YESIM NAZLAR: Good morning, good afternoon, and good evening to all. Welcome to the sixth webinar of the five mandatory Atlas III webinars and today we'll cover cybersecurity basics. Presenting today is Patrick Jones, Senior Director for Global Stakeholder Engagement. We will not be doing a roll call for this webinar, however we are taking attendants for the first 10 minutes on this call. After that, your participation will not be a valid entry for the required attendance metrics. If you are only on the phone bridge, please join the Zoom room as soon as possible as this is an attendance requirement.

We have French and Spanish interpretation for this webinar, so a kind reminder to please state your name when speaking that allows for the interpreters to identify you on the other language channels as well as for transcription purposes. Please also speak at a reasonable speed to allow for accurate interpretation. All lines will be muted during the presentation and opened for questions and answers at the end of the presentation.

If you have noticed we're running this webinar on Zoom. The features are similar to Adobe Connect but in order to view the participant list and chat box please click on the bottom of the screen. You will only be able to see the chat transcript from when you join the call, nothing prior to that. To raise your hand, please just click on the raise hand icon. Now I would like to hand the floor over to Joanna Kulesza, co-chair of the Atlas III Capacity [inaudible]. Over to you, Joanna. Thank you very much.

JOANNA KULESZA: Thank you very much, Yesim, thank you for the introduction. Thank you to everyone who is joining us today for the fifth, overall this 10th edition of our mandatory Atlas III webinar. My special thanks to Patrick for taking the time to join us today to give us and introduction into cybersecurity. We had the first edition of this webinar roughly 14 hours ago with your colleague, David Huberman, and David was very kind giving us a thorough focus on cybersecurity.

I particularly appreciate having Patrick here with us today given his background and stakeholder policy making privacy and the involvement with international organizations. With that in mind I'm very much looking forward to the presentation. The floor is yours Patrick. If you are speaking Patrick we can't hear you.

PATRICK JONES: Okay, I'm back. The internet dropped as soon as the call was about to start. Are you ready to begin?

JOANNA KULESZA: Yes, the recording has started. I've just concluded the introduction and handed over the floor to you. Your timing is perfect, we're ready to go.

PATRICK JONES: Okay. Thank you very much for having me deliver this webinar. For those who listened into yesterday's webinar you would have heard David Huberman from our office and the CTO team. I am Patrick Jones from our global stakeholder engagement team. I have been at ICANN for 13 years and I've worked in our security team, which was the

precursor the CTO team for about six years before joining the team that I'm in now.

I'm giving you this information based on my background at ICANN. Hopefully you'll find this useful as a good compliment to the tools that we have available on ICANN Learn. We have recently added a course on cybersecurity basics and I believe there is also one on DNS abuse. So, you should find those useful for getting an understanding into this subject.

With that we are going to advance to the next slide. We'll start by giving an overview of the essential elements that are inside any type of network and these could be things that are in a company's network or a university network or inside a government network. Most common you will see there will be mail servers which provide email calendar functions a host contact information.

There will be servers that will be databases. They might have customer data or employee data or other types of information that is stored by a government agency or an organization. There will be financial information and this could include everything to financials for a government or a company or an organization or organizational processes and procedures. These are standard for any type of organization.

The next slide. Now, because all organizations have these elements these are often attractive targets for attacks. These functions they perform a number of services. They may perform identity management which includes usernames and passwords, things like biometrics and

other forms of multifactor authentication. This could also include photographic key management.

There is data storage, which is what we do what we store and where we store it. Data retention is how long we store it for. There might be policies set around the security practices for the information in the networks. That there will be systems in place such as your hardware software and regular patching that occurs.

Then if your organization is connected to the internet and most organizations are then they'll have some infrastructure that they may have IP addresses. They will rely on the domain system to connect their network to the wider internet.

Every day these elements are under attack. Attackers are looking to penetrate systems. They try to extract data and exploit any vulnerabilities they can find in the systems.

Next slide. When we talk about the types of cybercrime, common elements of crime include phishing which is the practice of sending an email which presumes to be from an organization or a company or someone you trust in order to trick the recipient into revealing some type of personal information which might be passwords it might be credit card information. It might be credentials that allow the bad actor to then gain access to either email or some type of system and this is very common.

