TIJANI BEN JEMAA: Good morning, good afternoon, good evening, everyone. This is our sixth webinar in the framework of the capacity building program that At-Large/ALAC set for the ALSes representatives.

Today, we have Julie Hammer who will speak about the security and stability. She has already a presentation on the Adobe Connect.

I will first give the floor to Terri to give us the usual rules of housekeeping. Terri, please?

TERRI AGNEW: Thank you, Tijani. Good morning, good afternoon, good evening, everyone. Welcome to the PreATLAS II webinar on the topic of security and stability on Thursday, 5 May 2014, at 13:00 UTC.

We will not be doing a roll call as it is a webinar, but if I could please remind everyone on the phone bridge as well as the computer to mute your speakers and microphones when not speaking as well as state your name when speaking, not only for transcription purposes, but also to allow the interpreters to identify you on other language channels. We have Spanish and French interpretation.

Thank you, everyone, for joining. I'll turn it back over to you, Tijani.

TIJANI BEN JEMAA: Thank you, Terri. Now, Julie Hammer is ready for the webinar. Julie, good morning for you, and please take the floor.

JULIE HAMMER: Good evening. Thank you. It's evening here in Australia. Thank you, Tijani.

TIJANI BEN JEMAA: I am sorry. Okay.

JULIE HAMMER: No, not at all. I would like to present some information about ICANN's role in the security and stability of the Internet.

The outline of the webinar this evening is to define security and stability and then to define ICANN's role, to just [inaudible] on why security and stability is important, to talk about the Security and Stability Advisory Committee (SSAC), and just to give one example of a security attack.

I think it would be much longer than this webinar to try to cover the whole scope of security and stability, so I thought one example might be useful. Then at the end, we'll ask for questions.

Firstly, ICANN has a limited technical mission, and it is defined in a number of documents, including the Security, Stability, and Resiliency framework. But the second of these technical missions is to preserve and enhance the stability, security, and resiliency of the systems that allocate the Internet's unique identifier systems.

There are three other technical missions there. The first one is to coordinate the allocation of the Internet's unique identifier systems.

The third one, to maintain and operate the L-Root name server instance as steward for the community. The final one is to manage ICANN's own internal systems and to provide a publicly accessible portal to disseminate and share information.

I will only be covering the second technical mission there tonight.

The definitions of security, stability, and resiliency: security is the capacity to protect and prevent misuse of the Internet unique identifiers. Of course, by the Internet unique identifiers, you will all, I'm sure, know that we're talking about the naming and the numbering system, the DNS names and numbers.

The definition of stability is the capacity to ensure that the system operates as expected and that the users of the unique identifiers have confidence that the system operates as expected.

The definition of resiliency is the capacity of the unique identifier system to effectively withstand or tolerate or survive malicious attacks and any other disruptive events without that causing disruption or cessation of service.

ICANN with its role, there are certain things that ICANN is not. I think it's important to understand what ICANN is not as well as what ICANN is in this context of security and stability.

Firstly, ICANN is not a law enforcement agency. It's not a court of law or any type of government agency in this context. Law enforcement and governments do participate as stakeholders in ICANN's processes and

policy development, but ICANN itself does not have any law enforcement responsibilities.

ICANN is not responsible for policing the Internet or for operationally combatting any criminal behavior. ICANN is not responsible for determining what constitutes illicit conduct on the Internet. ICANN is not involved in the use of the Internet related to cyber-espionage or cyber-war. ICANN is not authorized to unilaterally suspend or terminate domain names.

Having said that, ICANN is able to enforce the contracts that it has with third parties, such as registries, including those domain name registration providers.

What ICANN does do is it plays a role in supporting the work of law enforcement or government agencies in carrying out legitimate actions at their request. The type of laws that surround that will vary from country to country, depending what legal framework is in the particular context.

ICANN does participate with the operational security community in studying, analyzing, and identifying malicious use or abuse of the DNS. ICANN does play the same part as any other interested stakeholder with regards to Internet protocols.

