Summary of Consultations and Comments related to the ICANN Global DNS-CERT Business Case

ICANN conducted consultations with a staff broad spectrum of stakeholders related to the concept of a DNS CERT starting beginning in December as part of the inclusion of this initiative in the ICANN 2010-2013 Strategic Plan and as a basis for drafting and publication of the Global DNS-CERT Business Case. The staff has continued consultations at the requests of organizations listed, conducted consultation sessions at the ICANN Nairobi meeting and tracked community dialogue on this topic. This document provides a record of these consultations and comments in response to numerous public comments about the origins of the DNS-CERT business case, to ensure a full record and accounting of these interactions and to further the community discussion of this topic. Private consultations with various community members are noted for purposes of providing a record of interactions that guided ICANN staff in the drafting of the Global DNS CERT business case. This summary includes the discussion logs from the ICANN meeting in Nairobi, Kenya 7-12 March 2010. This summary supplements and is released in conjunction with the Summary of Analysis and Comments of the publicly posted ICANN Strategic Security, Stability and Resiliency Initiatives and Global DNS CERT Business Case

List of Consultations

Private consultations before business case document published;

- Security Expertise, list/community Custodians
- Regional TLD association managers

Public Comments on draft ICANN 2010-2013 Strategic Plans

- Lise Fuhr, Dansk Internet Forum
- Yvette Wojciechowski, The Coalition Against Domain Name Abuse (CADNA)
- Bill Woodcock, Packet Clearing House
- Jeff Schmidt, JAS Communications LLC
- Eric Brunner-Williams, CORE

Staff Presentation at Forums

- TF-CSIRT meeting, FIRST TC
- CENTR GA
- APTLD AGM
- AfTLD AGM

- LACTLD/LACNIC (29/5/2010)

Consultations and comments logs - ICANN Nairobi Meeting

- Security Strategic initiatives public consultation
- ccNSO Tech Day
- GAC update security issues
- GAC-Board meeting
- Public Forum
- DNS Abuse Forum
- GAC Communique

Comments after ICANN Nairobi Meeting - Perspectives on a DNS-CERT

Summary of Comments

There are three types on consultations included in this record. First one is pre consultation record before the business case document being published. Second part is public comments to the draft 2011-2013 strategic plan, which includes the plan on developing DNS-CERT concept. Then the rest is all the other comments, questions and inputs expressed after the business case being posted for public review. The record of consultations is provided in chronological order.

Pre-consultations before business case document being published

ICANN consulted a range of organizations and groups focused on those addressed in the response capacity and gap analysis summary in the Global DNS-CERT business case. Those are private consultations. ICANN staff felt further exploration the DNS-CERT concept was welcomed in particular the requirement for a gap analysis and need of fill the gaps in response resource constrained operators. Overall, comments focused on the utility of leveraging and orchestrating existing efforts. Those inputs were incorporated to the drafting of the business case.

Pre consultations with Regional TLD managers are also private conversations, but they all invited ICANN staff to their members' meetings and provided an opportunity to introduce the idea and garner feedback that was utilized in the drafting of the business case.

Other inputs and comments

Other discussion and comments recorded as publicly available are captured and listed in this record.

Chronological Record

Person, organization	Date, Occasion	Comments
Paul Vixie, ISC	**14/12/2009**	Private-consultation
Barry Greene, Juniper	14/12/2009	Private-consultation
Bill Woodcock, PCH	14/12/2009	Private-consultation
David Ulevitch, OpenDNS	**14/12/2009**	Private-consultation
Andre Ludwig, NX.domain	14/12/2009	Private-consultation
Chris Morrow, Google	**14/12/2009**	Private-consultation
Rob Thomas, John Kristoff Team Cymru	**14/12/2009**	Private-consultation
Jose Nozario		Private-consultation
Steve Adegbite, FIRST		Private-consultation
Karl Hanmore		Private-consultation
Jose Nazario, Arbor	**15/1/2010, Public comments on draft 2010-2013 strategic plans**	I am writing today to express my support for the broad outlines ICANN has made in its draft 2010-2013 strategic plans. Specifically, it's a pleasure to see an expression of ICANN's possible role as a leader in global coordination to address security problems affecting DNS operators, registrars and registries, and ultimately end-users. DNS clearly is an underpinning for Internet operations, and the next few years are crucial to Internet security. A DNS-CERT can easily have many possible roles in helping global Internet security efforts. Under an ICANN umbrella, access to key constituents would be possible, much more so than from an outside body. DNS operations are multi-national, and therefore some body focused on DNS is required in a coordination or a support role. Furthermore, DNSSEC deployments clearly require investigations into scalability and impact, and ICANN's continued leadership will be key.

The past few years have seen a rise in domain generation algorithms (DGAs), most visibly this past year with the Conficker worm. In these scenarios, a successful response to block the attacker's access requires significant amounts of TLD coordination to prevent misuse of the domain names in the future. Ad-hoc efforts in the past have been attempted but quickly run into longevity and cost challenges. As a longstanding participant in the Conficker Working Group, I can say that ICANN's role was key to making last year's Conficker response a success. ICANN's willingness to lead demonstrated the positive impact that can be brought to bear, as well as gaps that the Internet security community must address.

An additional threat that an ICANN DNS-CERT would be valuable to address are attacks on the system of registries and registrars, which we have seen growing with an alarming frequency. ICANN's responsibility in helping to protect the DNS infrastructure makes a DNS-CERT key to future security and infrastructure plans. ICANN has shown leadership in 2009 in this area, and they can - and should - extend these efforts.

