ICANN79 | CF – How it Works Session #3: Securing your DNS Operation practices (All about KINDNS)
Sunday, March 3, 2024 – 3:00 to 4:00 SJU

NICOLAS ANTONIELLO: Hello, and welcome everybody to the session How it Works, All About KINDNS. My name is Nicolas Antoniello, and I'll be doing the role of participation manager for this session. Please note that this session is being recorded and is governed by the ICANN Expected Standards of Behavior. During this session, questions or comments will only be read out loud if submitted within the Q&A pod.

If you'd like to speak during the session, please raise your hand in Zoom. When called upon, virtual participants will be given permission to unmute Zoom. On-site participants will use a physical microphone to speak. Interpretation for this session will include English, French, Arabic, and Spanish. Please state your name for the record and the language you will speak if speaking a language other than English, and please speak at a reasonable peace. With that, I will hand the floor over to Adiel Akplogan.

ADIEL AKPLOGAN: Thank you, Nico, and welcome everyone to this session about KINDNS. So, KINDNS is an initiative that ICANN has started few months ago and launched exactly a year and a half ago. So, it is an initiative that's come as an additional tool to what we have been doing for several years now, which is to promote DNS operation best practice from different DNS component. And our goal is to simplify those practices for operators so

that they can simply and easily implement them in their operational framework.

So, KINDNS is for Knowledge-sharing and Instantiating Norms for DNS and Naming Security. So, it's a share knowledge that we try to frame into one single point of access. There is a website that gives more information about the program, the detail of the component of the framework, the way to participate, and more importantly, the self-assessment tool that we have developed. So, you can already start looking at the website when we are going through this.

Yeah. So, as I mentioned, if you are very familiar with the DNS or not, you may know about the Camel project, which try to identify all the RFCs that explain or touch onto the DNS, and it's a lot. So, if you are a DNS operator, either a resolver operator or an authoritative operator and want to follow all the information related to the DNS on how to run it, you need to dedicate very full-time resources to that only. And that's take a lot of time. Being big or small, it takes a lot of resources. Big operators can dedicate a whole team to that but small operators in many cases, they are lost, kind of lost in all of this.

So, the idea was to work with the community, get feedback from the operators on the ground and produce a very simple and clear framework that anyone can follow, that anyone can have as a goal as well. So, KINDNS is not just about telling people or bringing people to just do it now, but at least you give them an objective to reach. We aim at reaching that level of maturity of our DNS operation following this framework. So, that is the whole goal. We have worked for about a year with the community through the KINDNS mailing list and input from

some operators on the ground to come up with those most important best practices to have them frame and put them out there for people to self-assess themselves against, but also join as our ambassador or as promoter of those best practices.

So, throughout this input process and discussion, we came out with five different categories of best practice, two specific to authoritative server operators. And there as well, we split it in two critical zone operator or TLD operators because we think that people who are running critical or TLD authoritative server may have a little bit higher standard in practice that they have to implement. And then we have SLD operators. SLD operators are second-level operators. That's mean anyone that has a domain name has a responsibility around an SLD. And those two will have a different set of best practices that are required for them to be compliant with the KINDNS framework.

And then we have the resolver operators as well. The resolver operator that play an important role in the DNS ecosystem also have several practice to adhere to or to implement or to aim at. And there, we have three different categories. We have closed and private resolver operators that are resolvers that are used in a very controlled environment. We have share privates. Share privates usually run by ASPs. Because they run it for their customer, and they share it with people they decide to share it with. So, it is not strictly public as what you can see in a corporate environment, for instance. It's private, but with some level of share usage. And then we have the public resolver. Public resolver are those open to anyone. We have few that are very popular, like the 8. 8. 8. 8 run by Google, which is open. Anyone can just point their device to that that resolver.