Another type of cybercrime that we see is malware. This is software that has been created to disrupt the image or gain access to a computer system. These includes examples such as ransomware which is malware

that infects your machine and then your machine is locked up and in order to gain access to the machine the bad actor then says, "Pay me a ransom in dollars or bitcoin," or some currency and then will grant you the access again and that usually never happens.

Another example, a common element of cybercrime are robot networks or botnets. This is a network of computers that have been connected together with some type of malicious software code and they're controlled as a group.

We often see this at ICANN as robot networks or botnets that are controlled by domain names that rely on command and control systems. I'll talk a bit more about this as we go on.

Next slide. In an ICANN context you've very likely heard of the term DNS abuse but if you haven't, we'll talk a bit about that. Most organization whether that be government or commercial entities or individuals they use the domain name system to resolve their user friendly names to internet protocol addresses.

This is because IP addresses which are based on numbers are difficult for humans to remember but if you can link a name to a number then you can make it easier to be able to look things up using the domain name system and connect queries to computers.

Abusers attempt to disrupt the domain name system and your use of the domain name system for their own purposes and they may do this through disrupting commercial transactions such as bank websites. They might go after government websites and government services or they may go after social networks.

We also see news organizations are often targets and once you can exploit the domain name system you can trick defraud and deceive users. This is often done through maliciously registered domain names or it's done through redirecting and hijacking the name resolution and registration services or corrupting the DNS data.

Next slide. I'll talk a bit about some examples of what common cyber attacks look like. Some of these target vulnerabilities that are in the routing system of the internet they also target email systems. Typically we call the attempt to alter name resolution is part of DNS abuse. In the next slide we have an example of an incident that actually happened in April 2018.

Move to the next slide. This is an example, the domain was myetherwallet and it was a domain that was used to host cryptographic currency. This was a domain that was attacked and attackers used the routing infrastructure and the domain name system to redirect users to a fake website that was pretending to be myetherwallet.com and then once users entered their login credentials into the fake website the attackers were then able to use the login credentials on the real website and then steal the cryptocurrency that had been stored there.

The estimate are there were about 21 million dollars or cryptocurrency that were stolen using these harvested credentials and this was just one example of where misdirection and hijacking resulted in real dollars that were lost by users.

The next slide provides another example of sometimes a cyber-attack is motivated for political reasons. Late November of this year, in some

cases it's still going on, there were some very high profile and very coordinated attacks that have been referred to as DNS espionage and the sea turtle campaigns. This is an example, and it has been called military cyber offense prepositioning which is a fairly new term for gathering intelligence needed to launch military cyber-attacks.

From the research that's been presented in recent DNS conferences the researchers have identified that there were about 40 organizations in 13 different countries. Actually there were a lot more than this but in the initial attacks that happened primarily these were in North Africa Middle East, so United Arab Emirates was a frequent target. Government websites and businesses including some airlines.

These were targeting also energy companies, the national security organizations in these countries, some DNS providers that are very well known in Sweden and in other parts of Europe were also attacked, and a large hosting provider in the United States was also part of this. The attackers were able to infiltrate DNS email and certificate authorities and then obtain and decrypt documents.

ICANNs role is quite limited. One of the things that we are able to do is provide a platform for sharing experiences and raising the awareness of issues. At the recent ICANN meeting in Kobe, Japan, members of the ICANN Security Stability and Advisory Committee provided some workshops and practical guidance for the different stakeholders that were in attendance about things that you can do to protect and secure your networks that are quite common for anyone that has domain name assets.

I'll talk about some of those examples as we get further along, but the attacks that are happening really are impacting everyone from governments, corporations, law enforcement, and internet users at large. These happen daily and ICANN offices CTO teamwork with registry's registrars and other stakeholders in the internet community to share knowledge and information. Try to raise the awareness of what can be done and provide a platform for sharing information when these types of things occur.

