Statement of Steve DelBianco

Executive Director

NetChoice

Testimony before the

House Committee on Small Business

Hearing on

Contracting the Internet: Does ICANN create a barrier to small business?

June 7, 2006

Chairman Manzullo, Ranking Member Velazquez, and distinguished members of the Committee: My name is Steve DelBianco, and I would like to thank you for holding this important hearing. I'm pleased to testify on how ICANN's new Registry contract affects small businesses that are increasingly doing their business online.

I serve as Executive Director of NetChoice, a coalition of trade associations and e-commerce leaders such as eBay, Yahoo, VeriSign, and AOL, plus over 18,000 small e-commerce retailers. At both the state and federal level, NetChoice advocates against regulatory barriers to e-commerce. NetChoice members are familiar with the process of registering their domain names, building websites, and conducting e-commerce as both buyers and sellers. We are also concerned with growing threats to internet security, so we appreciate the importance of fast and reliable resolution of domain names.

I also appear before you as a genuine "small business survivor." In 1984 I founded an information technology consulting firm, and grew it to $20 million in sales and 200 employees before selling the business to a national firm. After that experience, I was drawn to Washington to help start a trade association that focused on the needs of small IT businesses like mine.

The title of today's hearing poses a rather complex question, but the answer from small business is simple: *Small business needs an Internet <u>that works</u>.* Our customers and suppliers must be able to quickly and reliably get to our website, buy online, check the status of an order, or just find the address of our nearest store. We need security and stability, and we're willing to help pay the costs to get a secure and stable Internet.

Internet Exposure and Commerce are Vital for Small Business

Small businesses are more competitive and viable when they have an Internet presence. Over three-quarters of small businesses say their website generates leads and that their business enjoys a competitive advantage or stronger economic footing because they have a website.[1] Of those businesses that don't have their own websites, nearly all want customers to find their business address and phone number in online "yellow pages".

[1] Source: eMarketer

Online retailers realized $172B from consumer sales in 2005 and expect over $300B by 2010, according to Forrester. Consumers use the Internet not only for routine purchases, but also for banking and online bill payment. A Harris Interactive poll found that online bill payment is catching-up with paper, as 35% of consumers now pay bills online, compared to 37% who still pay by check.

As consumers become confident with online banking and buying, they grow to depend on a secure and reliable Internet. But small businesses feel a growing concern with threats to the Internet's security and stability.

The Internet is Under Attack

The Internet has seen at least seven major attacks in the past six years. Recent attacks have targeted domain name servers, then hijacked those servers to amplify and accelerate the attacks. This year, a distributed denial-of-service attack disabled 1,500 websites using 32,000 hijacked computers.[2] Symantec estimates that denial-of-service attacks rose 51 per cent in the second half of last year, averaging 1,400 attacks per day.

These attacks can cripple the website of a small business, and they are becoming more widespread and destructive. Moreover, small businesses are experiencing *blackmail* via denial-of-service attacks, where a business owner is forced to pay-up in order to stop the attack.[3]

Attacks on the domain name system are also harming online consumers. Attackers can redirect web browsers to fraudulent sites containing very convincing scams. Increased security measures can help, but hackers and scam artists are creative and adaptive with their tactics. The bottom line for small business is that our customers face increasing threats to their ability to access our websites and to buy online. Who do we look to for help?

Who's Looking After the Security and Stability of Internet Domain Names?

For purposes of this hearing, there are four players who have a stake in keeping the domain name system safe and reliable:

- **ICANN**—The Internet Corporation for Assigned Names and Numbers is responsible for coordinating the management of the technical elements of the

[2] DDoS attacks are conducted by controlling and compromising multiple computers—by the use of "zombies" or "bots"—to send a flood of queries against a targeted website. DDoS attacks generally overload the target's network with a high volume of traffic while simultaneously opening many web pages so that the site runs out of resources to handle legitimate requests. See http://www.symantec.com/avcenter/venc/data/ddos.attacks.html

[3] Daniel Thomas, "Websites face more attacks – BLACKMAIL" *Financial Times*, May 31, 2006.

Domain Name System (DNS) so that Internet users can access websites and route their email to the right place. ICANN enters contracts with businesses to operate the DNS and distribute domain names to users.