And for those three categories of resolver, there is a set of best practices that we are encouraging recommending them to implement. And as a kind of cross cutting practice is the system hardening because you can implement all the best practices at the DNS, which is a service at that level. And if your system itself doesn't work following some basic security practice. You can do everything at the DNS level, but your system is still weak, and that weakness can leak into your DNS operation. So, we have also recommendation for overall hardening the core of your system. So, if you apply the self-assessment to your KINDNS practice within your DNS operation, you are also asked to self-assess yourself for how you are running your system in Jira and know if there is anything there that may impact your DNS operation in general.

So, the program has two aspects. The first is the self-assessment aspect where you can use the tool that we put out there to check where you stand in the way you operate your DNS operation. And then you can decide, then I want to join the KINDNS framework formally. What does it mean? It mean that you are saying publicly that yes, I'm adhering to these practices. I have them implement on my operation, day-to-day operation.

And I also will be happy to promote those practices around me to my customer, to people who are using my system globally. And also, saying it here, if you want to run, let's say, training around those practices, we are also available to help you give you the information and material you need to promote those practices. They are simple, and that the goal of KINDNS is to push simple to DNS operators so that they can implement them.

So, I mentioned the self-assessment. You can run the self-assessment online. You go to the website. You choose to self-assess yourself, and you have to answer a series of questions about how you run your DNS. It's a volunteer framework, so you provide the information as you are doing it. As much as you are honest, the outcome will reflect and will guide you to what to do. You will receive a report, and the self-assessment is, of course, anonymous. We don't collect any information about who is taking which assessment where anyone send you. You do it. You provide information about how you run your network or your DNS operation. And at the end, there is a report that is generated for you.

What is interesting in the report is that not only to tell you where you stand how is your ranking about the self-assessment, but it will also provide you a guideline on how to improve where you didn't rank well. Right? Among the seven practices, you can say, no, I'm not doing this. The report that will be generated at the end of the self-assessment will tell you, yeah. Here, you got like 0/10 because you said you are not implementing this. These are the guidelines. This is why it is important to implement, and these are the guidelines on how to implement that. And you can actually download that report, use it as a guideline of improving your system, have it handy, use it as well to why not convince your decision maker to put more money into your DNS operation, to know exactly what to do and have a proper planning and framework for evolving your DNS operation.

Participation in KINDNS is based on voluntary engagements. It is not something that ICANN is forcing on to operators. It is a framework that is out there. The information that are provided are also provided

voluntarily, and we try to build a kind of trust relationship between the KINDNS framework and the operator that are using it. When you participate, that mean you join KINDNS as participant. You become kind of a flag holder of those best practices in your day-to-day operation. Yeah.

So, we have launched the platform of self-assessment in the website a year and half ago. So, we have had a lot of interests and still have on people who use the self-assessment. Till now, we have about 1,500 people who use the self-assessment tool. And what we are showing here are some interesting findings from data that we anonymously collect from the response to the self-assessment about, for instance, why people are interested in KINDNS. You won't be surprised to see that the majority of people who go through the self-assessment say they are taking it to kind of understand where they stand in operating their DNS to see if they are implementing the best practices or not.

32% of those took it to finally join KINDNS. It helped them also improve their system so that they can formally enroll to the program. Because when you want to enroll to the program, you will answer some more detailed question about the practice. The self-assessment is between you and the self-assessment tool. And the usage of the self-assessment report is personal. We don't see that. But when you decide to enroll, to become participant to KINDNS, then you have to answer the same question, but provide us a little bit more detail about how you're implementing a specific practice. And we will ask additional question so that we understand. Because as soon as you say I'm practicing it, that's a public statement, and we want to make sure that you are doing

the right thing. So, people also take this the self-assessment to prepare themselves to enroll and become a participant.

And one interesting aspect of what we have noticed as well is 40% of the people who took the self-assessment took it to convince their manager to do the right thing. Right? That means people run the DNS, and they struggle a little bit to get more resources, for instance, to implement some of the practice. Right? So, taking the self-assessment and having the report can probably help them and say, hey. This is what we are seeing, and we need more support. And that was an interesting finding for us throughout this, and there are people who are taking this for different other reason.