Next slide. We'll get into before an incident happens a little bit of background of what ICANNs role is. Under our bylaws the bylaws provide a strong emphasis on ensuring that the internet system of unique identifiers is secure and stable. This is core to our work. The bylaws also include some commitments that include preserving and enhancing the administration of the domain name system and the operational stability reliability security global interoperability resilience and openness of the domain name system and the internet.

Some of the ways that we do that are providing a way for the contracted parties, for registrars and registries, to share information when there are vulnerabilities and when there are attacks that are happening. We also provide a convening platform at our meetings and through mailing lists were those that are either participating in understanding security threats that can share their information with us.

We also work with other partners in the internet ecosystem including the regional internet registries with regional topical domain organizations and others to work collaboratively to share our knowledge and experience.

Next slide. At ICANN there are some words that are commonly used. Those start with security stability and resiliency. What we mean in an ICANN context is that security is the capacity to protect and prevent misuse of internet unique identifiers. When we're talking about stability we're referring to ensuring that the system operates as expected and that users of those unique identifiers have confidence in the system that it's going to operate as they expect.

For resiliency we mean the capacity of the unique identifier system to be able to withstand malicious attacks and other events without disruption or without stopping of service for the sites that people rely on.

Next slide. We have a number of commitments for the security stability and resiliency of the unique identifier system. We do this through encouraging all stakeholders in the internet to participate in active policy development and through the technical work. I see the comment in the room chat, I believe the At-Large staff team will provide a link to the slides after the session is complete. Hopefully that answers the question.

Other commitments are that we often work collaboratively with regional stakeholders to help deliver either security training DNS training other types of capacity building. This is often request driven by the local organization. Sometimes we will do training around domain name security extensions, other times we'll do training around DNS abuse or recognizing and responding to DNS abuse. It depends on what the interest is of the regional organization that's requesting the training.

Next slide. Within ICANNs various stakeholder groups and advisory committees there are some communities that develop policies and procedures related to improving security stability and resiliency. One of those groups is in our governmental advisory committee, this is called The Public Safety Working Group. This group has been around, I believe, at least six or seven years and it was initially an effort to bring in the expertise of public safety organizations and law enforcement.

The Public Safety Working Group has been providing feedback on public comments. They focus on ICANN policies and procedures that relate to DNS abuse and cybercrime mitigation. Their work has contributed to improvements to the registrar accreditation agreement and other contracts that we have with contracted parties. They also provide a way to share their information to the Governmental Advisory Committee.

Two other advisory committees that focus quite extensively on security stability and resiliency issues first it's the Security Stability Advisory Committee of ICANN. This is an advisory committee to the board and the ICANN community. They work on regular DNS threat assessment risk analysis of threats to the domain name system and they often provides practical talks at ICANN meetings, public sessions. Some of the recent issues that SACC has brought to the community include internationalized domain name attacks.

Also their observations on the DNS espionage types of attacks. Coming up at the ICANN meeting in Marrakech the Security and Stability Advisory Committee will have some sessions of internet of things and their connection to security and stability.

Finally the Root Server System Advisory Committee provides advice to the board and community on matters relating to the operating of the root server system and this is an area where there is quite a bit of work on evolving the governance of the root server system. We've heard more about this at recent meetings but coming up in Morocco there will be, I believe, an opportunity for public comments on the proposed governance model for the root server system. There will be more work on this and more of an opportunity for community feedback in this area.

Next slide. Our relationships between registries and registrars or contracted parties are key tools for promoting security and stability and resiliency. The most recent registrar accreditation agreement has a duty to investigate abuse. It requires registrars to follow up and investigate either claims or evidence that has been provided of abuse with domain names that they manage and the most recent registry base agreement for top level domains includes a provision that prohibits registered name holders from distributing malware or abusively operating botnets doing phishing piracy trademark copy mark infringement or other types of practices that are generally categorized as malicious abuse.

Next slide. This is a visualization of how the contracted parties are connected in the internet ecosystem. We have a direct relationship between ICANN and the top level domain registry operator. This is governed by a registry agreement. There is also a contract between ICANN and the registrar and that is the registrar accreditation agreement.