The actual evolution of Internet protocols and related standards do not fall within ICANN's remit. Those, rather, reside with more technical organizations, such as the Internet Engineering Task Force and the Internet Architecture Board as two examples.

How then does security, stability, and resiliency fit into ICANN? There are quite a number of ways that we can think about that how that role manifests itself.

First of all, we can think of security as one of the core values that ICANN has. That is actually in accordance with the Affirmation of Commitments, the agreement that ICANN has with the U.S. Department of Commerce.

Secondly, security is one of the four focus areas of ICANN's strategic plan. Security is really an overall theme, cutting right across the organization within ICANN. Indeed organizationally, it is a department within ICANN. The ICANN has its own Security Team that looks at security issues both within and outside of ICANN. Security is an essential element in all projects and activities that ICANN undertakes.

Finally, security is a key stakeholder group within ICANN, and that is the Security and Stability Advisory Committee.

I guess as part of the introduction, the final thing to just have a quick look at is why is security and stability important? I guess it's pretty obvious to everyone, but to try and think of that in more specific terms, you might like to consider some of these points.

First of all, security and stability of the domain name system and of ICANN, security and stability contributes to the stability of the whole global economic environment. It assists in the prosperity of both developing and developed nations. The Internet and the domain name system actually assist nations in the conduct of their business. It

supports national security, emergency response, and the preservation of law and order.

Security and stability facilitates the correct functioning of critical infrastructure all around the world. It enhances opportunities for business and commerce. It enables the free flow of information. Finally, security and stability protects the interests of individual users of the Internet.

You can see that it's actually important from one extreme of the individual right through to the other extreme of globally important considerations.

I'd like now just to give you a little bit of information about the Security and Stability Advisory Committee (SSAC), which is one of the other ACs within ICANN, just as ALAC is.

The SSAC's charter is to advise the ICANN community and the ICANN Board on matters relating to the security and integrity of the Internet's naming and addressing allocation systems.

The SSAC was initiated in 2001, so it's been going for some 12 years now. it began operation in 2002. It provides guidance to the Board and to other SOs and ACs to ICANN staff and to the general community. As of March this year, there were about 40 members of the SSAC, all members being appointed for three-year terms which can subsequently be renewed.

The SSAC has a number of activities internally. It has its own membership committee which manages the interviewing of members to

come onto the SSAC and the reviewing of their membership on a three-yearly basis.

For ICANN meetings, there is a lot of planning to be done to present DNSSEC workshops and also to prepare for meetings with law enforcement. Each ICANN meeting, the SSAC and the law enforcement community meet for several hours and talk about topics of mutual interest.

The SSAC also has its own annual workshop where it gets together and does a strategic review of its work plan for the [following] year.

The SSAC also has a number of work parties. There's only a capacity to run three to four work parties at any one point in time. At the moment, those work parties are one looking at abuse metrics for the identifier system. Another one looking at public suffix lists. A work party working as all SOs and ACs are on providing input to the IANA transition. Another work party looking at providing input to the current work going on with JAS Global Advisors.

I'll just briefly give you an idea of the sorts of reports that the SSAC have produced in the last couple of years. There have been five reports produced on DNS security from search list processing, DNSSEC key rollover, an advisory on the mitigation of the name collision risk, a letter in response to ICANN Board regarding interdisciplinary studies. It was a particular question posed to the SSAC by the ICANN Board. And an advisory on internal name certificates and the risk they pose for new gTLDs.

In the category of DNS abuse, there was a report produced on distributed denial of services attacks leveraging the DNS infrastructure. There's been a report produced on internationalized domain names and two reports produced about registration data and the WHOIS system.

What I'd like to do, as I mentioned, rather than try to talk about all types of security attacks and security risks, which it's an evolving [inaudible], I'd like to give you just one example of a security attack. This particular one is a distributed denial of service type attack. It is one that the SSAC produced a report on last year, SAC65. I'd just like to give you a few more details on that.

I'm sure all of you would have heard of a denial of service attack. That is one that attempts to make a machine or a network resource unavailable to use [inaudible]. A denial of service attack is one that is sent by one person or machine. A distributed denial of service attack is one that is sent by more than one person or machine, a coordinated attack.