And there are other information that we were able to get from that. The majority of people who took the self-assessment are running both authoritative and resolver. That's happened very often in operator world. You run the authoritative for yourself. particularly if you are an ISP, you run it for your own domain name, but you also provide the resolver service to your customers. So, we have a huge number of people who-- I mean, the majority of number of people mentioned that they run both. 29% run authoritative server only. Yeah. And between those who run authoritative server, 29% run TLDs of those who took the assessment. 44 run second-level domain. And only 27 run both.

So, the majority, and that's also a good reflection of what's actually happened, the majority of people who use domain name are SLD operators because they are registering. They use the domain name for themself. So, that make sense. A good chunk of people who took the assessment are TLD managers, and we are very interested in also those

TLD managers because they run very critical aspect of the domain name system.

This is more statistic about some of the practice. This is what people say about public resolver operators, and the practice that we have there. For the public resolver, we have eight practices for public resolver operators. And the practice that is less implemented is the DNS over TLS, or DNS over HTTPS, which is implementing encryption, allowing encryption between user and resolver operators. Only 46% of people who took the assessment say they have implemented that practice specifically. Although in the practice, we have good number of people who have them implemented.

And on the DNSSES side, which has been part of our campaign of outreach for a long period of time, we are seeing a significant increase of authoritative server operators that have DNSSEC validation turned on. And this is also reflected here because most of them, 66% says that they have the DNSSEC validation turned on there. So, this also give us an idea, we, from the technical engagement team, to also know where we can focus our effort on when doing our capacity building, looking at where people are struggling at and what are the kind of information we are getting from the operators.

So, you can join the mailing list, the KINDNS discussed mailing list. That is where the discussion about the practice took place. But we intend to use that mailing list more actively to keep the community active around the best practices, but also to discuss the evolution of the practice framework. We already have few feedback, additional feedback on the practice, and we are in the process of integrating them into the

framework so that we reach a little bit more wider operators. So, the mailing list is an important tool in what we want to achieve because we want more and more feedback from the community. And we want to build actually community around this and let it run and grow by the community.

We use our engagement activity as well to promote this in different regions. So, at the regional level, the technical engagement team in collaboration with the GEC team run training around KINDNS practice specifically, encouraging and supporting operators in those regions to embrace the best practice framework and help them actually implement them.

So, this week, we are running a KINDNS clinic program. What it is, it is a one-on-one appointment that you can take with any of the technical team present here to talk about your specific case of DNS operation in any of those categories. So, you can have a very dedicated support in implementing KINDNS to take you through the self-assessment. You go through the reports and work with the team on how to implement the report, what are the tips, what you can do, and also keep in touch with the team beyond the meeting here. Continue working to improve your KINDNS practice.

There are a few evolutions of the program that are going on at the back end. We want to make the self-assessment a little bit more technical with aspect of it that is going to go beyond just answering the question and providing us the information that you want, but giving you tool that allows you to test your actual DNS operation and provide the output to the self-assessment so that we can check the implementation of those

practices. We have also start working with Zonemaster, those who run DNS, you know particularly TLD operators or authoritative server operators in general. We work with Zonemaster to develop a fork of Zonemaster specifically covering the KINDNS practices only. So, you can self-assess yourself from outside using Zonemaster and choosing the KINDNS framework so that the outcome of Zonemaster will be specific to your own operation and KINDNS in general.

We have started working with Manners because this is a mirroring of what Manners do for routing, so that to promote this together. And in KINDNS practice, the hardening the core, we reference to Manners' practice there as well because some of the practices of Manners really are relevant for hardening the core. So, we partner with Manners as well. We have run few workshops with Manners already jointly to promote both the DNS best practices and their acting best practice because at some point, they connect, and we want to make sure that we cover the whole ecosystem generally.

