PROPOSED STRATEGIC INITIATIVES FOR IMPROVED DNS SECURITY, STABILITY & RESILIENCY (SSR)

and

GLOBAL DNS-CERT BUSINESS CASE PAPERS

Summary and Analysis of Comments

ICANN originally conducted public comment periods on the *Proposed Strategic Initiatives for Improved DNS Security, Stability & Resiliency (SSR)* and *Global DNS-CERT Business Case* papers from 12 February to 29 March 2010. Based on requests from the community, both comment periods were extended by 15 days to 14 April 2010. In total, 13 comments were received in the forum for the Strategic Initiatives paper, and 25 comments were received in the forum on DNS-CERT, with some overlap from stakeholders commenting on both. This summary and analysis is a subset of the larger community consultations that were conducted by ICANN staff and occurred on these topics during the ICANN meeting in Nairobi, Kenya on 7–12 March 2010. The broader record on consultations on the DNS-CERT has been recorded in a separate document being posted with this one.

Summary of Comments

ICANN received input from a broad spectrum of stakeholders—governments, national computer emergency response teams (CERTs), ICANN advisory committees and supporting organizations, top-level domain registry operators, associations, and Internet organizations, businesses, Internet Service Providers and individuals from the DNS community. A detailed analysis of these comments is provided below.

Main Themes

The general input received strongly acknowledged the utility of ICANN raising the profile of strategic issues of DNS security, stability and resiliency in the context of a system-wide DNS risk assessment, gap analysis and requirements for a collaborative DNS incident response capability. However, significant concerns were raised focused on the DNS-CERT business case. Overall, these concerns addressed four main themes:

1. The requirements for a DNS-CERT must be analyzed in light of a deeper understanding of the threats and risks to the DNS, and such an analysis should precede specific proposals for a DNS-CERT.
2. The proposal was insufficient in detail and in analyzing gaps regarding current activities and capabilities related to DNS security and resiliency. Therefore, the proposal is potentially overreaching in the need for and resources required to support a DNS-CERT. Many commented on the need to examine the efforts of DNS-OARC as well as the global Computer Incident Response and Security Team (CSIRT) community and the utility of strengthening such efforts as an alternative or supplementary mechanism for addressing DNS security and issues and with a lower resource requirement. Two specific comments are worth noting:

a. That efforts to educate existing DNS operators and the CSIRT community might be a more effective application of resources.
b. That in certain regions, such as Africa, little exists in terms of CSIRT capabilities or linkage to existing DNS security and resiliency mechanisms.

3. The mission of establishing a DNS-CERT was outside of ICANN's limited role of technical coordination and, if needed, a DNS collaborative incident response community must include a broad range of stakeholders beyond those naturally part of the ICANN community. Many suggested the need to establish a working group to involve the ICANN supporting organizations and advisory committees as well as additional parties such as the global CSIRT community as the mechanism for analyzing the requirements, resources and organizational approaches to the DNS-CERT concept.

The comment forum on the Strategic Initiatives paper can be viewed at http://www.icann.org/en/public-comment/#strat-ini-ssr. The comment forum on the Global DNS-CERT Business Case can be found at http://www.icann.org/en/public-comment/#dns-cert.

Detailed Analysis

ICANN Advisory Committees and Supporting Organizations

The Chairs of ICANN's At-Large Advisory Committee (ALAC), Country Code Names Supporting Organization (ccNSO) and Generic Names Supporting Organization (GNSO) provided a joint comment on the DNS-CERT concept. The ccNSO and ALAC also provided individual comments.

ALAC-ccNSO-GSNO Chairs

The Chairs noted concern that ICANN's proposal lacked detail regarding the perceived problems the DNS-CERT would be established to address, the operational structure of the new entity, ICANN's role, and the budget, staffing and funding model for the initiative. Given the significance of the initiative, the Chairs requested an extension of the comment period (the comment period was extended to 14 April 2010) and establishment of a joint working group by the ICANN meeting in Brussels, including input from ICANN's SSAC, RSSAC, governments, CERTs and TLD managers. The Chairs asked that ICANN solicit the input of the working group on:

- The broad concept of a DNS-CERT;
- The current work being undertaken to mitigate DNS-related threats;
- The actual level, frequency and severity of these threats;
- The gaps in the current security response to DNS issues;
- Whether or not a DNS-CERT is a proposal they support; and
- If so, the logistics of the proposal.