ICANN has also shown concern over the impact of fast-flux DNS operations on the DNS infrastructure with the working group, in which I also participated. Already we've seen a significant drop in the number of fast-flux domains active in a given day, and their effective lifetime is dropping. ICANN's efforts in educating operators and the security research community have certainly been key to this result. Similarly, ICANN's move to allow for new TLDs and IDNs has security implications that will surely be abused in the immediate future. Any DNS-CERT can help ICANN's role in a coordinated response for the defense of the DNS infrastructure against such fraud and abuse.

Finally, DNS infrastructure attacks on the availability have been a problem for many years, although their scale and impact has been growing for many years. ICANN is uniquely positioned to provide assistance to all TLD operators in the DNS community. A DNS-CERT would easily have a beneficial role in protecting a key underpinning of the Internet.

These are but a few of the areas that need cross-border, Internet- scale responses that ICANN would be able to provide. A DNS-CERT's mission should be to support their constituency against

		these sorts of threats - and surely more in the coming years. Any DNS-CERT's success is measurable in the number of incidents that occur, the number attempted and the number that succeed, along with their impact. This includes losses from registry compromise, outages from DDoS attacks, use of DGAs by botnets, and fast-flux activity. The Internet security community is actively seeking ICANN's participation in security response, and a DNS-CERT effort is certain to have a major benefit to the future of the Internet. I welcome this proposal in the draft 2010-2013 strategic outline put forth by ICANN.
Andrew Cormack, JANET(UK)	18/1/2010	JANET(UK), as manager and operator of the .ac.uk ccSLD, operator of the.gov.uk ccSLD and provider of the JANET CSIRT, welcomes ICANN's proposal to establish a conceptual model for a collaborative DNS security response system. We consider that the global importance of Domain Name System is such that attacks on the system and vulnerabilities in the service must dealt with as quickly and effectively as possible. The response to the Kaminsky protocol vulnerability showed the benefits of having protocol and software experts, DNS operators and Computer Security Incident Response Teams (CSIRTs) working together to understand and resolve a problem. Building on that experience to develop a standing framework for trusted collaboration appears to us the best way to ensure that future incidents are dealt with as, or even more, effectively. Such a framework must permit the involvement of expert individuals and organisations from many different sectors: we consider that ICANN, through its engagement with both the CSIRT and DNS communities, is well placed to lead the development of the framework.
Lise Fuhr, Dansk Internet Forum	**21/1/2010**	DIFO supports the establishment of a DNS collaborative security response system to coordinate effective response to attacks on the DNS, and finds very useful to the Internet society in general.
Yvette Wojciechowski, The Coalition Against Domain Name Abuse (CADNA)	21/1/2010	To begin, CADNA would like to express its support of ICANN’s plan to work to improve DNS security. Many individuals and corporations rely heavily on the Internet for everything from socializing to conducting business, so ensuring security is one of the most basic and vital initiatives that ICANN must undertake going forward. However, in addition to the projects ICANN has outlined in its strategic plan—DNSSEC implementation and DNS CERT concept development—ICANN should have other important issues that would mitigate risks in the domain name space such as cybersquatting, phishing and malware covered in this plan opposed to such focus on new gTLDs.

Bill Woodcock, Packet Clearing House	**21/1/2010**	Addressing specifically the matter of the security and stability of the domain name system, PCH commends ICANN's actions in investigating the impacts of a larger root zone, ICANN's operational improvements to the L-root nameserver and the other zones under their direct care, and ICANN's initiatives to coordinate communications and remediation between critical parties in response to direct threats to the DNS. This last was particularly visible and beneficial in consolidating community response to the Conficker worm, among other challenges. As a consequence of this demonstrated competence and efficacy, PCH heartily supports ICANN's endeavors in the area of DNS security coordination. ICANN has shown itself to be the most appropriate institutional home for DNS security planning and liaison activities, supplementing, complementing, and coordinating the security staff and resources that reside in the network operations, equipment vendor, and academic communities. ICANN's plan to create a CERT specifically serving the needs of the DNS community is an appropriate and admirable one, and has PCH's unconditional support.
Jeff Schmidt, JAS Communications LLC	24/1/2010	The growing complexity of the overall DNS technology ecosystem is certainly on the rise. DNSSEC, IDN, root zone changes, and new TLDs - separately and together - will notably increase the complexity of the technical, operational, and administrative tasks required to effectively offer and consume DNS related services. History has shown that all variety of troublemakers will take advantage of such complexity. As such, I strongly support ICANN's plan to create a CERT specifically serving the needs of the DNS community.
Eric Brunner-Williams,	**28/1/2010**	From these experiences, and the unrelated but tangential inability to focus on what "high security" should mean (it is definitely not "accounting standards"), I am concerned by the detail-free plan to copy-a-Cert. Some obscure background. While I was at SRI two events occurred. One was a real event, but misinterpreted. The other a real event correctly interpreted. On both occasions I had discussions with a person responsible for a very large collection of computational assets. These discussions lead to DARPA's formation of the CERT at SEI, as a institution to facilitate communication