- **Registry Operators** — Businesses who maintain the database and systems to map domain names to their matching Internet addresses. Each Internet domain (.com, .org, .info, .net) is managed by a registry operator, under an exclusive contract with ICANN. Dot-com is operated by VeriSign, whose new registry contract is the subject of this hearing.
- **Registrars**—A business that resells domain names. GoDaddy and Network Solutions are among the largest registrars for the dot-com domain. There are 650 current dot-com registrars, which suggests there are no barriers to small firms seeking to enter the domain name registration business.
- **Domain name owners**—Individuals, businesses, and organizations who purchase domain names to establish their presence on the Internet.

While there are probably a few hundred small businesses operating as registrars, nearly all of America's millions of small businesses find themselves in the fourth category, as domain name owners. It's their perspective that we'll take in answering the question of whether ICANN's new registry contract poses any barriers to small business.

Small Business is Willing to Pay for Better Security and Reliability

At the same time the Internet is under attack, the volume of Internet domain-name queries is growing rapidly. A winning Internet security strategy calls for more than just a defense against known attacks and a readiness to repel new attack types. There must also be an investment plan to maintain and improve the Internet's performance under ever-increasing demands.

For small businesses, protecting their electronic storefronts is equivalent to buying surveillance cameras and hiring security guards for their physical locations. Companies already spend money on security for their own systems within their firewall. But security on the other side of the firewall is beyond their control. Small business needs—and is willing to help pay for—an Internet that is reliable and secure.

One criticism of ICANN's new registry contract is that domain name owners would face "unjust price increases" because annual fees may rise by less than $2 over the next six years[4]. From a small business perspective, this price increase would be a trivial matter compared to real concerns about the domain name system.

A national poll sponsored by the Association for Competitive Technology (ACT) found that small business owners widely consider their website domain name a good value for the

[4] John Berard of CFIT, in Warren's Washington Internet Daily, Vol. 7, No. 106, June 2, 2006, page 2.

money, and they place greater value on ensuring a higher-performing Internet than on keeping domain name prices low.[5]

Public Opinion Strategies conducted the poll just after ICANN approved its new dot-com contract. The poll focused on micro-businesses that are highly-sensitive to increased costs of doing business. More than half of the businesses surveyed had 3 or fewer employees and 87 percent had 10 or less.

62 percent of businesses preferred having a more reliable and better performing Internet, instead of keeping the cost of domain name prices low. The percentages are higher for businesses that rely heavily on the internet for e-commerce and communications, where 70 percent of respondents were more concerned about reliability. Eighty-four percent said that a less reliable Internet with slower speeds and periodic outages would have a negative impact on their business—including 56 percent who said it would have a major negative impact.

The message is clear—small business relies on the Internet for exposure and for e-commerce. Threats to the Internet security threaten their business. Small businesses would rather incur a small price increase for stability and security than face domain name disruptions.

Small Business Sees No Barriers in the New Registry Contract.

This hearing is entitled "*Contracting the Internet: Does ICANN create a barrier to small business?"* It's clear that price is not a barrier to a small business seeking its own domain name. Polls confirm that small business values a secure and reliable Internet and is willing to pay a modest price increase for more of the same.

Another complaint discussed today is that an exclusive contract with a right to renewal creates a "perpetual monopoly" that poses a barrier to small business. When we examine this complaint from the perspective of small business, it's clear that the registry contract *must* be exclusive so that one vendor is responsible and accountable. And the renewal option is an appropriate incentive for the registry operator to invest in Internet security and stability.

[5] See http://www.actonline.org/prdetail.aspx?PRID=60

Registry Contracts <u>Should</u> be Exclusive Contracts

Registrars and would-be registry operators complain that an exclusive registry contract creates a monopoly and denies the normal benefits of competition. However, this complaint loses its sting when you consider the nature of the services covered under this contract.

An exclusive contract is essential to focus responsibility and accountability on the vendor running a registry. The same is true for many outsourcing contracts that require accountability and consistency in the delivery of critical services, especially for infrastructure services that require significant investments.

For example, businesses typically select a single vendor to provide building security services. An exclusive contract keeps the vendor fully accountable for building security. A high-value, long-term contract could further motivate the vendor to invest in security systems and better employee training.

On the flipside, small businesses frequently seek contracts to become the exclusive vendor for a larger business customer. If selected, the small business typically invests significant resources to ramp-up its operations and capabilities to fulfill the contract requirements. Here in the Rayburn Building, you see everyday examples of exclusive agreements, for building maintenance and operation of the cafeteria downstairs.

