Comments on the Upcoming ICANN Joint Project Agreement

Phillip Hallam-Baker
Chief Scientist, Default Deny Security Inc.
hallam@defaultdenysecurity.com

The Role of ICANN

In ancient times, the kings of Burma, Thailand and neighboring states would gift particularly favored subjects a White Elephant as a mark of their gratitude and respect. Such animals were considered sacred and the law prohibited putting them to labor. Nor could a sacred animal gifted by the King himself be given away. All a White Elephant could do was to eat copious quantities of food.

Much (but not all) of the initial research funding that led to the formation of the Internet came from the US government working through DARPA and the NSF. Lacking a white elephant to bestow on their benefactor, the Internet pioneers bestowed guardianship of the allocation of Internet names and numbers.

ICANN Principles

Of the four principles set out for ICANN (bottom up, stability, private, competition), only stability represents an objective. The rest are means, not ends. And of the three means, only bottom-up represents a principle that has been important to the formation of the Internet.

The terms 'Private' and 'Competition' represent ideological commitments driven by internal US political debate. It is inappropriate and counter-productive to raise them to the same levels as the overarching objective of stability in the principles guiding the administration of an infrastructure that is global in scope.

Stability

ICANN represents the only visible mechanism for co-ordination and control of the Internet. ICANN claims responsibility for allocation of Internet Protocol (IP) addresses, for maintenance of the Internet DNS system that maps names (e.g. example.com) to IP addresses (e.g. 10.1.2.3) and for the administration of the IANA registry of protocol identifiers. If such claims are believed to be true, then ICANN is in charge of the Internet. While nobody can be quite sure what would happen if people were to stop accepting these claims, most people who understand the potential consequences would prefer not to find out.

The stability of the Internet depends critically on the stability of this mapping being maintained. For the Internet to be the Internet it is essential that microsoft.com resolve to the same set of Internet services regardless of where an end user might be.

The threats to stability come from two distinct sources, political and technical. While there have been no disasters over the past decade, this has been achieved by deferring rather than resolving the underlying issues. Consequently the probability of a future disaster has significantly increased and therefore the goal of stability has not been met.

Many people believe that US control of ICANN represents control of the Internet. While US nationalists who believe this conclude that the US must on no account surrender control of ICANN, a considerably greater number of non-US nationals draw the opposite conclusion from the same set of facts. In this world-view, ICANN represents the flag in a diplomatic game of capture the flag. I believe that it is this world-view that is behind moves to bring ICANN (or the functions of ICANN) within the remit of the UN through the ITU. Such moves are generally considered with distrust by the Internet standards community as the ITU represents the 'top-down' approach to protocol design that is the antithesis of the 'bottom-up' style that characterizes the Internet.

As Jon Postel correctly foresaw, the inclusion of country code TLDs in the DNS root has inserted the politics of every irredentist conflict in the world into the politics of DNS administration. The game of capture the flag takes on considerably more significance if the flag holder gets to decide what is and what is not a country and which parties are to be recognized as the legitimate representatives of that country. Consider the case in which a minor member of Congress seeks to curry favor with certain groups of constituents by proposing a bill to require ICANN to drop Cuba (.cu) or Palestine (.ps) out of the DNS root zone. Such a member of Congress would be guaranteed considerable media attention as the State department tried to avert the international crisis that would ensue should the measure succeed.

Although such diplomatic games may be considered preferable to actual conflict, the only benefit that a good-faith custodian can draw from control of the flag is to prevent it from falling to a bad faith actor.

From time to time there are proposals to employ the power of control of the DNS root zone (and on occasion .com) to provide beneficial infrastructure, such as to prevent Internet crime. While such proposals are almost invariably well intentioned, they are indistinguishable at the technical level from proposals that might be malicious. If for example the US FBI is given the ability to block Internet domains being used to perpetrate fraud, other governments will demand 'equivalent' access, including the ability to block criminal speech that is critical of the government. While there are technical architectures that could permit such capabilities to be deployed, ICANN is not a suitable venue through which they may be promoted.

To date it has been possible for the national stakeholders to defer these concerns as they understand that the position of ICANN ultimately relies on their consent. Any Internet service provider can reroute the DNS A-root by simply making a BGP path announcement for the IPv4 address 198.41.0.4. If roots A through M are all re-routed, anyone who uses the Internet within the scope of

those redirections will be operating under an entirely different DNS. It follows that a country who objects to some ICANN policy that it considers to be abusive can simply instruct its domestic ISPs to re-route all traffic to the DNS root IP addresses.