We are also actively working with a group of researchers on how we can measure the implementation of these practices and see how they evolve as we go into our outreach program. So, it is a very dynamic initiative. It is evolving. And we want to bring more and more operators on board. We want to bring more and more community on board to improve it and also get people to adopt it.

So, that will be it for my part of the presentation. The second part of the presentation would be driven by Nicolas. He will take you through the websites, particularly the self-assessment tool. We'll see how the outcome looks like and discuss if there's anything. But before we reach

that point, if there are any question, maybe we can quickly take them and move from there if there are.

NICOLAS ANTONIELLO: I'm not seeing any question in the chat room or in the Q&A pod. Yeah. Please state your name.

ABDALMONEM GALILA: Sure. This is Abdalmonem Galila. Actually, I think I need to read more about KINDNS. It's the first time for me to attend something like this. So, if you have time, if you manage to have some time, could you go for the assessment for one of ccTLDs now? It will be better. As I am confused. Maybe I am thinking KINDNS is a DNS framework or DNS campaigns that could help resolve our administrators or a DNS administrator on how to go for security and how to go for DNS. Somehow, I need to read more. I know. I am sorry for that. Thank you.

ADIEL AKPLOGAN: Yeah. So, he will take you through the self-assessment, and you'll see how it work. But it's more on the operation side. So, for instance, every operator know what they do in their operation. So, it's individual. You do your self-assessment, and that is related to you. As an assessment will be different from an operator to an operator, but the framework gives you an idea of what you need to do. At least you can follow that to improve how you run the-- Because that's what we want. We want an ecosystem that is more secure, that is resilient, and so on.

So, one of the practices, for instance, for the TLD operator or SLD operator is DNSSEC. Right? We have been promoting DNSSEC. It's one of the practices of securing your operation. It's not that if you run DNSSEC, then you have everything. So, the DNSSEC is one of the practices of this. And activating a validation at the resolver side is one of the practices. Then you have all the practice that you need to implement, but you will see that through the demonstration that Nico will do.

NICOLAS ANTONIELLO: So, thanks, Adiel, and thanks very much for the for the question. Indeed, we are going to go through some of the things you asked. First, my name is Nicolas Antoniello. I'm the technical engagement manager for the Latin American and the Caribbean region. Beyond that I'm part of the technical engagement team led by Adiel. And in the ICANN structure, we live under the office of the Chief Technology Officer. So, we are part of the OCTO, the office of the CTO department within ICANN. Okay?

Well, the idea now is I'm going to take you through the-- Using the website, I'm going to take you-- This is going to get a little bit more technical, but I will try to use language that everybody can understand whether you know about DNS, or you know nothing about DNS. Of course, this program is for operators, for DNS operators. But who is an DNS operator? A DNS operator is someone that operates a DNS server. No more, no less than that. You can be an operator if you run your own resolver at home. You can be your operator if you're part of a network operation center in an ISP, in an organization, in an enterprise,

wherever you operate, any kind of DNS server, which is two kinds, whether you operate a resolver or whether you operate an authoritative serve. So, this program is built for those operators. Okay? Any operator of any kind of DNS server.

Then I'm going to also go through, summarize some of the concepts that Adiel has just mentioned. First of all, let's talk a little bit about the operator categories here in the web page. Let me go a little bit back. Okay. So, we have, as Adiel already said, we've separated this in five types of operation. That five types of operation live under two groups. First group is authoritative—Sorry, I'm going to start the other way around. I'm going to start with the recursive server operators. Okay?

So, first group will be operators of recursive servers. Here we have three types of recursive server operators. We've divided this into what we call private resolvers. So, for the program, a private resolver will be a recursive server that it's only meant to be used by the one that operates it. For example, I have an organization. My organization has an IT team that runs a resolver, and that resolver will only be used by the devices within the organization. It won't be a public resolver. It won't be used by any customer of the organization. Only by the organization staff itself, the organization devices itself. That's a private resolver, so it's private.