You may have contracts, there definitely are contracts, between the registry and the registrars that support the names that they offer to users. That is the registry registrar agreement. Sometimes registrars use resellers but those resellers are not under contract with ICANN, so we often see questions from the community about issues that might be coming up at the reseller level, but those aren't covered under a direct relationship with ICANN.

Now registrars and resellers have a relationship with the registrar and that is typically the registrar agreement. For all of the registry agreements those are available on the ICANN website. There is a page on the ICANN website also about the registrar accreditation agreements. You can see these on our webpages. If you are using a registrar and you want to know what you registrar rights and expectations are you can usually find that agreement on the registrars website. If you can't you should probably -- or you could send a note to ICANN compliance and ask about this.

Next slide. ICANN has a subsidiary called Public Technical Identifiers and that is responsible for the operational aspects of coordinating the internet system identifiers. They allocate number resources either internet version four addresses IPV6 address or autonomous system numbers to the regional internet registries. They also maintain the root zone for the domain name system and administer the [inaudible] zone.

ICANN through PTI also maintains the trust anchor for domain name security extensions and then we coordinate over 3,000 registries for other protocols that are developed at the Internet Engineering Task

Force. This brings us to provide a little bit more background into what is domain name extensions, the DNSSEC, it's on the next slide.

When the internet technical community and researchers developed the domain name system security was not top of mind. If you think to the early 80's to 90's of internet use there were a number of major vulnerabilities that were discovered and as a response to this the technical community and the researchers came up with a new protocol called Domain Name Security Extensions. This was to add a level of security and protection to DNS data.

Now, a number of country code operators took the lead on implementing DNSSEC and then in 2010 ICANN signed the root zone with this protocol. This helps provide a level of assurance to users that the data that they are seeing is valid and true. It also provides a chain of trust from the top level of the domain name system down to the individual registry level. Now that the root is signed and extensions such as .com are signed then when banks airlines and other organizations implement DNSSEC then this allows DNS operators to validate all of the data that passes through is accurate. That way a user can't be maliciously redirected to a page that is not a true domain that you're intending to find.

Next slide. Domain Name Security Extensions relies on public key infrastructure technology. For your purposes you should know the key signing key is the topmost cryptographic key in the hierarchy. The key signing key is based on a public private key pair, so there's a public part that is the trusted starting point for validation that resolvers will use, and the private part contains the zone signing key. ICANN WPTI

maintains the zone signing key for the top level. Individual registries maintain a zone signing key for the zones that they're responsible for. Then this builds the chain of trust that provides a greater level of security for the domain name system.

Next slide. As I mentioned the PTI issues and manages and changes and distributes DNS keys. They sign the key set for Domain Name Security Extensions and they follow best practices as they are developed by the Internet Engineering Task Force and Internet Technical Community. We do several times a year key ceremonies, these are published and public, anyone can follow along remotely as we do the updates to the key signing key and the DNSSEC infrastructure. If you're interested in this these are usually published well in advance of the ceremonies on the ICANN website. It's a fascinating way to see how the internets key identifiers are secured.

Next slide. Our offices CTO team as well as our various engagement teams regularly participate in efforts to work with community partners on matters relating to internet identifier security and cybersecurity. We do this through how it works sessions at ICANN meetings, webinars like this one. We participate in technical workshops and trainings and through many different types of capacity building. For example, two weeks ago many of us were participating in session at the DNS Symposium in Bangkok, Thailand. Alongside that event and the other technical workshops that were happening there, there were capacity building trainings that were happening with THNIC as part of the Thailand Network Operator campaign.

These are very common throughout the year in different parts of the world. ICANN and partners participate in capacity building events to help share experiences and knowledge with other around the internet tech questions.

Next slide. When a cybersecurity incident is happening there is quite a limited role for ICANN but we will talk about what different organizations do. ICANN is a member of the Forum for Internet Response Security Team, so FIRST, and other national computer internet response teams are also members of FIRST. This is a platform for sharing information when attacks occur. They are often sharing this information with other network operators, with other public safety entities, this might include law enforcement it might include Interpol Europol or other global law enforcement bodies. It may also include coordinated response with top level domain registries and registrars. These are the major actors that may be involved in mitigating the scope of a cyberattack or providing some type of coordinated response.