Contemporary distributed denial of service attacks can actually use DNS reflection and amplification to actually achieve attack data bit rates in excess of 300 gigabits per second. The amount that what this means is – I brought a diagram that will illustrate this – is that the attacker is trying to flood the network with queries and responses so that the network, and in particular a target victim, can no longer function at all.

Underlying many of these types of attacks is packet-level source address forgery or spoofing, where the attacker is actually pretending to be the victim. The attacker generates and transmits data packets purporting or pretending to be from that victim's IP address.

It uses the query-response protocols, that is the very way that the DNS functions and it's designed to function, to reflect and sometimes to amplify responses to achieve attack data transfer rates exceeding the victim's network capacity so that effectively it shuts down the victim's ability to operate and often many other victims as well.

The DNS, because of the fact that it operates on a query-response type protocol, is especially suitable or, indeed, especially vulnerable for these types of attacks.

Just a couple of explanatory terms for the diagram that I'm about to put up. It has some network devices in it named authoritative name servers. What those are is a name server that actually gives the answers in response to questions asked about names in a zone.

If someone is trying to find a particular domain name or a particular website if you like, they would send a query to an authoritative name server. That name server would need to respond with the address of the domain name. An authoritative name server must, by definition, provide a response.

A recursive name server, or a caching name server, is one that actually stores query results for a period of time. It isn't by design an authoritative name server. It is one that is put in place by organizations to actually try and save time by having some frequently requested domain names more handy, if you like. It is one that if it doesn't have the answer to a query, it will refer the query on to an authoritative name server.

A recursive name server can be one of two types. It can be secure, where it will only respond to queries from authorized sources within its network. That is a very good way to design recursive name servers. For example, if a particular organization puts in place a recursive name server, it ought to secure it by only permitting it to respond to queries from authorized machines within the network.

An open recursive name server, however, simply responds to all queries irrespective of their source. That is where some of the problems in distributed denial of service attacks come in.

Looking at this diagram now, on the bottom you can see that we have the victim's machine represented and at the top we have the attacker. In the case on the left, this is an example where an attacker is using open recursive DNS servers. The attacker is pretending to be the IP address of the victim. That is it's forging its IP address and sending a query to the open resolver saying, "Where is this domain name?"

That open resolver is then sending that query on to a number of authoritative name servers. The response is coming back, but the response is not going to the attacker because the attacker is pretending to have the IP address of the victim. So the victim is getting the response, and the more queries the attacker sends out, the more responses will go to the victim and eventually exceed their network.

In the case on the right, we're talking about where the attacker is triggering a BotNet. He has control of the BotNet so that he's sending out one query, but the BotNet is then resending that query multiple, multiple times to authoritative name servers. All of the responses,

again, are going to the victim. The victim, basically, gets shut down because their network capacity is exceeded.

The contributing factors to this is that critical basic controls for network access and DNS security haven't been widely implemented as is necessary to maintain and grow a resilient network. Basically, a lot of the name servers out there have not been secured. The recursive name servers have not been configured to only respond to queries from authorized machines.

Secondly, there are increasingly higher speed Internet connections and growing power of individual end user devices, which results in an extraordinary and growing capacity for conducting very large-scale and highly disruptive distributed denial of service attacks using these unsecured DNS name servers. As our capacity on the Internet increases, so does the capacity of these perpetrators to actually cause damage.

The recommendations that the SSAC proposed in this report after looking at this issue and explaining the contributing factors is that ICANN should help facilitate an Internet-wide community effort to reduce the number of open resolvers and networks that allow this sort of network spoofing or imitation of victim devices. This effort should try to measure how frequently these open resolvers occur and to outreach to those organizations to try and get them to secure them.

In layman's terms, to actually identify and publicize the scale of the problem and provide information to assist network operators both to understand why they need to secure recursive name servers and how they should go about doing that.

Secondly, that all network operators should take immediate steps to prevent network address spoofing. They can do that by actually actively checking where the queries they are receiving are coming from and only responding to those from authorized machines. This is something called network ingress filtering.

