S. HRG. 109–1152

INTERNET GOVERNANCE: THE FUTURE OF ICANN

HEARING

BEFORE THE

SUBCOMMITTEE ON TRADE, TOURISM, AND ECONOMIC DEVELOPMENT

OF THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

SEPTEMBER 20, 2006

Printed for the use of the Committee on Commerce, Science, and Transportation

U.S. GOVERNMENT PRINTING OFFICE

71–638 PDF WASHINGTON : 2011

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

TED STEVENS, Alaska, *Chairman*

JOHN MCCAIN, Arizona
CONRAD BURNS, Montana
TRENT LOTT, Mississippi
KAY BAILEY HUTCHISON, Texas
OLYMPIA J. SNOWE, Maine
GORDON H. SMITH, Oregon
JOHN ENSIGN, Nevada
GEORGE ALLEN, Virginia
JOHN E. SUNUNU, New Hampshire
JIM DEMINT, South Carolina
DAVID VITTER, Louisiana

DANIEL K. INOUYE, Hawaii, *Co-Chairman*
JOHN D. ROCKEFELLER IV, West Virginia
JOHN F. KERRY, Massachusetts
BYRON L. DORGAN, North Dakota
BARBARA BOXER, California
BILL NELSON, Florida
MARIA CANTWELL, Washington
FRANK R. LAUTENBERG, New Jersey
E. BENJAMIN NELSON, Nebraska
MARK PRYOR, Arkansas

LISA J. SUTHERLAND, *Republican Staff Director*
CHRISTINE DRAGER KURTH, *Republican Deputy Staff Director*
KENNETH R. NAHIGIAN, *Republican Chief Counsel*
MARGARET L. CUMMISKY, *Democratic Staff Director and Chief Counsel*
SAMUEL E. WHITEHORN, *Democratic Deputy Staff Director and General Counsel*
LILA HARPER HELMS, *Democratic Policy Director*

SUBCOMMITTEE ON TRADE, TOURISM, AND ECONOMIC DEVELOPMENT

GORDON H. SMITH, Oregon, *Chairman*

TED STEVENS, Alaska
JOHN MCCAIN, Arizona
CONRAD BURNS, Montana
JOHN ENSIGN, Nevada
GEORGE ALLEN, Virginia
JOHN E. SUNUNU, New Hampshire
JIM DEMINT, South Carolina
DAVID VITTER, Louisiana

BYRON L. DORGAN, North Dakota, *Ranking*
DANIEL K. INOUYE, Hawaii
JOHN D. ROCKEFELLER IV, West Virginia
JOHN F. KERRY, Massachusetts
MARIA CANTWELL, Washington
FRANK R. LAUTENBERG, New Jersey
BILL NELSON, Florida
E. BENJAMIN NELSON, Nebraska
MARK PRYOR, Arkansas

CONTENTS

WITNESSES

APPENDIX

INTERNET GOVERNANCE: THE FUTURE OF ICANN

WEDNESDAY, SEPTEMBER 20, 2006

U.S. SENATE,
SUBCOMMITTEE ON TRADE, TOURISM, AND ECONOMIC DEVELOPMENT,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Subcommittee met, pursuant to notice, at 10:05 a.m. in room SR–253, Russell Senate Office Building, Hon. Ted Stevens, Chairman of the Committee, presiding.

OPENING STATEMENT OF HON. TED STEVENS, U.S. SENATOR FROM ALASKA

The CHAIRMAN. Let me start this hearing.

Senator Smith has been delayed. He will be along. I do thank him for scheduling this hearing on ICANN, and we want to thank the witnesses for coming to participate.

We're proud that the Internet was developed with research funding from the Department of Defense Advanced Research Project Agency to establish a military network. Today, the Internet continues to evolve and flourish, mostly through private investment. One critical part of the Internet is the management of domain names, and ICANN is the nonprofit corporation responsible for coordinating the management of the technical elements of the domain-name system of the Internet. It also oversees the distribution of identifiers used in Internet operations.

When ICANN was created, it was expected to transition into a freestanding, financially sound organization by the year 2000. The Department of Commerce extended this Memorandum of Understanding with ICANN several times, and the current MOU is set to expire within 1 month. ICANN's current system for managing the domain-name system is working, but the feeling is that more needs to be done to improve the process and transparency. And we're going to look forward to the statement of witnesses here today.

Senator Burns, do you have any comments?

STATEMENT OF HON. CONRAD BURNS, U.S. SENATOR FROM MONTANA

Senator BURNS. Well, no, Mr. Chairman, but I would say that there's quite a lot of interest in this, and to make sure that this moves forward, especially this issue between the two entities of ICANN and VeriSign, and make sure that they've got the resources

for an ever-increasing load that they have to handle. I look forward to getting an update. That's the reason I'm here today; I want an update on where we are on this process, because it's a very tender and—it's a very important issue, as far as the operation of the Internet is concerned.

So, thank you for this hearing, and we might get going to the witnesses.

The CHAIRMAN. Yes, we'll reserve the space at the beginning of the hearing for Senator Smith's statement that he may wish to put in the record.

Our first witnesses are John Kneuer, the Assistant Secretary for Communications and Information of the Department of Commerce, and Jon Leibowitz, Commissioner of the Federal Trade Commission.

I assume that it's all right if you start, Mr. Kneuer.

STATEMENT OF JOHN M.R. KNEUER, ACTING ASSISTANT SECRETARY FOR COMMUNICATIONS AND INFORMATION, NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION, DEPARTMENT OF COMMERCE

Mr. KNEUER. Thank you. Thank you, Chairman Stevens, Senator Burns, for this opportunity to testify before you on the progress of ICANN in meeting its obligations under its MOU with the Department of Commerce.

The Department continues to believe that the stability and security of the Internet domain name and addressing system can best be achieved by transitioning the coordination of the technical functions related to the management of DNS to the private sector. The vehicle for achieving this goal is the MOU between the Department and ICANN.

The CHAIRMAN. Can you pull that mike a little bit toward you, please? Thank you.

Mr. KNEUER. As the Committee will recall, ICANN was formed in 1998 in response to the Department of Commerce's call for a partner to lead the transition to the private-sector management of the DNS. The Department plays no role in the internal governance or day-to-day operations of ICANN; however, under the terms of the MOU, we offer expertise and advice on the transition, and monitor ICANN's performance of the MOU tasks.

The current MOU was deliberately crafted to permit the Department and ICANN to measure progress toward concrete goals and objectives. When this current MOU was entered into, in September 2003, ICANN had just completed an internal review and reform effort. As well, ICANN was in the process of implementing the structural and organizational changes that would be necessary to complete that process. In the course of the past 3 years, ICANN has successfully met many of the MOU's date-specific milestones.

The current MOU expires on September 30, 2006. Over the course of the past year, the Department has conducted an internal review of its relationship with ICANN. To complement the Department's internal review, NTIA initiated a public consultation process to obtain views of all interested stakeholders in ICANN. We received and analyzed over 700 written responses from individuals, private corporations, trade associations, nongovernmental entities,

and foreign governments. The public consultation revealed broad support for continuing the transition of the DNS to the private sector through a continued partnership between the Department and ICANN. A majority of interested stakeholders continue to endorse the original principles put forth in the DNS transition: stability and security, competition, bottom-up policy coordination, and broad representation. Equally important, the consultation process revealed strong support for more specific focus on transparency and accountability, and the continued involvement of the Department of Commerce in this transition.

As we approach the end of the term of this MOU, we are working with ICANN to negotiate the next phase of our continued partnership.

I would also like to focus briefly on the WHOIS database. The U.S. Government continues to believe that ICANN should enforce the existing contractual obligations of domain name registrars and registries in the collection and maintenance of accurate registrant contact data. The Department and other U.S. agencies strongly support continued timely access to accurate and publicly available WHOIS data. We believe WHOIS data is critical to meeting a variety of public policy objectives, including those of law enforcement and intellectual property concerns.

In conclusion, the Department continues to be supportive of the private-sector leadership in the coordination of the DNS. The Department continues to support the work of ICANN as the coordinator of these technical functions. Both ICANN and the Department agree that preserving the security and stability of the Internet DNS is a critical priority that will guide the next stage in the transition process.

Thank you, and I'll be happy to answer any questions.

[The prepared statement of Mr. Kneuer follows:]

PREPARED STATEMENT OF JOHN M.R. KNEUER, ACTING ASSISTANT SECRETARY FOR COMMUNICATIONS AND INFORMATION, NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION, DEPARTMENT OF COMMERCE

Mr. Chairman,

Thank you and the members of the Committee for this opportunity to testify on the progress of the Internet Corporation for Assigned Names and Numbers (ICANN) under the Memorandum of Understanding (MOU) between ICANN and the Department.

The Administration recognizes the critical importance of the Internet to the economic and social well-being of the United States and the global community, and is committed to its future growth. The Department has been charged with preserving the stability and security of the Internet's underlying infrastructure—the domain name and addressing system. I am pleased to have this opportunity to share the results of our efforts to date, as well as our perspective for the future.

The Department's Relationship With ICANN

The Department continues to believe that the stability and security of the Internet domain name and addressing system (DNS) can best be achieved by transitioning the coordination of the technical functions related to the management of the DNS to the private sector. The vehicle for achieving this goal is the MOU between the Department and ICANN. As the Committee will recall, ICANN was formed in 1998 in response to the Department of Commerce's call for a partner to lead the transition to private sector management of the DNS.

In September 2003, the Department and ICANN agreed to renew the MOU for a period of 3 years, with several date-specific milestones and broad tasks aimed at guiding ICANN to a stable, independent, and sustainable organization. The expectation of the Department was that the three-year timeframe would allow ICANN suffi-

cient opportunity to formalize appropriate relationships with the organizations that form the technical underpinnings of the Internet, secure the necessary resources to ensure its long-term independence, improve its mechanisms for broad participation by all Internet stakeholders, and continue to improve its decisionmaking processes. The Department plays no role in the internal governance or day-to-day operations of the organization. However, under the terms of the MOU, the Department monitors and ensures that ICANN performs the MOU tasks, and offers expertise and advice on certain discrete issues.

As you may recall, this relationship was the focus of much debate at last year's United Nations World Summit on the Information Society. To provide clarity to this debate, the Administration issued the *U.S. Principles on the Internet's Domain Name and Addressing System.* In this set of principles, the Administration reiterated its commitment to preserving the security and stability of the Internet domain name and addressing system; recognized that governments have legitimate public policy and sovereignty concerns with respect to the management of their country code top level domains; reaffirmed its support for ICANN; and encouraged continued dialogue on Internet governance issues. After much discussion and debate, and with your help and support, the international community arrived at a consensus on the importance of maintaining the stability and security of the Internet, the effectiveness of existing Internet governance arrangements, and the importance of the private sector in day-to-day operations of the Internet.

Measuring Progress

The current MOU was deliberately crafted to permit the Department and ICANN to measure progress toward discrete goals and objectives. When this MOU was entered into in September 2003, ICANN had just completed an internal review and reform effort, and was well into the process of implementing the structural and organizational changes called for through that process. In the course of the past 3 years, ICANN has successfully met many of the MOU's date-specific milestones, which included the following:

- developing a strategic plan addressing administrative, financial and operational objectives;
- developing a contingency plan to ensure continuity of operations in the event ICANN incurs a severe disruption of such operations, by reason of bankruptcy, corporate dissolution, natural disaster or other financial, physical or operational event;
- conducting a review of corporate administrative and personnel requirements and corporate responsibility mechanisms;
- developing a financial strategy to secure more predictable and sustainable sources of revenue;
- improving its processes and procedures for the timely development and adoption of policies related to the technical management of the DNS;
- implementing reconsideration and review processes, including an Ombudsman and commercial arbitration clauses in ICANN contracts;
- developing a strategy for the introduction of new generic top level domains, including internationalized domain names;
- enhancing broader participation in ICANN processes by the global community through improved outreach, regional liaisons, and multilingual communications;
- publishing annual reports on community experiences with the WHOIS Data Problem Reports System, used to report inaccuracies in the submission of WHOIS data by domain name registrants; and
- publishing annual reports on the implementation of the WHOIS Data Reminder Policy, which domain name registrars are required to send to domain name registrants.

ICANN has also made steady progress toward the MOU's broader tasks, including: entering into an agreement with the Regional Internet Registries to facilitate the development of global addressing policy, and developing and implementing new accountability framework agreements with many country code top level domain operators.

WHOIS Policy Development

I would like to focus briefly on the WHOIS database issue. First, the U.S. Government believes that ICANN should enforce the existing contractual obligations of domain name registrars and registries for the collection and maintenance of accurate

registrant contact data. The Department and other U.S. agencies [1] strongly support continued, timely access to accurate and publicly available WHOIS data contained in the databases of information identifying registrants of domain names. We believe WHOIS data is critical to meeting a variety of public policy objectives and have been proactively advocating this position at ICANN meetings. At the most recent meeting in June 2006, the United States formally tabled a statement clarifying our perspective that a public WHOIS database is essential to:

- assist civil and criminal law enforcement in resolving cases that involve the use of the Internet, combat intellectual property infringement and theft;
- support Internet network operators responsible for the operation, security and stability of the Internet;
- protect the rights of consumers by facilitating, for example, their identification of legitimate online businesses; and
- assist business in investigating fraud, phishing, and other violations of laws.

We are continuing to advance our perspective within ICANN, including working with other governments to develop more formal public policy advice on the purpose and use of WHOIS data.

Future Relationship

The current MOU expires on September 30, 2006. Over the course of the past year, the Department has conducted an internal review of its relationship with ICANN. To complement the Department's internal review of ICANN's progress under the MOU, the National Telecommunications and Information Administration (NTIA) initiated a public consultation process to obtain the views of all interested stakeholders. In May 2006, NTIA issued a *Notice of Inquiry on the Continued Transition of the Technical Coordination and Management of the Internet Domain Name and Addressing System* to solicit views on such issues as:

- ICANN's progress in completing the core tasks and milestones contained in the current MOU, and whether these activities are sufficient for transition to private sector DNS management by the scheduled expiration date of the MOU, of September 30, 2006;
- Whether the principles underlying ICANN's core mission (*i.e.,* stability, competition, representation, bottom-up coordination and transparency) remain relevant and whether additional principles should be considered;
- Determining whether the tasks and milestones contained in the current MOU remain relevant, and/or whether new tasks would be necessary;
- Assessing whether all key stakeholders are effectively represented and involved in ICANN's activities, and if not, how that could be accomplished; and
- Whether new methods or processes should be considered to encourage greater efficiency and responsiveness.