Then we have a second type of recursive server, which we call the shared private resolvers. A shared private resolver is a resolver that is meant to be used by the customers, normally used by the customers of an organization or a business. For example, if you run an ISP, normally ISPs provide all of its customers with a resolver, with a DNS resolver.

That will be a shared private resolver because it's private. Because it's not going to be accessible by anyone in the Internet so it's not a public resolver. But it's not meant to be used only by the organization, but the customers of the organization, only by the customers. So, it's a shared private resolver for the program.

And then we have a third type of resolver, which we'll call the public resolvers. Those are resolvers run by certain organizations that are meant to be used by anyone in the Internet. So, anyone can have access to those and can use them as resolvers. Examples of these open resolvers are the well-known run by organizations like Google, the 8888, the one that has the IPv4 address 8888, the one that has the 1111 IP address, the 999, the quad 9. So, it's the quad 9, the Cloudflare one, the Google one, and so on. There are not hundreds of them, but there are many of them that are optionally any anyone connected to the Internet can use them as a resolver because they are open resolvers. Okay?

Why we do this distinction between private resolvers, shared private resolvers, and public resolvers? Because the operation has some base basic best practices or common best practices that are, again, that are common to all of them, but they have some differentials in operational terms. For example, if you're operating a public resolver that is accessible to anyone, you'll probably will have to review very well your security policies and your security measures because your servers will be exposed to all the Internet, and then it could be used for good or for bad. And you will have to, or you will need to protect from bad activity that may use a DNS resolver to perform an attack.

So, we are not talking only about attacks that target the resolver itself, but attacks that use the resolver to attack a third party. So, basically in a more common language, there are types of DNS attacks that may use these open resolvers as a weapon to attack a third party. So, you have to protect from that.

If you run a private resolver, as your resolver is going to be only used by devices within the organization, you will more likely don't have that issue because you control your organization, you have your organizational security practices in place. So, if anyone is using your DNS to attack someone or attacking your DNS server, it's it will probably come from within the organization and not from the outside. So, it will be maybe it will be easy to track or to control. So, there are differences in operation, and that's why we have these three. We have classified this recursive resolver, recursive server operations in three groups.

Then we can go to the authoritative server operators, and we divided this in two subcategories or types of authoritative server operations. One, a program called TLDs and Critical Zones. So, these are the operators of authoritative servers in charge of TLD, so a country code top-level domain DNS authoritative server or a generic top-level domain authoritative DNS server.

Then it's also critical zones, and critical zones is a more broader term. What is a critical zone? Well, a critical zone could be whatever the operator think that it could be critical. And for example, there are, let's say, for some countries at governmental level, the operation and the continuity of operation of the authoritative servers that host the domains for governmental services are critical because if those go

down, people won't be able to access those public services. Right? So, those are critical zones, whether they are or they are not in the top level of the DNS.

So, they could be second level, but they still could be critical zones. For example, for others, educational domains, so domains that you assign to educational institutes, could also be considered critical zones and so on. Domains related to health services, etcetera, financial domains related to financial services, etcetera, etcetera. We included here whether or not they are at the top level. They could be second level, third level, whatever.

And then there comes all the other, which is other second-level domains or whatever level zone. So, any other authoritative server will fall into this other SLD zones category. Okay? And again--

ADIEL AKPLOGAN: If you're on the website and trying to follow, if you click on the operator's category there, you will see everything that's Nicolas is explaining. Then you can have the different category and what we put in there. You can read it.

NICOLAS ANTONIELLO: Thanks, Adiel. That's the classification for the program. So, if you're going to use and you'll be part of this program, you will have to go through all of this or all of those that are appropriate to your type of operation, whether you operate a recursive or authoritative server and then fall into those five different classifications. Okay?