Thirdly, that recursive DNS server operators should take immediate steps to secure any open recursive DNS servers and, again, make sure that they only respond to the queries from authorized sources.

Fourthly, that authoritative DNS server operators – that is the name servers that must respond to every query – should support efforts to investigate authoritative response rate limiting. Some vendors of server equipment actually have software that enables the number of responses that can be transmitted to be limited within a particular time period.

What that does is if there is a DDoS attack, that even if the number of queries exceeds a certain amount the authoritative server will not respond to queries above a particular rate. Thereby, the network capacity does not become exceeded.

Fifthly, DNS server operators should put in place operational processes to ensure that their DNS software is regularly updated and to communicate with their software vendors to keep abreast of the latest developments.

It's like your virus checking software. There are always new threats arising. If you are unable to keep your software up-to-date, you're not going to be able to combat any new threats, and similarly with DNS

servers. Unless the software is upgradeable in the field to be able to deal with new types of threats, then the DDoS attack will be successful.

Finally, manufacturers or people who configure customer premise networking equipment – that's the terminology for equipment that companies have within their organizations to actually maintain their own networking and their own computer systems – those manufacturers should take immediate steps to secure those devices and ensure that they are able to be upgraded in the field when new software is available to fix any security vulnerabilities and to aggressively replace any equipment installed that cannot be upgraded.

Basically in colloquial terms, make sure customer network equipment doesn't respond to unauthorized queries. Make sure that all the equipment has software that can be upgraded, and replace any equipment that can't be.

That's the particular security issue in some depth. Obviously, there are quite a number of other security issues that from time to time will manifest themselves. But I guess to just reinforce that ICANN's role in maintaining the security and stability of the unique identifier system, the naming and addressing system, is one of its most important functions. That protects everybody operating on the Internet, not just the Internet service providers but businesses, governments, all the way down to the end user.

That completes my presentation. I'll throw back to you, Tijani.

TIJANI BEN JEMAA: Thank you very much, Julie, for this presentation. First of all, I will open the floor for questions. Everything is clear for you? Everyone is very clear? She addressed particularly one case.

Yes, Alan Greenberg? Alan, please?

ALAN GREENBERG: Not a question; just a comment. Earlier on in the slides, you gave a list of perceived bad things that ICANN is not responsible for. I guess it's worth pointing out – although perhaps it's obvious – that although we're not responsible for fixing those problems, to the extent that those malfeasance things or perceived bad things are facilitated by weaknesses in the DNS, we do have a role to play in that case. I hope you'll agree. I think you'll agree.

TIJANI BEN JEMAA: Julie?

JULIE HAMMER: Yes, I think [inaudible] next slide.

ALAN GREENBERG: I think it's the next one.

JULIE HAMMER: Yep. That's some of the points here. I think, Alan, you're absolutely correct, and that's trying to capture that on that second slide: what ICANN does. So, yes, and good to reinforce that point.

ALAN GREENBERG: I mean, it struck me where you talked about cybercrime and cyber-warfare. To the extent that those are facilitated by DNS weaknesses, we do have a role to play to try to plug those weaknesses, although we're not responsible for the actual actions. Anyway, I just wanted to clarify. Thank you.

JULIE HAMMER: Absolutely. Yes, thank you.

TIJANI BEN JEMAA: Thank you, Julie, and thank you, Alan. Olivier Crépin-Leblond?

OLIVIER CRÉPIN-LEBLOND: Thank you very much, Tijani. Question regarding the issues. How does the SSAC select the issues that…

TIJANI BEN JEMAA: You're far away, Olivier. Olivier, you are far away.

OLIVIER CRÉPIN-LEBLOND: I'm far away? Well, this is no different. Is that better?

JULIE HAMMER: Much better.

TIJANI BEN JEMAA: Now it's good. Now it's good, yeah.

OLIVIER CRÉPIN-LEBLOND: Okay, thank you. Sorry, apologies for that. The question was: how does SSAC select issues that it deals with? If the ALAC or At-Large community has some concerns about something to do with security and the DNS, could it ask SSAC for advice?