While this property of the DNS may be properly considered to be a technical defect insofar as it may be exploited by criminals, the opportunity of exit that it affords is the safety valve that keeps ICANN and US control of ICANN in check. Should ICANN defect and act in a manner that was widely disapproved of, it can and would be replaced.

The technical measures to prevent the malicious redirection of the DNS root described in the current iteration of DNSSEC would foreclose this possibility of exit, effectively shutting the safety valve. As such DNSSEC as currently designed is a profoundly destabilizing technology.

While it may seem counter-intuitive that the addition of security measures should lead to a reduction of stability, it is well understood that security measures alter the balance of power. In the case of DNSSEC, the security measures would tilt the balance of technical control even further in the direction of ICANN and the US administration. This is a clear cause of concern for French, Russian, Chinese, Egyptian and Brazilian participants in ICANN and almost certainly explains at least part of the resistance to DNSSEC deployment.

Technical issues concerning DNSSEC are dealt with in the second section. For the purposes of discussing ICANN principles it is sufficient to observe that while stability of the DNS is rightly considered to be a foundational principle, the interests of stability may conflict with the needs of security. It is therefore necessary to list both stability and security as separate foundational principles.

Private

In UK government terms, ICANN is, was and always will be a QUANGO, a Quasi Non-Governmental Organization. It exercises governmental functions without being subject to governmental accountability. The insertion of 'Private' in the ICANN principles does not make it any less governmental in character. It merely announces that it is not to be subject to governmental accountability. It does not protect it from governmental interference.

Despite the fact that ICANN is demonstrably not private, very few outside observers have concluded that the problems with ICANN stem from the lack of external control. Rather, it is the risk that government control be abused that is concern. While entirely removing government influence from ICANN removes one incentive for abuse, very few external parties believe that the probability of abuse would be reduced if ICANN was accountable to no-one but itself.

The foundational principle should be accountability. The term 'private' suggests the antithesis of accountability: a body charged with a public function for the private good.

Competition

The term 'competition' likewise reflects US domestic political discourse and ideology rather than something that is fundamental to the functioning of the Internet. While competition is one

consequence of the principles of openness that distinguishes the Internet from the legacy telephone and postal networks that preceded it, it is a consequence, not a fundamental principle of the Internet.

While ICANN has succeeded in introducing competition between DNS registrars, it has failed to establish a competitive market for DNS registry services. There was only one generic DNS TLD of any consequence in 1998 and it is clear that there will only be one generic DNS TLD of any consequence in 2012 when the .com contract comes up for renewal. And it is equally clear that there will be only one provider capable of servicing a contract for the entire .com domain at that time.

Nor is it necessarily in the personal interests of the ICANN management to succeed in this respect. While nominally a non-profit, ICANN has profited certain members of its management very handsomely. As with cost-plus contracting in other areas of government, ICANN management can expect the rewards of failing to control expenses to be considerably greater than those of effectively reducing them.

The only apparent benefit of this activity is to the registrars selected to run the new TLDs and to ICANN which proposes to charge applicants a substantial fee whether their application is accepted or not. The size of these fees creates a clear conflict of interest for ICANN which despite its nominal status as a non-profit has demonstrated a considerable interest in maximizing revenues.

ICANN should cease attempts to introduce new TLDs entirely. The lack of competitive provision of registry services to support .com should instead be addressed by restructuring the .com registry contract to allow multiple service providers to bid for provision of services within the .com registry. Over time the second tier TLDs should be phased out entirely and the .com domain promoted to become the sole generic root.

Some of the technical infrastructure required to support competitive provision of registry services in .com has already been deployed. The DNS J root is currently supported at 62 separate service locations through use of anycast technology. It is not a large step to go from one company supplying services through 62 independently operating servers to multiple companies competing to supply the same service.

ICANN can and should take responsibility for ensuring the development of technical standards for the DNS that support and enable this form of competitive provision of the services it requires. Unfortunately ICANN has largely abdicated the role of supervising technical standards, a topic covered in further detail in the security section.

Openness

Contrary to the notion common during the dotcom bubble, the Internet was designed as an engine of communication, not commerce. Raising the term 'competition' to a fundamental principle suggests that the principal purpose of ICANN is to protect the commercial interests of the parties involved in the running of the Internet.

If this is in fact the objective, we should remind people that the Internet was built for people, not corporations. In the early 1990s, the corporations had their own vision of the future of communications, 'interactive TV'. Interactive TV was designed to enable consumers to become more efficient consumers of information provided by the established media corporations. The idea that private individuals might want to become content providers or that others might want to consume the content created was simply not considered.