Then we have this section called platform hardening. And this goes beyond the classification we previously talked about. And this is like taking steps, taking further steps in order to secure or increase the security, the resiliency of your DNS, of a DNS server operation. And there are a lot of practices here that are good to implement if you want to harden your infrastructure, right, your platform. And that goes from some simple or recommendable or agreed common practices that you should implement to some more advanced ones, okay, that you should consider implementing when you are deploying a platform.

And if you see, some of them says must, so that is strongly recommended. If it says must, it's something that is strongly recommended. And some of them are not that strongly recommended, but recommended or something that you should implement, but it's not a must. Suggested. Yeah. Of course, all of this, as well as any standard, is optional. So, there's no obligation to implement none of what is here. Only that they are common practices, and they are recommended and suggested procedures.

Okay. Then we have these tools and guidelines section. Right? And this is one of the key elements of the program. First, we have this assessment and tools. Right? And this is probably the key part of the program, which is the self-assessment that Adiel just talked about. I'm going to go a little bit, deep into this. This self-assessment, as Adiel mentioned, is optional, of course. It will be optional to provide information about who is taking the self-assessment. If you want to provide information, you can provide information, name of the company, name of the organization that is taking the self-assessment. If you don't want to disclose that information, it's okay. You can still

take the self-assessment without disclosing any information about who is taking the self-assessment.

At the end of this-- Oh, okay. The self-assessment. Let's try to take the self-assessment. During the self-assessment, you will be presented a series of questions. This is the name of the organization. It's optional. I can put Nico here, like my organization name, or just leave it blank. It will be the same. You can still take the self-assessment. And then it will ask me, okay, why are you taking this self-assessment? You have to select any option here, for example, okay, to know where I am standing in terms of implementing best DNS operational practices.

Then I have to select what type of DNS operation I have. If I run an authoritative server, if I run a recursive server or if I run both of them. If my DNS infrastructure is managed by a third party or if I manage my own DNS server. Let's suppose that my organization is an ISP, an Internet service provider, and I run a recursive server to provide my customers with recursion, with DNS recursion. That will be recursive server operations. And then the type of recursive server operations, as I mentioned, if in this example I am an ISP, I will run a share private recursive resolver.

And then here is assessment. Here are all the questions that you will have to answer in order to go through this self-assessment. So, it's a series of practices. Here, you are presented with six practices, and you will check all practices that you are currently implementing. Okay? For example, practice 1 says, oh, I have DNSSEC validation, turn it on in my resolver. So, my resolvers have the capability of validating DNSSEC

information coming from the authoritative servers. So okay. I have DNSSEC. I check that.

Practice 2 says I use access lists to restrict who may use my recursive resolver. So, this is a shared private resolver, and I want only my customers to be able to use it. I should have a security system, a security method that it's called normally called access list that will block anyone but my customers in accessing the server. So, I say, okay. Yes, I have this. This is kind of a common practice if I want my server not to be public. Yeah. And you don't want a public resolver if you are not running a public resolver. If you're running anything but a public resolver, you will need an access list to block access. Okay?

Then practice 3, I have QNAME minimization. And I don't even know what QNAME minimization is, so I will leave that in blank. Right? Okay. Practice 4. My resolver don't run on the same server. No. No. I have a resolver running in the same physical server that I run my authoritative server because I also have an authoritative server for internal use, and I don't have much money. And I just get a physical server. I put it a virtual machine in that. I created two virtual servers. On one of those virtual servers, I run the authoritative server, and on the other one, I run the recursive server. Or even worse, I have one machine, one operating system, and I run both servers, authoritative server and recursive server in the same machine. So, I don't comply with this practice, so I won't check it. Okay?

Practice 5. My recursion service are resilient using at least two distinct servers that take diversity into consideration. No. No. I don't have that. And the infrastructure that serves my DNS service is actively monitored.