		between academic and industry employed computer scientists and governmental agencies with a lower skills profile in the problem domain. Times have changed, the original CERT has shifted its mission over time, there is now a US CERT, and perhaps the original government agencies have improved their facilities and their technical abilities. The point is, CERTs are not a given thing, they are a box into which some money and some purpose is put. We should decide how much money and what purposes, not just "start a CERT". We have no way of knowing at present, what registries present zero resource acquisition cost to authors of distributed systems similar to the Conficker .C variant, which could use those resources to construct rendezvous points. No one has done the unglamorous labor of foreach(TLD in IANA) {ask cost of rendezvous resource acquisition questions}. The next instance of a .C will have us again asking "Does .el (Elbonia, Lower) support automated registration?" We also have no way of knowing at present, what the actual cost of event response is, let alone a means to reasonably present it to some jurisdiction attempting to prosecute for damages. These are important things to get done. If we are not careful, an "ICANN CERT" will captured, much like the ICANN SSAC function during the fast-flux hosting effort, by retail cops-and-robbers concerns that missed the fundamental issues of rapid update by registries as a fundamental tool of modern dns exploiting systems, and zero effective cost of registration, again by modern dns exploiting systems. At that point we would have a "CERT" which "makes the suits smile" but does us no good when competent and motivated programmers target infrastructure.
TF-CSIRT meeting, FIRST TC	28/1/2010	- Support ICANN’s initiatives on Security Stability Resiliency activities including DNS-CERT - Suggested the conduct of a survey to find how much ccTLDs and National CERTs security response collaboration
Alain Aina, AfNOG	**21/1/2010**	Private-consultation
Jonathan Shea, APTLD	20/1/2010	Private-consultation
Peter Van Roste, CENTR	**23/1/2010**	Private-consultation
CENTR GA	25/2/2010	Briefing to the members and questions and answer session

APTLD AGM	**1/3/2010**	Briefing to the members and questions and answer session
Eric Akumiah AfTLD		Private-consultation
AfTLD AGM		Briefing to the members and questions and answer session
DNS-OARC board members		Private-consultation
ICANN Nairobi meeting, Security Strategic initiatives public consultation	8/3/2010	- Peter Van Roste, General Manager for CENTR, the European Association of ccTLDs. I had a couple of questions and comments which do not affect; I must say the principle of this discussion, because I think it's a very relevant one to have. And I suggest I just go through them and you can take whatever you want from that. You mentioned that there were plenty of community calls that were at the basis of this DNS-CERT ID and for us it would be very useful to understand where those originated from. Because the ccTLD community has a rich history of helping out its members and if some of the members of that community would claim that they do not have access to that relevant information then it's very important for us to figure out how we can improve that. And also because, from what I've heard both within the CCNSO, the CENTR community and APTLD, the Asian community, of which I attended a meeting last week, that claim did not originate from those corners. So that would be very helpful in particular because it would also help within understanding what the exact nature of their needs is. And from what we see, and based on the information that you've shared with us, I think that we identified a real problem, that is, during the Conficker attacks there was an issue with communication but it seems that issue can be solved in a much cheaper way than a $4 million dollar organization. There are the obvious overlaps with the existing processes which you point out but by just pointing them out we still think they are still relevant and they're still there so we need to figure out how we could solve that. And then it's also unclear on how it fits into the overall budget. From what I understand, it's not included in the overall budget at the moment. The business plan itself mentions that ICANN would be prepared to basically kick start it. But I always find it, running an organization myself; I find it a very tricky process of starting something and then looking for funding. Mainly because we have seen that process on a number of other occasions such as the trainings for instance for ccTLDs on a technical level.

	I think it’s very important that during this consultation, the right question is asked. And that question should be, “If you think you’d benefit from a DNS-CERT, would you be willing to pay for it?” Because obviously everybody is always interested in free candy. - CERT is a trademark of CERT/CC, have you checked if you can call this project CERT, DNS-CERT? - it looks like DNS-CERT should not be operating CERT. Because there is not much work to operate incident on that. It should be like CERT/CC, coordinating CERT. Mostly producing documents advisory and this also clear that at least DNS-CERT specific organization will be to the level of regions. Like Europe, America, Southeast, South, North. So in this case, a major impact and work of DNS-CERT will be producing very consistent recommendations and advisory. Have to deal with this. - Also, at the next meeting, it was told that actually project of DNS-CERT will require only few full time personnel at ICANN or IANA, and all other will be located to the regional CERT that will be actually acting in coordination for handling incidents. At this presentation I haven’t heard this. Because this is what would be logical. Three staff and all are sharing on duty-sharing cycle. All over the world. In this way organize the most effective work and CERT in many countries. - Alan Aina; I am from African region, so. Just to say that in our community, I think our community is part of what we call a resource constrained. And I think it would be different, we don’t have in our region, we don’t have a cc coordination center in the countries so people may need to get information directly from this CERT if you’re going to, so I think you need to think in how you can design this thing to meet the various needs of the region because we have different region and different needs. So as I said, we don’t have cc’s so many countries in our region, so don’t target them who use the local cc to send information to the community. I think it will change but for now I think there is a need maybe for our, for some constituencies to directly get information from the DNS-CERT, central point. And we are working to share information in our community to ask our people to comment which we have a couple of weeks before the end of the comment times. And we appreciate the idea and thank you. - I hear a lot of community support for that. But I hear quite a few rumbles within this community about the CERT proposal because it almost feels as though that is being pushed forward in advance of that analysis that might demonstrate the need and whilst there is support, both within the Affirmation of Commitments and the Strategic Plan for building on the security and stability role of ICANN, don’t assume that that means widespread support for this initiative

and that gives me concern. Particularly when you look at the proposed budget line, which of course will draw a lot of attention and comments.

So I kind of wonder the extent to which this is going to be actively supported within the community and whether strategically it might be better to build up that support more over time with the Number One Initiative actually feeding and informing that discussion that hopefully results in the outcome.