ALAC

ALAC provided separate input on both the Strategic Initiatives paper and DNS-CERT Business Case, echoing the separate comments from the ccNSO. The ALAC statement noted concern about the shifting definition of "community" from what is "traditionally used in ICANN to mean our stakeholders, actors, interested parties (reflected by the makeup of the constituencies and

sub units if our various ACs & SOs) and often extended to include public input from Internet users and domain name registrants, to one that is limited to a community of security and threat response interested parties." ALAC noted that it "looked forward to wider and more globally inclusive engagement of key stakeholders and the ICANN community (including SSAC and RSSAC) of the gap and or risks as well as needs analysis that will allow the desired outcomes to be best achieved.

ccNSO

The ccNSO called for more engagement with existing security stakeholders including the CERT/CC and CERT Network, RIRs, root operators, registrars and TLD registries in developing the DNS-CERT concept. The ccNSO noted that "lack of dialogue leads to the potential for duplication of efforts and confusion, rather than clarification, of specific roles and responsibilities." They encouraged ICANN to provide a clear understand of who asked for this initiative and precisely what issues it is supposed to mitigate.

The ccNSO stated: "ICANN must complete a detailed survey of the range, severity and frequency of current and potential threats to the security and stability of the DNS and an analysis of whether these threats can be mitigated by existing structures and stakeholders." The ccNSO also noted that it was unclear whether ICANN intended to provide the funding for the DNS-CERT from its own internal budget, should it be unable to obtain the support of third parties. "The size of the exercise and financial commitment also gives rise to questions regarding whether establishing a new, dedicated DNS-CERT is the best solution to perceived capacity gaps, or whether this amount of funding could be better spent supporting current activities."

The ccNSO cautioned ICANN against moving too quickly with the DNS-CERT concept. "As stated in Nairobi, the ccNSO shares and supports ICANN's focus on security-related issues, though recommends a measured, strategic, inclusive response. ICANN must follow due process in consulting stakeholders, gathering evidence and developing a response strategy, rather than proposing a solution to a problem that is not clearly identified."

Government and National CERT Inputs

ICANN received comments from the governments of France, the United Kingdom, and the United States, and comments from the national CERTs of Malaysia and Sri Lanka.

France

The government of France thanked ICANN for initiating a public debate on the topic of security and resilience of the DNS. France welcomed the joint initiative of the ALAC, GNSO and ccNSO to request the creation of a cross-community working group on the topics raised in the Strategic Initiatives paper, and recommended that a cross-community workshop be organized during the upcoming ICANN meeting in Brussels, Belgium. "France believes that the discussion should not be limited to the ICANN community [i.e., should include all actors involved in the DNS security chain such as ISPs, technical organizations, etc.] and should take advantage of the opportunities for dialogue offered inter alia by the Internet Governance Forum."

France agreed with other comments that the DNS-CERT concept had been proposed by ICANN before sufficient opportunities for discussion in the community had occurred. "A preliminary

consensus has not been built yet on the definition of the problem itself, the various dimensions and the actors involved. DNS security improvement is of interest for all stakeholders and should be discussed in a cross-community manner." As with others, France stressed the need to avoid confusion between global and local security issues regarding the DNS infrastructure, distinguish clearly between preparedness and reaction measures, and identify gaps between what already exists and what is needed to address DNS security and stability.

United Kingdom

The United Kingdom appreciated the focus in the Affirmation of Commitments that ICANN would seek to "preserve the security, stability and resiliency of the DNS" and "the two documents posted for public comment are an important step forward in meeting the goal set out in the [Affirmation]." The United Kingdom stated that the Strategic Initiatives provide "a good starting point for discussions about the way in which ICANN might focus its effort. We agree that the good work that is going on is largely ad hoc in nature and we can see a leadership role for ICANN in attempting to put that on a more sound footing."

The UK suggested that the key areas going forward must:

- Better understand emerging threats,
- Understand how those threats translate into risk for DNS operators and users,
- Improve the ability for such information to be shared, and
- Create a culture of emergency preparedness in the DNS community and promote tests of contingency plans.

According to the UK, ICANN needs to clearly "position its own efforts so as to gain maximum support from its closest stakeholders—the DNS community—as well as to connect to wider efforts to promote cyber security in the IGF and elsewhere."