Next slide. When an attack is happening it's very difficult to identify the source of that attack. But it is important that those that are responding try to identify the internet protocol addresses that are being used, f there are domain names involved in the attack, identify who the registrant is or who, at least, where the registrar and registry are located. Then those organizations can then try to check their databases to see if they are able to help identify where the source of the attack might be coming from. Attribution requires other data sources. This might include the registration contact data that are associated with those domain names or internet protocol addresses or autonomous system numbers.

Next slide. As I mentioned earlier ICANN has a team within our office of the CTO and they work with other organizations through trusted security communities to help coordinate responses to attacks. This team provides a deep understanding of what happens and what's needed to respond when an attack is happening. The team often participates with law enforcement organizations registries and registrars. We've had a history of sharing our experiences after these attacks occur at our ICANN meetings.

We do provide on our website a [inaudible] of disclosure process that security researchers and others can use to report vulnerabilities and bugs to ICANN. An example of this happened a few meetings back when a member of the ICANN community discovered a vulnerability in Adobe Connect. The Adobe Connect systems were taken down during the meeting and we now have moved on and switched to the system that we're using today with Zoom. But that only occurred through the quick response of a member of the community who submitted the research that they had identified this vulnerability to us.

That is one example of a way that we work to coordinate with others. We then took that information and went to Adobe and shared the knowledge that the systems could be exploited in that way and they were able to start to make adjustments to their own networks and systems.

Next slide we go into our role after a cybersecurity incident has occurred. Some of the things that we do are sharing our experiences at events like the recent DNS Symposium or the DNS Operational Analysis and Research Community or at Network Operator Group meetings.

Then the internet technical community researchers and others can take this information back and harden their networks. They can perhaps define attacks, identify new policies that need to happen, perhaps some changes to our contracts or their contracts or perhaps it identifies protocols that need to be improved or redeveloped. Then other things that can be done include sharing this information with network operators law enforcement governments companies and others.

Next slide. We are getting towards the end and then we're going to open this up for question. But a key takeaway for this group is that the domain name system it's no longer just a technical function that's run by system administrators, it is seen as critical infrastructure that is used to support our daily communications everything from email web browsing applications. It is the gateway all of your internal systems. It is also becoming a platform for other things such as internet enabled devices lightbulbs refrigerators and other things. Then this is critical for policy makers and decision makers to be aware of their DNS infrastructure. If your domain name system infrastructure is compromised then all of your systems and networks are really at serious risk.

Now on the next slide we get into some recommendations that ICANN has made. So, going back to February of this year ICANN and other organizations published a set of recommendations for the wider internet community of things that you can do that include implementing strong and recognized best practices for authorization of access to your networks. Authentication of your systems, dual encryption, do patching of your networks and systems. Check to see that you have strong email security. These can be found in the link below and this is an

announcement from February 15th. One of the important recommendations is that having DNSSEC enabled on domains actually did help limit the impact of the attack.

The next slide; Security stability and resiliency is a key focus area ICANN and for the community. We do define cybercrime to include things like the distribution of malware, attempts at phishing, operating botnet command and control networks, using the DNS in a way that enables fraudulent or deceptive business practices or enables piracy. Quite a lot of effort in the community is underway to contribute to work that increases the resiliency of the system increases the security and stability that we rely on every day.

With that I hope that there are questions and I will do my best to either provide answers that point you in the direction of where you can find those answers. I'm just seeing now some questions in the Zoom chat. It looks like the common question was; denial of services attacks can put down internet networks including servers hosting domain names. No mention is made concerning attacks to the network infrastructure so is it deliberate or an omission?

To Dave's question denial of service attacks are one type of attacks. I didn't want to go into too much detail of the different types of attacks we've seen, so it's not a deliberate omission other than I was trying to keep the content at quite a high level. But happy to go into more questions.

JOANNA KULESZA: Patrick, if I might, this is Joanna. We had [inaudible] from Joan Katambi. If Joan can hear us and has her mic on I'm happy to give her the floor for the comment or question. Joan are you with us? Joan? No, that does not seem to be the case. I'm wondering if we have any more questions from the participants? You are more than welcome to raise your hand.