The Renewal Option is an Appropriate Incentive for Investment

The renewal terms in ICANN's registry contracts are being criticized as anti-competitive. But those making the complaint ought to know better. Renewal options are actually common in longer-term service contracts to provide incentives for making investments that improve contract performance.

There are many forms of the renewal option in ICANN's registry contracts. The operators of the cafeteria downstairs might invest in a new grill or espresso machine if they're confident that their contract would be renewed upon expiration. Landlords often give tenants a purchase option as an incentive to maintain and improve the property.

I have some first-hand experience with service contracts, since my own business was selected to provide software help-desk support for a large credit card company. I invested heavily in hiring and training help-desk staff, rented new space for the operation, acquired new computers and an integrated call management system. We even bought electronic scrolling sign boards to alert the staff about callers in the queue and hold times.

To have any hope of recovering this huge up-front investment, I insisted on renewal terms that gave us a favorable chance to renew the contract after its initial term. To earn the renewal, we had to satisfy several metrics for service levels. In addition, we could not have any sustained failures to meet new or emergency initiatives that could be expected over the term of the contract. "Best efforts" wouldn't be good enough—we had to be able to recover and deliver if unexpected call volumes hit us out of the blue.

My experience is fairly typical, and tells me that ICANN is right to include a renewal option in its registry contracts. While a renewal option helps the incumbent to retain the contract upon expiration, the incumbent will lose the contract if it fails to satisfy the functional requirements in the new contract.

The performance requirements ICANN has set to earn renewal are imposing, especially when you consider the open-ended responsibilities imposed on the registry operator. Contract sections 3.1(a) and (b) require the Registry operator to meet any future "consensus policy" adopted by ICANN to improve security and stability and to resolve disputes about domain names.

Small business appreciates ICANN's anticipation of new security and stability challenges, and we appreciate ICANN's ability to negotiate such open-ended requirements into its registry contract. While such open-ended obligations could be very difficult for any operator to fulfill, NetChoice would be among those arguing against renewal if an incumbent registry operator failed to meet the contract's performance requirements.

To summarize so far, a renewal option is appropriate for ICANN's registry contracts, since small businesses want ICANN and its registry operators to spend whatever it takes to address the stability and security of the Internet's domain name systems. And the discussion above counters complaints about exclusivity and the domain name price increases allowed in ICANN's proposed registry contracts. Below, we suggest the real motivation behind the complaints of a few businesses, and conclude with a discussion of what really concerns small business about the domain name system.

Loss of Leverage is What's Really Bothering the Big Registrars

As noted above, small business isn't concerned about a $2 increase in domain name fees, and nothing about ICANN's new registry contract presents any barriers to the small businesses that rely on the domain name system for their websites, e-commerce, and e-mail. So, what's really behind the complaints that motivated this hearing? I suggest the real issue

is that a few large registrars will lose some of their leverage over ICANN once the new contract takes effect.

As I understand it, the largest domain name resellers, or registrars, currently exercise control over ICANN's budget, and thereby influence ICANN policies that affect how the resellers do business. Resellers have this control because ICANN must obtain their approval to assess the "Registrar Variable Fee" that provides for most of ICANN's funding. I find this perplexing, since businesses and consumers are paying these fees for their domain names, yet resellers can withhold our fees from ICANN in order to give themselves leverage and control over ICANN policies.

In that regard, these resellers act like a legislative appropriations committee. ICANN cannot fund its operations or make significant policy changes without the approval of domain name resellers.

Moreover, the current ICANN funding agreements require that two-thirds of the registrars must approve the fees they will pay to ICANN, which gives even more control to a few of the largest registrars. This has forced ICANN management to make concessions to the largest registrars in exchange for their approval to fund ICANN. I attended the ICANN meeting in Vancouver last December, where the chair of ICANN's Finance Committee complained that ICANN expenditures were being delayed and possibly diminished because registrars had not yet approved the fees in the budget that was adopted for 2005-06.

ICANN's new registry contract, however, would reduce some of the leverage held by the large registrars, since the registry operator would be contributing a greater share of ICANN's fees. ICANN wants this change for dot-com and for all future registry contracts, since it would increase operating revenue while decreasing the leverage of large resellers with their own agendas. Moreover, ICANN is anxious to demonstrate to the world community and to the U.S. government that it is independent and adequately funded by guaranteed revenue—with no strings attached.