NTIA received and analyzed over 700 responses from individuals, private corporations, trade associations, nongovernmental entities, and foreign governments. NTIA invited a representative sample of these interested stakeholders to participate in a public meeting on July 26, 2006. Representatives from the Regional Internet Registries, the root server operators, registrars, registries, country code top level domain operators, the Internet Society, the Internet research and development community, trademark interests, the user community, the business community, and a representative from the Canadian government shared their perspectives on the questions NTIA posed to the global Internet community. Well over one hundred interested stakeholders participated in the public meeting.

This public consultation process revealed broad support for continuing the transition of the coordination of the technical functions related to the management of the DNS to the private sector through the continued partnership between the Department and ICANN. A majority of interested stakeholders continue to endorse the original principles put forward to guide the DNS transition—stability and security; competition; bottom-up policy coordination; and broad representation. Equally important, the consultation process revealed strong support for a more specific focus on transparency and accountability in ICANN's internal procedures and decision-

[1] NTIA chairs an interagency ICANN Working Group composed of representatives from the Department of Commerce, the Justice Department, the Federal Trade Commission, the State Department, the Patent and Trademark Office, the Federal Bureau of Investigation, the Internal Revenue Service, and the Department of Homeland Security that develops and coordinates U.S. positions on issues pending before the ICANN Governmental Advisory Committee.

making processes, and the continued involvement of the Department of Commerce in this transition.

As we approach the end of this term of the MOU, we are working with ICANN to negotiate the next phase of our continued partnership.

Conclusion

In conclusion, the Department continues to be supportive of private sector leadership in the coordination of the technical functions related to the management of the DNS as envisioned in the ICANN model. Furthermore, the Department continues to support the work of ICANN as the coordinator for the technical functions related to the management of the Internet DNS. Both ICANN and the Department agree that preserving the security and stability of the Internet DNS is a critical priority that will guide/govern the next stage in the transition process.

Thank you and I would be happy to answer any questions that you may have.

The CHAIRMAN. Thank you.

Mr. Leibowitz?

STATEMENT OF HON. JON LEIBOWITZ, COMMISSIONER, FEDERAL TRADE COMMISSION

Mr. LEIBOWITZ. Thank you, Mr. Chairman, Senator Burns. I'm pleased to be here in this beautiful, newly renovated hearing room on behalf of the Federal Trade Commission.

I ask that the Commission's written statement be made part of the record. My oral testimony reflects my own views, and not necessarily the views of any other Commissioner.

This morning I want to focus my remarks on the importance of continued, unrestricted access to WHOIS information. Simply put, our ability to protect consumers is being placed at risk by a movement within ICANN to limit WHOIS to technical purposes only and, thus, prevent law enforcement and the public from using this critical resource to identify scammers who operate websites.

Those who want to restrict access to WHOIS databases are no doubt sincere in their efforts to protect privacy. I've met with them and I know they are. But the irony of their position is that any attempt to cabin WHOIS information so narrowly could actually jeopardize the ability of the FTC and other law enforcement authorities to protect people's privacy by stopping, for example, spam, spyware, and identity theft. That's an outcome nobody wants.

Because this is such an important issue, in June the Commission sent a delegation to the ICANN meeting in Morocco, where we joined with several of our foreign consumer protection counterparts to emphasize to ICANN the importance of access to WHOIS. We understand that in the wake of that meeting the ICANN advisory body is reevaluating its earlier decision.

Mr. Chairman, we certainly hope so, because the future of ICANN is really on the line here. It has to show the leadership necessary to properly govern the Internet.

Having said that, I've met with the ICANN Board, they do understand the seriousness of the WHOIS issue, and my strong sense is that they're committed to doing the right thing.

From our perspective at the Commission, access to WHOIS databases raises four important considerations: first, law enforcement's ability to obtain information about malefactors who use Internet websites; second, consumers' ability to know who they're dealing with when they engage in e-commerce; third, businesses' ability to

serve important functions; and, fourth, very important individual privacy interests.

First, law enforcement. The FTC frequently challenges a wide variety of Internet-related threats, for example, spam, spyware, phishing, deceptive health claims, and get-rich-quick schemes. Whether acting to stop fraud or otherwise protecting consumers, our investigators need to identify offenders who hide behind the electronic shield of the Internet.

For the past decade, we've used WHOIS databases in virtually all of our Internet investigations. In fact, WHOIS is often one of the first tools we use to identify wrongdoers.

Sometimes, we can unmask the bad guys and learn their whereabouts from WHOIS databases. And even when scammers provide false information—and, sadly, all too often WHOIS information is inaccurate—WHOIS data may still provide invaluable leads. Con artists sometimes provide the same phony information for multiple websites, so WHOIS sometimes enables us to link seemingly unrelated scams.

Second, consumers themselves need to know who they're doing business with. This is especially true in an online environment. Continued public access to WHOIS data provides consumers with essential contact information if an online seller fails to deliver goods or services as promised. Consumer self-help is vital to ensuring consumer confidence in our market economy—and, often, to resolve disputes before they reach law enforcement.

Third, business access to WHOIS data also serves an important public policy purpose. Last week, I was on the West Coast, meeting with some of our leading Internet companies. These companies frequently rely on WHOIS databases to take real-time action against phishers and identity thieves who are using their brands to target their customers. Impeding businesses ability to quickly take down scams will only further the risk of serious consumer harm.

Of course, the FTC is concerned about legitimate privacy interests. We have always recognized at the Commission that individual noncommercial registrants may require protection from public access to their contact information without compromising appropriate access by law enforcement. Think, for example, of the dissident who needs anonymity. But from our perspective, anyone selling a product or engaged in commercial activity should have to publicly reveal who they are. It's just that simple.

Mr. Chairman, we do want to thank you for your leadership on this issue, also you, Senator Burns. And I think I'm getting close to my time limit, so I'm happy to answer any questions, with Mr. Kneuer.

[The prepared statement of Mr. Leibowitz follows:]

PREPARED STATEMENT OF HON. JON LEIBOWITZ, COMMISSIONER, FEDERAL TRADE COMMISSION

I. Introduction

Good morning, Mr. Chairman, and members of the Subcommittee, I am Jon Leibowitz, a Commissioner of the United States Federal Trade Commission (FTC or Commission).[1] I appreciate the opportunity to appear before you today to discuss Internet governance. Specifically, my testimony will focus on the importance of continued public and law enforcement access to WHOIS databases. Simply put, the

FTC is concerned that attempts to limit the purpose of WHOIS databases will hinder its ability to protect consumers and their privacy.

As you know, WHOIS databases are information directories containing contact information about website operators. The FTC has long recognized that WHOIS databases are critical to the agency's consumer protection mission, to other law enforcement agencies around the world, and to consumers. In fact, 4 years ago, the Commission testified before Congress on the importance of improving the accuracy of information in WHOIS databases.[2] Most recently, in July 2006, the Commission testified before a subcommittee of the House Committee on Financial Services on the importance of preserving public access to WHOIS data.[3]

The Internet Corporation for Assigned Names and Numbers, commonly referred to as ICANN, is currently engaged in a policy development process that could modify the information that is maintained on public WHOIS databases. In April 2006, ICANN's Generic Names Supporting Organization (GNSO), the organizational body within ICANN that is evaluating the proposed changes to WHOIS databases, voted to limit the purpose of WHOIS databases to technical purposes only.[4]

Because of its concern about preserving access to WHOIS databases, the FTC attended the ICANN meeting in Marrakech, Morocco in June to highlight the importance of public access to WHOIS databases. On behalf of the FTC, I participated in a panel comprised of representatives of law enforcement agencies from other countries. I was joined by the Chairman of the Independent Post and Telecommunications Authority in the Netherlands (OPTA) that enforces anti-spam laws, and a Deputy Director of Japan's Telecommunications Consumer Policy Division in the Ministry of Internal Affairs and Communications. Together, we emphasized the importance of law enforcement access to WHOIS databases and encouraged the GNSO to reconsider its decision to adopt the narrow purpose definition for WHOIS databases. The Commission understands that, in part because of these discussions, the GNSO is re-evaluating its decision.

The FTC is pleased to continue this dialogue today by providing this statement on the importance of public WHOIS databases in enforcing consumer protection laws and in empowering consumers. First, the testimony provides some general background about the FTC. Then, the testimony describes how the FTC uses WHOIS databases for its law enforcement purposes, discusses the importance of consumer and business access to WHOIS data about *commercial* websites and other legitimate uses of WHOIS data, and addresses the privacy concerns that some stakeholders have raised about public access to WHOIS databases. The statement concludes with some of the FTC's recommendations on how to move forward.

II. FTC Enforcement of Consumer Protection Laws

The FTC is the only Federal agency empowered to enforce both competition and consumer protection laws. The principal consumer protection statute that the FTC enforces is the FTC Act, which prohibits "unfair or deceptive acts or practices."[5] The FTC Act authorizes the FTC to stop businesses from engaging in such practices. The FTC also can seek monetary redress and other equitable remedies for consumers injured by these illegal practices.

The FTC has used its authority against "unfair or deceptive acts or practices" to take action against a wide variety of Internet-related threats, including Internet auction fraud,[6] Internet-based pyramid schemes,[7] websites making deceptive health claims,[8] and websites promoting "get rich quick" schemes.[9] More recently, the Commission has focused its actions against deceptive claims delivered through spam,[10] "phishing" schemes,[11] and spyware—all violations of consumer privacy that WHOIS data help us eliminate.[12] In many of these cases, the FTC has worked cooperatively with its consumer protection counterparts across the globe.

In addition, the FTC has made a high priority of protecting consumers' privacy and improving the security of their sensitive personal information, both online and offline. The FTC has brought several law enforcement actions targeting unfair and deceptive practices that involve the failure to protect consumers' personal information.[13] Indeed, as announced earlier this year, the FTC created a new Division of Privacy and Identity Protection to address specifically the need to protect consumer privacy and the security of consumers' personal information.

The FTC also promotes consumer welfare in the electronic marketplace through education, outreach, and advocacy. For example, FTC staff provides guidance to businesses advertising and marketing on the Internet[14] and to consumers about what they should look for before making purchases and providing information online.[15]

III. How the FTC Uses WHOIS Databases

FTC investigators and attorneys have used WHOIS databases for the past decade in multiple Internet investigations. WHOIS databases often are one of the first tools FTC investigators use to identify wrongdoers. Indeed, it is difficult to overstate the importance of quickly accessible WHOIS data to FTC investigations.

For example, in the FTC's first spyware case, *FTC* v. *Seismic Entertainment,* the Commission charged that the defendants exploited a known vulnerability in the Internet Explorer browser to download spyware to users' computers without their knowledge.[16] The defendants' software hijacked consumers' home pages, delivered an incessant stream of pop-up ads, secretly installed additional software programs, and caused computers to slow down severely or crash. The spyware in this case was installed using so-called "drive-by" tactics—exploiting vulnerabilities to install software onto users' computers without any notice. Using WHOIS data, the FTC found the defendants, stopped their illegal conduct, and obtained a judgment for millions of dollars in consumer redress.[17] It is uncertain whether the FTC would have been able to locate the defendants without the WHOIS data.

In another matter, the FTC cracked down on companies that illegally exposed unwitting consumers to graphic sexual content without warning.[18] The Commission charged seven entities with violating Federal laws that require warning labels on e-mail containing sexually-explicit content. In these cases, accurate WHOIS information helped the FTC to identify the operators of websites that were promoted by the illegal spam messages.

Information in WHOIS databases is most useful when it is accurate. Indeed, the Commission has advocated that stakeholders work to improve the accuracy of such information, because inaccurate data has posed significant obstacles in FTC investigations.[19]

In some instances, though, even inaccurate WHOIS information can be useful in tracking down Internet fraud operators. One of the FTC's recent spyware cases involved defendants that used free lyric files, browser upgrades, and ring tones to trick consumers into downloading spyware onto their computers.[20] Rather than receiving what they opted to download, consumers instead received spyware with code that tracked their activities on the Internet. In this particular investigation, several of the defendants' websites were registered to a non-existent company located at a non-existent address. Despite the registrant's use of false information, FTC staff was able to link the websites to each other because all of the registrations listed the same phony name as the administrative contact in the WHOIS databases. Of course, with a "narrow purpose" WHOIS, it is not clear that even such inaccurate registration information would be available.

Having "real-time" access to WHOIS data is particularly important for a civil law enforcement agency like the FTC. Where a registrar is located in a foreign jurisdiction, the FTC often has no other way to obtain the information it needs. The FTC cannot, in most cases, readily require a foreign entity to provide us with information. Thus, particularly in cross-border cases, WHOIS databases are often the primary source of information available to the FTC about fraudulent domain name registrants.[21]

In short, if ICANN were to restrict the use of WHOIS data to technical purposes only, it would greatly impair the FTC's ability to identify Internet malefactors quickly—and ultimately stop perpetrators of fraud, spam, and spyware from infecting consumers' computers.

IV. How Consumers Use WHOIS Databases

Consumers also benefit from access to WHOIS data for commercial websites. Where a website does not contain contact information, consumers can go to the WHOIS databases and find out who is operating the website. This helps consumers resolve problems with online merchants directly, without the intervention of law enforcement authorities. Indeed, it is crucial that consumers continue to have the ability to settle disputes prior to—or instead of—law enforcement involvement.

Consumers do in fact regularly rely on WHOIS databases to identify the entities behind websites. FTC staff recently searched the FTC's database of consumer complaints, and found a significant number of references to the term "WHOIS." These results indicate that when consumers encounter problems online, the WHOIS databases are a valuable initial tool they use to identify the people with whom they are dealing. Consumer access to WHOIS also helps the FTC because it allows consumers to gather valuable contact information that they can pass on to the Commission—information that might no longer be available by the time the agency initiates an investigation because the website operators have moved on to different sites or different scams.