JULIE HAMMER: The answer, Olivier, to that last part is definitely yes. The SSAC will respond to any parts of the SOs and ACs within ICANN if they have a particular security question that they want looked into. Sometimes the Board asks SSAC to look into a particular issue.

A lot of the topics that the SSAC look into are actually raised by SSAC members themselves, and then they're prioritized at the annual planning session. Even though I must confess that sometimes other things arise throughout the year that might actually affect the priority of those. So it's a combination of both from without and within that the topics arise.

TIJANI BEN JEMAA: Okay. Thank you, Julie. Now, Carlos Raúl. Carlos, please?

CARLOS RAÚL GUTIERREZ: Yes, thank you very much. Julie, it's a wonderful presentation for the non-technical people, so I really liked the presentation. But I have a question. Can you give orders of magnitude of the problem with these unsecured servers? Where are they? What is the number? How much does it cost to replace? Who do the owners of these servers respond to in the ecosystem? Regional registries or who? Who can convince them to go through this upgrade of security? Thank you very much.

JULIE HAMMER: Thank you, Carlos. Indeed, part of the problem is that we don't have a real grasp on how many of these unsecured servers there are. That is what is behind the first recommendation that SSAC made in SAC065 to try and get some metrics on how many open resolvers there are out there. There really isn't a lot of information on that.

I guess how much it would cost is really very dependent on what the technology is in a particular server that you're talking about. That is one of those almost unanswerable questions.

The difficulty is in convincing DNS operators that this really is something that they ought to spend both effort and dollars on when, to some extent, there is no direct benefit to them. It certainly makes them non-vulnerable to DDoS attacks, but does that actually prevent them earning money? Not necessarily. So part of the problem is actually convincing people to do what is the best thing for the user when, in fact, it's going to come out of their hip pocket.

TIJANI BEN JEMAA: Thank you, Julie. Now, we have Otunte Otueneh. Otunte, please? You might be muted; *7 to unmute. Are you able to speak? Otherwise, until we find the technical problem with Otunte, I will give the floor to Alberto Soto. Alberto, please?

ALBERTO SOTO: Thank you very much, Tijani. I understand the technical issue, and I think that [inaudible] that they're unsecured in their DNS should not really come from ICANN but actually from other stakeholder which is the local government. They are the ones who should make the appropriate law for security in all of the information systems within their jurisdiction.

Why is that so? Because all of the attacks committed, all of the vulnerabilities in information systems, were not on the DNS. They were not on the WHOIS system. But actually people believe that this is so.

We have talked to the final users, and people believe that vulnerability comes from the lack of ICANN involvement, and this is not so. I think that the multistakeholder model should…

DAVID (INTERPRETER): Go ahead. We apologize. We are not hearing the speaker correctly.

ALBERTO SOTO: Then the other parties should be involved in that. Thank you very much.

TIJANI BEN JEMAA: Thank you. Julie?

JULIE HAMMER: Thank you, Alberto. I think it would be good if governments could legislate for something like this to happen, but some of this infrastructure doesn't necessarily come under the control of governments and might not even reside within the jurisdiction of a government to actually impact the citizens of the nation. Some of these attacks are actually global attacks. I think if governments were able to legislate it, it might resolve some of the problem, but I don't think it would take it all away. But I certainly appreciate your comments.

TIJANI BEN JEMAA: Thank you, Julie. Otunte, are you able to speak now? If you are not, please drop a line in the chat so that I understand the problem. And another question to the staff. Is he on the bridge or on the Adobe Connect?

JULIE HAMMER: Tijani, if I may?

TIJANI BEN JEMAA: Yes.

JULIE HAMMER: While that's being sorted, Maureen has kindly pointed out that Sunil Lal has asked a question in the chat: "How can one become an SSAC member?"

