Rethinking the role of ICANN and the gTLD Whois to enhance the security and stability of the DNS

A proposal for the GNSO Task Force on Whois Services

prepared December, 2006

BACKGROUND

I) The purpose of Whois

It is widely accepted that the primary original uses of the gTLD Whois service is to use it for the purpose of coordinating technical actors as they seek to resolve operational issues related to the security and stability of the DNS and a well-functioning internet.

Present day examples of this are many;

- Network operators and service providers use Whois data to prevent or detect sources of security attacks of their networks and servers;
- Emergency response and network abuse teams use Whois data to identify sources of spam and denial of service attacks and incidents;
- Commercial internet providers use Whois data to support technical operations of ISPs and network administrators;
- ISPs and Web hosting companies use Whois data to identify when a domain name has been deleted, and remove redundant DNS information from ISP name servers

The importance of this original purpose was reaffirmed in the GNSO council's recommended[1] definition on the purpose of Whois:

> *"The purpose of the gTLD Whois service is to provide information sufficient to contact a responsible party for a particular gTLD domain name who can resolve, or reliably pass on data to a party who can resolve, issues related to the configuration of the records associated with the domain name within a DNS name server."*

The scope of use has increased considerably beyond this over time, a subject that has already been substantially considered by the GNSO Whois Task Force and Council. The scope of use of the internet has also changed over time, as have the management tools used to administer these uses.

In each of these examples, the truly useful information is not the contact information for the domain name registrant in question, it is the name server information for the name in question. Unfortunately, neither is reliable or truly useful in any real way because authoritative information about DNS resources doesn't live in a gTLD database, it lives inside the DNS itself.

[1]Decision taken 12 April 2006, http://gnso.icann.org/meetings/minutes-gnso-12apr06.shtml

The validity of the data in a gTLD Whois database has no impact on the operational integrity of the DNS.

Due to this disconnect between these two systems, network systems managers rarely rely on gTLD Whois service when they seek to investigate or resolve serious network operations and technical coordination issues. An entirely different set of tools and resources that relies on authoritative data have evolved that support the requirements of these types of users. For example, a network administrator might use "dig"[2] or "nslookup"[3] to determine the source of a DNS problem or the network location of a mail server being abused to send spam email. All of these tools are publicly available at no charge, internet standards based, and in widespread use.

Furthermore, from a network management perspective, not only is the data in the DNS more authoritative (and therefore useful), it is also more comprehensive. A typical DNS record can include information about the network location of any and all web servers, email servers and other resources associated with a specific domain name – at all sub-levels associated with the specific DNS entry (i.e., the second, third and fourth levels of the domain hostname). The gTLD whois service contains none of this important information.

When DNS data is used in conjunction with the IP Address Whois data sourced from providers like ARIN or RIPE, a network administrator is able to form a fully authoritative view of not only the services associated with a specific domain name, but also the identity of the entity that physically hosts those resources and how to contact that entity. All of this data exists outside the gTLD Whois system.

II) ICANN's Role

The scope and authority of ICANN's policy-making responsibilities is limited by its bylaws;

> *The mission of The Internet Corporation for Assigned Names and Numbers ("ICANN") is to coordinate, at the overall level, the global Internet's systems of unique identifiers, and in particular to ensure the*

[2] dig (domain information groper) is a flexible tool for interrogating DNS name servers. It performs DNS lookups and displays the answers that are returned from the name server(s) that were queried. Most DNS administrators use dig to troubleshoot DNS problems because of its flexibility, ease of use and clarity of output. Other lookup tools tend to have less functionality than dig. (source: "dig man page")

[3] NSlookup is a program to query Internet domain name servers. NSlookup has two modes: interactive and non-interactive. Interactive mode allows the user to query name servers for information about various hosts and domains or to print a list of hosts in a domain. Non-interactive mode is used to print just the name and requested information for a host or domain.

stable and secure operation of the Internet's unique identifier systems. In particular, ICANN:

1. Coordinates the allocation and assignment of the three sets of unique identifiers for the Internet, which are:

a. Domain names (forming a system referred to as "DNS");

b. Internet protocol ("IP") addresses and autonomous system ("AS") numbers; and

c. Protocol port and parameter numbers.

2. Coordinates the operation and evolution of the DNS root name server system.

3. Coordinates policy development reasonably and appropriately related to these technical functions.

ICANN's role is primarily that of a technical coordinator and developer of policy to support that coordination.

III) ICANN's Scope

There are many other uses of gTLD Whois - most or all of which have been documented by the GNSO Whois Task Force[4]. Creating policy to manage, influence, prevent or encourage most of this use is out of scope for ICANN.

IV) Technical coordination in the real world

Most technical coordination of DNS administration, abuse and network management issues occurs without ICANN's involvement. Private sector coordination is more likely through CERT, NANOG, Reg-OPS and other forums, than those operated by ICANN. These initiatives are often ad hoc and key players do often not understand the importance and value of participation. This is an area where small improvements in the overall level of cooperation between the various initiatives would lead to substantial improvement in the overall security of the internet and DNS infrastructure.

[4] http://www.does-not-exist.org/mail-archives/council/msg00927.html

Policy Implications

Given that the original beneficiaries of the gTLD Whois service have developed superior alternate methods of coordinating their activities, and that the remaining uses of this service are out of scope relative to ICANN's scope and mission, and that the abuse of this data has caused a significant barrier to the security of millions of Internet users, we propose the following;

1) that ICANN waive all Whois publication requirements for gTLD registries and registrars;
    a. If the Whois publication requirements cannot be waived for the registries and registrar, then registrars should be limited to only publishing contact information for the person or entity responsible for managing the authoritative DNS server;

2) that ICANN immediately undertake to create a study of where it might best contribute to coordinating the network management activities of registration interests, network operators and service providers and law enforcement agencies. This should be done with the goal of ensuring that emergency response and technical abuse prevention is well coordinated and the overall interests of internet users are appropriately protected by a secure and functional domain name system.

3) That ICANN undertake to develop a statement of best practices that registration interests should apply when working with law enforcement interests, network operators and other legitimate parties concerned with public safety, legislative enforcement, network management and abuse, and the protection of critical information technology infrastructure.