocence in the early designs of the Internet because we must recall that they weren't using computers for that connection that hosted the biggest commercial secret in the US, the payroll of General Motors or also research work done in universities and the authors of the initial protocols decided to connect these computers on the edge of … Cryptography at that time was advancing at giant steps. There was a lot of development on public

keys and asymmetrical cryptography and [inaudible] computing science made it impossible to keep all these protocols in the network. So that was the beginning of the principle of intelligence on the edge.

So, I think that there was not an intention to ignore security. They just kept it on the edge. It was only years later that the DNS was taken to the application layer.

We also have protocols. And I think it is implement to make this point of clarification. And then for LACRALO discussions, it is very important for us to maintain a culture of asking questions about security. That is why we need to resort to people with a technical background with technical expertise, especially with ccTLDs that are the main contact points for us and with institutions such as universities, banks, and providers and civil society organizations. It is very important for us all to protect our websites, our web services. Thank you.

AUGUSTO HO: Harold, do you have a question?

HAROLD ARCOS: I have a question for Gerardo. I'm sorry, I hadn't seen it before. Gerardo is asking the following. According to the example about winter, the possible solution for a complex problem regarding DNSSEC, perhaps it would be better to work in an interdisciplinary manner. That is the question.

DR. PABLO RODRIGUEZ: Let me check if I understood you correctly. Let me paraphrase that question. I think that you are asking whether, given the complex nature of DNSSEC, is it possible to work this with a multi-disciplinary approach? Is that the question?

HAROLD ARCOS: Yes. This question goes back to the example that you gave about what would happen in wintertime among the potential solutions. One would be to have a multi-disciplinary approach.

DR. PABLO RODRIGUEZ: There are many problems that have to do with different situations, different industries, and DNSSEC is a solution that, given its very own nature, requires other solutions.

In our industry, we have a saying. There is no single silver bullet that can solve all problems. So you cannot control the beast totally. You just can dance with the beast. So you need to adapt to all the circumstances as they evolve.

One possible answer could be the following. Different callers, different researchers and developers, look for different solutions to address other vulnerabilities and they can do that because DNSSEC has already paved the way for them to build on that and to come up with new protocols that can help provide a broader solution. So multi-disciplinary work is always useful.

So, the short answer would be yes, of course, whenever you have a multi-disciplinary [theme] that will be useful. But in this case, you also

need to take into account that over and over again you will come up with certain unforeseen elements. That is why years later we are forced to look for other solutions to overcome those solutions that at a given time were the best ones we could have.

AUGUSTO HO: Are there any more questions, Harold?

HAROLD ARCOS: I don't see anymore questions in the chat. I'm just checking to make sure that I have not overlooked any questions like I did with Gerardo's question. No, there are no more questions in the chat and no hands raised.

AUGUSTO HO: Okay. Let's move on now to our next item on the agenda. We will give the floor to Sylvia Herlein. She's going to have five minutes to talk about comments on behalf of the ALAC members.

SYLVIA HERLEIN: Hello. Good evening. Let me briefly comment on what the ALAC has been working on for the last month. But before starting, let me say that as you well know, the ALAC meetings are open to the entire community, not only to ALAC members. So it is always good to remind everyone that you can participate in those meetings and it is actually good that you participate because we want to listen to all views.

In March, we had to vote for different ALAC recommendations. One of them relates to IANA. That was the recommendation for an amendment of [inaudible] contract for IANA. Actually, I always voted in favor of those recommendations, and when you have to cast a vote, you need to support the excellent work that is being done by all the working groups.

So, actually, if you have a concern or a question, you need to contact the group before getting to that point of voting for those recommendations.

Then, we issued a statement on the European Economic Initiative on the network security. That is the NIS2 initiative. I think that Harold was going to type in the link here, in case you want to find out more information about the revised directive in NIS2.

Then, we also worked on the recommendation about individual participants. There was also a final review of the SSR2. That is the Security, Stability, and Resilience 2.

Then, the ALAC advice to the Board on new gTLD subsequent procedures. So we voted on all those recommendations between March and April and we still have some more issues under discussion right now. So I invite you to take part in the meetings.

I don't know whether or not Harold has pasted the link so that you can have more information about what is being discussed within ALAC. Thank you.

AUGUSTO HO: Thank you, Sylvia, for this presentation. Now we are going to move on to the next presentation. Let me just welcome Sergio. Sergio has just joined

us. So now we move on to the working group chairs report. You will have between three and four minutes to present your report. First we will start with IDN Universal Acceptance working group report by Sylvia Herlein again. Go ahead, Sylvia.

SYLVIA HERLEIN: Well, in my working group, you know that we have two subgroups, one dealing with IDNs. Last year, we engaged in very interesting work, quite different from what had been done before. And this year, we will resume that work. In particular, tomorrow we will have a meeting in our working group.

The plan is to make contact with all the [inaudible] of Latin America and the Caribbean in order to submit the summary report that we had prepared and that we wanted to share with them through LAC TLD and that was not possible.