United States

The US Government thanked ICANN for initiating a public discussion on the two proposals related to DNS security and stability. In the letter, Lawrence Stricking, Assistant Secretary for Communications and Information, US Department of Commerce, stated that the National Telecommunications and Information Administration (NTIA) "believes the concept of a DNS CERT has merit and deserves serious and thoughtful consideration," but urged ICANN to develop a more complete risk assessment and "to work with all relevant stakeholders in developing a thorough gap analysis to permit the community to effectively evaluate [the] proposed effort and subsequently to determine the best path forward."

The US Government noted that the Strategic Initiatives for system-wide DNS Risk Analysis, Contingency Planning and Exercises, and for the DNS-CERT concept did not provide sufficient data in which to form an informed opinion on the proposals. The letter suggests that ICANN:

- Explain how the proposed efforts would take into consideration and avoid duplication of existing activities from entities such as DNS-OARC and national CERTs.

- Develop a more complete record on threats and vulnerabilities of the DNS that a DNS-CERT would help mitigate.

The US Government also noted "any activity ICANN undertakes in this area should be consistent with its role as a technical coordinator of the DNS." NTIA wanted to make clear that nothing in the Affirmation of Commitments mandates either of the two proposed Security initiatives or implies any particular role for ICANN.

Malaysia CERT

Malaysia CERT stated: "our organization feel[s] that the DNS-CERT initiative has merit and could improve response time particularly in dealing with security incidents that has DNS implications. We therefore support the establishment of the DNS-CERT by ICANN and look forward to having a close relationship with the organization in the future."

Sri Lanka CERT

Sri Lanka CERT noted its support for a DNS-CERT concept. "To secure the cyber space from various DNS related security issues it is very important to setup such an organization called DNS-CERT. Then there is a single point of contact for each and every CERT to liaise with to handle such issues. . . . As Sri Lanka CERT we strongly believe that DNS-CERT will be a very important body to secure the cyber space from malicious activities related to the DNS."

Stakeholder Comments – Registry Operators, TLD Associations and Internet Organizations

Inputs were received from AFNIC, APTLD (Asia Pacific Top Level Domain Association), CENTR (the Council of European National Top Level Domain Registries), the gTLD Registries Stakeholder Group, DNS-OARC, the Internet Society, JPRS, Nominet, InternetNZ, and Neustar.

AFNIC

AFNIC, the operator of the dot-fr and dot-re ccTLDs, noted that improving the security of the DNS infrastructure is a major goal for organizations like it and any initiative in this area is welcome. "We firmly believe that the success of such initiatives relies on their ability to grasp the decentralised nature of the management of the Internet. For this initiative to be a success, its perimeter has to be carefully considered, in order to build a critical mass of involved stakeholders so that global progress can be made." It remains unclear to AFNIC which stakeholders have endorsed the DNS-CERT initiative. AFNIC urged ICANN to provide more detail on the scope of the project. As the project raises concerns over duplication of efforts, and funding is not clear, AFNIC stated it was highly premature for a DNS-CERT concept at this time. AFNIC noted that the DNS-CERT paper cited the collaborative work against Conficker, but that no comprehensive report has been published on the anti-Conficker effort, analyzing and extracting lessons.

AFNIC remarked that careful attention should be paid to the legal issues surrounding exchange of data and the sharing of sensitive data.

> *In summary AFNIC is willing to extend its existing contribution to security and stability of the Internet, even beyond its role of TLD manager. Building a network of*

> *trusted parties both at national and international levels is key to this objective. Such network should reach to all involved stakeholders, and allows [the sharing of] technical information and expertise in confidence. Existing initiatives such as DNS-OARC or FIRST could in this respect be reinforced and would probably welcome ICANN's support in this regard. ICANN could in particular be extremely helpful in encouraging registries and registrars to join these initiatives.*

Finally, AFNIC noted its support for initiatives to consolidate risks and weaknesses to the DNS.

APTLD

APTLD stated that it welcomed the opportunity for the community to consider the DNS Strategic Initiatives paper and DNS-CERT concept, but that they would appreciate a more detailed study and fully developed business case, prior to any implementation of a DNS-CERT. APTLD noted particular concern with the organizational framework, the scope of the work and funding for the initiative.