The Organization for Economic Cooperation and Development (OECD) has recognized that consumer access to WHOIS data about commercial websites serves an important public policy interest. In 2003, the OECD Committee on Consumer Policy issued a paper unequivocally stating that "[f]or commercial registrants, all contact data should be accurate and publicly available via WHOIS."[22] In support of this conclusion, the paper states:

> Easy identification of online businesses is a key element for building consumer trust in the electronic marketplace. Because a website has no obvious physical presence, consumers are deprived of many of the usual identifying characteristics that help instill trust in a traditional retailer . . . While the most obvious location for an online business to provide contact details is on the website itself, domain name registration information can serve as a useful compliment [sic].[23]

This OECD paper represents an international consensus about the importance of accurate and accessible WHOIS data for consumers.

V. Other Legitimate Uses of WHOIS Data

There are other legitimate private users of WHOIS databases—businesses, financial institutions, nongovernmental organizations, and intellectual property rights owners—all of which heavily rely on access to accurate WHOIS data. Although the FTC does not represent these entities' interests in the WHOIS debate, their use of WHOIS databases can help consumers. For example, a financial institution concerned about the misuse of its name by "spoofing" its website is not only protecting its own business interests, but it is also protecting its customers from being "phished."

The Red Cross recently explained how it used WHOIS data to shut down fraudulent websites that mimicked its website after Hurricane Katrina in connection with donation scams.[24] The simple yet crucial point is this: many legitimate uses of WHOIS data by the business community and other nongovernmental organizations have an important, and often ignored, consumer protection dimension. Their continued access to WHOIS information often helps protect consumers from online scams and deception.

VI. WHOIS Databases and Privacy

Concerns about the privacy of domain name registrants have driven much of the WHOIS debate. The FTC, a primary enforcement agency for U.S. consumer privacy and data security laws, is very concerned about protecting consumers' privacy. Thus, the Commission has always recognized that registrants engaged in noncommercial activity may require some privacy protection from *public* access to their contact information, without compromising appropriate real-time access by law enforcement agencies.[25] The FTC supports the further study of how this goal could be achieved. In the meantime, however, at the very least, the FTC believes that ICANN should preserve the *status quo* and reject limiting the WHOIS databases to technical uses.

Restricting public access to WHOIS data for *commercial* websites would deprive the public of the ability to identify and contact the operators of online businesses and would contravene well-settled international principles. If people want to do business with the public, they should not be able to shield their basic contact information. The 1999 OECD Guidelines on Electronic Commerce state that consumers should have information about commercial websites "sufficient to allow, at a minimum, identification of the business . . . [and] prompt, easy and effective consumer communication with the business."[26] Thus, commercial website operators have no legitimate claim for privacy, and the public should continue to have access to their WHOIS data.[27]

Moreover, the existing availability of WHOIS databases can actually help enforcement agencies find out who is violating privacy laws and, consequently, help prevent the misuse of consumers' personal information. For example, WHOIS databases were invaluable in FTC investigations in phishing cases where the defendants sought to steal sensitive personal and financial information from consumers. In addition, the spyware cases discussed earlier also involve serious threats to consumer privacy, as spyware can monitor consumers' Internet habits and can even retrieve sensitive consumer information, including financial information, by logging keystrokes. WHOIS data has helped the FTC to stop these privacy violations and, hopefully, will continue to do so.

VII. Recommendations

In light of the FTC's experience in enforcing consumer protection laws, the FTC made several recommendations to the ICANN community at its meeting in June. This testimony summarizes the recommendations the Commission made to the

ICANN community and then concludes with a recommendation that Congress enact the U.S. SAFE WEB Act, which the Senate passed on March 16, 2006.[28]

A. Recommendations to ICANN Community

The FTC made three recommendations to the ICANN community. First, the FTC recommended that the GNSO reconsider and reverse its position that the WHOIS databases should be used for technical purposes only. If this narrow purpose were to be adopted, the FTC, other law enforcement agencies, consumers, and businesses would not be able to use the WHOIS databases for their legitimate needs. This would hurt consumers around the world and could allow Internet malefactors to violate consumer privacy with impunity. The Commission understands that the GNSO is currently taking steps to incorporate the input of the FTC and other law enforcement agencies into its final recommendation to the ICANN Board.

Second, the FTC encouraged members of ICANN's Governmental Advisory Committee (GAC) to continue their outreach with law enforcement colleagues in their respective countries to reinforce the serious law enforcement and consumer protection implications of losing access to WHOIS databases. The Commission is pleased to note that GAC members from several countries are undertaking such an effort.

Third, the FTC recommended that ICANN carefully consider improvements in WHOIS databases. For example, as the OECD statements referenced above make clear, there is simply no reason to prevent access to contact information for a commercial website. The FTC urged ICANN to consider additional measures to improve the accuracy and completeness of domain name registration information. The FTC is also interested in exploring the viability of "tiered access" as a solution capable of satisfying privacy, consumer, and law enforcement interests.[29] Restricting the purpose of the WHOIS databases does not satisfy any of these interests and is a step in the wrong direction. Maintaining accessibility and enhancing the WHOIS databases would make great strides toward improving the safety and fulfilling the promise of the Internet.

B. U.S. SAFE WEB Act

The FTC has previously recommended that Congress consider enacting the U.S. SAFE WEB Act, passed by the Senate on March 16, 2006. The Commission continues to recommend enactment of this legislation, which would give it additional tools to fight fraud. Even with the current access to WHOIS databases, the Commission needs these additional tools. If the Commission's access to WHOIS data becomes unavailable, the Commission's need for the tools provided by the U.S. SAFE WEB Act becomes even more critical.

The U.S. SAFE WEB Act would make it easier for the FTC to gather information about Internet fraud from sources other than WHOIS databases. For example, the U.S. SAFE WEB Act would help the FTC obtain information and investigative assistance from foreign law enforcement agencies. It would also allow the FTC to obtain more information from the private sector and from financial institutions about Internet fraud. The FTC's ability to obtain information under the U.S. SAFE WEB Act is no substitute for real-time, desktop access to WHOIS data. Where such data is limited, inaccurate, unavailable, or inapplicable, however, having access to a broader range of investigative sources about Internet and other cross-border fraud would surely help.

VIII. Conclusion

In sum, the FTC believes that improvements need to be made to the current WHOIS database system and is committed to working with others toward a solution. In the meantime, ICANN should ensure that WHOIS databases are kept open, transparent, and accessible so that agencies like the FTC can continue to protect consumers, and consumers can continue to protect themselves. Further, Congress should enact the U.S. SAFE WEB Act to provide the FTC with additional tools to fight Internet and other fraud. Together, these tools will help ensure that consumers are free from deceptive practices that undermine the promise of the Internet.

ENDNOTES

[1] This written statement reflects the views of the Federal Trade Commission. My oral statements and responses to any questions you may have represent my own views, and do not necessarily reflect the views of the Commission or of any other Commissioner.

[2] Prepared Statement of the Federal Trade Commission on "*The Integrity and Accuracy of the 'WHOIS' Database,*" Before the Subcomm. on Courts, the Internet, and Intellectual Property of the Comm. on the Judiciary, U.S. House of Representatives, May 22, 2002.

[3] Prepared Statement of the Federal Trade Commission on "*Public Access to WHOIS Databases,*" Before the Subcomm. on Financial Institutions and Consumer Credit of the House Comm. on Financial Services, U.S. House of Representatives, July 18, 2006.

[4] The GNSO vote is not final. After considering other recommendations submitted by the WHOIS Task Force, the GNSO will make formal recommendations to the ICANN Board, which has the ultimate responsibility for making the final decision on any proposed changes to the WHOIS databases.

[5] 15 U.S.C. § 45.

[6] *E.g., FTC* v. *Silverman,* No. 02–8920 (GEL) (S.D.N.Y., filed Aug. 30, 2004).

[7] *E.g., FTC* v. *Skybiz.com, Inc.,* No. 01–CV–396–AA(M) (N.D. Okla. filed Jan. 28, 2003).

[8] *E.g., FTC* v. *CSCT, Inc.,* No. 03C 00880 (N.D. Ill., filed Feb. 6, 2003).

[9] *E.g., FTC* v. *National Vending Consultants, Inc.,* CV–5–05–0160–RCJ–PAL (D. Nev., filed Feb. 7, 2006).

[10] *E.g., FTC* v. *Cleverlink Trading Ltd.,* No. 05C 2889 (N.D. Ill., filed May 16, 2005) (enforcing the CAN–SPAM Act).

[11] *E.g., FTC* v. _____, *a minor,* CV No. 03–5275 (C.D. Cal. filed 2003).

[12] *E.g., FTC* v. *Enternet Media,* No. CV 05–7777 CAS (C.D. Cal., filed Nov. 1, 2005); *FTC* v. *Odysseus Mktg., Inc.,* No. 05–CV–330 (D.N.H. filed Sept. 21, 2005); *In the Matter of Advertising.com,* FTC Docket No. C–4147 (Sept. 12, 2005).

[13] *E.g., In the Matter of CardSystems Solutions, Inc.,* FTC Docket No. C–4168 (Sept. 5, 2006); *In the Matter of DSW, Inc.,* FTC Docket No. C–4157 (Mar. 7, 2006); *United States* v. *ChoicePoint, Inc.,* No. 106–CV–0198 (N.D. Ga. filed Feb. 15, 2006); *In the Matter of BJ's Wholesale Club, Inc.,* FTC Docket No. C–4148 (Sept. 20, 2005).

[14] *E.g.,* "Advertising and Marketing on the Internet—Rules of the Road," *http://www.ftc.gov/bcp/conline/pubs/buspubs/ruleroad.htm.*

[15] *E.g.,* "Consumer Guide to E-Payments," "Holiday Shopping? How to be Onguard When You're Online," *http://www.ftc.gov/bcp/conline/pubs/alerts/shopalrt.htm*, "How Not To Get Hooked By a Phishing Scam," *http://www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.htm,* and OnguardOnline.com (consumer education website providing practical tips concerning online fraud and other online threats).

[16] *FTC* v. *Seismic Entm't Prods., Inc.,* No. 04–377–JD, 2004 U.S. Dist. LEXIS 22788 (D.N.H. Oct. 21, 2004) (Order of Default Judgment, Permanent Injunction and Other Equitable Relief entered Mar. 22, 2006).

[17] *See* News Release, Court Halts Spyware Operations, May 4, 2006, *http://www.ftc.gov/opa/2006/05/seismic.htm*.

[18] *See* News Release, FTC Cracks Down on Illegal "X-Rated Spam," July 20, 2005, *http://www.ftc.gov/opa/2005/07/alrsweep.htm.*

[19] *See supra* notes 2–3. FTC investigators have had to spend many additional hours tracking down fraud on the Internet because of inaccurate WHOIS data—hours that could have been spent pursuing other targets. *See also* U.S. Government Accountability Office, Report to the Subcomm. on Courts, The Internet, and Intellectual Property, House of Representatives, "Internet Management: Prevalence of False Contact Information for Registered Domain Names" (Nov. 2005) (noting that, based on a random sample of domain names from the .com, .net, and .org domains, 8.65 percent of websites were registered with patently false or incomplete data in the required WHOIS contact information fields).

[20] *FTC* v. *Enternet Media,* No. CV05–7777 CAS (C.D. Cal., filed Nov. 1, 2005).

[21] The number of cross-border complaints received by the FTC continues to rise. In 2005, 20 percent of the complaints in the FTC's Consumer Sentinel database had a cross-border component, compared to 16 percent in 2004, and less than 1 percent in 1995. *See www.consumer.gov/sentinel.*

[22] OECD, *Consumer Policy Considerations on the Importance of Accurate and Available WHOIS Data,* DSTI/CP(2003)1/REV1 (April 30, 2003), available at *http://www.olis.oecd.org/olis/2003doc.nsf/LinkTo/dsti-cp(2003)1-final.*

[23] *Id.*

[24] Red Cross Comment to GNSO WHOIS Task Force Preliminary Report, March 14, 2006, *http://forum.icann.org/lists/whois-comments/msg00043.html.*

[25] *See supra* notes 2–3.

[26] OECD, *Guidelines for Consumer Protection in the Context of Electronic Commerce* (1999), available at *http://www.oecd.org/dataoecd/18/13/34023235.pdf.*

[27] Consistent with this approach, the European Union's Distance Selling Directive *requires* that European websites *selling* to consumers include the name and address of the website operator. European Distance Selling Directive (Directive 97/7/EC), Article 4.

[28] Undertaking Spam, Spyware, And Fraud Enforcement With Enforcers across Borders ("U.S. SAFE WEB Act"), S. 1608, 109th Cong. (2006) (sponsored by Sen. G. Smith, passed by the Senate, Mar. 16, 2006).

[29] Tiered access refers to a system in which different categories of stakeholders would get different levels of access to WHOIS databases.

The CHAIRMAN. What was the example you used?

Mr. LEIBOWITZ. Oh, of dissidents. Right. We believe that you can make a—at the Commission, you can make a distinction between commercial and noncommercial entities. So, if someone's selling a product on the Internet, they should have to publicly reveal their contact information. All too often, that contact information is hidden behind proxy registrations, even for commercial entities. And a lot of the time, when someone is a scammer or trying to rip off consumers, they deliberately use proxy registrations to try to cloak themselves in Internet anonymity. It makes it much harder for us to go after these malefactors. And that's true for law enforcement agencies in the United States and, really, around the world. But we also recognize that some people may need some anonymity if they're not engaged in a commercial activity. It seems to us that makes sense. But this is an issue that needs to be thought through by ICANN and by NTIA.

The CHAIRMAN. Thank you very much.

Mr. Kneuer, I think the $64-billion question is, should this agreement be extended? It expires in a month.

Mr. KNEUER. And I think the short answer is yes, it should be extended. We conducted a public consultation over the summer. We had more than 700 written comments. We had a public forum at the Department of Commerce, where interested stakeholders, from governments to private companies to registrars and registries, attended. I think that consultation reflected broad support for ICANN, that the private-sector management of the DNS is clearly the appropriate path forward, that ICANN is clearly the appropriate vehicle for that private-sector management. But I think there was also clear indications that—in order for ICANN to be a really lasting and sustainable institution, that we need to continue to make more progress on issues of accountability and transparency, and the vehicle of the MOU to help them through that process is still appropriate.

