The ICANN Accountability Dilemma
A Response to the 2009 ICANN Notice of Inquiry
Issued by the
National Telecommunications and Information Administration

Michael M. Roberts[1]

The 2009 ICANN NOI[2] provides an opportunity not only to assess current issues in the transition, but also to take a longer view after a decade of experience in guiding the evolution of the DNS under the Joint Agreement. The NOI asks, "*Is this still the most appropriate model..."* and these remarks are directed to that question.

A. Introduction

Much has changed in the Internet and at ICANN over the last ten years. The net is more than twice as large, having passed a billion connected devices some time ago, and its patterns of use have shifted dramatically in the direction of social and personal uses. Several of the leading providers - Google, Facebook, et al - did not exist in 1998. Convergence of voice, data and video applications is continuing rapidly at both the high end and the low end. ICANN's budget and staffing have grown by a factor of ten, and the number of domain names in registration has also grown by nearly an order of magnitude.

ICANN faced challenges at the time of its creation, and it faces significant ones today as the Internet environment within which it operates continues to evolve. Many observers believe that ICANN has fallen short of the lofty aspirations set forth in the 1998 NTIA White Paper,[3] even with its obvious successes in guiding the management of domain names and keeping the name resolution process functioning as well today as it did ten years ago despite amazing growth. In a pioneering effort without a model or legislative precedent, it not surprising that this would be the case.

B. Accountability Dilemma

One overarching problem - accountability - still dominates the relationship between ICANN and the U.S. Government, and between ICANN and its broader community, as documented in the comments that ICANN's own outreach has received. Accountability is the predominant and common factor in ICANN's Presidential Strategy Committee's public comment process. If a solution can be found to the accountability dilemma, many other issues will be more manageable.

In 1998, the White Paper described an early termination of U.S. involvement in the affairs of ICANN:

"the U.S. Government would continue to participate in policy oversight until such time as the new corporation was established and stable, phasing out as soon as possible, but in no event later than September 30, 2000."

But after ten years, this goal has not been realized and ICANN is still saddled with not one, but two contracts tying it to the Department of Commerce. It is clear that accountability and independence are intertwined, and a decision on independence is also a decision on accountability. In this context, accountability means clarity with respect to process and structure such that governments and private sector stakeholders are assured of fair and equitable treatment in ICANN decisions. It is possible that the delays and related stakeholder concerns in ending the MOU/JPA are more a reflection of unease over the accountability problem than they are a lack of accomplishment on the various tasks set forth in these documents.

---

[1] Managing Director, The Darwin Group, Inc. The writer was ICANN President and CEO, 1998-2001.
[2] <http://www.ntia.doc.gov/press/2009/OIA_ICANNJPA_090427.html>
[3] <http://www.ntia.doc.gov/ntiahome/domainname/6_5_98dns.htm>

C. Rationales for Continued Involvement

A number of rationales have been offered for continued U.S. involvement, which has lasted ten years rather than the two years originally envisaged:

• the authors of the White Paper misjudged, or could not fully predict, the geopolitical environment in which ICANN would find itself over time;

• rapid changes in the Internet, and particularly in its security environment, have made the commitment to full independence infeasible;

• ICANN has not demonstrated the ability to satisfy its stakeholders on the subject of accountability;

• changes in U.S. domestic politics changed attitudes at the White House about ICANN independence.

It is likely that each of these points, to one degree or another, has influenced decisions by NTIA to extend the JPA and IANA agreements numerous times. Previous NOI responses have also supported JPA extensions. The question then arises, given the variety of views contained in these rationales, whether a single solution exists that would finally allow the U.S. government to retreat from oversight of ICANN.

One way to assess the current situation is to ask what conditions need to exist, going forward, for the White House and Congress to feel comfortable about granting independence to ICANN? A short list would include:

• the political, economic and operational environment of the Internet would have to be more stable and predictable than it is at present;

• the institutional foundations, quality of governance and structure for accountability within ICANN would need to be robust and accepted by the community;

• the principal stakeholders in ICANN, including national governments, would need to be confident that the time was right for ICANN independence.

Unfortunately, none of these conditions exists today, and it is not clear that any of them are progressing in the right direction.