> *APTLD would like to reiterate that we support ICANN participating in enhancing the security and stability of the Internet, and we appreciate ICANN's proposal. However, we believe that ICANN must look into how the existing network could be enhanced, before seeking to establish another organisation that requires significant resources, while there are significant doubts in its potential efficiency and effectiveness.*

CENTR

CENTR noted its support for the increased focus on security in the ICANN Strategic Plan and that it shared some of the goals in the DNS-CERT business case. CENTR notes that as proposed, the DNS-CERT concept overlaps with existing entities such as CERTs, OARC and FIRST. CENTR notes that more information is needed to understand how a DNS-CERT would avoid duplication of efforts in the community. CENTR stated that ICANN should focus first on building a common assessment of risks and weaknesses. CENTR believes this should enable ICANN to clarify the exact scope of its initiative. Then would it be relevant to discuss whether new structures are necessary.

DNS-OARC

DNS-OARC, of which ICANN is a member, welcomed the additional attention that ICANN has brought to the subject of its mission, and agreed with ICANN's position that additional funding and resources for this area would be beneficial. DNS-OARC noted some concerns about potential overlap.

> *DNS-OARC encourages education and awareness in mitigation of threats and handling incidents, and welcomes ICANN's raising the profile of the need for this. We feel it is necessary that this awareness is developed inside organizations that already have a responsibility for parts of the DNS community (such as TLD registries). Subsequently, these organizations can join already established vetted communities like FIRST or DNS-OARC.*

DNS-OARC noted it would be more effective to fully recognize established activities, and dedicate a more modest budget to addressing the gap.

> *This can be through support and funding to establish, assist and enhance trust and co-operation between these existing organizations. Building education and awareness of incident handling and mitigation of threats, including development of response teams within, and further consensual co-operation between, existing ICANN constituency organizations will lead to a decentralized global cooperative. We believe that this will be far more effective, with greater ultimate reach and legitimacy than a single central DNS-CERT.*

InternetNZ

InternetNZ, responsible for New Zealand's dot-nz ccTLD, noted that the DNS-CERT concept was not new, but part of DNS-OARC's long-term objectives when it was formed in 2004. InternetNZ congratulated ICANN on bringing up the strategic need to secure the DNS. They stated that the proposals presented by ICANN were under-developed in some areas, over-developed in some less relevant areas and that ICANN should incorporate the concerns raised into a new proposal that is balanced and comprehensive.

As with some of the other comments, InternetNZ noted concern about the scope, justification and potential overlap of a DNS-CERT. InternetNZ provided a series of positives and negatives for a DNS-CERT, including that work in this area requires trust and reputation with existing entities working to secure the DNS. "If the DNS-CERT were established within an existing incident response organisation with an existing trust model [not ICANN] then this issue could be tackled quickly."

InternetNZ indicated that a DNS-CERT did not seem to fit within ICANN's multi-stakeholder model. "Managing an organisation with such a different set of stakeholders would not be beneficial to either ICANN or the DNSCERT, but without a different set of stakeholders it would be difficult to create the trust needed." InternetNZ recommended that ICANN amend the proposal and remove excess detail that may constrain a third party from performing a DNS-CERT function, and include an option for funding the DNS-CERT as an external venture. They also asked that ICANN ask for expressions of interest from third-party organizations interested and capable of running a DNS-CERT.

ISOC

ISOC submitted a letter to the ICANN Board and included its comments in the forum on the DNS-CERT and the Strategic Initiatives papers. With regard to the proposals posted for comment, ISOC agrees that taking steps to strengthen global DNS security, stability and resiliency is important. ISOC has strong concerns about the development of the proposals and their future path in the ICANN community.

ISOC believes the proposals have been put forward prematurely—without the full backing of ICANN supporting organizations and advisory committees, or with the broader community, and including the technical community. ISOC is also concerned that the proposals may be broadening ICANN's mandate, and could potential distract ICANN's attention and resources

from its central coordinating mission. ISOC recommends that the DNS-CERT and Strategic Initiatives be brought forward with the global Internet community to ensure that all relevant bodies may have the opportunity to contribute to enhancing the security and stability of the Internet's domain name infrastructure.

JPRS

JPRS agreed with the concept of a DNS-CERT, but that ICANN should look at existing organizations for security maintenance such as DNS-OARC and national CERTs. "We think enhancing capabilities of existing organizations should be considered first, rather than creating yet another organization."

JPRS noted that the proposed $4 million USD cost proposed for initial funding of the DNS-CERT was a huge amount, and that the DNS-CERT function should be overlaid onto the existing organizational framework for efficiency. Finally, JPRS stated that not as much attention has been given to network operator groups and local DNS operators, and more outreach to these areas should occur as discussion of the DNS-CERT concept continues.