So, tomorrow we are going to get together to discuss that and we want to build on all the efforts made last year because this report was well prepared by Gabriella, so we want to continue working on ideas.

We are now in the phase of understanding how IDNs work. We want to talk to the ccTLDs so that they tell us more about the process, about their operation, why some ccTLDs need certain special characters, like the special N in the Spanish language, the Ñ.

And then, as far as universal acceptance is concerned, we are very happy because since July last year we have been working relentlessly and now our work is very [inaudible]. We can confirm now the course

for technical programs and IT students. I think that the flyers were going to be shared. We have flyers in English, Spanish, and Portuguese and we have five instructors who are well known in the field who are going to participate in this course.

The course will start on May the 4th. I see now that the links are being pasted in the chat to the Wiki page, so that you can find out more detailed information. We will have four 90-minute sessions. They will be officially delivered in Spanish with simultaneous interpretation into English.

We already have 60 people who have registered for the course, with Marcelo Rodriguez from the Communications group and with Adrian Carballo from the Capacity Building Working Group. We are working closely together and we are very happy because we have been able to come out with something that is fantastic and this can set a very good example.

We can also invite all the other RALOs to attend the first course on universal acceptance. We are working hard on this. We have received feedback from students from the University of Buenos Aires who told us that they were interested in the topic but they didn't know what it was used for. We have also had registrations from java programmers and programmers working with other languages.

So we are now focusing on education training on universal acceptance. Even when people don't know what universal acceptance is about, if they just have a minimum amount of knowledge of programming they will be able to attend this course. And in July, we will deliver a course for

end users and all the members of our ALSes will be invited to take part in that.

Now we are asking our ALSes to help us disseminate information about this because of course we are planning to have another edition of this course but we don't know when, so we can wait until May the 3rd or May the 2nd to have more people registered. So please disseminate this information that we are sharing with you in the chat because I think this is worthwhile and this is going to be a very important milestone in our region. I don't know if you have any questions. I'm available. I would be glad to take any questions. Thank you.

AUGUSTO HO: Thank you, Sylvia. Now I'm going to give the floor to Adrian Carballo, chair of the Capacity Building Working Group. We are running out of time, Adrian, so please proceed with your report.

ADRIAN CARBALLO: Thank you, Augusto, for giving me the floor. First of all, let me thank Dr. Pablo Rodriguez for his excellent presentation. He has provided us with a lot of updates and information. He has exceeded our expectations and I have witnessed all the hard work that he has done in order to transfer all this knowledge. Thank you, Pablo.

As to our working group, let me say that we are still making progress with the ICANN Academy in Spanish. We don't have much time but let me briefly tell you about the content for this training call.

There will be four modules. I'm just going to give you the headlines. The Internet Ecosystem and ICANN, the Domain Name System and its Structure; Security, Resiliency, and Privacy; Internet and its Impact on Society and the Economy. Those are the titles of the modules.

So we are making progress with this course. I'm going to give the links to Harold and to the staff so that they can share it with you so you can have access to more detailed information.

Sylvia Herlein said we have made significant progress with the universal acceptance course. We have been working very well as a team. We have high expectations. The course will be first aimed at technical people and then at end users.

So, I have a special request for you. Please help us disseminate this course. We have information on Facebook and Twitter and we are trying to attract as many people as possible. We are also putting together schedules for a number of webinars that would be held.

This would be my report and I would be glad to take any questions. Thank you.

AUGUSTO HO: Thank you very much, Adrian. Very quickly I will give the floor to Carlos Aguirre for his report on the GDPR. Two minutes.

CARLOS AGUIRRE: Thank you, Augusto. I want to take this chance to congratulate, like Adrian and Sylvia did, Pablo for his presentation. It was clearly

spectacular with clarity and ability that [inaudible]. Congratulations, Pablo. Everything you explained, very well understood.

Now, moving on to the core of my group on [inaudible] GDPR. Let me tell you that we have started with this group a short time ago. It has been set up some time ago, and we are now at the stage of calling for participation and adding participants. We have been requested by the LACRALO chair to cooperate on this. We are working on the contacts to see how to have members join this group. We are also working with the director of the Capacity Building group to provide some reference person on this matter to have a webinar and I really wish that would be as clear as Pablo's presentation today because the issue here is to be able to understand what this is all about. A very sensitive issue, such as personal data protection in WHOIS. Without a doubt, this is of great relevance and that is why we want to show or to explain what this is about.

To make an overview, the GDPR—the General Data Protection Regulation--was adopted by the European Union and was made effective in 2018. ICANN, during 2017, worked on how to adapt to this that was coming, and in April 2018 before the resolution was started to implement the GDPR, make it effective, launches a temporary specification for gTLD specification data that has been ratified at the beginning of 2019 and all these issues require an update, required from us to be updated on a continuous basis, because as Pablo was explaining, those [inaudible] with data are everywhere. So this is something that we have to pay attention to at all times.

