Additional Information from George Asare Sakyi in support of his application as a Volunteer on the security, stability and resiliency of the DNS Review Team SSR-RT.

1. Introduction

It was in April 1999 in France during an operation and maintenance program that I had better understanding of the potentials of the emerging internet technology. As a result, I enrolled to study webpage designing and its administration in 2001. After the training I was admitted to pursuit an MSc degree program in Engineering and Management at the University of Exeter in 2002 and graduated in 2004. My project work was entitled, "Establishing the need for a platform for e-business for the manufacturing companies in the south east of England." The project work actually made me to appreciate the need for a very strong security measures to ensure a safe platform for the e-business project and that has made me to develop special interest in the security and safety of every network that I work with.

2. Head of Broadband unit

Upon my return to Ghana I was appointed as the Head of the Broadband unit and tasked to deploy broadband solution to replace the dial up system that was in place at the time. With my understanding in information security and encryption technologies, I was involved in the design and the deployment of individual customers and corporate customers' local area networks. As the head of the broadband unit in a company that was, and is still a major internet service provider in the country, it was my responsibilities to ensure that all servers and routers are safe and secure for our value customers to transact their business in real time without fail. Again it was my responsibilities to ensure that our network is well fortified against intruders. I have experience in the various attacks that are committed on the internet the common being identity stealing against individual subscribers but there are bigger attacks against registrars which does not only affect individual but customers on a complete DNS

3. Various method adopted by attackers on DNS

There are various forms that these attackers use against registrars to gain control over an entire domain portfolio which include the following;

1. Stealing a password or impersonating a registrar through an email that may essentially be a spear phish,
2. Scan registrar Web sites for Web application vulnerabilities and exploit these vulnerabilities. E.g. SQL insertion.
3. Social engineering a point of contact in an organization

Once they have compromised the account, the attackers change the contact information and the DNS information. The reason why these accounts are so valuable to the attackers is because

when you own a legitimate domain, it is much harder for law enforcement and for responders to brand intrusions and intellectual property intrusions.

4. **Solution to reduce attacks**

With my background in e-business and information and communication security issues I can say the model of attach is not unique to the registrars only but also to other financial industries, and major online merchants like eBay and Amazon, but the difference is a tighter security measures these other institutions take to overcome these attackers.

I am therefore in full support of SSAC report SAC 40 which recommends various measures to reduce attacks on our DNS. This report was published on, 19 August 2009 and a copy could be obtained from the link below.

http://www.icann.org/en/committees/security/sac040.pdf

Below are the recommendations of SAC 40 report which include the following that registrar should consider;

1. Multifactor authentication,
2. End-point verification,
3. Granular access controls,
4. Diversity in customer correspondence.

5. **Experience in National Technical committee works**

I have experience working on various committees but the following are internet related committees.

1. Ghana Emergency response Team set up to assist individual or corporate organization that may be in distress as a result of internet fraud or internet failure in a real time transactions. This appointment took effect in September 2009
2. National Technical committee set up to transfer the operations of dot gh ccTLDs from a private company NCS to National Information Technology Agency NITA, the now accredited Agency to handle our ccTLDs. This appointment took effect in February 2010
3. A representative of Ghana Institute of Engineers on the National Technical committee at the Ghana standard board tasked to set up standards for the ICT Industries in the country. This appointment took place in May 2010

6. **Conclusion**

I will say I am an experience telecom engineer who does objective analysis base on factual evidence. I have a clear understanding of the review committee's work and I will see it an honor

to work with other experts to analysis the extent to which ICANN will successfully implemented the security plan, the effectiveness of the plan to deal with actual and potential challenges and threats, and the extent to which the security plan will sufficiently be robust to meet future challenges and threats to the security, stability and resiliency of the Internet DNS, which is one of the objectives of ICANN's.