Neustar

While supporting ICANN's efforts to focus attention around areas of DNS security, Neustar noted that the proposals overreach and make assumptions not yet supported by concrete data and/or necessary community involvement and input. Neustar supports the concept of a collaborative study of threats to the domain name portion of the DNS as suggested in the Security Strategic Initiatives paper (Section 5.1.1), and would welcome the opportunity to participate in working groups as suggested in Sections 5.1.3 and 5.1.1.1. Neustar also supports the formation of a joint SO/AC working group as recommended by the Chairs of the ccNSO, GNSO and ALAC. Neustar also believes the concept of a DNS-CERT has value and is worth further consideration.

As with other commenters, Neustar noted that they believe ICANN has not yet adequately engaged or consulted with existing DNS security entities and DNS service providers to evaluate the threats or relevant resources, groups and mechanisms. They note that DNS-OARC already exists and could be an effective and less costly alternative to the formation of a new group. Neustar indicated that it would not support ICANN's involvement in a DNS-CERT in a funding or operational capacity. Neustar is concerned about the startup resource projection for a DNS-CERT and the overall increase in ICANN's budget related to SSR activities. "ICANN needs to explain to the community how it would fund such a significant incremental expense [in ICANN's operating budget], and what existing programs would be impacted by any reallocation of funds."

Nominet

Nominet generally welcomes ICANN's strategic focus on DNS security and stability and recognizes the importance of this work as highlighted in the Affirmation of Commitments. Their comments echoed those previously provided by CENTR and the ccNSO. Nominet states that ICANN's efforts in security Strategic Initiatives should be in partnership with other operators of Internet infrastructure and could be extended to those involved with communications and computer network security. Nominet suggests that more work be done to engage a broader

section of the community to assess how to avoid duplication of effort and how best to get value from cooperation. Nominet welcomed in principle the approach for system-wide DNS Risk Analysis, Contingency Planning and exercises, but that collaboration should be wider than the "DNS community." Nominet suggests that ICANN clarify how the proposed expert advisory/working group would relate to existing ICANN advisory committees (SSAC, RSSAC) or with expertise from the ICANN community. Nominet also suggests that ICANN draw on expertise from CERTs to embed DNS expertise in the existing computer and network security response capability.

Nominet recommends that ICANN focus on identifying work that could be addressed under a system-wide DNS Risk Analysis, in partnership with other organizations active in the DNS. Nominet also recommends that ICANN look to widen the membership of the join SO/AC working group that may be formed to include FIRST, key CERTs and others active in emergency response. Nominet also indicated that "effort needs to be put in to developing industry best practice guidelines and encouraging TLD operators and registrars to be involved and active in local CERTs, raising awareness of DNS issues in the CERTs and improving their own understanding of security response procedures."

RySG

The Registries Stakeholder Group (RySG) noted that ICANN's proposed role in the security Strategic Initiatives seemed unclear and over-broad, and may be outside ICANN's direct role in coordinating Internet naming and numbering resources. They suggested that further work be conducted to define the capabilities, funding and kinds of incidents to be addressed by a "CERT"-like function for the DNS community to respond to future large-scale security incidents. The RySG recommended that ICANN engage in further consultation with key operators and community members to:

1. Develop a clear articulation of the threats facing the DNS that require system-wide, concerted and structured action.
2. Identify what elements of the DNS threat review are properly within ICANN's technical coordination mission.
3. Perform a gap analysis to see if there are needs that are not already addressed by industry and governments (including an examination of existing entities and role with the identified threats).
4. Identify relevant stakeholders.
5. Once the first four elements had been conducted, then it would be appropriate to decide ICANN's role, the location and funding of any functions related to the two Strategic Initiatives.

The RySG agreed "core DNS issues are within the scope of ICANN's security and stability mission. ICANN should be concerned with threats to the DNS itself—those that could seriously impact the functioning of the DNS or Internet," including:

- Significant technical risks to core protocols or functions such as the Kaminsky bug, load issues associated with DNSSEC or expansions of the root zone.

- Reliable, resilient operations of the root server system and top-level domains.

Business Community

Comments were received from the business community including AT&T, NetChoice, PayPal, PRESENSE Technologies GmbH, and the United States Council for International Business (USCIB).

AT&T

AT&T noted its support for ICANN's increased focus on security, stability and resiliency issues, and stated that ICANN should take a forward-looking approach that threats to the DNS and the Internet generally continue to expand and evolve.