- With respect to the system-wide analysis of DNS, are we talking about just at the top level? Or are we talking top to bottom? Because I haven’t yet understood, maybe I haven’t been paying close enough attention. Are we talking about all of the DNS operations that are run by organizations and enterprises and independent operators or are we just talking about the DNS operations that are run by the top-level domain providers?
- In the analysis of the Conficker and the subsequent kinds of activities, the technical issue was that DNS was being used as a communication mechanism for the control of these bots. And as you said, this morphed from an initial use of just a couple of top-level domains to 110 top-level domains and focused on top-level domains that were perhaps more permeable or more susceptible to exploitation than others. I remember from the discussions that we understood, at least in the abstract, that the use of DNS for that purpose was one of several possible similar mechanisms that almost any system that provided open registration. So we could be talking about Facebook or we could be talking about some other form of socially open system that allowed many, many people to join in and it would not have to be a domain name registration per se, it could be a comparable mechanism that is quite separate. So the question is, if we put all of this energy into trying to understand how to prevent Conficker and its successors, is that too narrow and is the problem sort of bigger than that? In which case, mounting this effort may be, however expensive it is, may be sort of not matched to the broader problem that’s actually out there and that it’s not just a DNS problem. So we might want to back up and take a much broader look at this and join forces across a much broader community than just ICANN or just the DNS community.
- Rudolf Mayer from SIDN, the registry for .NL. I have a question about the CERT idea. One of your slides showed something like an inventory of existing organizations being active in some parts of the field. Before ICANN drew up this plan, did you actively go into a dialogue with these organizations and what they thought of this plan and if they would support it?

- I think it would have been much better if you had come up with a joint proposal supported, actively supported, by those organizations. Is there are particular reason why you didn't? You can't go back to that phase but it might really help you if in this present phase, if you could actively get those organizations to voice their support and to make clear that they are going to contribute to the idea. I think that would really help in getting the support for this plan.
- Mathieu Weill, from AFNIC, the .FR registry. I share Lesley's suggestion that maybe the current situation, it's strengths and weaknesses should be further investigated before launching a $4 million dollar project on the table.

I am also echoing Rudolf's comment because AFNIC happens to have a member who is in the OARC Board. You've mentioned OARC. And my understanding of the reactions from the OARC community to this proposal was that – antagonism could be a word – at least, support would not probably be the word I would use. And so I urge you to get the actual written comments, I'm sure it will come, before the end of March. But I think it's important that you take these into account in the course of the project.

My question then to you would be that my feeling from the gap analysis that you've been doing is that you have identified holes where you would like to fit in. And one of these seems to be the ability to coordinate all DNS operators. That relies on the ability to get in touch efficiently and reliability with these operators. And my feeling is that a number of people have already tried to do that. And they failed. What makes you think that you would have the ability to succeed where others have failed in this field?

Can you comment on any feedback from the various existing organizations that currently support security efforts from the list into 2.8.3 and the paper?

- Oscar Robles from NIC Mexico, the ccTLD for Mexico, .MX. My initial reaction to this idea was that it seems to be a good idea because there is this gap of DNS coordination requirements globally. But when I see the budget, something starts to change in my mind. Even if you give me $100 million budget, I could come up with a better idea than this one, maybe Page because that's a lot of money. So rather than going through details of how is this $4.2 million is going to be spent, I think that what I would ask you is to come up with a detailed set of goals and measurable objectives and concrete and clear, that could give us an idea of what is what this group is proposed to actually comply. Because at this moment, it seems to be too wide and I don't know, maybe in three years it won't be $4.2 million, so it would be $20 millions, and it's a

		never ending story of organizations with huge budgets and missions with no clear and concrete objectives. - Just a short commentary about the expectations concerning the funding model because I think that this is an important aspect and from the document that was produced by ICANN, apparently the $4.2 million, ICANN says that it will provide the funds to start up the DNS-CERT and then hopefully this should become a self-organizing and self-funding body. But of course, the community is starting to understand or is interrogating about how to reach an independence and how the funding model will function. Because for what regards to the ccTLDs, of course the security is one aspect that is part of the service that they offer. But then if we invent this supra-national coordination body, this will have to find ways to sustain and to find a sustainable model and one option is solidarity by all the agencies that need some overall coordination but such kind of funding models rarely function in a satisfactory way. So an elaboration about that is quite important.
ICANN Nairobi Meeting, ccNSO Tech Day	**8/3/2010**	- Dave Dagon, Georgia Tech I do note on the ICANN's public comment website there is a proposal for a DNS CERT. I think there are many different types of mechanisms that could be used to accomplish large scale DNS monitoring. Since ICANN is currently considering the wisdom of a DNS CERT creation I think that is a very useful vehicle for doing just that. I believe the comment period is still open and won't close and off the top of my head I believe it's March 19th or so. I would urge people who are listening to this presentation to give a serious look at the proposal that Yuri Ito has put forward and to comment appropriately on it. I, for myself, I'm going to be endorsing it and I think it's a great idea. I think our work in the Mariposa case is an example of how creative use of DNS monitoring can be used to help clean up infections on the internet. I am a researcher at a university and ideally this would be an activity that becomes the daily chore of people working at a CERT. I would urge people to consider that proposal closely. I think it deserves a close read. - , Nominet There are a lot of Registries out there that actually are DNS CERTS because they operate the national CERT itself. What I would like to see in this DNS CERT effort, I mean I actually like the effort behind a DNS CERT. I think there needs to be a lot more cooperation between CCTLD's and GTLD's, Registrars and their constituencies among mitigation of threats and mitigation of