Yes. I have monitoring in place. I monitor different the health of the server, the number of queries I get, etcetera, etcetera. So, I comply with that practice. I click next. You see, do you have a public facing or internal portal for customer to access and manage their DNS servers? No. Because I run a recursive server, we don't need this. And that's all. The self-assessment is done. Right?

I can continue and take a second assessment that will go deep into security practices. These security practices are not particularly only for DNS servers. These are security practices that are normally for many, many other services, including the DNS server operations. For example, Adiel mentioned Manners, which is a program about best practices, but not for DNS, but for routing. Actually, yes, as Adiel said, this KINDNS program, it's a kind of sun of manners. We took the same idea, and the ISOC originally developed it for routing best practices and created this program called KINDNS, which is for DNS operations best practices.

So, it has a lot of other security measures or security recommendations that you should implement. Some of them has to be with routing. Some of them has to be with ensuring or securing your DNS infrastructure in particular, etcetera, etcetera, but let's not take this at this moment.

ADIEL AKPLOGAN: Just one thing. The connection with Manners is very key because all DNS, you know that all DNS server has an IP address, right? So, usually, we look at the DNS operation, but securing the IP address and the network, the routing that access your DNS is also critical. So, you see the link, direct link with Manners there very clearly.

NICOLAS ANTONIELLO: Yeah. And to add to what Adiel have done, normally, we have this-- Not normally. Sometimes, more frequently than we wish. We normally do capacity building about DNS, about routing, about many, many, many things that has to do with Internet or network networks in general, but we focus on a specific topic. Like now, we are focusing on DNS. And we kind of we risk losing the sight of the whole thing. Right?

So, as Adiel mentioned, DNS is not an isolated thing. It needs IP addresses. It needs a whole network to run. You need routers, which are the equipment that are used to take the information from one place of the Internet to the other. And you need routing protocols. You need a lot of stuff, security equipment, security measures in place, etcetera, etcetera. So, that's the idea of connecting-- This is the idea of this part of the program connecting the DNS operations with the rest of the network operations, as a part of an ecosystem. Again, we are not going through this because it will take a lot of time to go through all those practices, but you're invited to also that.

So, I click end, and here, the system will give me a kind of score. Okay? And says your total score for this assessment is 50%. So, you are implementing 50% of what? 50% of what? This program collected as the best common agreed operational practices for this type of DNS operation you selected. I selected remember that we are doing only resolver operation, and within resolver operation, we are doing share private resolver operations. Okay? From those six practices that were there, my score is 50%. Okay?

And then I have these two options. One is download my report. So, I click here, and it will generate a PDF with all the information, and with more information than what I have gone through. It will give me a clear sense of where I'm standing in terms of DNS operation. It will tell me, okay. You should implement this, this, and this that you are not implementing yet, and I have resources within the program to go and implement those parts of the practices that I'm not yet implementing. Okay?

If I do not download the report and I close this page and I want after this to download the report, I will have to go again through all the report because this program, this web page is not getting or keeping any information about the survey, about the self-assessment beyond this point. Okay? So, I should download it. I'm not going to do it now, but I should download the report. Okay? And then I can take, of course, I can take the self-assessment again if I remember that I forgot. Oh, I remember what is QNAME minimization, and I said I didn't click that because I thought it was another thing. I just take it again, do it again, and download the report. This is just this is for you and only for you. No one will look at this if you don't want to. So, there's no sense in lying in this self-assessment because it will tell you where you are standing in terms of best practices. If you click all of them, it will be as if you don't do it. Okay? Unless you, of course, comply with all the good practices.

Okay. So, that's the end of the self-assessment part. And remember, you have a self-assessment for each type of operation that you have. Okay. Let's download. Let's download it and have a look at the report. It will generate the file, and then download. All right. Let me share the PDF that is generated. So, this is the report that I just download. As you

see here, it's the completeness date. It tells me about what type of self-assessment I took, what are the main operational practices. It says that I operate a share private resolver only.