D. Stable Internet Environment

With regard to the environment of the Internet itself, a recent White House report[4] offers a sober assessment:

> ***The Nation is at a crossroads.*** *The globally-interconnected digital information and communications infrastructure known as "cyberspace" underpins almost every facet of modern society and provides critical support for the U.S. economy, civil infrastructure, public safety, and national security. This technology has transformed the global economy and connected people in ways never imagined. Yet, cybersecurity risks pose some of the most serious economic and national security challenges of the 21st Century. The digital infrastructure's architecture was driven more by considerations of interoperability and efficiency than of security. Consequently, a growing array of state and non-state actors are compromising, stealing, changing, or destroying information and could cause critical disruptions to U.S. systems... The United States faces the dual challenge of maintaining an environment that promotes efficiency, innovation, economic prosperity, and free trade while also promoting safety, security, civil liberties, and privacy rights.*[1] *It is the fundamental responsibility of our government to address strategic vulnerabilities in cyberspace and ensure that the United States and the world realize the full potential of the information technology revolution.*
>
> ***The status quo is no longer acceptable.*** *The United States must signal to the world that it is serious about*

[4] "Cyberspace Policy Review," <http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf>

addressing this challenge with strong leadership and vision. Leadership should be elevated and strongly anchored within the White House to provide direction, coordinate action, and achieve results. In addition, federal leadership and accountability for cybersecurity should be strengthened.

It goes without saying that the name and address systems of the Internet fall within the scope of the critical infrastructure concerns described above and that NTIA, along with other federal agencies, will be deeply involved with improvements in this area, including ICANN's potential contributions.

Recognizing that Internet security is a transnational effort, the report speaks to international cooperation:

> ***Partner Effectively With the International Community***
> *International norms are critical to establishing a secure and thriving digital infrastructure. The United States needs to develop a strategy designed to shape the international environment and bring like-minded nations together on a host of issues, including acceptable norms regarding territorial jurisdiction, sovereign responsibility, and use of force. In addition, differing national and regional laws and practices—such as those laws concerning the investigation and prosecution of cybercrime; data preservation, protection and privacy; and approaches for network defense and response to cyber attacks—present serious challenges to achieving a safe, secure, and resilient digital environment. Addressing these issues requires the United States to work with all countries— including those in the developing world who face these issues as they build their digital economies and infrastructures—plus international bodies, military allies, and intelligence partners.*
>
> *In the past decade, federal communications, infrastructure, and cybersecurity-related policies developed along multiple paths. A more integrated approach to policy formulation would ensure mutually reinforcing objectives and allow the United States to leverage its international opportunities with consistent, more effective positions. The United States should adopt an integrated approach to national interests across a range of substantive areas—including cybersecurity and the protection of free speech and other civil liberties—to develop consistent policies.*

The conclusion of this report, and numerous others, is that the Internet, and especially its security aspects, are unstable and require strong new federal leadership to ensure that necessary improvements are designed and implemented. The White Paper did not adequately foresee the increasing importance of tending to these mounting security challenges, occasioned by a decade in which the Internet has evolved into an infrastructure extraordinarily critical to global economic prosperity and security while at the same time its vulnerabilities have been exploited for malicious ends.

E. Robust ICANN Institutional Foundation and Governance

The interagency task force, which was given responsibility in 1997 for devising the means by which the Domain Name System would be privatized, found itself hemmed in on all sides by difficult U.S. political and legal constraints. As a result, ICANN has to this day an exceedingly flimsy legal foundation. The high water mark of lack of support for ICANN from NTIA was achieved in the following language in the White Paper:

"this policy statement is not a substantive rule, does not contain mandatory provisions and does not itself have the force and effect of law."

While possibly not intended, this language, and other provisions of the White Paper, had the effect of weakening the perception of ICANN's authority and responsibility, especially overseas, where some of the nuances of domestic politics and U.S. bias toward free market solutions were not appreciated. Without receiving firm legal legitimacy from the U.S. Government, ICANN struggled in its efforts to help coordinate the many autonomous organizations that have a role in Internet operations. A number of important infrastructure organizations that must see ICANN as a reliable partner, including the regional address registries, the root server operators, the country code registries in Europe and elsewhere, and the Internet Engineering Task Force, adopted arms length relationships with ICANN that persist to this day and diminish the effectiveness of its work.

No other government in the developed world has attempted to exert leadership in an important area of Internet infrastructure with no relevant statutory basis. With a new administration and a new focus on White House

leadership for critical infrastructure, a firmer legal basis for ICANN may be achievable. The recent cybersecurity report cited above makes the following statement:

> *The Administration should partner appropriately with Congress to ensure adequate law, policies, and resources are available to support the U.S. cybersecurity-related missions. Congress has demonstrated interest and bipartisan leadership regarding the cybersecurity-related needs of the Nation, and the Administration would benefit from Congressional knowledge and experience.*

ICANN's efforts to self-create legitimacy have been effective only to a limited extent. Seeking to enhance its acceptability to its partner organizations as well as Internet users, it has repeatedly sought to develop a governance that is representative, transparent, and accountable, yet still allows effective discharge of its mission. It has undergone two rounds of "reform" since its inception and is currently in the midst of a review of Board functioning. These efforts have proven less than satisfying to both Internet users and to the other organizations involved in Internet coordination.