I will start with the questions. We had a similar intervention yesterday that I found most useful. David was kind enough to give us a few pointers but I'm wondering Patrick what your perspective is on the usual things that end users can do to increase their cybersecurity awareness or resilience of their own devices or the services that they are using? I found that question to be particularly useful for the community. I'm wondering if you have any comments that you would be willing to share with us on that?

PATRICK JONES: Yes. I wasn't able to hear David's presentation from yesterday, so my answer may be slightly different from his. But as an end user one of the first things you can do is if you have a domain name and you've obviously gone through a registrar you should ask you registrar if they offer DNSSEC, Domain Name Security Extensions and to add that to the services that you are getting from the registrar.

You can also employ email security. You can try not to reuse passwords across multiple sites that you rely on. Try to also be aware of who has access to your critical domains or your critical services. Who has access to email for the corporation or the government agency that you're responsible for? Who has access to your key databases that you rely on.

If you are just a regular user and you don't own domains but let's say you bank online be careful about where you use the password that you use for online banking or you use for your email. If you are able to use two-factor or multi-factor authentication do that. Some banks now offer this. I would start there and hopefully that's useful.

JOANNA KULESZA: Thank you Patrick. We have a few more questions in the chat box, I hope you can see them. If there is any kind of an issue just let me know and I'm happy to read them out for you.

PATRICK JONES: I'll go to Satish's question; how will DNS evolve in the future? There are some who argue given the importance of other ways to access online resources the role of DNS may decline over the years.

That is something that I've heard but if you take applications and they are either on your Smartphone or your tablet or some device in the background unknown or unseen to the user those applications rely on internet protocol addresses or perhaps names to connect outward from the app to machines that aren't within the app.

DNS is still a key underlying technology in things that are used. It is being used more and more as more devices are being connected. From an ICANN perspective we're not seeing the diminished importance of the DNS. Perhaps there are new ways that the DNS is being used and exploited or becoming a common underlying infrastructure.

At our meetings we are trying to raise the awareness of the evolving technologies through sessions such as tech day, how it works sessions that are led by the CTO team, and just other internet evolution sessions. We have these with the board and the technical experts group. They will often have discussions about far reaching technology change with the DNS. Those are good sessions to follow and observe.

A question from Michael about governance that seems to be necessary for cybersecurity and what approach for its success. One of the things that we try to do from the team that I'm in, our Global Stakeholder Engagement Team, is encourage active participation in ICANNs technical and policy work. If this is something that you're interested in, DNS security issues, at our meetings there are a number of ways where you can get involved.

Some of those are just come to tech day at a meeting or follow remotely. There are working groups that come up from time to time that rely on community volunteers. If cybersecurity policy or technical [inaudible] try to participate in those efforts either at ICANN or at our partner organizations and then you'll be able to see what the key topics that are being discussed are and where those might align with your interests.

JOANNA KULESZA: Patrick we had one more question from Michael that focused on financing and support for securing the countries in the global self. Then I double checked with Joan, she would also like to take the floor and ask

a question. Michaels question is also in the chat box if you are willing to just --

PATRICK JONES: Let me go back up. Efforts around development are often discussed at forums such as the Internet [inaudible].

JOANNA KULESZA: Patrick, we can't hear you. I can't hear you.

YESIM NAZLAR: Patrick, if you are speaking, we cannot hear you.

JOANNA KULESZA: I think we might have lost Patrick there for a while. Yes, it looks like. Pardon that, our team will call him back and he will be right back. We just might ask you to be patient for a minute. The Adobe gremlins made it to Zoom I presume Sharon. Just for the speaking order we have the question from Michael that is being addressed by Patrick as soon as we get him back.

I have two hands up, one is from Joan who seems to be dropped again, and I have a hand up from Abdalmonem Galila whom I would like to give the floor to next as soon as we get our speaker back. I have two other questions that have popped up in the chat box and I am hoping for all of those to be answered in the next seven minutes we have left with Patrick.