These are the practices that-- the practices relate to DNS security practice 1, 2, and 3. I implemented practice 1 and 2, but I didn't implement QNAME minimization because I don't know what is QNAME minimization. I know what it is, but, yeah, let's do it by just for example. And I'm sure that many of you already know what it is, but just as an example. Okay? But it may happen that someone operating a DNS server doesn't know what it is, and it's okay. It's perfectly okay.

And then the operational practice related to availability and resiliency of your DNS servers, which are practice 4, 5, and 6. I only have practice 6 implemented, so the other two scores with a 0. Okay? So, that's the 50% score. And then it comes. For practice 3, which is the one that I didn't check because I'm not implementing, it tells you what it is, and it gives you a link, a guideline, a series of guidelines about how you may implement it. The platform also has, the program also has examples of configuration, of basic configuration or some of the most common servers. For example, if you're operating a resolver, you may be using bind software. You may be using outbound software. Those are two of the most used software in the world to run a resolver. It will show you examples of how to configure QNAME minimization in bind, how to configure QNAME minimization in outbound, etcetera, etcetera. S

So, it's explaining what is that practice that you are not implementing, how, and giving you further links and sources of information on how to deploy it, how to implement it. Okay? The same for practice 4 that I

score 0 and the same for the practice 5 that I also score 0. So, if I ever go through all of these and I found out that I can implement it. Go, I implement it, take the self-assessment again, and I'll score 100%. Okay? So, this is the idea, the whole idea of the program to build something useful and a single window or a window that puts together all the information and all the links to access that information. The program does not make standards. We do not generate standards. We do not generate best practices. We just collect them in a single place. Why?

Because as Adiel mentioned, if you are a new technician, for example, and want to deploy a DNS server, whether you are running an authoritative or a recursive server, you will have to go through over 150 standards and best practices. Okay? Standards and best practices, if you have gone through at least one of those, are tens or even sometimes hundreds of pages each. So, it's a lot of information you have to read. And that information, if you are talking about standards, yes, you go to the IETF site, and you have all of them there. But if we are talking about best practices, those best practices are not in a single place. They are spread all over the Internet. So, you first will have to guess which are the most trustable sources of best practices, etcetera, etcetera.

What we try to do here is the same, again, the same as Manners does for routing, collecting the best practices, and presenting those in a place that is more friendly to read and to go through, but for DNS operations. Okay? And let me just close this. I'm going to stop sharing this. I'm going to share back to the KINDNS site if I can find it because I just I think I closed the browser and I just-- Okay. I got it. I found it. Let me share

it again. Okay. That's the, again, at the KINDNS website. So, that's the report you can download here. Okay?

Let's go to the home page. And then we have these tools and guidelines resource here. We've gone through the assessment tools. We have a dashboard that shows some statistics about the program and some of those statistics that Adiel already showed, and then we have these guidelines. This is also a good resource of information for those willing to learn more about those practices that you don't have yet implemented or maybe practices that you have implemented, but you want to learn more or refresh what they are and how they work. So, you have here a lot of information and guidelines depending on the kind of the type of operation that you run.

And then you have here, this DNS security resources that, again, will give you-- This is a collection of sources for best practices, standards, etcetera, etcetera. Some of them, in this case, they are classified in the organization that has produced that recommendation or that document. And we have a series of documents, in this case, produced by ICANN, a series of standards produced by the IETF, resources of information about DNS produced by organizations like DNS-OARC, RIPE, APNIC, NANOG, so network operator groups from different parts of the world.

NANOG is the network-based group for North America, but each region has a network operation group. And there are some sub regions like the Caribbean that has its own network operator group like CaribNOG, which also has many sources of information. And some private companies like Google, ISC, or other companies that produce

information, documentation, and recommendations about how to configure your service. Okay?

We are on top of the hour. We are going to do a 15-minute break, and then we are going to use some minutes from the following session. So, we can break now. We can pause the recording and come back in 15 minutes. Okay?

[END OF TRANSCRIPTION]