The CHAIRMAN. How long has the current agreement been in place?

Mr. KNEUER. The current agreement was for 3 years. Historically, we have extended these MOUs periodically from 1 year to 3 years. The 1-year extensions would come up quickly, so we made the last one 3 years. I think it would be appropriate to consult with ICANN concerning our review of the record, to come up with an appropriate time period that clearly indicates that we continue to be committed to the transition, but, at the same time, provide adequate time for ICANN to make some measurable progress on these issues of transparency and accountability.

The CHAIRMAN. Have you discussed the length of that MOU, the time frame, with your counterparts in other countries?

Mr. KNEUER. Not in other countries. This is an agreement between the Department of Commerce and ICANN.

The CHAIRMAN. But doesn't it have international implications?

Mr. KNEUER. It does have international implications, and I speak periodically and fairly regularly with my regulatory counterparts in other countries around the world that have interest in this. The issue of more governmental involvement in ICANN was an issue that was raised at the World Summit on the Information Society in Tunisia last year, and the clear answer to that was that the continued private-sector model was affirmed.

The CHAIRMAN. Well, I've had indications from other Senators that when they started to open up and seek a domain name, they found that name had already been reserved by someone else, but it was for sale to them. Have you looked into that?

Mr. KNEUER. Not explicitly in that context, but that's clearly something that we're happy to work on with you, or your staff.

The CHAIRMAN. Mr. Leibowitz, has the FTC gone into that at all?

Mr. LEIBOWITZ. Well, I think, for the most part, this—I think it's called "domain-name tasting" and "parking," where people may sample a domain name without having to pay, or may just hold it for a certain amount of time, even if they don't use it. They raise some public policy questions for us, because, again, a lot of the fraudsters hide behind temporary Internet websites. And so it is a concern. We've talked to NTIA about it. We've talked to ICANN about it, too. And we know that—we know that they're taking this seriously.

The CHAIRMAN. Well, isn't it part of identity theft if someone goes and takes my name and registers it as a domain name, and then uses that domain name out to—in the world? Isn't that identity theft? Why don't you look at that?

Mr. LEIBOWITZ. Well, we do, and we brought a number of cases in this area. I mean, technically, identity theft is when they do something bad with your name, like steal your credit card information or steal other personal information.

The CHAIRMAN. Well stealing my name is still stealing, isn't it?

Mr. LEIBOWITZ. It's a very legitimate public policy concern, and it's something that we have looked at. We've brought a bunch of cases against phishers, identity thieves, cybersquatters, and other Internet malefactors.

The CHAIRMAN. Thank you.

Senator Burns?

Senator BURNS. Well, they could have mine.

[Laughter.]

Senator BURNS. Not very many people have gone through a business failure. And I had to go through one, one time. And I prayed—something like that.

But, anyway, how long should we extend this MOU? I mean, you're recommending that it be extended. How long should it be extended?

Mr. KNEUER. Well, as I said, we're in discussions with ICANN about the appropriate formalization of our relationship, going forward, and the period of time. Like I said, we've done longer extensions and shorter extensions. I think the important thing, at the end of the day, is that we provide enough time for ICANN to achieve meaningful progress on these issues of accountability and transparency, and, at the same time, we don't create, an "in-perpetuity," going forward. I want to be cognizant of the fact that this

is a transition that we undertook, that we intend to complete, but, at the same time, I want there to be enough time to be realistic for real change to take place.

Senator BURNS. Well, Mr. Kneuer, have they—what milestones have they not met to complete this transition?

Mr. KNEUER. Most of the milestones that ICANN has met were with regards to the brick and mortar of putting together an institution, having a budget in place, coming up with contingency plans, having staffing, making sure that they have technical competency and expertise. On the issues of accountability and transparency and on having the invested support of all of the constituencies that make up ICANN, having firm relationships with the root-zone operators, and with the regional Internet registries, they've made progress on some of these. But the larger thematic of making sure that each of those constituencies are confident that ICANN has processes in place that are transparent and that there are means for accountability, it's those broader thematic developments that I think we need to be focused on going forward.

Senator BURNS. OK. I think maybe—that's all the questions I have for this panel, Mr. Chairman. We should talk more about those milestones and Internet transparency, what's expected by the Department, what's expected by us, because we're talking about an organization that's very, very important to us.

So, I thank you for that information.

Mr. LEIBOWITZ. Mr. Chairman?

The CHAIRMAN. Senator Pryor?

Pardon me.

Mr. LEIBOWITZ. I was just going to say, Mr. Chairman, could I just come back to a question you asked me? You asked me about people who are doing basically bad things to American consumers on the Internet. And a lot of those folks are from out of the country. And your Committee passed a bill, the U.S. SAFE WEB Act, which would allow us to more effectively work with foreign law enforcement agencies—really, to protect American consumers by sharing information. It has passed your Committee. It passed the Senate by unanimous consent, and the House hasn't taken it up yet. And anything you can do to help act on this noncontroversial bill, which really would help us do the things you want us to do, would be really appreciated in the waning days of this session and this Congress.

The CHAIRMAN. Thank you for that.

Senator Pryor?

STATEMENT OF HON. MARK PRYOR,
U.S. SENATOR FROM ARKANSAS

Senator PRYOR. Thank you, Mr. Chairman.

Mr. Leibowitz, let me follow up on that point. It sounds like that this Committee and the Senate have acted to try to put some tools in your hands that you feel like we need, and it sounds like that has a big international dimension to it. Is that right?

Mr. LEIBOWITZ. That's exactly right, Senator.

Senator PRYOR. And I assume one of the real challenges you have is the international aspects of the Internet.

Mr. LEIBOWITZ. Well, of course it is, because at this point, right now, we can't share confidential information, by law, with our foreign law enforcement sister agencies. It's an anomaly in the law and everyone agrees that it should be changed. And foreign law-enforcement agencies can't share information with us, because it's FOIA-able. So, of course, they won't do that. And if we can empower them to help us, I think that will be enormously helpful in trying to do the things you want us to do and really bringing more cases effectively.

Senator PRYOR. Does the Federal Trade Commission have any real control over the Internet right now?

Mr. LEIBOWITZ. No, we do not have control over the Internet. We try to bring cases, when we can, against Internet malefactors, of course, and we have brought a number of them.

Senator PRYOR. Should it have any control over the Internet?

Mr. LEIBOWITZ. Well, I think we should have the ability to effectively prosecute cases. And we can do some of that now, but we could be much more effective if this legislation was passed. And one of the reasons why we're so concerned about this movement within ICANN to limit access to what's now public information is that it will make it even more difficult for us to find out who the bad guys are. It will be particularly hard for us if we have to go to Internet registrars—and there are 800, I believe, of them, more or less—in foreign countries, and they don't have to give us any information, and that information isn't available.

Senator PRYOR. Right, OK. And, I'm sorry, you're going to have to pronounce your name for me. Is it Kneuer?

Mr. KNEUER. Kneuer.

Senator PRYOR. Mr. Kneuer, I am very interested in the possibility, at least, of setting up a dot-xxx domain. I think that—and I may have it wrong, but I think that this would be a—an important step to cleaning up the Internet. I have a real concern. I have two young children—not that young; sixth and seventh grade—and they're just getting, kind of, prime Internet-exposure age, and I have a lot of concern about them. And I think every parent in America is concerned, or should be concerned, about the Internet. And I think the dot-xxx domain could be an important step in maybe making the Internet safer in a lot—in a lot of different ways for our children and for this country, and, really, for the world. But as I understand it, NTIA urged ICANN to reject the dot-xxx domain, and I'm curious if you know how that happened and why that happened?

Mr. KNEUER. Thank you, Senator. I absolutely share your concern. I've got two small children of my own—too small for the Internet, but I constantly worry about what happens when they get to be the age of your children, and older.

ICANN did consider the adoption of a dot-xxx domain name, and they ultimately did not adopt that. There was communication from NTIA and the Department of Commerce into the ICANN process on two fronts with regards to dot-xxx. The first was a communication that said, "As you are examining this, there appears to be a great deal of interest from a great deal of entities about this, and, as part of your bottom-up deliberative process, you should have an opportunity, and create an opportunity, for all interested stake-

holders to express their views." So, we wrote a letter asking them to do that. Other governments wrote similar letters.

I wrote a second letter, later, talking about, precisely, the potential public policy benefits that would flow from dot-xxx. If there were to be a dedicated domain, let's make sure that there are enforceable steps to make sure that pornography is limited to those sorts of sites. And it was simply a factual inquiry to say, "We've heard a list of public policy commitments. Are they being made enforceable?"

As I said, ultimately through the process, dot-xxx was not fully adopted, but——

Senator PRYOR. Is that because you just want more time to examine the value of dot-xxx?

Mr. KNEUER. Well, I think it was through—as I said, communications we made into the ICANN Government Advisory Committee. Other governments made similar inquiries. Large numbers of private entities made comments, both in favor of and against. I don't believe we ever established a formal position, one way or another. Our comments with regards to dot-xxx, which are public, were along the lines of process, making sure that everybody had an opportunity to weigh in, and then raising factual questions about, what would be the potential enforcement of these public policy benefits that could accrue from dot-xxx?

Senator PRYOR. Will ICANN revisit this in the future?

Mr. KNEUER. I believe, under ICANN's processes, there are periods for reconsideration and review. My understanding is they're currently undergoing that with regards to dot-xxx. There is a fairly transparent and open application process for the establishment of new top-level domains, so I don't believe that there is anything that would preclude further consideration of whether it is dot-xxx or some other domain name.

Senator PRYOR. And that's my last question, that you mentioned, transparency and openness and accountability. I think both of you have talked about this in your statements and in answering questions. What can NTIA do to help improve the level of transparency and accountability? What needs to happen there?

Mr. KNEUER. Well, I think that is the function of our MOU. The MOU does not create a relationship between the Department of Commerce and ICANN that is one of regulator and regulated; it is much more of a partnership. This was a U.S. Government function that we unilaterally are transferring to the private sector. And we have the MOU to help them with that transition and to help them develop those processes. So, to the extent being dedicated to being a closer observer than perhaps others might be, and sharing with them our insights and our views, being a sounding board for those sorts of issues, we help them work through this transition. So, that would be my expectation of what the ongoing relationship would entail, us helping them come up with processes that are transparent to the constituent membership, and the interested stakeholders so that they understand how they can interrelate with ICANN, that all views are heard and considered through the bottom-up coordination process, and that decisionmaking is accountable.

Senator PRYOR. Thank you, Mr. Chairman.

The CHAIRMAN. Well, thank you very much.

Pardon me for mispronouncing your name, Mr. Kneuer. I don't know whether you want to be "Knowwer" or "Knewer," but sorry.

[Laughter.]

The CHAIRMAN. We do appreciate your help and consideration. I thank you for your plug for the bill we've passed in the Senate, and we still are trying to wait and see whether the House will pass that. It passed over here unanimously, so it should not be causing any problems over there. We do thank you for your help.

Mr. KNEUER. Thank you, Mr. Chairman.

The CHAIRMAN. Do you have any further questions, Senator?

Senator BURNS. I do not.

The CHAIRMAN. So, we'll turn to panel 2, then. Gentlemen, thank you very much.

Our next panel is Dr. Paul Twomey, President and CEO of Internet Corporation for Assigned Names and Numbers; Mr. Ken Silva, Chief Security Officer for VeriSign; and Ms. Christine Jones, General Counsel and Corporate Secretary for The Go Daddy Group.

We thank you very much for being willing to testify here today to help us further understand the situation with regard to ICANN.

Dr. Twomey, would you like to commence, please?

STATEMENT OF DR. PAUL TWOMEY, PRESIDENT/CEO, INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS (ICANN)

Dr. TWOMEY. Good morning——

The CHAIRMAN. Pull the mike toward you, please.

Dr. TWOMEY. All right. Thank you.

The CHAIRMAN. Thanks.

Dr. TWOMEY. Good morning, Mr. Chairman, and members of the Committee. May I say how pleased I am to be—appear again in front of your Committee. Thank you for the opportunity to speak before the Subcommittee in my role as President and Chief Executive of the Internet Corporation for Assigned Names and Numbers.

ICANN is a private-sector organization performing a global function, with our main office in Marina del Rey, California. ICANN has been recognized by the world community as the global authoritative body on the technical and organization means to ensure the stability, interoperability of the DNS and the distribution of Internet protocol addresses and other unique identifiers.

Since appearing before the Senate Committee on Commerce, Science, and Transportation nearly 2 years ago——

The CHAIRMAN. I hate to tell you, but people in the back of the room are not hearing you.

Dr. TWOMEY. OK, sorry.

The CHAIRMAN. Can you pull the mike toward you, sir?

Dr. TWOMEY. There we go. Thank you sir.

The CHAIRMAN. Thank you.

Since appearing before the Subcommittee nearly 2 years ago, ICANN has continued to take great steps forward in solidifying its role as the international private-sector entity tasked to provide technical coordination of the domain-name system. Since its origins in 1998, ICANN has helped secure a stable and secure Internet that creates a presumption of universal resolvability. ICANN has

fostered greater choice, lower costs, and better services to DNS registrants, including over 10 million businesses in the United States alone.

The Internet requires a stable and secure system of unique identifiers if it is to serve the global community efficiently and reliably.

At the core of ICANN's mission is global interoperability of a single Internet. ICANN was established to serve the Internet community by maintaining the stability and security of the Internet's unique identifier system and fostering competition, where appropriate, to give Internet users greater choice at optimal cost.

ICANN's successful coordination of its community underpins the operation of the global Internet. Each day, the system supports an estimated 30 billion resolutions, nearly ten times the number of phone calls in North America each day. There are currently more than 1 billion users of the Internet. Due to the universal DNS resolvability, secured and coordinated by ICANN, the Internet addresses resolve in the same way for every one of the Internet's global users once online.