When they make decisions and investments to ensure the Internet's security and stability, ICANN and its registry operators <u>should not</u> be held-up by registrars who have little interest in either security or stability. Registrars compete via branding campaigns and by running users through a gauntlet of value-added services (some of dubious value). Their relative competitive position is not affected by domain name performance since all registrars resell the same batch of domain names.

If ICANN and its registry operators have to beg a "permission slip" from registrars for every security investment, the Internet infrastructure will not be as responsive to new threats and the demands of growing traffic. The approval process would be painfully slow, and integrated technical proposal would be picked-apart by conflicting stakeholders.

From all appearances, the loss of some registrar leverage is why Network Solutions and GoDaddy have pushed the Committee to hold this hearing. They, like resellers in many industries facing change, don't want to lose any of their leverage on wholesalers and manufacturers. However, ICANN needs to reduce the leverage held by resellers, and the new registry contract terms do just that.

What Really Concerns Small Business? *Domain Name Abuses and the Specter of the UN Taking Control of the Internet.*

Small businesses have little concern about modest price increases for domain names when that money goes towards Internet security and stability. And none of the complaints about the registry contract present barriers to small businesses that use the Internet. Since the Committee seeks to know what concerns small business about the business of domain names, we turn now to our two real concerns: abuses of the domain name system; and the idea that the United Nations has designs on "governing" the Internet.

Abusive Internet Practices Harm Small Businesses

While ICANN's registry contract addresses security and stability, there are other important concerns for small business. The domain name arena is fraught with abusive, fraudulent and unfair practices that hurt small businesses. These practices decrease the value and increase the cost of domain names and are misleading to potential customers.

Cybersquatting

Cybersquatting occurs when speculators buy domain names that are closely related to the names of other businesses, with the intent to sell these domain names at a big markup over the actual registration cost. Victims of cybersquatting can sue under a 1999 federal law known as the Anti-Cybersquatting Consumer Protection Act, and can initiate arbitration proceedings under the authority of ICANN.

For a small business, the time and expenditures necessary to understand and assert these legal remedies are often more than the owner can afford. Consequently, most small

businesses either continue to lose prospects to cybersquatters, or are conned into paying ransom for the related domain name.

Parking

A "parked" website is one that closely resembles a popular domain name, but is designed to exploit a user's misspelling or typographical errors. Small business is harmed when its potential customers are misled by these sites. Based solely on traffic generated by user errors, parking sites earn easy money when users click on ads displayed on the page.

For example, I tried a few typographical variations on 1800Contacts.com, the leading telephone and online seller of replacement contact lenses, and a NetChoice coalition member. If I type 18OOcontacts.com instead of 1800contacts.com (letter O instead of numeral zero), I arrive at a page designed to steer me into buying contacts from competing lens sellers.

18OOcontacts.com points to a server owned by Sedo, the current leader in "Parking" domain names.[6] Sedo's parking site is designed to generate ad revenue when users who intended to go to 1800Contacts start clicking on sponsored links—*for other lens sellers*. (screen capture shown below).[7]

[6] For information about Sedo, see http://www.sedo.co.uk/about/index.php3?tracked=&partnerid=&language=e

[7] See http://www.18oocontacts.com/

When I click on the 1800Contacts.com link that often shows on this page, I am re-directed to yet another page showing ads for other lens sellers. In other words, the hyperlink for 1800Contacts.com is falsely labeled in order to generate.

Parking sites confuse and divert potential customers. 46% of users prefer to type the domain name of a known website directly into the browser's address bar.[8] But when typos happen, legitimate businesses shouldn't lose customers who fall into traps designed to generate ad revenue. What's more, the ad revenue generated by parking drives up the price if the intended business tries to acquire the domain from the parking operator.

Expiration Extortion

"*Expiration Extortion*" describes a common Registrar practice of forcing a domain owner to pay an exorbitant ransom to reinstate a name that's been allowed to expire. GoDaddy, for instance, informed me that for $80 they would reinstate a domain name for

[8] North America Domain Name Study, Windward Directives, June 2005.

which I had paid GoDaddy only $8 to initially register. *Expiration Extortion* also describes the speculative game of snatching expiring domain names for resale to their former owner – or to the highest bidder.