		incidence. The way it takes form with one organization doing this, I think you can use a somewhat smaller budget and go to existing organizations like the national CERTS and like, for instance, groups like DNS ORK and RASG and the likes and help them educate. Basically more like a starfish model than a spider model. My last point is next to that there is already a lot of effort going on. We have at least I am part of several mailing lists that handles threat and incidences. Some of them which are unknown to the public and the reason for that is the secret handshake stuff but some of them are known like the NSD mailing list that basically helps organizations like Nominate to take down domain names. Also for instance within DNS ORK there is a disclaimer here, I'm a Director of DNS ORK so I'm not here to start promoting DNS ORK but the organization exists and we do have meetings, we do have mailing lists, we do have threat mitigation and so like I said, I do like a major push forward for organizations like Nominate to join their efforts because DNS gets more and more abused on the internet. I'm not 100% sure about the module that is projected currently.
ICANN Nairobi meeting GAC update security issues	9/3/2010	- Sri Lanka Rep; First and foremost I would like to thank the ICANN team for the excellent presentation. From the Sri Lankan point of view we warmly welcome the initiative that will perhaps lead to the establishment of a DNS CERT. We hope that in the long term there will be closer collaboration between national CERTS, I know Sri Lanka has one, India has one and some of the Sri Lankan regional countries in Southeast Asia we have one. And some of our national CERTS have already been admitted into the FIRST as full members. In that context we hope there will be closer collaboration with the national CERTS ongoing work that you are planning to have. My question would be whether you plan to have collaborative links with national CERTS and your plan for DNS CERT in the long term. - European Commission Rep; First of all, I want to say how much we welcome this initiative. It is the first time we have real global vision there. But at the same time it is highly ambitious when you talk about business cases and you talk about funding, you are really a full plate with the program you have. Because it's not a technical issue, it's very much an issue of trust and working together and working in an area where we have a number of countries and organizations.

I think that is something I really appreciate and I wonder how you are thinking in this system because basically you are operating in a peer system but you have a hierarchal root. Are you going to try to deal with that issue?

The second issue I wanted to point out and here we're in the GAC you mentioned some kind of coordination collaboration, information exchange with countries that have their own CIIP protection programs, which of course are not only restricted to DNS. So how do you see these relationships?

- Italy Rep;

The more visible and the one more elaborative up to now is the one concerning the DNS CERT. There have been already some confrontation with the public here yesterday and so there is a curiosity from those present about how to integrate the effort with the present CERTS also managed by the Registry. For example in Europe there is a coordination about this kind of problems.

So then the other point that is to be examined is the future how this will be, the future of funding more. How then this DNS CERT will be able to be able to be funded after ICANN provided the initial start up fees? So this is quite relevant and I think the GAC should welcome this move and then continue participating in the debate.

- Netherlands Rep;

I was wondering if because we had a pre-consultation on this with the stakeholders back home, we have a CERT that is trying to modify into a net CERT, one question I think is important and I think Stefano mentioned it in how much effort you set into having expert institute and people just in one place versus the effort you put into string and knowledge exchange and networks between the already SERTS who are there. I think the second point is the most important asset of the CERT, the way they quickly exchange information and they have knowledge about threats and how to overcome them.

- Maria

I also have some comments that are actually very much in line with my other colleagues. It is actually about the added value and creating this ICANN global CERT because of the activities and contacts and trust on the national level. I would like to ask you instead why don't you focus more on capacity building or activities in parts of the world that actually might need more knowledge instead of doing things that is already going on in the national CERTS?

		I also want to know if you've had a discussion with the ccNSO and the CERTS at the national level and in that case I want to know their comments. - UK Rep DNS CERT that is going to be I suppose at the sharp end of ICANN's security efforts. So it is important that that's got right and we look forward to more information about the scope and scale of the DNS CERT. - US Rep I think at this point we just want to flag that similar to others who have raised concerns about how it would work with the national CERTS, potentially duplicity of work and others we do have those concerns and really want to be informed. The GAC should want to be informed of the views of the other stakeholders in ICANN whether it's the Registrars, Registries, the ccNSO, and really hope that going forward the GAC discussion is informed by that view as well. - Norway Rep If you sort of contact our national SERTS it would be nice to get information to the GAC for their country. So it would be nice to know if ICANN is contacting the national entities in dealing with this. - Steve Crocker, SSAC chair Greg tries to consult with us, we try to provide some advice and I think all of that is appropriate. So I appreciate the pointing to us and asking what our role might be in it. But I can tell you absolutely we're not going to stand up a CERT. Among the many competitors subtract us from that list.
ICANN Nairobi Meeting, GAC-Board meeting	**9/3/2010**	- Rod Beckstrom, ICANN CEO We're going to be asking you for your advice on domain name security and on the DNS CERT and what can be done and particularly to learn the lessons from you as well. What has been accomplished in your countries? I have experience with CERTs in several countries but we need to learn more. So that will be coming and I just want to express my concern to this group because I don't want to wait until Brussels.
ICANN Nairobi Meeting, Public Forum	11/3/2010	- Rod Beckstrom, ICANN CEO Since I took office eight months ago, I have met with many registry operators and registrar operators around the world. I have even participated in dedicated discussions, informal discussions with those parties, and the information I just received from one of the DNS providers

that have shared information with you is the first time I have heard of a decrease in attacks.