ICANN is entering into six new agreements with gTLD registry operators in the last 2 years, including .net, .travel, .cat, .jobs, .mobi, and .tel. All the pending agreements have set out language with a greater accountability to ICANN on security and stability concerns, and also provide greater opportunities for ICANN to act in the event of actions of registries or such other issues that might arise from registry operator actions or practices.

One particular agreement, the dot-com agreement, is part of a larger overall settlement of a longstanding dispute with VeriSign over its desire to introduce new registry services. That dispute arose with the creation of ICANN and has been resolved in a way that would enhance the performance of both entities to the benefit of all the users of the Internet.

ICANN has been engaged in a longstanding and important relationship with the U.S. Government and—since ICANN's inception. And I note the previous panel's discussion of the MOU.

ICANN continues in its relationship with the U.S. Government and has recently entered into a new 5-year arrangement for ICANN to manage the Internet, assign names, and a numbers authority, IANA function—sorry—the Internet Assigned Numbers Authority. Additionally, ICANN and the NTIA are in the final stages of discussions which will confirm an appropriate continuing relationship toward the transition of the coordination of the technical functions related to the management of the DNS to the private sector. And this, we think, will recognize ICANN's global private-sector role, providing technical management of the DNS in a manner that provides stability and security, competition, coordination, and representation.

One of the greatest achievements of ICANN has been the successful creation, support, and coordination of an ICANN community in creation of bottom-up policymaking processes supported by various stakeholders involved in the DNS. The evolution of this process continues in many ways, but may I point to two important recent actions:

This week, the ICANN Board, having reviewed the comments about ICANN and its processes, and particularly issues around

transparency and accountability that the Committee has already mentioned, generated from the Committee during the past year, has commenced review of its own guiding principles and is publishing, soon, a set of private-sector management operating principles which will be offered for public review.

And last week, the London School of Economics provided ICANN—an ICANN-commissioned independent third-party review of one of ICANN's key policy development supporting organizations, the Generic Name Supporting Organization. The information contained in this review will likely result in consideration of additional improvements to ICANN's GNSO and supporting organization structure. Such ongoing evolution and review is an important part of our policy process.

May I just make some quick notes, then, on the issue of WHOIS, to state that ICANN is dedicating resources in this operational budget to better enforcement of the existing policy we have for WHOIS. There is a process presently underway among some of the constituencies of the ICANN process to discuss the WHOIS topics, as has been pointed out by previous speakers, but there is a long way to go before there would be any change; and, if there was any discussion coming from many of the other constituencies, there may be no change at all. I'd like to point out that all of the people who we're representing here today have all had the opportunity, and will continue to have the opportunity, to input into that discussion, but, at the moment, there is no change to ICANN's WHOIS policy.

Since 1998, our self-governance model has succeeded in addressing stakeholder issues as they appeared and bringing lower costs and better services to DNS registrants. One point I'd like to particularly point out, partly coming to the question from you, Chairman, is that ICANN's uniform domain name—Universal Domain-Name Dispute-Resolution Policy has been successful and of great value to individuals, businesses, and intellectual property holders. The policy enables them to assert—in allow them to assert their rights on domain names and to bring an online arbitration system for dealing with just the sorts of disputes that you pointed out between people who should own a particular domain name. The UDRP has resolved more than 17,000 disputes over the rights to domain names and has proven to be an efficient and cost-effective way of alternate dispute resolution.

If I could just finish my testimony by pointing out that in the introduction of new gTLD registries and introduction of greater competition amongst registrars, domain-name costs to registrants in the lifetime of ICANN have declined by as much as 80 to 90 percent, with savings both for consumers as—consumers and businesses. ICANN looks forward to working closely with people giving evidence here, the Committee, and others, as we go forward to completing our transition to private-sector coordination.

Thank you.

[The prepared statement of Dr. Twomey follows:]

PREPARED STATEMENT OF DR. PAUL TWOMEY, PRESIDENT/CEO, INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS (ICANN)

Introduction

Good morning, Chairman Smith, and members of the Committee. Thank you for the opportunity to speak before this Subcommittee in my role as President and CEO of the Internet Corporation for Assigned Names and Numbers (ICANN). ICANN is a private sector organization performing a global function, with our main office in Marina del Rey, California. ICANN has been recognized by the world community as the global authoritative body on the technical and organizational means to ensure the stability and interoperability of the DNS, and the distribution of IP addresses.

ICANN's Role in Internet Governance

Since appearing before the Senate Committee on Commerce, Science, and Transportation nearly 2 years ago, ICANN has continued to take great steps forward in solidifying its role as the international private sector entity tasked to provide technical coordination of the domain name system (DNS).

The limited and distinct mission of the Internet Corporation for Assigned Names and Numbers is clearly set out in Article I of ICANN's Bylaws. 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 as they relate to these technical functions.

Since its origins in 1998, ICANN has helped secure a stable and secure Internet that creates a presumption of universal resolvability. ICANN has fostered greater choice, lower costs and better services to DNS registrants, including over ten million businesses in the United States alone. The Internet requires a stable and secure system of unique identifiers if it is to serve the global community efficiently and reliably.

At the core of ICANN's mission is global interoperability of a single Internet. ICANN was established to serve the Internet community by maintaining the stability and security of the Internet's unique identifier systems, and fostering competition where appropriate to give Internet users greater choice at optimal cost.

ICANN's successful coordination of its community underpins the operation of the global Internet. Each day this system supports an estimated 30 billion resolutions, nearly 10 times the number of phone calls in North America per day. There are currently more than one billion users of the Internet. Due to the universal DNS resolvability secured and coordinated by ICANN, the Internet addresses resolve in the same way for every one of the Internet's global users once online.

ICANN has entered into six new agreements with gTLD registry operators (including .NET, .TRAVEL, .CAT, .JOBS, .MOBI, and .TEL) in the last 2 years (and has finalized negotiations and is waiting for approval of 5 others). All of the pending agreements have set out language with a greater accountability to ICANN on security and stability concerns, and also provide greater opportunities for ICANN to act in the event of actions of registries, or such other issues that might arise from registry operator actions or practices., including: (a) the .COM agreement (which is currently pending approval by the U.S. Department of Commerce) and (b) four other registry agreements for .ASIA, .BIZ, .INFO and .ORG (which are subject to review by the ICANN Board of Directors during the next ICANN Board Meeting).

The .COM agreement is part of a larger overall settlement of a long-standing dispute with VeriSign over its desire to introduce new registry services. That dispute arose with the creation of ICANN and has been resolved in a way that would enhance the performance of both entities, to the benefit of all of the users of the Internet. ICANN and VeriSign Board's have both approved settlement documents that would permit the parties to act together in a concerted way to protect the overall security and stability of the Internet. Further, if VeriSign were ever to act in a manner that is inconsistent with the interests of the Internet community, ICANN has built additional mechanisms into the agreement to resolve such disputes promptly and effectively.

Continuing Relationship With the United States Government

ICANN has been engaged in a long-standing and important relationship with the U.S. Government since ICANN's inception, which has been administered by the U.S. Department of Commerce's NTIA. ICANN is about to successfully complete the sixth separate amendment to its original Memorandum of Understanding with the DOC.

ICANN will continue in its relationship with the U.S. Government, having recently entered into a new 5-year arrangement for ICANN to manage the Internet Assigned Numbers Authority (IANA) function. Additionally, ICANN and the NTIA are in the final stages of discussions, which will confirm an appropriate continuing relationship and will recognize ICANN's global private sector role providing technical management of the DNS in a manner that promotes stability and security, competition, coordination, and representation.

ICANN's Private-Sector Multi-Stakeholder Model and its Continuing Evolution

One of the greatest achievements of ICANN has been the successful creation, support and coordination of an ICANN Community and creation of the bottom-up policymaking process supported by various stakeholders involved in the DNS. Since ICANN's creation, the Internet community stakeholders, have vigorously discussed and reviewed ICANN's mission and values. Accordingly, ICANN has continued to build into a robust entity, and has continued to evolve ICANN's multi-stakeholder model, which remains encapsulated in ICANN's Bylaws and its Mission and Core Values.

The evolution continues in many ways, but most recently in the following actions:

1. This week, the ICANN Board, having reviewed the comments about ICANN and its processes generated from the community during the past year, has commenced a review of its own guiding principles and is publishing a set of Private-Sector Management Operating Principles (ICANN PSMOPs), which will be offered for public review.

2. Last week, the London School of Economics provided an ICANN-commissioned independent third-party review of one of ICANN's key policy development supporting organizations, ICANN's Generic Name Supporting Organization (GNSO). The information contained in this review will likely result in considerations of additional improvements to ICANN's GNSO and supporting organizational structure.

ICANN's Continuing Accomplishments

Since 1998, ICANN's self-governance model has succeeded in addressing stakeholder issues as they have appeared, and bringing lower costs and better services to DNS registrants and everyday users of the Internet.

ICANN has been continuing its efforts to manage and adapt in the face of continued and dynamic growth of the Internet. ICANN, with the efforts of the ICANN Security and Stability Advisory Committee, has worked to make the Domain Name System more resistant to external attack.

ICANN has undertaken significant work in relation to Internationalized Domain Names (IDNs) that will enable people across the world to interact with the Internet's domain name system in their own languages, which will work to avoid the creation of alternate root systems. Working in coordination with the appropriate technical communities and stakeholders, ICANN's adopted guidelines have opened the way for domain registration in hundreds of the world's languages.

ICANN's Uniform Domain Name Dispute Resolution Policy (UDRP) has been highly successful and of great value to individuals, businesses and intellectual property holders. The policy enables them to assert in allowing them to assert their rights against domain name squatters and infringers of intellectual property interests. The UDRP has resolved more than 17,000 disputes over the rights to domain names, and proven to be efficient and cost effective for those utilizing this alternative dispute resolution mechanism.

After significant study and discussion, and working with the accredited gTLD registrars, ICANN developed a domain name transfer policy enabling domain name holders to transfer management of their domain name from one registrar to another readily. The implementation of this policy has been highly successful and has been an important step in providing additional registrar market changes and greater choice to consumers.

ICANN continues to introduce new Top Level Domains to give registrants right of choice. These include the introduction of seven new gTLDs in 2000 and four additional ones so far from the 2004 sponsored top-level domain name round.

ICANN re-bid the .NET registry during 2005, resulting in a new agreement being executed between ICANN and VeriSign. ICANN has proposed five additional gTLD agreements with the registry operators of .ASIA, .BIZ, .COM, .INFO, and .ORG. All of the newly proposed registry agreements contain new language supporting ICANN's role in the security and stability of the DNS.

The market competition for generic Top Level Domain (gTLD) registrations established by ICANN has lowered domain name costs in some instances by as much as 80 to 90 percent, with savings for both consumers and businesses. Additional detail is provided below.

Registry-Registrar Level Competition

Since ICANN was founded in 1998, ICANN has entered into many private arms-length agreements with registries (that operate the generic top-level domains), and with registrars (who are accredited by ICANN to sell domain names directly to consumers). Through these actions, ICANN has provided a private-sector solution and helped break down the monopoly position by a single dominant company, which provided both registry and registrar functions to the majority of consumers purchasing domain names.

In 1998, there were only three main generic top-level domain name registries (.COM, .NET, and .ORG) from which domain names could be purchased by American small businesses. Only one company was running all three registries, Network Solutions (which was later acquired by VeriSign). Most registrations by small businesses were in .COM.

There was a single registrar in 1998. That same company that ran the registries, Network Solutions, was the only registrar from which a consumer could purchase a domain name. The price of a single domain name in .COM in 1998, was approximately $90.00 per domain name. The .COM Registry still controls a significant amount of the marketplace, but now less than 50 percent of the market, including ccTLD operators.

The price for a .COM registration today depends upon where you purchase the name from, but in some instances the price of a domain name has been reduced by as much as 90 percent. Today, the price ranges from $7 to $35 per domain name. Go Daddy is now the largest registrar, displacing Network Solutions, which has been spun out of VeriSign.

Consumers can choose from over 845 ICANN-Accredited Registrars, derived from more than 250 unique business groups (a significant number owning interests in multiple registrar companies), located in over 40 countries.

Between 2000 and today, 11 new generic top-level domains have signed agreements with ICANN. Five of those (.CAT, .JOBS, .MOBI, .TEL and .TRAVEL) having signed agreements with ICANN in the last 18 months.

Conclusion

In conclusion Mr. Chairman, ICANN is committed to its continuing role as the private sector steward of a stable and globally interoperable Internet, and is committed to fostering competition in the domain name marketplace.

The CHAIRMAN. Thank you very much. We will look forward to coming back to you with some questions concerning your position.

Our next witness is Mr. Ken Silva, the Chief Security Officer for VeriSign.

STATEMENT OF KEN SILVA, CHIEF SECURITY OFFICER, VERISIGN

Mr. SILVA. Thank you, Mr. Chairman.

My name is Ken Silva, and I serve as Chief Security Officer for VeriSign. I also serve as the Chairman of the Internet Security Alliance, as well as serving on the Board of Directors for the Information Technology—Information Sharing and Analysis Center. I'm also an advisor to the Bush Administration's National Security Telecommunications Advisory Council.

Internet governance is an important issue today, because the Internet is so critical to our national and economic security. The technology of the Internet has transformed personal communications, banking and finance, government processes, and manufac-

turing. For example, 25 percent of America's value moves over our networks each day.

The United States is not the only country focused on Internet governance, however. A number of countries, such as China, Cuba, and Syria banded together last year in an attempt to shift control of the Internet over to the United Nations or the International Telecommunications Union. They did so, because they believe the United States has too much control over the Internet. Their efforts were not successful, in large part due to the outstanding efforts by the State Department and the Commerce Department. These countries, however, have not given up on their goal. The dramatic rise in usage bears out the Internet's importance globally.

The dot-com bust gave the illusion that the Internet growth had slowed down, but, in fact, it has actually grown at a remarkable rate. At the height of the dot-com boom in 2000, for example, there were roughly 250 million people using the Internet. Today, that's about a billion. So, that's about a 300-percent increase since—over 300-percent increase since 2000.