Net Choice

NetChoice acknowledged ICANN's increased focus on security through monitoring security threats, working with the community to ensure infrastructure operators take appropriate measures. NetChoice also noted that ICANN's activities in this area are highlighted in the Affirmation of Commitments, but none of this suggests that the DNS needs a centralized approach to security. NetChoice asks that ICANN examine whether there is clear need for a new information coordinator, and whether coordination would have made a difference in responding to recent attacks on the DNS. NetChoice stated that ICANN should improve its support for existing security teams, rather than design a new team of its own.

PayPal

PayPal stated that the proposed initiatives extended beyond what ICANN provided in its *2009 Plan for Enhancing Internet Security, Stability & Resiliency*, and that nothing in the Affirmation of Commitments requires ICANN to undertake these initiatives or to establish a timeline for their implementation. "We believe that some benefit can be gained by doing system-wide risk analysis and contingency planning provided that it is properly scoped to fall within ICANN's 'limited technical mission.' However, we are not convinced that the proposal, as presented, is properly scoped." PayPal also notes that the proposed DNS-CERT initiative does not track with ICANN's 2010–13 Strategic Plan. PayPal provided alternative language for the scope of a DNS-CERT initiative: "Given the proposal's reliance on the Strategic Plan, one might expect that the mission would read: Work in partnership with other organizations to ensure that DNS operators and supporting organizations have sufficient expertise and resources to enable coordinated, timely, and efficient response to threats to the security, stability and resiliency of the DNS."

PayPal indicated that the revised mission would be consistent with the Affirmation, Strategic Plan and ICANN's traditional role, and would serve to partially answer some of the thoughtful concerns submitted by others in the comment forum. It would also properly limit ICANN to a cooperative role and the DNS-CERT's role to one of responding to actual incidents and attacks. PayPal questioned the funding and staffing analysis in the DNS-CERT concept paper, and suggested that alternatives be seriously considered to the one proposed by ICANN.

PRESENSE Technologies GmbH

Till DArges of PRESENSE Technologies GmbH noted a technical clarification on page 8, Section 4.2.4.2 of the Strategic Initiatives paper, that PRESENSE, not ENISA, conducted the 1st Workshop

on Internet Early Warning and Network Intelligence (EWNI2010) on 27 January 2010. The correct URL for the workshop should also be http://www.pre-sense.de/ewni2010.html.

USCIB

USCIB welcomed ICANN's focus on DNS security, stability and resiliency. "ICANN's proposal for a number of short and long range initiatives, including the establishment of a DNS-CERT, merit serious consideration and USCIB encourages ICANN to engage in further consultation with operators of the DNS, businesses and all members of the ICANN community to further develop these initiatives. USCIB believes that the establishment of a Working Group on these issues, as called for by the chairs of the GNSO, ccNSO and ALAC, is appropriate to gather the experiences and inputs of the community before undertaking the DNS-CERT and other SSR initiatives." USCIB also supported a thorough gap analysis, within an arrangement for sensitive data sharing, collaboration with existing organizations involved in DNS security, operators and businesses to avoid duplication of efforts. Finally, USCIB notes that, given the questions regarding the clarity of the underlying threats and the need to further develop the proposed initiatives, any proposal for a DNS-CERT budget should be made carefully, as the ultimate initiative may vary substantially from what's proposed presently. Of course, once a gap analysis and consultation with the community have been concluded, the proposed initiatives can be appropriately scoped to promote both enhanced security of the DNS and to reinforce the ICANN industry-led, bottom up, multi-stakeholder consensus model.

Individuals

Comments in this category included input from Alain Aina, Jean Robert Hountomey, Bob Hutchinson, Joe St Sauver, and David Smiley. The individuals generally supported broader engagement on the issues raised in the Strategic Initiatives and DNS-CERT papers (and several provided their support for the DNS-CERT concept). The general observation was that further collaboration was needed with a broader set of the community, including existing institutions and organizations.

Alain Aina

Alain Aina stated his support for a DNS-CERT. "We have welcomed the idea of setting up DNS-CERT. Indeed it should be noted that many nations in the Africa region has no CERT/CSIRTs and DNS operators are far from existing institutions acting around the DNS. It should be remembered that in the past, some operators, especially those of the community of country code domain names, have enjoyed working with ICANN on actions aimed at undoing some malicious activities around the DNS." Aina asked that continuing discussions on this topic "not reinvent the wheel, see how to collaborate with the existing [community], consider the alternatives' acceptable cost, and see how to undertake the initiative without leaving the prerogatives of ICANN."