I have been told by many, many parties of increasing attacks and even outages in registrars and registries. I have to take that at what I hear it at. Those parties don't generally wish to disclose publicly those transactions, and I think the industry can do more to be transparent about that, but I have heard growing concerns from the largest parties, from some of the smallest registry operators around the world. I have heard as recently as this week that they have only begun to look at cybersecurity and the security of their systems and the integrity of their systems from attack and from data manipulation and usage for different attacks.

So many concerns have been brought to me by major CEOs of registry, registrars, and different operators around the world.

I would like to propose -- and I'm very happy to hear that the SSAC is going to look at this.

I would like to mention a couple of dilemmas we have. And actually, let me give you some other background. Before I went to the GAC meeting yesterday, I was told that there was a set of governments that were going to try to block ICANN moving forward with the DNS cert. Okay?

I have experience working with governments, and discussions on authorities. And I have seen those discussions and debates stall and thwart critical cybersecurity efforts. And I didn't -- and in the ICANN context or even in that meeting, several countries came up to me afterwards, representatives and said, "We very much do want to do a DNS cert and be engaged in it with you. Please move ahead, please involve us, and thank you for what you said," including another one that approached me last night and offered the assistance of introducing another 20 countries into such a plausible effort.

At the same time I am not presupposing that a DNS cert would be inside ICANN as opposed to on the outside. I do believe, and let me also share this. Some governments might not want ICANN to do anything in DNS cert or in cybersecurity efforts. Much of the community wants ICANN's role to be extremely limited. One of the other dilemmas we face, and I like Steve's proposal of a group to look at DNS availability, because it's more than just about security and stability. I want to quickly read from the Affirmation of Commitments paragraph 3. This document affirms key commitments by the Department of Commerce and ICANN, including commitments to preserve the security, stability, and resiliency of the DNS, preserve it. Secondly, paragraph subpoint D, facilitate international participation in DNS technical coordination.

	As a CEO, I feel that ICANN is probably living up to the facilitation of DNS technical coordination at some level. As a CEO, I am concerned we are not living up to our contractual commitment of preserve the security of, which is very strong language. And my concern was that as an organization, after the community supported, albeit be a lot of debate, the concept of the DNS cert somewhere, the notion that governments might seek to block ICANN from moving forward or the community from working on this through an ICANN platform, was very distressing to me. I would also -- so I think the community needs to engage in some process, perhaps in what Steve said as a working group, to discuss what does the Affirmation of Commitments specifically mean with respect to the security and stability of the Domain Name System, and also what does it mean with respect to the facilitation of the technical coordination. Because there's other bodies that are involved in that. So as a CEO, I can say we need clarification. And I think it goes beyond just the SSAC's role, which is critical. But we need to define those expectations because otherwise we have a contract where we are committing to do something, but we have a bottom-up policy and community process, parts of which say you shouldn't do that at all. So how do we resolve those two? I don't know the answer to that but I think we need to have a process, we need to discuss it, and the other comment I am going to make is one of the concerns I have as a CEO is that as an industry or as ICANN, depending upon how you look at it, I have not yet been told of a comprehensive model of the Domain Name System. A model that can be tested and simulated for different attacks. Not that any model is ever perfect. But without a model, that can assess the entire DNS system and how it's affected by attacks and what its vulnerabilities are, how can we know of its ultimate ability to withstand new attacks? And so I would also like us to investigate as a community and had good discussions with SSAC on that, and that may be the place, or maybe ICANN is the place, but here is the next dilemma we need to discuss: ICANN's fundamental business model is being supported by domain name registrars and registries. Typically in advanced countries. Because many registries around the world, perhaps most, do not contribute financially to ICANN. At the same time, those registries are asking us and me for security assistance in what they are

doing. Capacity building, training hot lines, et cetera. So how do we resolve that issue? There needs to be a discussion or a debate in the community. We are very open to it but until we have a comprehensive model, until I hear that all registries and registrars are secure, I am concerned. And I have heard even this week of the concerns that others have. So at the same time, I defer, for ultimate technical advice and judgment, to the SSAC and to other groups in the community. And I look forward to a discussion. I do hope we can create one or more working groups on this topic, and I look forward to participating and moving the ball forward.

CHRIS DISSPAIN, ccNSO Chair
I'd like to read to you a letter that the Country Code Names Supporting Organization has written today to Rod.
Dear Rod, I'm writing to convey the ccNSO council and members' concerns regarding your comments made to the joint meeting of the ICANN board and the Governmental Advisory Committee on Tuesday, the 9th of March.
Your inflammatory comments to governmental representatives regarding, in your view, the precarious state of the security of the DNS, have the potential to undermine the effective and productive relationships established under ICANN's multistakeholder model. Your alarming statement to the GAC infers that current security efforts are failing.
This could cause great concern among governments regarding how elements of critical Internet resources are operated and managed in their countries. In particular, your remarks have the potential to damage the effective relationships that many ccTLD operators have developed with their national administrators. In the circumstances, it is difficult to comprehend why, despite a brief discussion on your DNS CERT proposal, the full details of your security-related concerns were not raised during your meeting with the ccNSO earlier this week.
The ccNSO council is also concerned about your intention to write to governments about their DNS, asking whether or not such DNS is able to withstand the perceived new levels of attacks. This has the potential of compromising the manner in which ccTLD managers in those countries operate. It also has the potential to undermine ccTLD managers' ongoing efforts to make their DNS more robust and resilient against attacks. We urge that if such measure is to be taken, it be first dealt with through the ccNSO.
Further, your comments discount the huge efforts of many of the ICANN community to ensure

the ongoing security and stability of the DNS including the Root Server System Advisory Committee, Security and Stability Advisory Committee, and the ccNSO. It diminishes the efforts of those that collaborate with ICANN, such as the IETF and the CERT community. In addition, a number of the top 20 registries in the ccNSO state that you have not spoken to them on this topic.