The SSAC members, I think I mentioned, go through an interview process. I'm probably one of the least technical SSAC members. I was proposed to SSAC as the ALAC liaison. The SSAC have a policy that, whether someone is a liaison or not, they have to be accepted by the SSAC as a full member and participate as a full member of SSAC. I had to go through the interview process and I – as I'm sure many other liaisons – I have to participate fully in the activities of the SSAC.

Other mechanisms whereby people can become SSAC members is they may be suggested by another SSAC member as someone whose skills might fulfill a particular niche that the SSAC might be lacking. Or they may indicate to the SSAC themselves that they would be interested in joining.

The SSAC itself does have a policy of not becoming too large. So 40 at the moment is actually quite large for the size of the SSAC. It's certainly a much more restricted process than becoming a member of the ALAC or some of the other constituencies.

TIJANI BEN JEMAA: Thank you, Julie. I have the question of Otunte. He said, "In my region, there are issues of credit cards not being allowed for use on the Internet. What could be the reasons?" This is the first question.

The second one is: "Some equipment manufacturers are said to implant surveillance chips in equipment. Is SSAC concerned about this?"

JULIE HAMMER: I think these are certainly general security issues. The issue of credit cards not being allowed for use on the Internet, that sounds like – I'm not quite sure whether he is suggesting that companies or banks are not allowing credit cards to be used – but I would assume that that's to protect the users from having their information stolen and used. There are a number of ways that can happen. I'm just not quite sure what is behind the question there.

With regard to the second part of the question – I'm just trying to get back to the wording of it – implanting surveillance chips. That is not really a DNS issue. The SSAC is concerned with security issues associated with the naming and addressing system of the Internet.

A surveillance chip implanted in equipment I guess, while it's certainly an issue of concern, I'm not sure that it's a DNS issue as such. The SSAC needs to contain its focus to issues that are within ICANN's remit and that are really associated with the DNS.

TIJANI BEN JEMAA: Thank you very much, Julie. I do understand what you say, and I confirm that those are not DNS security and stability issue. Those are security issues in general, but that doesn't have anything to do with the DNS.

I still have Olivier now. Olivier Crépin-Leblond, please?

OLIVIER CRÉPIN-LEBLOND: Thank you very much, Tijani. I was just going to add something to the discussion regarding the credit card security and so on. It is true, of course, on the one hand that the reliability of a domain name and the ability of this domain name to be stolen or misused is a big issue.

Of course, the implementation of DNSSEC, which requires certificates, etc., which stop the use by hackers of some way to be able to provide you with the wrong website although the domain name is absolutely correct, so some kind of interception that a hacker would do. When we use DNSSEC, this kind of interception cannot happen anymore.

As a result, that does help with the security of transactions on the Internet because you are aware at that point that the – you can get little pieces of software, by the way, which will tell you if the domain is signed or not – you will be more aware that the domain name is DNSSEC signed.

Of course, when you do any transaction [inaudible] key is on your browser that shows or sometimes they show other types of icons to show that the connection is secure. But it's true that SSAC doesn't deal with the credit card [inaudible].

TIJANI BEN JEMAA: Thank you, Olivier.

JULIE HAMMER: Thank you, Olivier. I should have thought to mention that myself and I didn't, so thank you. That's a really terrific point to make.

TIJANI BEN JEMAA: Olivier, please, try to find a way to speak in the microphone because you are as if you are very far so we barely understand you.

Any other questions? If there is not, I will thank very much Julie Hammer for her presentation and her patience to answer our questions.

I will thank you all for attending this webinar. Please, don't forget to fill in the evaluation sheet that you received together with the invitation. Those evaluation sheets will make us improve the process, improve the system, improve the capacity building program until we reach the best possible.

Thank you very much, and bye-bye.

JULIE HAMMER: Thank you, Tijani. Everyone.

TIJANI BEN JEMAA: Thank you for all the interpreters, the staff, and everyone who worked with us on this program. Thank you, Julie.

JULIE HAMMER: Thank you, all. Bye-bye.

UNIDENTIFIED FEMALE: The meeting has now been adjourned. Thank you, everyone, for joining today's webinar. Please, remember to disconnect all remaining lines at this time.

[END OF TRANSCRIPTION]