So, there are two questions we would pose today. The first is, is the Internet able to meet the growing demands on its infrastructure? And the second, is the Internet secure and reliable, and will it continue to be so?

VeriSign's role in supporting the Internet's infrastructure gives us a unique perspective on the Internet and these questions. VeriSign operates two of the 13 authoritative "root" servers, including the A root. VeriSign also manages dot-com and dot-net domain registries.

So, let's start with the first question. Is the Internet able to meet the growing demands of the infrastructure? The answer is yes, as long as we continue to promote investment in the infrastructure. While users have increased 300 percent since 2000, the volume of traffic has increased 1900 percent. VeriSign is very proud of the fact that dot-com and dot-net systems have had 100 percent uptimes 7 years straight. To support these functions, VeriSign has invested hundreds of millions of dollars in building a global network of computers that are a critical component of the Internet's infrastructure. VeriSign is not alone in this. There are more than 250 other such registries. It is, therefore, essential that a framework is in place, for all operators, that drives operational excellence so we can meet the demands of the Internet.

Now to the second question. Is the Internet secure and reliable? While the Internet has operated remarkably well, we can never get lulled into a false sense of security. What makes for good security today is a vulnerability tomorrow. The very growth of Internet users, broadband capacity, and the number of Internet-enabled devices has created an opportunity for hackers, organized criminals, and, even more serious, terrorists to attack our networks. Therefore, we must continually probe our weaknesses and invest in and strengthen our networks.

Let me give you some historical examples of what I'm talking about here.

In October 2002, the Internet community got a wake-up call when 13—all 13 of the DNS root servers came under a heavy denial-of-service attack. That attack was viewed at the time as the

largest attack ever to hit the Internet. It was viewed as a national crisis. Dick Clark, at the time, raised a red flag to this. There were a number of hearings on this subject, and a massive investigation by government to ensure that the root server system was secure.

That attack, unfortunately, in 2002, while it was a massive attack and did affect a large number of the root servers, would be considered a very weak and feeble attack today. Just a few months ago, in January of this year, we observed an attack that was ten times that size and was targeted at the dot-com servers. We weathered that attack, but 1,500 other websites over a 6-week period of time did not bear the attack as well. Now, these hackers targeted their victims over a 6-week period of time, and they used about 32,000 of what we estimate to be a half a million available resources to them. So, that's just 6 percent of what's available. This could have been much worse, and the fact—and, in fact, would have taken down even the largest ISPs, had it been directed at any of them.

The lesson learned there is that we must be prepared against these threats. VeriSign, for example, has invested over $250 million on the Internet infrastructure, and expects to continue to invest significantly in the near-term to strengthen against the new, more devastating attacks. To put this investment in perspective, VeriSign today can manage 10,000 times the capacity of Internet traffic that it handled in 2000.

We must move forward as an industry and a community to strengthen the Internet. In the last year, several steps have been taken by the community to ensure a strong Internet. Progress has been made on introducing internationalized domain names and expanding the number of Internet addresses. ICANN has also established a framework for registry operators that, one, gives ICANN the authority to fire an operator if it fails to meet its performance levels; two, provides incentives for continued investment; and, three, imposes safeguards for consumers. This new framework advances the objective of security and stability by ensuring the necessary investment into the critical infrastructure.

To conclude, Mr. Chairman, the last 5 years have brought painful lessons on the importance of preparation. We must not lose that vigilance, and we must continually take steps to strengthen the Internet so it remains reliable and always available.

I thank you for this opportunity to testify.

[The prepared statement of Mr. Silva follows:]

PREPARED STATEMENT OF KEN SILVA, CHIEF SECURITY OFFICER, VERISIGN

Good morning, Chairman Smith, and distinguished members of the Committee. My name is Ken Silva and I serve as Chief Security Officer of VeriSign.

VeriSign operates intelligent infrastructure services that enable and protect billions of interactions every day across the world's voice and data networks. The company is headquartered in Mountain View, California, and it has additional corporate facilities in Virginia, Kansas, Washington State and Massachusetts.

Thank you for the opportunity to testify today. I have a prepared statement, which I would request be inserted in the record.

Internet governance is not a topic that 5 years ago would have been the subject of a Congressional hearing. The Internet was still relatively new and was not thought of yet as critical to our national and economic security.

We have all witnessed, and learned, a lot over the last 5 years. We have had tragic reminders that our critical infrastructure and national symbols are targets. We

have seen how not adequately preparing for events can have disastrous consequences. And we have seen how questions of who controls our critical infrastructure, such as the port issue, can spark controversy.

And the United States is not the only country focused on Internet governance. In fact, a number of countries such as China, Cuba, and Syria last year sought to shift control of the Internet over to the United Nations or International Telecommunications Union. They did so because they believe the United States has too much control over the Internet.

Their efforts were not successful in large part due to the outstanding efforts by the State Department and Commerce Department. These countries, however, have not given up on their goal.

Internet governance is an important issue today because the Internet is critical to our national and economic security. The technology of the Internet has transformed personal communications, banking and finance, government process and manufacturing. Twenty-five percent of America's economic value moves over network connections each day. If the Internet were to go down for a just few hours, we would lose hundreds of millions of dollars of economic activity. If it went down for several days, U.S. economic activity would be severely curtailed; payrolls would not be met, securities transactions not cleared; invoices not paid.

So whether it's Wal-Mart, the House of Representatives or a soccer mom checking e-mail to see if today's practice is still on, we all rely on the Internet.

The dramatic rise of Internet usage bears that out.

The dot-com bust gave the illusion that Internet growth slowed down, but in fact it has grown at a remarkable rate. At the height of the dot-com boom in 2000, for example, roughly 250 million people used the Internet. Today, according to Internet World Stats, more than 1 billion users worldwide rely on the Internet, a 300 percent increase since 2000.

So, there are two questions we would pose today:

- Is the Internet able to meet the growing demands on its infrastructure?
- Is the Internet secure and reliable?

VeriSign's role in supporting the Internet's infrastructure gives us a unique perspective on the Internet, and these questions.

VeriSign operates two of the 13 authoritative "root" server operation centers that direct Internet traffic, including, at the request of the U.S. Commerce Department, the "A" Root Server. In this server, we maintain the authoritative address list of all Internet top-level domains. VeriSign also manages the "dot COM" and "dot NET" domain registries. These are the central databases that enable you as an Internet user to simply type in a domain name on your computer, such as "verisign.com," and connect it over the Internet to the machine that hosts the proper website.

Let's start with the first question: Is the Internet able to meet the growing demands on its infrastructure?

The answer is yes, as long as we continue to promote investment in the infrastructure. The explosion of Internet-enabled devices and applications—text messaging, music downloads, VoIP, Blackberries and device-to-device communications—has created exponential growth in Internet traffic far surpassing the increase in users. While users have increased 300 percent since 2000, the volume of traffic on .com and .net has increased 1,900 percent.

VeriSign is proud of the fact that the .com and .net systems have had 100 percent uptime 7 years straight. To support these functions, VeriSign has invested hundreds of millions of dollars into building a global network of computers that are a critical component of the Internet's infrastructure.

VeriSign is not alone in this. There are more than 250 domain registries in the world—for domains such as .fr for France, .de for Germany and what are called generic top-level domains such as .info, .org and .biz. All of these domains have registry operators that, like VeriSign, must operate and invest in critical infrastructure to keep the systems running smoothly.

It is therefore essential that a framework is in place for all operators that drives operational excellence so we can meet the coming demands for the Internet, such as broadcast quality video and other real-time high-bandwidth applications.

Now, to the second question: Is the Internet secure and reliable?

While the Internet has operated remarkably well we can never get lulled into a false sense of security. What makes for good security today is vulnerability tomorrow. We must continually probe our weaknesses and invest and strengthen our networks.

This very growth of Internet users, broadband capacity and number of Internet-enabled devices has created an opportunity for hackers, organized criminals and even more serious terrorists to attack our networks. Some do so for technical tro-

phies, some for political objectives, but today, most bad behavior on the Internet is done for financial gain.

In fact, the very devices and increased bandwidth that make the Internet more robust and user friendly are being deployed to compromise the Internet. Now that computers are always-on, they are easily accessible to hackers and other abusers to hijack. And the increased bandwidth and computing power available literally gives hackers more ammunition to utilize against the infrastructure:

- Regular PCs are being hijacked to mount these attacks. According to CipherTrust, more than 180,000 PCs are illegally hijacked each day and turned into zombies.
- Hackers are utilizing the computing capacity available to their advantage. While a Jupiter Research report in 2004 found that the typical home needed less than 3 Mbps of bandwidth, that level has steadily grown and given the demands of gaming and video that capacity is expected to grow to 57 Mbps by 2009. That means that hackers will have 19 times the computing capacity available to them in the PCs they hijack in that period.

Let me give you some historical examples of what types of attacks we as a community have experienced.

In October 2002, the Internet community got a wake-up call when the 13 DNS root servers, which serve as the heart of the Internet addressing system, came under heavy denial of service (DoS) attack. In these attacks, the hackers send countless bogus inquiries to domain-name servers, which are computers that direct Internet traffic. By sending phony website requests to these servers, they overload and disable them, making websites unavailable.

These attacks significantly impaired the operations of several of the root servers. The industry stepped up, and today an attack of that scale and type would be a blip on the radar.

But hackers never give up innovating. In early January 2006, for example, a hacker systematically disabled over 1,500 websites using hijacked PCs. In these attacks, the hacker didn't directly attack the domain-name servers. Instead, they sent their traffic to a legitimate server with a DNS query and a forged source address.

In this case, the hacker also made the DNS query larger, by a factor of 70 times, which amplified the attack and further disabled the victims servers.

These hackers used hijacked PCs to target their victims over a six-week timeframe. And the scary part is the hacker used a small fraction—32,000 of 500,000 PCs (or just 6 percent)—available to them. This could have been much worse, but it was still severe enough to significantly disrupt the operations of 24 registry operators as well as hundreds of businesses.

These attacks remain under investigation.

The lesson learned is that we must be prepared against all threats. VeriSign, for example, has invested over $250 million in the Internet infrastructure and expects to continue to invest tens of millions of dollars in the near-term to strengthen it against potential attacks.

To put that investment in perspective, VeriSign today can manage 10,000 times the capacity of Internet traffic that it handled in 2000.

Looking Toward the Future

The Internet is made up of a number of entities that all must work together. The root servers serve at the heart of Internet enabling Internet traffic to get to the right address, over 250 domain name registries around the world ensure that each of the domains is operational, service providers such as EarthLink provide service to businesses and consumers, and registrars provide the services that consumers use to register domain names.

The task of maintaining the technical coordination of these sometimes disparate layers falls on ICANN, which gains its authority through a Memo of Understanding, or MOU, with the Department of Commerce.

The Internet community's challenge is to promote innovation so that consumers can do more while strengthening the infrastructure.

In the last year, several steps have been taken by the Internet community to ensure a strong Internet. Progress has been made on introducing internationalizing domain names and expanding both number of Internet addresses available. ICANN has also established a framework for registry operators that both rewards strong performance and provides incentives for investment and imposes safeguards for consumers.

ICANN has implemented new agreements for the .net and .mobi agreements, and proposed new agreements for .com, .info, .biz and .org that incorporate these principles. These agreements, for example, give the operators flexibility to increase

prices while protecting Internet users by, in some cases, imposing limits on the levels of increases and requiring a six-month notice so consumers could lock in at existing prices.

This new framework advances the objective of security and stability by ensuring the necessary investment into the critical infrastructure.

Finally, the question comes to ICANN itself. At the heart of the question is ICANN's independence and what that means for the core infrastructure of the Internet. ICANN has taken steps, through its registry agreements, to become more financially independent. Under the old model, one industry controlled ICANN's budget and that was an unhealthy system.

ICANN has taken steps to get additional funding from the registries without conditions, which means it will have more independence.

To conclude, Mr. Chairman, the last 5 years have brought painful lessons on the importance of preparation. The Internet has worked—in fact, been taken for granted—because we have stayed a step ahead of both the dramatic rise in Internet traffic as well as the nefarious efforts to do it harm.

We must not lose that vigilance and continually take steps to strengthen the Internet so it remains reliable and always available.

Thank you for this opportunity to testify.

The CHAIRMAN. Thank you very much.

I see Senator McCain is here. Senator, have you got a time-frame or do you wish to make a statement?

STATEMENT OF HON. JOHN MCCAIN,
U.S. SENATOR FROM ARIZONA

Senator MCCAIN. Thank you, Mr. Chairman. I just would make a brief comment. Thank you for holding this hearing.

I would point out that since the NTIA published its White Paper on the governance of the Internet's naming and addressing system, we obviously—our government has aspired to turn over the technical management of the DNS to private nonprofit that would be committed to several principles.

I apologize for not being able to stay. I wanted to thank the witnesses. This is a very important issue. And one of my many concerns is truly making sure that competition and the resulting benefits to consumers exists in the DNS.

And a lot of people don't understand this issue, Mr. Chairman, but I think it's a very important one, and I thank you for holding this hearing, and I hope we can move forward to a resolution to it.

I thank you, Mr. Chairman.

The CHAIRMAN. Thank you very much.

We'll next turn to Christine Jones, General Counsel, Corporate Secretary, for Go Daddy Group. Glad to have you with us.

STATEMENT OF CHRISTINE N. JONES, GENERAL COUNSEL/
CORPORATE SECRETARY, THE GO DADDY GROUP, INC.

Ms. JONES. Thank you. Good morning, Mr. Chairman, and members of the Committee.

I'm Christine Jones—as you said, General Counsel and Corporate Secretary of The Go Daddy Group. We're happy to be here with ICANN and VeriSign. We are ICANN's largest benefactor and VeriSign's largest customer, so we feel it's only fitting that we should be sitting here at the table with them today.

I'm going to focus my remarks on three principal issues that you raised with earlier witnesses: the renewal of the Memorandum of Understanding between the Department of Commerce and ICANN,

the .com Registry Agreement, and the security and stability of the Internet.