Jean Robert Hountomey

Jean Robert Hountomey noted that ICANN and ISOC chapters are being contacted for assistance in "resource constrained environments" (even if this is not their roles) because:

- They are more known.

- People want a single entity to talk to.
- People are under pressure and don't have the time or the resources to start looking around dealing with emergency cases.
- People need a proxy to act on their behalf to reach the world and to be reached from the world by a trusted party.
- People need someone to rely on who has the knowledge or can find the knowledge or the resources needed for them.

Hountomey stated ICANN has been play a big role on this with other organizations and "my opinion is that the community deserves to have a dedicated body that can stand between different existing players while filling the concerns that are not yet addressed by those identified players."

Bob Hutchinson

Bob Hutchinson indicated the debate in Nairobi around the DNS-CERT proposal has reinforced the need for a broader engagement on DNS security, and highlighted some concerns with the proposal as introduced. Hutchinson states that while the global DNS community can benefit from increased support on security matters, it is unclear whether a new CERT—either autonomous or housed within ICANN—is the right vehicle to provide that support. He added that it would be better for ICANN to expand upon the discussions begun in Nairobi to consider a wider range of issues and solution sets. Hutchinson stated "ICANN's focus should not be oriented toward operating and managing the day-to-day DNS infrastructure security, but should focus on sponsoring SSAC fellowships and long-term research designed to measure, model and thwart interference with DNS."

Joe St Sauver

Joe St Sauver expressed his support for the DNS-CERT proposal, and said that many DNS issues are inherently pan-national and are not a good fit for national CERTs and may be currently handled in a semi-formal or informal way by existing organizations. St Sauver noted that the DNS is too important and too complex for DNS incident handling to be done in a purely informal fashion. "The very diversity of fora in which these issues come up is perhaps the most compelling reason why it would be good to have a single designated and professional operated entity that authoritatively "owns" DNS-related security issues when they come up—and they do come up." St Sauver did not think a DNS-CERT eliminated the need for any of the existing organizations, but it would complement and regularize incident handling for DNS-related incidents.

David Smiley

David Smiley provided an extensive set of comments (particularly comments related to clarification and improvement of the DNS-CERT and Strategic Initiatives proposals that will be incorporated by ICANN staff). Smiley stated: "The Internet would be better served (with greater efficiently and without political ramifications) by simply improving DNS awareness of the various existing organizations with their established constituency relationships."

Next Steps

ICANN intends to work with the community on a discussion of these issues identified with the SSR initiatives/DNS-CERT. Specifically:

- Work with the community to leverage the broad support for deeper understanding of systemic DNS threats and risks by developing a community-based approach to conducting such a risk analysis.
- ICANN staff will continue outreach and education efforts related to raising awareness and capacity to respond to DNS security and resiliency challenges in conjunction with the FIRST global CSIRT community, regional TLD associations and others. Specifically, a DNS Security workshop is planned at part of the annual FIRST general meeting and conference in June 2010. Additionally, ICANN is engaging with the CERT/Coordination Center at Carnegie-Mellon University to have CERT/CC facilitate a survey of CSIRTs with National responsibility related to issues related to DNS security and response capabilities.
- We recognize that community prefers that ICANN staff not be the operators of a DNS-CERT, and the community may prefer other structures. ICANN seeks to engage with proposals that another body be considered if funding and appropriate guidelines can be developed. The principal role of the ICANN going forward is to work with others to facilitate the broad-based community discussion on the requirement for and best approaches to establishing necessary capabilities. ICANN staff will work with the Board and ICANN community to establish the approach to most effectively play its facilitating role.
- Conduct discussions with the community on the Operational Requirements and Collaborative Approaches Workshop findings as a basis for concept development/mission refinement for a community DNS CERT/collaborative response capability. ICANN staff has organized this workshop prior to the conclusion of the comment period on the SSR Initiatives/DNS-CERT business case, inviting experts from across the DNS operational and cyber security/CERT response communities, including those of the DNS-OARC and RISG organizations. The intent of the workshop was specifically to address known concerns related to the requirements for collaborative response against specific threats, potential overlap with existing organizations such as the DNS-OARC, RISG and CSIRT community. The workshop findings are posted for public comment on the ICANN website at http://www.icann.org/en/topics/ssr/dns-cert-collaboration-analysis-24may10-en.pdf. Additionally, the ICANN Conficker after-action report was posted on the ICANN website on Conficker Summary and Review at http://www.icann.org/en/announcements/announcement-11may10-en.htm. This report also discusses DNS collaborative response capabilities and requirements in light of the Conficker situation.