While the effects of the Web on the power and influence of the mainstream media are now understood, it is only rarely acknowledged that this was an intentional outcome.

The Clinton administration embraced the Internet and the Web as part of a comprehensive strategy to disintermediate the establishment media. Instead of complaining about 'the filter' as a later administration described the media, the Clinton administration sought to break its power. I was a part of that effort as one of the contributors to the design of the Web at CERN and later at MIT.

At the time I was working on the Web at CERN, a few hundred miles away the city of Sarajevo was under siege by Serbian forces already implicated in multiple genocides. Dictators, whether communist, fascist or merely kleptocratic all depend on total control of the means of communication. The Internet poses a challenge to that control and thus the long term survival of their regimes. If not for the fact that the Internet has become the engine of the new global economy and is thus essential for the dictator's short term survival, the Internet would undoubtedly be banned.

Lenin once defined a capitalist as someone who will sell you the rope to hang him with. The Internet represents an elegant reply: The United States has gifted dictatorial regimes around the world a rope with which they are quietly but efficiently hanging themselves.

Security of the DNS

Contrary to what its name implies, DNS Security (DNSSEC) is not a security solution for the DNS. Deployment of DNSSEC is thus no panacea for the Internet security issues affecting ICANN.

Attempts to deploy DNSSEC have thus far spanned over fifteen years. In the meantime the uses of the DNS have changed dramatically and a commercial infrastructure of commercial Certificate Authorities has been established. Current plans for deployment of DNSSEC require participation by parties who are clearly uninterested in the task while unnecessarily excluding the CAs who are specialists. Moreover, as was previously demonstrated, the provision for root key management by ICANN is profoundly destabilizing of the entire ICANN system.

Purpose of DNSSEC

DNSSEC was originally designed in the early 1990s to provide a Public Key Infrastructure (PKI) for the Internet using the DNS as the base. As such the design of DNSSEC has many similarities (and some notable differences) to the design of the X.509v3 based technology adopted by Netscape in 1995, that has since become established as the industry standard.

As such, the original architecture of DNSSEC is entirely reasonable: It attempts to create a simple but effective mechanism for public key distribution using the Internet directory system (the DNS) as the base in the same way that X.509 was originally designed to leverage X.500, the now obsolete directory system designed to support OSI networking. In order to do, DNSSEC provides cryptographic security controls to protect the *integrity of information published by the DNS*.

Authentication of DNS data

A basic principle of computer system engineering is known as 'garbage-in, garbage-out'. DNSSEC only provides security for information that comes out of the DNS. It does nothing for the security of the information going into the DNS.

Even though the DNS protocols have known security vulnerabilities to man-in-the-middle substitution attacks, the vast majority of actual criminal attacks have come from an attacker impersonating the legitimate domain name holder and persuading the registrar responsible for administering the name to perform an unauthorized change to the domain name.

While DNS registrars are nominally the authoritative source of information on DNS name holders, almost none have infrastructure designed to manage the process securely. Mere provision of an authenticated means of publishing non-authenticated data does not significantly reduce risk.

Competition from SSL/TLS

The chief obstacle to deployment of DNSSEC today is the fact that Secure Sockets Layer (SSL), subsequently renamed Transport Layer Security (TLS) already provides greater security functionality.

DNSSEC as currently designed secures the relationship between a DNS name (example.com) and an IP address (10.2.3.4). The security provided by DNSSEC is thus contingent on the security of the Internet routing infrastructure (known as BGP). Not only is BGP not secure, we currently have no agreed approach to securing it.

SSL on the other hand, at a minimum, secures the relationship between a DNS name and an Internet service endpoint. Using SSL and a Domain Validated digital certificate (the lowest level of security offered commercially) provides a connection that remains secure even if the BGP routing layer is compromised.

While this level of security is higher than the level that DNSSEC is designed to achieve, it still only demonstrates that the party running a server bought a DNS domain name. For most business transactions, we would like to establish *accountability*. This is the purpose for which Extended Validation certificates are designed.

Signing the Root

The current DNSSEC design envisions a monolithic PKI hierarchy with the DNS root zone (i.e. ICANN) at the apex of the hierarchy.

While such designs have been frequently proposed, none has ever successfully deployed. It was the argument over management of the root zone that ultimately led to the collapse of the IETF Privacy

Enhanced Mail (PEM) project and the emergence of Phil Zimmerman's Pretty Good Privacy (PGP) alternative.

