Supplementary Submission No. 40.1

House of Representatives Standing Committee on Communications

ANSWERS TO QUESTIONS ON NOTICE

The Internet Corporation for Assigned Names and Numbers (ICANN)

Inquiry into Cybercrime

8 October 2009

Topic: **Protocols**

Hansard Page: **COMM 4**

Question:

- **Information on new protocols and how they will facilitate security.**

CHAIR—Will the security protocol that you are presently in the process of implementing prevent that sort of thing occurring?

Dr Twomey— No, not necessarily. It may not prevent the use of the domain names. It is more likely to have rapid takedown provisions for when a particular domain name has been identified. Police, the banks and other technical people who work in this area will identify such domain names literally within minutes when they are being used for these sorts of attacks. We are also moving towards making certain in our contracts that there is provision for rapid takedown. I think I can supply more information to the committee on some of that, because we have made some announcements in the last 24 hours of some of our requirements in this new top-level domain space. I can supply you with more information on notice if you like.

CHAIR—We would appreciate that.

Additional Information: Our proposals in regards to the establishment of new gTLDs have a number of major provisions in this regard. We are requiring that all new gTLD registries institute a anti-abuse policy that details procedures for addressing reports of malicious conduct occurring via registered domain names to include how rapid takedown/suspension of those names would occur. These registrars would also have to have a designated anti-abuse point of contact publicly identified responsible for taking action in support of these policies. Addtionally, the new GTLD proposed provisions include the requirement for having "thick WHOIS" data available at the registrar level which will facilitate action by the response community in specifying domain names and identifying individuals involved in potential malicious conduct. More detail regarding these proposals is available at http://www.icann.org/en/topics/new-gtlds/mitigating-malicious-conduct-04oct09-en.pdf.

House of Representatives Standing Committee on Communications

QUESTIONS ON NOTICE

The Internet Corporation for Assigned Names and Numbers (ICANN)

Inquiry into Cybercrime

8 October 2009

Topic: **Registrars**

Hansard Page: **COMM 9 and 10**

Question:

- **Provide information on raising the performance of registrars and mechanisms for addressing cyber crime.**

Mr BILLSON—The Australian Computer Society thinks the ICANN framework is an opportunity to reduce internet crime by raising the performance of registrars and having vigilance over the way they make allocations of domain names and IP addresses and things like that. I was just wondering how such an idea would be given effect. Rather than having the cash criteria for activation, I wonder whether there could be a list of serial offenders of stolen credit cards used to register names or some quality assurance framework that delves a bit deeper into the behaviour of the registrars and their relationship with the people who are starting up these dodgy IP addresses and domain names. Is that something that you think is within reach?

Dr Twomey—Again, I can respond more fully on notice and send you more information. Just in the last 24 or 48 hours we have posted for public consultation a series of possible recommendations for the new generic top level names we are considering, including a whole series on malpractice or malfeasance type problems. We have some recommendations that we are putting forward for community comment now which might address some of the things that you are raising. I do not want you to misinterpret my previous answer. We do not just pull people down for the fees. I used that as an example. I will try to send through to you the most recent set of postings we have had for why we have taken registrars down.

Additional Information: Regarding ICANN's efforts to address malicious conduct in the establishment of new gTLDs, the full set of measures that will be mandatory is detailed at http://www.icann.org/en/topics/new-gtlds/mitigating-malicious-conduct-04oct09-en.pdf. Additionally, ICANN has proposed the establishment of a voluntary verification programs for high security zones that envisages establishing criteria for how registries and registrars will both establish stronger controls over who gets to register domain names in such TLDs as well as operational IT security controls to improve trust that registered names will not support malicious conduct. While the specific criteria for the program have not been established, a concept paper for the program is available at http://www.icann.org/en/topics/new-gtlds/high-security-zone-verification-04oct09-en.pdf. A technical expert advisory group has been established within ICANN to further develop this proposal.

Specifics on the recent ICANN actions to terminate or deny renewal of registrar contracts are available at http://www.icann.org/en/compliance/. Since 8 October 2009, ICANN has terminated or not renewed 9 registrars.

House of Representatives Standing Committee on Communications

QUESTIONS ON NOTICE

The Internet Corporation for Assigned Names and Numbers (ICANN)

Inquiry into Cybercrime

8 October 2009

* * * *

Dr Twomey—It may be a site—I do not know—registered under .ua, which is the country code for the Ukraine. We have no powers to set policy for how .ua runs. That is a domestic issue. We do recognise that .ua exists and we recognise who runs .ua at the top, but you have to remember that I am talking about the registry, not the process of the registrar selling a domain name to someone. You might also find—and we often find this is the case—that the domain name is in .ua but the actual data is sitting in the United States. Often in a lot of these areas, because of the protection of the First Amendment in the United States, all sorts of funny things that you think are being held in country X are actually being held in the US or other places because of legal protections. I want to draw your attention again to the fact that for the top-level domains that we have policy rights over, which are the generic top-level domains—the .coms, .nets or .orgs that are not particularly linked to a country code—we are looking at increasing obligations on registrars and mechanisms for addressing those sorts of concerns. I will send these to you in written form.

Additional Information:

ICANN has proposed the establishment of a voluntary verification programs for high security zones that envisages establishing criteria for how registries and registrars will both establish stronger controls over who gets to register domain names in such TLDs as well as operational IT security controls to improve trust that registered names will not support malicious conduct. While the specific criteria for the program have not been established, a concept paper for the program is available at http://www.icann.org/en/topics/new-gtlds/high-security-zone-verification-04oct09-en.pdf. A technical expert advisory group has been established within ICANN to further develop this proposal.

In addition to the high security zone program, ICANN continues policy development work on the basic Registrar Accreditation Agreement (RAA) between itself and the Registrars. Last May, the ICANN Board approved a revised RAA that included provisions strengthening registrar obligations and strengthening ICANN's compliance mechanisms. This Agreement is available at http://www.icann.org/en/registrars/ra-agreement-21may09-en.htm. Currently, within ICANN's Generic Names Supporting Organization (GNSO) and At Large Advisory Committee (alac), have established a joint working group on protecting registrant rights to included enhanced RAA provisions. The activities of this working group can be found at https://st.icann.org/raa-related/index.cgi?joint_alac_gnso_wg_and_at_large_workspace_on_raa_related.

House of Representatives Standing Committee on Communications

Inquiry into Cyber Crime

Additional Question

1. The Committee understands that the ICANN Security and Stability Advisory Group have proposed that 'white listing' be used to mitigate the threat of malware:
    a. Can you explain how 'white listing' works and what is required to implement it?

Additional Information: "White listing" references to a category of information security controls that call for a organization using Internet services such as domain name resolution to only allow connection to/use of those names and/or addresses that it knows can be trusted, blocking the use of all others and thereby severely limiting opportunities for importing malware from connections made by phishing e-mails or downloads from web surfing by members of the organization. The implementation of such an approach does require an organization to develop strong awareness of how it uses Internet services such as routing and domain names resolution to support operations to identify what IP addresses and domain names can be permitted. Therefore, "white listing" usually requires a fairly skilled IT and security staff or a similarly effective outsourced provider.