A public consultation is planned for the ICANN meeting in Brussels on 20–25 June 2010 on the SSR Initiatives/DNS-CERT, focusing on how to approach a baseline threat/risk assessment and address concerns related to the concept development/mission refinement for a community DNS CERT/collaborative response capability. ICANN staff hopes to engage with others to leverage

existing activities such as those developed by the IT Sector Coordinating Council, ENISA, CENTR, ccNSO IRPWG and other organizations. The discussions in Brussels with the community are intended to focus attention on next steps for improving DNS security, stability and resiliency with modifications based on the input received.

Comments on Security Strategic Initiatives paper

ALAC - http://forum.icann.org/lists/strat-ini-ssr/msg00010.html

AT&T - http://forum.icann.org/lists/strat-ini-ssr/msg00009.html

Bertrand de La Chapelle on behalf of France - http://forum.icann.org/lists/strat-ini-ssr/msg00005.html

Till DArges on behalf of PRESENSE Technologies GmbH - http://forum.icann.org/lists/strat-ini-ssr/msg00000.html

InternetNZ - http://forum.icann.org/lists/strat-ini-ssr/msg00008.html

Internet Society (ISOC) - http://www.icann.org/correspondence/amour-to-dengate-thrush-14apr10-en.pdf

Neustar - http://forum.icann.org/lists/strat-ini-ssr/msg00004.html

Nominet - http://forum.icann.org/lists/strat-ini-ssr/msg00006.html

PayPal - http://forum.icann.org/lists/strat-ini-ssr/msg00012.html

Registries Stakeholder Group (RySG) - http://forum.icann.org/lists/strat-ini-ssr/msg00007.html

Lawrence E. Stricking, US Department of Commerce on behalf of the US Government - http://forum.icann.org/lists/strat-ini-ssr/msg00002.html

Comments on Global DNS-CERT Business Case paper

(or referenced DNS-CERT and were submitted in the Strategic Initiatives forum as a duplicate)

AFNIC - http://forum.icann.org/lists/dns-cert-proposal/msg00004.html

Comment from ALAC, ccNSO & GNSO Chairs - http://forum.icann.org/lists/strat-ini-ssr/msg00001.html

APTLD - http://forum.icann.org/lists/dns-cert-proposal/msg00007.html

AT&T - http://forum.icann.org/lists/dns-cert-proposal/msg00016.html

Alain Aina - http://forum.icann.org/lists/dns-cert-proposal/msg00021.html

Bob Hutchinson - http://forum.icann.org/lists/dns-cert-proposal/msg00017.html

ccNSO - http://forum.icann.org/lists/strat-ini-ssr/msg00003.html

CENTR - http://forum.icann.org/lists/dns-cert-proposal/msg00002.html

DNS-OARC - http://forum.icann.org/lists/dns-cert-proposal/msg00009.html

InternetNZ - http://forum.icann.org/lists/dns-cert-proposal/msg00010.html

Jean Robert Hountomey - http://forum.icann.org/lists/dns-cert-proposal/msg00020.html

Hiro Hotta on behalf of JPRS - http://forum.icann.org/lists/dns-cert-proposal/msg00001.html

Adli Wahid on behalf of Malaysia CERT - http://forum.icann.org/lists/dns-cert-proposal/msg00011.html

NetChoice - http://forum.icann.org/lists/dns-cert-proposal/msg00019.html
Neustar - http://forum.icann.org/lists/dns-cert-proposal/msg00012.html

Nominet - http://forum.icann.org/lists/dns-cert-proposal/msg00013.html
Registries Stakeholder Group (RySG) - http://forum.icann.org/lists/dns-cert-proposal/msg00014.html

Joe St Sauver - http://forum.icann.org/lists/dns-cert-proposal/msg00005.html
Rohana Palliyaguru on behalf of Sri Lanka CERT - http://forum.icann.org/lists/dns-cert-proposal/msg00006.html

Dave Smiley - http://forum.icann.org/lists/dns-cert-proposal/msg00003.html

United States Council for International Business (USCIB) - http://forum.icann.org/lists/dns-cert-proposal/msg00015.html

US Government - http://forum.icann.org/lists/strat-ini-ssr/msg00002.html