While modern Internet applications do in fact use the X.509 PKI technology employed in PEM, they do so with one major modification: There is no ultimate root authority.

Even the US Federal government, an organization whose executive functions are constitutionally embodied in a single individual has no single root certificate. The Federal Bridge CA was constructed for political reasons, not technical needs: The US Federal agencies could not come to agreement as to who would manage the root.

The single rooted hierarchy concentrates power at the apex of the DNS infrastructure. Such a concentration of power would be highly undesirable even if DNSSEC as presently designed provided a compelling security benefit.

Sunk Costs Fallacy

One of the great frustrations of observing progress of DNSSEC over the past fifteen years has been the constant invocation of the sunk costs fallacy. In 2000, myself and others pointed out that certain technical aspects of DNSSEC made it impractical to deploy in large TLDs such as .com. Instead of the technical requirement being accepted as a necessary criteria for deployment, the requirement was resisted for almost five years.

The same thing occurred some years later when it was pointed out that other technical aspects of DNSSEC were incompatible with the European Union Privacy Directive. Instead of accepting the minimal technical changes required to legally deploy DNSSEC in .de and .uk, the working group charged with developing the DNSSEC specification argued amongst itself for two years.

Fifteen years after work on DNSSEC begun, the specification is still not ready for deployment and lacks endorsement by any major platform or application vendor.

Dysfunctional Relationship to the IETF

One of the key reasons that ICANN has failed to meet the expectations of many ICANN participants is the dysfunctional relationship between ICANN and the IETF. Three times a year, hundreds of people attend ICANN meetings around the world in the hope and expectation that their input will lead to improvements in the security and internationalization of the DNS. Then nothing happens as the true technical standards making power lies in the IETF, a consensus based organization in which each individual participant is considered to represent nobody but themselves.

Such a system cannot but fail to meet the reasonable expectations of ICANN participants. ICANN openly solicits public input, dutifully writes it down and does nothing with it.

While this relationship is clearly dysfunctional from the ICANN perspective, it is not necessarily considered so by IETF participants. Indeed one prominent participant in both ICANN and IETF suggested that such a state of affairs is positively desirable as the ICANN process is rather too inclusive in his view.

An even more troubling aspect of the relationship between ICANN and the IETF is that the IETF is a subdivision of ISOC which in turn has a contractual relationship with ICANN through participation in the .org registry contract. This arrangement represents a clear conflict of interest for the parties concerned. It was abundantly clear to any potential bidder for the .org registry contract that the ISOC/Afilias bid would be the winner.

Alternative Approaches

At present ICANN creates more obstacles to the deployment of an effective DNS security infrastructure than it removes. The insistence on deployment of a fifteen-year-old architecture that only serves to permanently entrench ICANN control is counterproductive. ICANN should instead focus on redefining and refocusing the DNSSEC architecture so that it builds a common interest with other stakeholders rather than treating them as rivals.

National Stakeholders

Rather than attempting to use DNSSEC as an excuse to extend its control of the DNS infrastructure, ICANN should accept that this is not going to be acceptable to other national stakeholders.

The US cannot secure the Internet by itself. A DNSSEC solution that only creates a signatory role for the US will only be supported by the US. A DNSSEC technical solution that creates multiple apex signatory roles has the potential to co-opt national stakeholders that are opposed to the current proposal.

Certificate Authorities

Over a hundred commercial Certificate Authorities have jointly issued over a million existing domain validated SSL certificates. Rather than treating SSL as a rival technology to be replaced, ICANN should look for technical measures that allow this existing resource to be leveraged to 'bootstrap' DNS security.

Recommendations

While ICANN and many members of the Internet Community have argued that the US should relinquish its role in the administration of ICANN, this is not currently a viable option. While the continued US role in the administration of ICANN represents a liability rather than an opportunity for the US, the alternative of leaving ICANN effectively answerable to no-one is worse for all concerned.

Before agreeing to an extension of the JPA the Department of Commerce should:

- Specify the objectives of ICANN to be stability, security, openness and accountability.
- Require that ICANN propose a technical solution for signing of the DNS root zone that is endorsed by a clear majority of the national stakeholders.
- Require ICANN to develop a technical infrastructure enabling competition for the supply of registry services in the .com zone.

- Require ICANN to cease activities designed to merely increase revenues.
- Require substantial restructuring of the conflicted ISOC management of the .org domain replacing this backdoor subsidy with an explicit grant.