The Go Daddy Group is an Arizona corporation. It consists of eight ICANN-accredited registrars, including *GoDaddy.com,* our flagship company. When I joined Go Daddy in 2002, it was a very small registrar, with well under 100 employees. Today, we have over 15 million domain names under management, and we're the number-one registrar in the world. That means we register a domain name once every 3 seconds or less. And every time we do, VeriSign gets another $6 from us. We currently employ over 1,200 people, and we do not utilize any offshore outsourcing of any kind. And we're committed to that.

I want to talk about the renewal of the Memorandum of Understanding. There was a DNS White Paper, which was first published in 1998. That paper articulated that principles of accountability, competition, private, bottom-up coordination and representation, were necessary for guiding the transition to private sector of the Internet domain-name system. And we believe that those principles still remain relevant today.

ICANN has made some progress toward achieving some of the goals there, but not all of them. Specifically—and this was a question that came up with the government witnesses—ICANN has not yet achieved the competition goal, nor have they achieved this private, bottom-up coordination and representation called for even in their own bylaws. And the events of the last 2 years call into question whether or not ICANN will ever be able to accomplish those goals in the future.

The MOU, which is set to expire next Saturday, should be extended, but it should also be modified to stress the need to correct these deficiencies and require a clear roadmap from ICANN as to how it will regain the confidence of the community upon which its existence relies. This Committee's commitment to ensuring ICANN appropriately administer that system is vital.

Private, bottom-up coordination and representation should be a guiding principle in the ICANN policymaking process. While we have repeatedly urged ICANN to abide by this principle, they have chosen, instead, to conduct business behind closed doors and without input from the ICANN community. Unfortunately, ICANN has yet to commit to—or perhaps they are unable to commit to—openness, transparency, and accountability. The manner in which the new dot-com agreement was negotiated is a relevant example of ICANN and VeriSign getting together off the record, creating a mutually beneficial policy, and then boldly announcing that they have made a decision without input from any of the stakeholders.

ICANN is responsible for an important public trust. To preserve that public trust, it is vital that all stakeholders have access to and recognize input into these types of discussions. The entire Internet community should be made to fully understand the reasons for ICANN's decisions and to have effective and unbiased recourse if they have reason to question those processes and decisions.

ICANN's bylaws specifically state—and I'm quoting—"ICANN and its constituent bodies shall operate, to the maximum extent feasible, in an open and transparent manner and consistent with procedures designed to ensure fairness," and, "in carrying out its

mission as set out in these bylaws, ICANN should be accountable to the community for operating in a manner that is consistent with these bylaws."

Now, despite those provisions, there is no appropriate accountability mechanism in place to impartially review ICANN Board actions. It doesn't exist. There are two accountability and review mechanisms defined in the bylaws. One is called "reconsideration," and one is called "independent review." "Reconsideration" is basically the Board reviewing itself. And "independent review" is a mechanism which is entirely untested and has never been used.

We believe there needs to be an independent evaluation of how these accountability mechanisms have worked, or will work, and the implementation of any adjustments recommended as a result of that evaluation should be undertaken before any final transition can be contemplated.

So, we believe the MOU must be revised to include openness and transparency as overall guiding principles if we are ever to see an effective transition of the Internet DNS management to the private sector through ICANN.

We would be happy to be involved in the process of determining appropriate revisions, if that assistance would help move the ball forward. We'd be happy to volunteer to be involved in that.

On security and stability, like all of us in this room and at this table, Go Daddy believes that the security and stability of the Internet is vital. We devote considerable time and resources to working with law enforcement on preserving the integrity and safety of the Internet by quickly closing down websites and domain names engaged in illegal activities. We work with law enforcement agencies at all levels and routinely assist in a wide variety of criminal and civil investigations. We're also quick to respond to complaints of spam and phishing and pharming and online fraud, and the subject matter of yesterday's hearing, Internet child pornography. And we work closely with anti-fraud and security groups such as the Anti-Phishing Working Group, the Digital PhishNet, the National Center for Missing and Exploited Children, and CyberTipline.

I personally, and this company in general, have made it a high priority to use our position as a registrar to make the Internet a better and safer place, and we feel very strongly about that.

We recognize that VeriSign also has an important role to play in the security and stability of the Internet. They manage the entire infrastructure that supports the largest generic top-level domain, the dot-com. That's why it's incredible to us that ICANN did not include an infrastructure investment requirement in the proposed dot-com agreement. In negotiating that agreement, VeriSign ensured that their revenue would increase, and ICANN ensured that their budget would benefit, but who's going to ensure the benefits of the public interest, as well? This Committee should insist that the agreement between VeriSign and ICANN require VeriSign to invest in continued infrastructure in the future.

VeriSign has over a billion dollars at stake—$1 billion—if the proposed .com Registry Agreement is not approved. Because a substantial portion of that $1 billion comes from Go Daddy customers, I'd like to focus on that agreement for a minute.

According to ICANN, 75 percent of all generic top-level domains are registered in the dot-com. Dot-com names accounted for over 80 percent of the growth in the generic top-level domain-name space in 2005. Today, there are over 56 million dot-com names registered. One of those is *SenatorStevens.com,* I'm sure. We'll be happy to try to help to track that down, if you'd like. That number is projected to grow to over——

The CHAIRMAN. Let me say that was just an example.

[Laughter.]

The CHAIRMAN. I don't want to get involved in this anymore than I already am.

[Laughter.]

Ms. JONES. Yes, too late, sir.

[Laughter.]

Ms. JONES. OK, so that number is projected to grow to over 61 million by the end of the year, and to over 350 million—350 million—dot-com names by the end of 2012. That means VeriSign gets this huge windfall, if this agreement is approved.

The form of presumptive renewal in the proposed agreement is simply anticompetitive. The form of renewal eliminates the possibility that dot-com could ever be rebid to allow true market mechanisms to set the price for dot-com.

It's important to note that when the dot-net contract was rebid last year, it resulted in a price reduction of over 28 percent, from $6 down to $3.50, a price that was appropriate to the then-existing market conditions.

Other legitimate monopoly companies, such as the Bell Companies, for example, must justify their price increases, and VeriSign, the monopoly provider, should be required to do the same.

I'd like to thank you, Chairman Stevens and Senator Smith and the members of the Committee, for the generous invitation to testify today. We agree that the secure future of the Internet is paramount to the overall success of our economy, and that of the global community, as well. Your commitment to bringing attention to this issue is sincerely appreciated.

Inasmuch as the current agreement between ICANN and VeriSign does not expire until November 10, 2007, I respectfully request that this Committee direct the NTIA not to approve the agreement until such time as it has been reviewed in an open and transparent manner by the entire ICANN community.

Thank you.

[The prepared statement of Ms. Jones follows:]

PREPARED STATEMENT OF CHRISTINE N. JONES, GENERAL COUNSEL/CORPORATE SECRETARY, THE GO DADDY GROUP, INC.

Introduction

Good morning Mr. Chairman and members of the Committee. I am Christine Jones, General Counsel and Corporate Secretary of The Go Daddy Group, Inc.

First, I would like to thank you, Chairman Smith, for the kind invitation to testify today regarding Internet governance and the future of the Internet Corporation for Assigned Names and Numbers (ICANN). We are thankful for your attention to this important issue and for recognizing that the Internet is a resource significant enough to deserve the attention of the U.S. Senate. We agree that its secure future is paramount to the overall success of our economy, and that of the global community, as well. The future of ICANN rests with the public that it was formed to benefit. That community's confidence in ICANN has been shaken by the lack of open-

ness and transparency; by the apparent unwillingness of the ICANN Board of Directors to be accountable to anyone but itself; and, the giant step backward that is now being taken by the introduction of anticompetitive registry agreements that threaten to undo what progress has been made.

The Memorandum of Understanding between ICANN and the Department of Commerce should be extended and modified to stress the need to correct these deficiencies and require a clear roadmap from ICANN as to how it will regain the confidence of the community upon which its existence relies. This Committee's commitment to ensuring ICANN appropriately administer that system is vital.

Background

The Go Daddy Group, Inc. consists of eight ICANN-Accredited registrars, including *GoDaddy.com.* When I joined Go Daddy in early 2002, it was a very small registrar with well under 100 employees. Today, we have over fifteen million domain names under management, and are the number one registrar in the world. That means we register a domain name once every 3 seconds or less. Go Daddy is also the largest provider of hostnames in the world today. We currently employ over 1,200 people and do not utilize offshore outsourcing of any kind.

The Go Daddy Group devotes considerable time and resources to working with law enforcement on preserving the integrity and safety of the Internet by quickly closing down websites and domain names engaged in illegal activities. We work with law enforcement agencies at all levels and routinely assist in a wide variety of criminal and civil investigations. We are also quick to respond to complaints of spam, phishing, pharming, and online fraud and work closely with anti-fraud and security groups such as the Anti-Phishing Working Group, Digital Phish Net, the National Center for Missing and Exploited Children, and CyberTipLine. I personally, and the company in general, have made it a high priority to use our position as a registrar to make the Internet a better and safer place.

The Go Daddy Group has been an active supporter of ICANN processes for over 5 years. We continue to believe in the validity of the transition of management of the Internet Domain Naming System (DNS) to the private sector, but we have serious concerns regarding the progress of that transition to ICANN.

The *DNS White Paper,* first published in 1998, articulated that principles of accountability, competition, private, bottom-up coordination, and representation are necessary for guiding the transition to private sector management of the Internet DNS. We believe those principles remain relevant, but our testimony will explain why we also believe those principles have not yet been fully accomplished by ICANN, and why the events of the last 2 years bring into question whether ICANN will be able to accomplish them in the future.

Competition

Significant progress has been made in regards to competition at the registrar level. However, that is only half the equation. The .com extension still maintains overwhelming dominance among the generic top level domain (gTLD) registries. In addition, the new form of registry agreement that has been proposed for the .com registry, as well as the other gTLD registries, threatens to further entrench that dominance and even negate competition at the registrar level:

Proposed .com Registry Agreement

It's important to first understand the current metrics involved with the .com registry:

- According to the monthly registry reports posted on ICANN's website, .com still accounted for 75 percent of all gTLD registered domain names at the end of 2005, and accounted for over 80 percent of the growth in the gTLD name space during 2005.
- The number of registered .com domain names is growing at increasing rates year over year. The .com registry increased by over 16 percent in 2003, over 25 percent in 2004, and almost 34 percent in 2005.
- There are over 56 million .com names registered as of the date of this testimony. That represents a 25 percent growth so far in 2006 and projects to 35 percent growth for the year, to over 61 million .com domain names.
- If .com just maintains a 34 percent growth rate over the life of the proposed agreement, it will grow to over 350 million domain names by the end of 2012.
- As a result, the incremental revenue from the 7 percent price increases in 4 of the 6 years as allowed in the proposed agreements will provide VeriSign a windfall of over $1.8 billion.

- For example, if you go to *www.GoDaddy.com* and register the domain name *www.ChairmanSmith.com,* you would pay a maximum of $8.95 per year for that domain name registration. Of that $8.95, by the current .com contract, $6.00 goes to VeriSign, $.25 goes to ICANN as a transaction fee, and the balance of it goes to operating expenses and profit for Go Daddy. Taking this example further, if some portion of the current 56 million .com names are renewed, under the proposed agreement, $6.00 would still go to VeriSign, plus an automatic increase of 7 percent in 4 out of the next 6 years, an increase without price justification. This is an extraordinary profit and these are just the renewals.

Of course, that windfall will come at the expense of consumers. The increasing costs of .com will result in a leveling effect of .com retail prices. At the same time, it provides VeriSign a marketing fund of gigantic proportions in comparison to its so-called competitors. As a public company with a fiduciary responsibility to its shareholders, VeriSign will no doubt use these funds to market and innovate at a level with which other gTLDs will not be able to compete. Given the market power that .com continues to hold, allowing VeriSign this windfall is inappropriate for an organization committed to the promotion of competition.

The form of presumptive renewal in the proposed .com agreement is also anti-competitive. It substantially allows a perpetual agreement unless VeriSign breaches its agreement *and* fails to cure. It even allows for repeated breaches with only monetary fines as the penalty. This form of renewal eliminates the possibility that .com could ever be re-bid to allow true market mechanisms to set the price for .com. It is important to note that when the .net contract was re-bid, it resulted in a price reduction of over 28 percent, from $6.00 per .net domain name to $3.50. a price appropriate to then existing market conditions.

In addition, this form of presumptive renewal leaves no way ICANN can ever decide to re-bid .com based on VeriSign's performance as a steward of the .com name space. Note the four conditions below (emphasis ours) under which ICANN could decide not to renew .com under Section 25.B of the current agreement. They no longer exist in the proposed COM agreement.

Registry Operator shall be awarded a four-year renewal term *unless ICANN demonstrates that*: (a) Registry Operator is in material breach of this Registry Agreement, (b) *Registry Operator has not provided and will not provide a substantial service to the Internet community* in its performance under this Registry Agreement, (c) *Registry Operator is not qualified to operate the Registry TLD during the renewal term,* or (d) the maximum price for initial and renewal registrations proposed in the Renewal Proposal exceeds the price permitted under Section 22 of this Registry Agreement.

Removing the above requirements is particularly alarming given that under the proposed agreement, VeriSign is not required to make infrastructure investments or demonstrate that such investments are being made. What are they going to do with the $1.8 billion windfall? How do they intend to accommodate the projected growth of the .com name space to over 350 million domain names, an increase of almost 600 percent over the life of the proposed agreement? It is a serious mistake on the part of ICANN to not ensure that appropriate investments in infrastructure will be made, especially considering their overall mission of the security and stability of the Internet. The .com name space is too important to simply assume that a wide open presumptive renewal is enough incentive for the registry operator to make appropriate investments. The proposed .com agreement must, therefore, be refined before it is approved by the NTIA.

Future of New gTLDs

We believe an effective and objective process for introducing new gTLDs is another important change that needs to take place to increase competition at the registry level. In fact, that is one of the specific tasks set out in section II.C. of Amendment 6 of the Memorandum of Understanding under which ICANN currently operates with the Department of Commerce:

> 8. Continue the process of implementing new top level domains (TLDs), which process shall include consideration and evaluation of:
>
> a. The potential impact of new TLDs on the Internet root server system and Internet stability;
>
> b. The creation and implementation of selection criteria for new and existing TLD registries, including public explanation of the process, selection criteria, and the rationale for selection decisions;
>
> c. Potential consumer benefits/costs associated with establishing a competitive environment for TLD registries; and,

d. Recommendations from expert advisory panels, bodies, agencies, or organizations regarding economic, competition, trademark, and intellectual property issues.