Regarding the technical issues I will try to make sure if we can go a little bit over the time that was scheduled for us. Once again, apologies for the technical issues and hopefully they will be tended to effectively in the next few minutes.

Looking at the chat box, thank you Glenn for converting the slides to the eBook. As you can see the slides are available on the attached Wiki page already. Glenn has been kind enough to transform them into an eBook as well. Most appreciated, thank you, Glenn. Yesim, are we trying to call Patrick up? Are we waiting for him?

YESIM NAZLAR: Joanna if I may. I'm Skyping Patrick. He says that the internet has dropped again. I'm just trying to get him on the phone, apologies for the delay for that.

JOANNA KULESZA: Thank you so much. Any way we can get the audio would be great because we are done with the slides. It's just Patrick that we would be needing now, so dialing him up would be wonderful. Thank you. I see Abdalmonem typing the question. I understand that's the question you wanted to ask with the hand up. I'm going to put that into my questions list waiting for Patrick when he's back with us.

Please kindly note that the slides and the webinars themselves will be available on the ICANN wiki and a similar course is also available on the ICANN Learn website.

YESIM NAZLAR: Sorry, I'm still waiting for Patrick to share his number with me. I'm not able to get a response from him for now.

JOANNA KULESZA: Thank you, Yesim. If there are any comments from the participants, they are also more than welcome to share them with the group.

YESIM NAZLAR: I'm going to try a number that I'm able to find from our Outlook list. He just shared his phone number as well. If you can please bear with us for a minute or so we'll be able to get him on the bridge.

JOANNA KULESZA: Thank you very much. Thank you, Abdalmonem, for the positive feedback. I must admit that together with Alfredo we are very happy that the webinars have gathered a high participation and we're thinking about evolving this process probably during the next face to face meeting either in Marrakech or in Montreal.

I see Joan's hand going up and down. Joan's with us, she wants to share her comments. That is most welcome. But I understand this might be a question.

PATRICK JONES: Hi, I'm back. Even in a developed place we still have network connectivity issues. It's very frustrating, thank you for bearing with me.

JOANNA KULESZA: Not a problem, Patrick. We have Joan as well, she wanted to ask a question. I would suggest we take Joan's question first and then I have a list of three more questions that popped up in the chatroom. I'm trying to [inaudible] whether we would have permission from our interpreters to go a little bit over time. Would this be okay with you Patrick or are you rushing off to another appointment?

PATRICK JONES: No, this is fine. Now that I'm on connected to the phone hopefully it will stay. Let's go ahead.

JOANNA KULESZA: Wonderful. I am going to give the floor to Joan and try to ask for an extension with regard to the interpretation. Joan, the floor is yours.

JOAN KATAMBI: Hello. Good afternoon from Uganda. Joan is my name for the record. Can you hear me?

PATRICK JONES: Yes.

JOAN KATAMBI: My question to you Patrick and I want to thank you so much for the presentation. Does ICANN have a type of security policy that is available to the public. Number two, does ICANN have a cybersecurity strategy

that is available and it can be viewed by the public? Those are my two questions. Thank you.

PATRICK JONES: On your second question it's not a cybersecurity strategy so much as its a part of our overall IT & strategic plan that security elements are there. We recently published our FY21 to 25 strategic plan and two of the five main strategic objectives relate to DNS and unique identifiers security.

If you look a little further back in our history, we've had a security stability and resilience framework and that document is published on the ICANN website although that work is being updated.

There is a review team underway that is looking at security stability and resiliency issues. I would say the best document right now to look at its not focused only on security but the overall ICANN strategic plan has security elements in it. Then your first question can you repeat that again?

JOAN KATAMBI: Does ICANN have a cybersecurity policy in place. I would say, for example, in Uganda we have a cybersecurity policy but the strategy and we're waiting for approval.

PATRICK JONES: For the networks that we operate we do have internal facing policies related to how we use our networks and systems but that's not a document is published. We do have the [inaudible] statement for

implementing domain name security extensions but that's not really what you're asking about. I don't think that we really have a cybersecurity policy for the organization that is a public document. But we do have internal practices that we follow.