A fundamental issue these reforms have attempted to grapple with is the inability of any Internet organization, under current circumstances, to effectively represent the interests of several billion users without normal democratic mechanisms, e.g. membership and elections. After the captured Board election of 2000, ICANN retreated to an appointment process for Directors through the use of a Board Nominating Committee. Although conscientious Directors have thereby served on the Board, ICANN suffers from the perception in many quarters that it is undemocratic and unrepresentative. This is a structural difficulty that will not go away soon.

In short, political constraints of the 1990s ruled out ICANN receiving a firm legal basis at the beginning. Inherent practical difficulties have hobbled ICANN's efforts to self-generate its legitimacy. The result has been to severely undercut a key premise of the White Paper's roadmap for Internet coordination.

F. Stakeholder Confidence

> *"ICANN's greatest strength, and its greatest weakness, is that it's different."*
> - Anon

The framework articulated in the White Paper resulted in the creation of a unique organization with a diverse set of constituencies and stakeholders. The government transferred to ICANN management of the previous DARPA responsibilities for Internet numbering and addressing, carried out by Jon Postel's IANA organization in California, along with the domain name registration supervision responsibilities carried out by Network Solutions in Virginia under contract to the National Science Foundation. The former was dominantly a non-commercial, public trust activity, while the latter was a highly profitable commercial activity attempting to cope with the extraordinary growth of the dot-com name registry and associated problems, particularly trademarks and cybersquatting. The government further burdened ICANN with an expectation that the new organization would find a bottom-up representation mechanism to replace the nominally top down structure of the research agency contracts.

As a result, ICANN's split personality has never fully satisfied any of its stakeholders. It's doubtful that in its present form that it ever will. ICANN has lacked a willingness to fully engage the broader business user communities, focusing primarily on its contracted registries and registrars. The civil society participants in ICANN have always felt that the organization has not stepped up to its public trust responsibilities, and have not only asked for more democracy but also actively sought a broader mission in which ICANN would address issues of economic development, human rights, etc. Many from the business user community support the public trust role, but strongly oppose extending ICANN into broader areas of Internet governance and development.

The domain name registry/registrar side of ICANN's stakeholder community, which also provides its $60M per year financing through a fee on domain name registrations, has felt that the public interest equated to unreasonable restrictions on their current and future business activities.

Perhaps most importantly, in the absence of any specific statutory authority for ICANN, the stakeholders have been left without an effective recourse to legislators that characterizes democracy in the U.S. and in many other countries.

As can be seen in the responses to this NOI, and to previous ones, stakeholder support for ICANN is low, and enthusiasm for termination of the JPA even lower.

G. Conclusions

To summarize the foregoing points, the White Paper misjudged the need for continued U.S. Government involvement in matters of Internet critical infrastructure when creating ICANN. Political limitations prevented seeding ICANN with legitimacy at its inception. The subsequent recognition that an entirely hands off policy would not work has resulted in a series of extensions to the ICANN contracts over a period of more than ten years. ICANN's efforts to generate satisfactory accountability have failed to meet the expectations of stakeholders and the U.S. Government.

Except for those who profit economically from the existence of ICANN, there is little support for an independent ICANN among industry, civil society and other governments, principally because of the accountability problem. In the tense international geopolitical environment which exists today, with many threats to the security and integrity of the Internet, it does not serve the national interest of the United States to entrust critical Internet infrastructure to an organization that lacks effective accountability mechanisms, either through ties to an elected government, or through an equivalent accountability mechanism obtained through international agreement.

H. Alternative ICANN Models

It is beyond the scope of this paper to develop detail on proposed alternative models for the relationship between the U.S. Government and ICANN. The following suggestions may serve as a point of departure for policy development.

1. Until such time as the Internet security situation improves sufficiently, oversight of the stability and integrity of the root zone and its associated servers should continue to rest with the U.S. Government or with a consortium of governments of which the U.S. is a leading member.

2. Until such time as ICANN, its major stakeholders, and representatives of governments have reached agreement on a satisfactory accountability mechanism for ICANN, the U.S. Government should maintain its present contractual relationships with the organization.

3. NTIA should re-examine the premise in the White Paper that DNS management should be conducted entirely outside the purview of the U.S. and other governments. Considering the pending anti-trust litigation involving ICANN and VeriSign, this review should specifically include the hazards of a completely unregulated marketplace for the domain name system in view of the major market failures in the U.S. and elsewhere in recent years.