Domain names are generally registered only for a year, although most owners renew before the year is up. Among all registrants, the average term for domain registration is 1.3 years.[9] Last year, the renewal rate for dot-com and dot-net domain names was 75%. That means 25% of names aren't renewed, so every day there's an average of 22,000 expiring domain names released by registries.

A company called Pool.com has perfected the science of snatching domain names as they expire, or "drop". Pool runs 80 servers in Sterling, Virginia that fire into action every day when dropped domain names are released at 2pm. According to Pool.com's president, Taryn Naidu, "*It's like going to the horse races every day*."[10] The race is won by whichever company, blasting multiple commands per second, snatches the dropped domain name.

Imagine if Pool.com were in the business of buying expired auto registrations instead of expiring domain names. Pool could snag your car registration if you failed to renew it by the expiration date, then sell the registration back to you or to another bidder who's willing to pay more.

Small businesses are increasingly frustrated and concerned about abusive domain name practices like parking, cybersquatting, and expiration extortion. ICANN acknowledges these concerns in the Covenants of its new Registry Agreement, where it indicates the potential for "prohibitions on warehousing of or speculation in domain names by registries or registrars."[11]

Next, I'll describe an even more frightening threat to the future of the Internet; a threat that may be fended-off if ICANN's new registry contracts help it become stronger and more independent.

---

[9] ASCII Com/Net for Q1 2006

[10] As quoted by Peter Hum, "The New Cybersquatting: What'$ in a Name," The Ottawa Citizen, March 16, 2006.

[11] Draft Registry Agreement, Section III.1(b), page 4, at http://www.icann.org/topics/vrsn-settlement/revised-com-agreement-clean-29jan06.pdf

The Internet Needs a Manager, But the UN Wants to be <u>Governor</u>

There's a growing risk that ICANN's technical role for managing domain names would be usurped by the United Nations. The World Summit on the Information Society (WSIS), a UN agency that studies technological development, met last November in Tunisia to discuss Internet Governance. The UN Working Group on Internet Governance (WGIG) released a report last June that included controversial policy recommendations for the future of the Internet. Thanks in part to a unified message from Congress, representatives from the broader international community agreed to let ICANN continue managing the Internet under U.S. oversight – for the time being.

Truth is, the Internet needs a manager—not a governor. ICANN has a limited technical role and works with private sector interests who have invested a trillion dollars to bring Internet connections to over a billion people around the world.

Governments, on the other hand, are too ready to regulate when problems arise, have an unlimited appetite for expansion, and are accustomed to the powers of taxation. Imagine an expanding ICANN, under pressure from worldwide governments, using the Internet to advance a range of social welfare programs. A tax, or "contribution," would be levied on domain names to fund programs to "bridge the digital divide" and promote local content.

While ICANN is far from a perfect manager, it provides the needed separation between Internet technical operations and governments. According to the Center for Democracy & Technology, ICANN's bottom-up coordination of technical functions is the best way to preserve the democratic and decentralized character of the Internet.

If there's anything that everyone at today's hearing should be able to agree upon, it's that we need ICANN to be strong and independent so it can fend-off interference from the UN and from governments. The new dot-com contract provides ICANN with enough revenue to perform its technical role and resist influence from governmental bodies – including the U.S. government. We should focus our efforts on how to stabilize and strengthen ICANN, not second-guess its contracts for technical operation of the Internet.

Conclusion

ICANN is a work-in-progress on the way to a bold and optimistic vision. I can think of no precedent for a multi-national, public-private partnership to manage an enterprise as complex and dynamic as the Internet. ICANN has made progress in its 7 year history, but it needs more financial and operational independence to meet its mandate for a secure and reliable Internet.

The Internet has become an irresistible target for hackers, criminals, and unfair or deceptive practices, all of which are concerns to small business that rely heavily on their websites, e-commerce, and e-mail services. Small businesses are understandably upset when our customers are confused or diverted, when our domain names are held for ransom, and when we hear the UN seeks to control the Internet.

ICANN's new Registry contract provides incentives for a strong defense against these threats, and incentives to improve performance of domain name services. Moreover, it provides ICANN with adequate and reliable revenues to react to new security threats while managing challenges brought on by the Internet's exponential growth.

Compared to these real concerns, the complaints that provoked today's hearing are inconsequential distractions that do not nearly warrant Congressional interference with ICANN's effort to adopt a new registry contract. I close by thanking the Committee for considering the concerns of small business about the domain name system, and I look forward to your questions.