JOANNA KULESZA: Thank you, Patrick. This is Joanna. I have three more questions. Is it okay if I read them out to you and you can try to [inaudible] to them. We also have consensus among our interpreter who have kindly agreed to work with us until 10 past the hour, so we have roughly eight minutes. I will read out the questions, look forward to Patrick's answers and then time permitting I will reopen the queue if any more questions or comments come up.

The first question is from [inaudible] who wants to know how DNS ethical issues should be addressed and enforced. That's the first question. The second one is from Ibtissam Kaifouf, who wants to know what security issues for the DNS are opposed by the 5G and 6G wireless technology. Then the last one from Abdalmonem Galila who would like to know in the context of new protocols related to DNS like DoH or DoT where is ICANN [inaudible] more for DNSSEC and what more for [inaudible] I understand with those new DNS related protocols.

I hope those questions are clear Patrick. If they are not please kindly ask our participants to give more feedback. I'm going to give you back the floor, but if you need more clarification just let us know and we'll try to specify.

PATRICK JONES: Thank you very much. On the DNS ethical issues we have to be very careful. ICANN Org doesn't get involved in issues related to content on the DNS. Our work is focused on policy and technical issues related to the functioning of the system. So if there are issues related to how the identifiers are used to deliver content those discussions really don't take place at ICANN Org. We may provide a convening platform for the stakeholders that are interested.

We have a business constituency that participates in our work and we have an intellectual property constituency and they participate in policy work. But from an ICANN Org standpoint issues related to content, which I think is what the person asking the question is asking when they talk about ethical issues, those don't really happen at ICANN. Hopefully that answers the question.

For the next one security issues related to 5G technology. This is one that is around emerging technology issues. We did a DNS forum for the Middle East in Dubai back in February and one of the cohosts of the event was from a telecom operator who gave us a talk about 5G issues. I think we'll be hearing more about these types of internet technology evolution issues at our meetings. I would say watch the agenda for our upcoming meetings in Marrakech and Montreal.

I expect we'll start to hear more from other organizations that are active in this. One of our partners is GSMA, which is responsible for-- it's an umbrella organization for telecom operators and they are very focused on 5G implementation. They've come to our meetings and we'll probably hear more from them.

Then lastly from Abdalmonem, DNS over HTTPS and DNS over TLS, so DoH and DoT are topics of high interest from government from internet service providers and others. There were panels on these DNS technology evolution topics at the recent DNS symposium in Bangkok.

We'll be hearing more about DoH and DoT and ICANNs interest in facilitating the discussion of these protocol enhancements at the meeting in Morocco, probably at other meetings. So, you will hear more about this from ICANN Org.

JOANNA KULESZA: Thank you very much, Patrick. That was most information. We have an okay from Abdalmonem. I understand that was a satisfying answer. We have four more minutes. I'm wondering if there are any more questions or comments. Please feel free to raise your hands. I have not seen any questions come up in the chat box, I might have missed anything. If there is anything more you would like raised now is the time to do it.

It seems our participants are satisfied with all the information that has been shared. With that in mind I will move on to closing the webinar. Thank you so much, Patrick, for taking the time and overcoming the technical difficulties to join us and answer our questions. Thank you everyone who joined us, who stuck around. Some of you have participate in more than just the mandatory webinars, thank you very much.

Thank you to our wonderful staff were we would not have been able to do this without you. Last but not least thank you so much to the

interpreters who have made this a truly international and global enterprise with providing interpretation to the webinars themselves.

That's all from us. Please keep in mind that the webinars will be available on the At-Large wiki. The slides are there already and once again thanks to Glenn for reediting all of this content into handbooks that are freely available online as well.

If you have any more questions or issues feel free to reach out to me or Fredo, our staff or the entire team behind the webinars. We are happy to guide you further. I hope these have been useful in one way or another. We are very much looking forward to seeing you at Atlas and within our realm At-Large. Thank you so much, enjoy the rest of your day.

PATRICK JONES: Thank you.

YESIM NAZLAR: Thank you all for joining today's webinar. This webinar is now ended and have a lovely rest of the day. Bye-bye.

[END OF TRANSCRIPTION]