At a broader level, your statement has the potential to strengthen the positions of those that criticize ICANN and who would prefer to see changes to how Internet numbering and naming resources are managed. The ccNSO council would like to reiterate that security remains a core strategic and operational priority for the ccTLD community, and we remain strongly committed to working with ICANN, other Internet stakeholders, and governments, to ensure the stable and secure operation of the DNS.

Our concerns lie not with your focus on security issues, but with your precipitative unilateral analysis of such an issue and the public and inflammatory manner by which your views have been communicated. We agree that as the CEO of ICANN, it is your responsibility to address these issues. But it is equally your responsibility to do so through ICANN's bottom-up, consensus-based multistakeholder model. It is also the responsibility of those in positions of influence within ICANN to show due care when making statements on complex, cross-cutting issues to ensure effective analysis and stakeholder engagement without unnecessary confusion or concern. Nearly finished.

Regarding the issue at hand, we suggest that ICANN work with all relevant internal and external stakeholders to develop a clear analysis of the current mechanisms in place to ensure the ongoing security of the DNS. As a first step, we urge you to share with us and other stakeholders the underlying facts or studies that originally led you to make your statements. Only after analyzing the entire security landscape, with the buy-in of all stakeholders, can ICANN develop a clear strategy and operating plan for improvement. The ccNSO stands ready to contribute to this process.

- Steve Delbianco, NetChoice.
Comments are my own.

I think the CEO's role is to raise the alarm when he or she sees the need to do so. I think that's appropriate. And as to the CEO's direct style of communication, that's no surprise. It's exactly what the corporate world is all about. So I do think you're right to sound the alarm, but maybe not so right to rush to the conclusion that we need to build a DNS CERT to solve it. Now, I know you clarified earlier that it might be inside, it might be outside. And that's an important distinction. Because to use the chair's analogy of some three hours ago, with a -- respect to burglars, remember burglar proofing the house, the chair said just because I can't make a perfectly burglar-proof house, that's not going to stop me from building the house. You're going to go ahead and do it. That metaphor works here, if we know and sounded the alarm that burglars are present and threatening the house, that doesn't mean we create our own police force, complete with cars, 24/7, 365, two shifts, pension plans, badges, and uniforms. Instead, we would find a way to tie our house security system into the local police department, we might even preprogram our telephone to dial 911 in case of an emergency. So there's a lot of things we can do to take this alarm and turn it to action that works with existing CERT as opposed to creating our own.

- Bob Hutchinson, Dynamic Ventures
I would like to reiterate that existing CERT channels support millions of computer users every day, and the advisories that come through them get translated into numerous languages all around the world. These channels are effective and long-running channels in our industry, and we should attempt to use them as much as possible for this kind of information.

It's not clear at all to me why you need a separate CERT. But I -- I'm glad that the proposal was made in order to get a dialogue about how this section of networking can clarify its own support picture for the user community. For example, I checked your Web page, and there is no linkage off of the ICANN Web page for people to find which CERTs are being supported or which information they need to get. So that's one improvement that could be made right away.

- Kurt Erik Lindqvist, Autonomica, I root server.
We also provide slave services to around 60 TLDs. And I would like to echo what Steve conveyed. We don't see an increase in effects today. On the question of a DNS CERT, I must -- I'm not

		convinced that looking at the DNS system in isolation adds any value. The stability and robustness of security -- we take this pretty serious – is dependent on many factors. And there are a lot of other issues that affect this ability. You break out the DNS, you will lose the view of these factors. And that's why some of the CERTs are very effective, because they can see cross functional, see how a lot of these issues are linked. The other reason CERTs are successful is because they have a very close tie to the community, direct connections. I'm not convinced that a central DNS CERT around the globe will have that linkage and even be effective. I think that what ICANN could do is do capacity-building and help work to get an recurrent CERT, existing CERT inside the kind of frameworks. Because adding more frameworks, adding more structure will just be taking focus away from these issues. I think that's where ICANN can do different. Also help in establishing new CERTs.
ICANN Nairobi Meeting, DNS Abuse Forum	**11/3/2010**	- Nii Quanor, Now the kinds of things I think would help would be that we haven't quite focused you know the DNS side of issues within the CERTs themselves. At the same time the CERTs do perform similar functions as one would want for DNS, there's no real known community practices that are documented that we could share across in the region. Now we need to actually build a community around DNS operators. There's an attempt going on with AFTLD for the CCs but in general we need to let people feel that there is a committee of people who are addressing DNS related issues. And have them then evolve those practices that may be of interest. Now that's a group, may participate as a point of contact within the existing CERTs because I don't think in Africa where we are just beginning to start building CERTs to have an CERTs. You know it would be too hard for us, we may not even have the resources, so it would be much better to organize a community and channel it through their listing CERTs. Now operators should include a DNS issues in their acceptable use policies, so that people will begin to get informed from routine - in a routine way. Now with respect to certain Africa you can see that we are very much in the infancy. According to this site they are forenamed includes Kenya which is very good South Africa acting more issues and Tunisia. But I'm aware also of very strong activity in Egypt, I'm also aware of activity that has