But the most important thing is to have people understand what this is about, why it is important. And as I was saying today, we are now at the stage of setting up the group composition, recruiting people who may be interested in joining. And with the Capacity Building group, we are trying to find someone who could teach a clear webinar as a kickoff. So this is what we're doing now. This is what we are designing. It's still [inaudible] but very keen, very eager to move forward because we believe this is a core discussion and should not be overlooked by end users because this is relevant for them.

This is all on my part. Augusto, thank you.

AUGUSTO HO: Thanks to you, Carlos. I will now give the floor to the Communications Working Group and I will kindly ask Marcelo Rodriguez who is with us to report.

MARCELO RODRIGUEZ: Thank you. Hello. Good evening. How are you all? Despite the short time available, let me take a minute to thank you for the work undertaken in the field of communications. We have been very busy in the deliveries for further distribution. Later on, once the English translation is ready of the LACRALO news number 2. So the materials have been already submitted for translation.

With a great pleasure, I want to thank Sergio, [Franco], and the Communication Working Group members' contribution because they were very helpful. Their input made emphasis on recent regional

information. Specifically, ICANN70's activities. And then [inaudible] on the areas of each participant.

Sylvia has posted on the chat that the Word Doc has been sent with the document, with the entire document. We hope we can see this very soon ready for distribution.

Another thing. There is a universal acceptance course on which we are also involved, together with Sylvia and Adrian. All these groups have been involved in the organization of this activity. You can see on the slides the design given to us by Sergio. I think the only change with it was the starting date. The rest is the same. It's very clear. There is [inaudible].

I want to thank again for this opportunity to continue working with you and being responsible for this work on communications. So whatever we can do this year, 2021, despite the restrictions.

So, that's all and good evening to all and take care. Thank you.

AUGUSTO HO: Thank you, Marcelo. Now, [inaudible] I should provide a regional update. Let me start by saying that ICANN70 was my first, the first time a virtual assembly was held and ICANN [rules]. Actually, we had four events.

The first was in the week prior to ICANN70. March 15 there was a virtual General Assembly. Also, the 17th was a training event with David Plum who referred to LACRALO's [strengthening] ICANN policy development efforts. And there was a discussion on universal acceptance as well. Very welcome by everybody.

On the same week as ICANN70, there was a roundtable where we discussed the strategic plans for the Latin American and Caribbean region and look to the future, of the way ahead.

Let me make a special mention of the social event closing ICANN70. It was highly successful. Let me comment [inaudible] social event. It was really appreciated by the Board. There was a tour around the region, where many people connected, very much enjoyed with the participation of [inaudible] form the Yucatan Peninsula.

Sergio Salinas, are you here with us? If you are here, I will you give you the floor to share with us.

SERGIO SALINAS PORTO: Thank you, Augusto. It is my responsibility now to present on the last item, LACRALO elections. I apologize for not being here before but I had prior commitments.

As you know, we had sent in elections for the majority of the LACRALO positions. There is one election for ALAC members. Sylvia Herlein is leaving. She was Region D and now it's turn for Region A.

Then we have also the election for the LACRALO vice chair who will replace Augusto when his term is over in 2023. But before that, there are two years of accompanying the chair and taking on some responsibilities as he did today relating to Board decisions.

Then we have two positions for chair-elect and chair secretary. Sorry, secretary-elect. This is because [Kerry] resigned. It will be for a four-month term until November to fill in that position of secretary.

Then we will have another one for secretary for 2021-2023. And afterwards, with the vice-chair elect, will be the formal chair and vice chair.

Then we have the ALAC NomCom representative and we have this [inaudible] that Vanda Scartezini is able to be reappointed. So, according to our rules, we guarantee the extension of her term for her to be with that for two whole years.

Having said this, and because of the time, if you have any questions, you can take my email. I see Harold has posted in the chat all the links for the elections. The elections will be in May. I do not remember the day. Sylvia, perhaps you can post it in the chat as well.

But we have to think about renewing positions. We have to see how to do that. It will be on May the 10th. Thank you, Sylvia.

I see Alejandro's hand was up. Perhaps … Augusto is leading. You are leading the chair. Perhaps, Augusto, you can give Alejandro to report this activity on the record. Alejandro, you have the floor.

ALEJANDRO PISANTY: I will be very short. In addition to congratulating you, Sergio, for everything you have presented and organized, the report that Sylvia has mentioned—the ALAC comment on the SSR review of the domain name system, SSR2 was [conceived] on the draft [that are made together with Greg Shatan]. This is a contribution that has been directly requested because I was responsible for the first review.

I want to have it on record for the LACRALO as a LACRALO contribution. So [inaudible], it is very good to see how we make much significant contributions.

I [inaudible] a comment for Alex. Alex, I want to meet you tomorrow at some point in time.

Of course, we can have it organized.

AUGUSTO HO: So that is all from our agenda. We are out of time a little bit way past. I want to thank everyone, the staff, interpreters, etc. Thank you, all. And congratulations and good evening, everyone.

[END OF TRANSCRIPT]