		started in Ghana and (unintelligible) in many other countries are now beginning to you know address this issue. What will be useful is clear you might say blueprint, guidelines, approaches, that can be readily you know you might say adopted for the particular locations that they are working in. So that would be something that would be useful. Now I also think that it's better to act the DNS CERT as a function of this new CERT because we don't have critical mass yet. - Eric Brunner-Williams Why is a centralized CERT a better choice than funding hires and training in the periphery? - McTim, I just wanted to answer Eric I think from an African perspective. And what Yurie said is pretty spot on. I mean we like to have the intelligence at the edges of the network so they can react and that's a good idea. But for us in Africa we don't have a lot of cash, so having independent CERT in every economy is just not going to work. So we've got to work together with the ccTLD and the country over here in Kenya for example (kicked in that) or the KENIC or sorry the CCK. There are people in each economy that are active and interested and knowledgeable about these issues and we need to leverage their presence and their interest instead of building a separate CERT in each economy from scratch. We'll never be able to afford that.
ICANN Nairobi Meeting, GAC Communique	10/3/2010	The GAC welcomes information about the "Global DNS-CERT Business Case" and the initiative to launch a global strategy concerning the medium-long term planning about security of the DNS presented in the recently published documents "Proposed Initiatives for Improved DNS Security and Resiliency". Concerning the DNS CERT, the GAC recommends that ICANN informs the relevant GAC Representatives about its consultations with national and regional CERTs and is concerned about possible duplication of efforts.
Perspectives on a DNS-CERT by Paul Vixie	**18/3/2010**	**Perspectives on a DNS-CERT** This week at the ICANN meeting in Nairobi, a plan was announced by ICANN staff to create a

"CERT" for DNS. That's a Community Emergency Response Team (CERT) for the global Domain Name System (DNS). There are all kinds of CERTs in the world today, both inside and outside the Internet industry. There isn't one for DNS, and that's basically my fault, and so I have been following the developments in Nairobi this week very closely.

As the original founder of DNS-OARC (that's the Operations, Analysis, and Research Center for DNS, on the web at WWW.DNS-OARC.NET), I've fielded a lot of questions from folks asking me what I think about all this. (See related CircleID interview). The original DNS-OARC plan (written in 2002 or so) called for a 24x7 monitoring and response and coordination function very similar to what's now being proposed by ICANN. Everybody I talked to in 2002 understood the need for this, based on the excellent track record of US-CERT and JP-CERT and even the IT-ISAC. We knew it had to be done by the DNS industry itself, rather than added to the remit of some existing government-supported CERT or ISAC.

Somewhere along the way we got distracted. Or to more accurately place the blame, I got distracted. DNS-OARC was a huge undertaking, and one that I significantly underestimated. ISC started DNS-OARC using NSF research money, and I think NSF was happy with our results -- but producing those results used up a lot of ISC's management bandwidth. DNS-OARC has received unprecedented participation and support from members of the DNS industry, who had never done anything quite like this -- but the cycle time for bringing in new members was six to 18 months rather than the six to 18 weeks I planned on. Much has been achieved, but building the data and resources needed to develop OARC's necessary "critical mass" was something that ISC had to rely on partners and members for, and those folks have busy lives and long to-do lists even without this kind of stuff.

Eight years on, ISC has successfully spun DNS-OARC out as a separate non-profit corporation with its own board of directors. DNS-OARC has some fifty (50) members, comprising an unprecedented community of the key technical people from major DNS TLD registries, root operators, vendors and service providers. It has created a set of tools, experience and infrastructure vital for monitoring and analyzing the health of the DNS, and has accumulated an unparalleled set of DNS data captured from the live Internet.

But all this took years longer than I expected, and may have been a more dramatic time investment than DNS-OARC's elected trustees were expecting.

So the reason there is nothing like a "DNS CERT" in the world today is that I, as the founder of DNS-OARC, said that DNS-OARC would handle it, and then I didn't follow through. I plead ignorance and ambition -- we got a lot of other great stuff done, including the existence and independence of DNS-OARC itself, so I'm not exactly weeping with guilt. But, when Rod Beckstrom (President of ICANN) got up at the microphone in Nairobi and said, the world needs something like this, and if nobody else is going to build it, he would, I thought, he's absolutely right, it's still 2002 in here, and it's time we -- the DNS industry -- got this done. We need a 24x7 monitoring and response and coordination function, with full time analysts looking at real time DNS events and participating in a global mesh of DNS NOCs.

Beckstrom's vision that some $4.5M is needed to get DNS-CERT properly off the ground is to be commended, and is one familiar to us at DNS-OARC, where our reach has regularly exceeded our grasp. But we've also learned some lessons over the years, not least that the DNS community guards its autonomy fiercely, and will react adversely to anything that smacks to them of unilaterally imposed central control. Something like a DNS-CERT can only be done at the grass roots level, which is both a constraint and a boon. This explains some of what we've been hearing in the hallways at how, despite its merits, there is some disquiet about the way the DNS-

CERT proposal was presented. It is exactly why we went for an autonomous, neutral, membership governance model for DNS-OARC. We have to work cooperatively to ensure that DNS remains 100% available to serve as the Internet's map.

I call upon the world's governments, and upon the GTLD and CCTLD operators, and upon ICANN itself as well as other Internet governance organizations including CENTR, to support DNS-OARC Inc. in finishing what I started; and I call upon DNS-OARC Inc.'s trustees and members to use ICANN's excellent "gap analysis" for the "DNS-CERT" as the starting point to make this happen.

So, the next phone call all of those folks get may be from me, making this appeal personally. Let's make 2010 the year we (all) finally get this done.