Define and implement a predictable strategy for selecting new TLDs using straightforward, transparent, and objective procedures that preserve the stability of the Internet (strategy development to be completed by September 30, 2004 and implementation to commence by December 31, 2004).

A successful process for new gTLDs is an important element for introducing competition into the gTLD space. The trickle of new gTLDs we have seen so far has done little to change the market power that .com has maintained since before the initial publication of the *DNS White Paper* in 1998.

The Policy Development Process that will ultimately recommend a process to fulfill the principles stated in task 8 above was initiated by the Generic Names Supporting Organization (GNSO) early in December 2005. The current timeline calls for these recommendations to be presented to the ICANN Board of Directors at the end of this year, a best case scenario. It will be well into 2007 before the evaluation of the success of any resultant process could even begin to be undertaken.

We believe fulfillment of this task is crucial to the future of ICANN and believe it important not to complete the transition of the management of the Internet DNS until a successful and sustainable process for the introduction of new gTLD is firmly in place.

Competition exists at the registrar level only. The .com name space continues to overwhelmingly dominate the gTLD domain name market. The anti-competitive form of registry agreements being contemplated by ICANN and the DOC could very well threaten existing competition even at the registrar level. Promoting competition, and doing so successfully, needs to remain a core task for ICANN if it is to maintain the support of the public it has been formed to benefit.

Private, Bottom-Up Coordination, and Representation

- The principles of private, bottom-up coordination, and representation cannot be fully realized without ICANN's commitment to openness, transparency, and accountability. ICANN is responsible for an important public trust. To succeed, it is vital that all stakeholders have access to those processes;
- Fully understand the reasons for ICANN's decisions as a result of those processes;
- And have effective and unbiased recourse if they have reason to question those processes and decisions.

Indeed, ICANN's own bylaws state: "ICANN and its constituent bodies shall operate to the maximum extent feasible in an open and transparent manner and consistent with procedures designed to ensure fairness," and "In carrying out its mission as set out in these Bylaws, ICANN should be accountable to the community for operating in a manner that is consistent with these Bylaws."

ICANN's Articles of Incorporation state that ICANN is a nonprofit public benefit corporation and is not organized for the private gain of any person. As such, Directors are bound in the bylaws to act in the best interests of that public benefit and to do so in an open and transparent manner.

However, a number of examples over the last few years demonstrate the failure of the ICANN Board and Staff to follow through on these obligations.

The .net Registry Agreement

The registry agreement that resulted from the .net re-bid was executed by ICANN before the final draft was posted for public comment. This agreement represented a significant shift in ICANN's policy regarding the management of the gTLD DNS and name space. The public that ICANN's actions supposedly benefited cried out loud and hard about these policy changes without due process within the community. The community pointed out several problems with the agreement that they believed benefited only the registry and ICANN's corporate structure at the community's expense. Ultimately, some minor compromises were agreed to by the winning registry, and the ICANN Board publicly apologized and committed to do better.

The .com Registry Agreement and Law Suit Settlement

The ICANN Board's idea of doing better was posting a notice that it had reached a settlement agreement with VeriSign to end a long-standing lawsuit. While it is true that ICANN posted the settlement agreement for public comment, there had been no prior indication of what ICANN was doing in this regard, or that it again was considering changes in long understood policy in order to settle the suit. In fact,

these policy changes were the exact same ones that the community had complained about in regards to the .net Registry Agreement.

Once again, as this Committee well knows, the community that ICANN was supposedly benefiting by this settlement made its displeasure known loud and clear, especially in regards to the unexpected and early renewal of .com registry agreement that was part of the settlement. Ultimately, minor changes to the .com registry agreement were agreed to by ICANN and VeriSign. These changes did little to address the overwhelming concerns of the Internet community. Once again, ICANN chose to benefit itself at the expense of the public as a whole.

Other Registry Agreements

Most recently, the ICANN Board posted proposed new agreements (not renewals) to the .biz, .info, and .org registry operator agreements. Once again, there was no prior notice that, despite the previous outrage expressed by the Internet community regarding the .com and .net agreements, the ICANN Board was going to implement the exact same policy changes in all new gTLD DNS and name space management agreements. This belies ICANN's promise to do better and is in direct contravention to their obligation to operate an open and transparent manner.

This fact is even more serious as it relates to these proposed new agreements. After the .net and .com agreement fiascos, the Generic Name Supporting Organization (GNSO), which was appointed by ICANN's bylaws for the specific purpose of recommending policy regarding the gTLD DNS and name space, initiated a Policy Development Process (PDP) to address the concerns raised by the community. It now appears that the ICANN Board of Directors no longer believes it is bound by its own bylaws and is moving ahead without waiting for the outcome of the GNSO's PDP findings. This is yet another poignant example of why the Department of Commerce must maintain control over ICANN, even after the current Memorandum of Understanding expires on September 30, 2006.

Lack of Appropriate Accountability and Review Mechanisms

All of the above is exacerbated by the fact there are no appropriate accountability mechanisms in place to impartially review ICANN Board actions. There are currently two accountability and review mechanisms defined in ICANN's bylaws:

- Reconsideration—This is basically the Board reviewing itself. The criteria the process calls for is restrictive and not useful for most instances where affected stakeholders question an action of the Board. In addition, the fact that transcripts or recordings of Board meetings have never been made available make it difficult if not impossible for those affected by Board actions to effectively evaluate whether their concerns or questions meet the criteria of the bylaws.
- Independent Review—This mechanism is entirely untested and has never been used.

We also invite you to visit ICANN's website and see if you can discover how to take advantage of either of these accountability mechanisms. It is next to impossible to find anything of substance about how to file either a Reconsider Request or a Request for Independent Review, or even who the Independent Review agent actually is.

We believe there needs to be an independent evaluation of how these accountability mechanisms have worked, or will work, and the implementation of any adjustments recommended as a result of that evaluation should be undertaken before any final transition can be contemplated.

The interests and support of the community ICANN is supposed to benefit is shifting. The World Summit on the Information Society (WSIS) and the resultant Internet Governance Forum (IGF) is an outcome of that shift. These failures on the part of ICANN to adhere to the principles espoused in its own bylaws and Articles of Incorporation are accelerating that shift. It is clear that ICANN's Memorandum of Understanding with the Department of Commerce must be extended and modified. Openness and transparency are only hinted at in the current Memorandum of Understanding. We believe the Memorandum of Understanding should be revised to include openness and transparency as overall guiding principles if we are to ever see an effective transition of the Internet DNS management to the private sector through ICANN.

Conclusion

The future of ICANN rests with the public that it was formed to benefit. That community's confidence in ICANN has been shaken by the lack of openness and transparency; by the apparent lack of the ICANN Board of Directors to be accountable to anyone but itself, and the giant step backward that is now being taken by

the introduction of anti-competitive registry agreements that threaten to undo what progress has been made.

The Memorandum of Understanding between the Department of Commerce and ICANN should be extended and modified to stress the need to correct these deficiencies and require a clear roadmap from ICANN as to how it will regain the confidence of the community upon which its existence relies.

Thank you again, Mr. Chairman, for the opportunity to be heard on these important issues. Your commitment, and the commitment of the members of this Committee, to bringing attention to issues impacting the future of the Internet is sincerely appreciated. I would be happy to answer any questions you may have.

The CHAIRMAN. Senator Smith is here, and I do want to yield the Chair to him. I've got to say that from my perspective, we ought to have a go-lightly approach, because I think the worse thing to happen to the Internet would be to have us start trying to regulate it from Congress. We have to find a way to assist, to make sure that the transparency and responsibility, and, really, antimonopoly concepts, are there for someone like the FTC or the Department of Commerce to make proper inquiries, and, if necessary, deal with it. But I don't think we want to start a process of increasing regulation on the Net.

I do agree, however, that we've got a real difficult problem, because we're just back from China, some of us, in August, and we've had some conversations over there about the Net and about the U.S. domination of the management of the Net. We have to find some way to take this to an international forum where we can get an agreement that this is a process that the governments of the world ought to keep their hands off, but ensure it will function through proper transparency and proper participation for all users. I don't know how we're going to walk down that road, but we're going to continue to have an interest in, and pay attention to, and have hearings on, this matter to let more and more people express their points-of-view, and hopefully we might even work up a trip to go to meet with some of our counterparts in other governments, particularly in the very large governments, such as China and India and the very populated countries that want to have more of a role in how this process functions in their country. But it's a very delicate issue, as far as I'm concerned.

So, I'm happy to see you back, Mr. Chairman.

STATEMENT OF HON. GORDON H. SMITH, U.S. SENATOR FROM OREGON

Senator SMITH [presiding]. Thank you very much, Chairman Stevens. And I apologize to all of you for an unavoidable emergency, but I'm glad to be here.

The CHAIRMAN. Could I just do one thing? I'd like to place in the record, the Glossary of Internet Governance Terms and Organizations that was prepared by our staff to help us understand the process we have here today.

Thank you.

[The information referred to follows:]

Glossary of Internet Governance Terms and Organizations

ccTLD	Country code Top Level Domain	Two-letter long top-level domain (TLD) used and reserved for a country or a dependent territory (.uk for United Kingdom, .jp for Japan, etc.)
DNS	Domain Name System	Translates domain names into IP addresses
gTLD	Generic Top Level Domain	TLD domains used worldwide, such as .com, .org, .net and .info
ICT	Information and Communication Technology	General term for the use of technology in managing and processing information, especially in large organizations
IANA	Internet Assigned Numbers Authority	Operated by ICANN, oversees global IP address allocation, DNS root zone management, and other Internet protocol assignments. The technical side of ICANN is referred to as "the IANA function"
ICANN	Internet Corporation for Assigned Names and Numbers	Oversees a number of Internet-related tasks, including managing the assignment of domain names and IP addresses, including the introduction of new generic top-level domains
IGF	Internet Governance Forum	Created at 2005 WSIS in Tunis. IGF's first meeting is scheduled for October 2006 in Athens
ITU	International Telecommunications Union	International organization within the U.N. where governments and the private sector coordinate global telecom networks and services; WSIS and IGF (see below) fall under ITU's purview
NGO	Non Governmental Organization	Group or association that acts outside of institutionalized political structures and pursues matters of interest to its members
NTIA	National Telecommunications and Information Administration	Agency of the Department of Commerce serving as principal adviser on telecommunications policies, including economic and technological advancement
Registrar		A body recognized by a registry to sell/register domain names (GoDaddy, AfterNic, eNom, etc.)
Registry		A company or organization maintaining a centralized database for the TLDs or for some IP address blocks
WGIG	Working Group on Internet Governance	U.N. working group set up after 2003 WSIS in Geneva to make proposals for Internet governance at the 2005 WSIS in Tunis
WHOIS		Method of querying a registry or registrar database to determine the owner of domain name
WSIS	World Summit on Information Society	A series of meetings on information and communications, including Internet governance, under the purview of the IU and UN

Senator SMITH. Thank you, sir.
Senator Burns?
Senator BURNS. Thank you, Mr. Chairman.

Dr. Twomey, you have a Working Group on Internet Governance here from the U.N. What kind of a group is this, and what standing does it have with regard to ICANN?

Dr. TWOMEY. Thank you, Senator. Good to see you again.

Senator BURNS. Good to see you.

Dr. TWOMEY. That working group has actually completed its work. It was an input to the U.N.'s World Summit on Information Society. It, also, has finished its work. The implications for ICANN have not been anything significant, in terms of the need to change, although you and Senator Stevens have pointed out the international interests, obviously, in some of these areas.

The U.N. continues to run a—what's called the Internet Governance Forum. It's basically, a meeting point for discussion. But, in terms of ICANN's own operations now, there is—although this is an ongoing area for monitoring, they don't have direct effect at all.

Senator BURNS. In other words, they don't have any official standing with ICANN, then.

Dr. TWOMEY. No.

Senator BURNS. And we heard, in the testimony of Ms. Jones, of the 5-day waiting period. Are you doing anything to address that? I guess it caused—some problems are created by that grace period. Can you address that situation and bring us up—tell us, kind of, what it is and how it affects your operation.

Dr. TWOMEY. Senator, you're pointing out there's a—with the registries, some of them have agreements—well, they have agreements with registrars which allow for the registration of a name, but not for the payment of that name, within—for a 5-day period. And there is an emerging pattern of people putting names in, in day one, and seeing whether there's any value in those names, particularly for online advertising, by day five. If there's not, they keep it—if there is, they keep it; if it's not, they give it back. There are some aspects about this that our compliance people are actually looking into, but there are also aspects about this which are part of the market operating.

Senator BURNS. Do you want to comment on that, Ms. Jones?

Ms. JONES. Well, we have provided, upon ICANN's specific request, detailed information about registrars who are engaged in the practice of purchasing—or registering domain names and then deleting them before the 5-day grace period expires.

Senator BURNS. Is that term—that's "tasting"?

Ms. JONES. We would call that "domain-name kiting."

Senator BURNS. Kiting?

Ms. JONES. Yes. So, it would be like "check kiting," but only with a domain name, where you register it and then you get a refund before the 5-day grace period ends, so you never have to pay for it, essentially. We've provided information, and they've assured us that they would investigate further, to the openness and transparency discussion that we had earlier. We haven't heard anything back from them.

We would like for the whole entire practice to be eliminated. It does appear to be, at least in spirit, a violation of the contract that registrars have as a part of their accreditation.

Senator BURNS. What is the cost of that registrar? What does it cost?

Ms. JONES. Well, for example, with a dot-com name, it would cost $6 to register the name, and then you would get the entire $6 back when you cancel the registration within that 5-day period. So, it wouldn't cost you anything. And that's the insidious part of the whole practice, is that basically you're using domain names, and taking them away from other legitimate users, without paying for them.

Senator BURNS. OK. I guess—maybe the next question—Dr. Twomey said—can you justify doubling your budget in the last 5 years?

Dr. TWOMEY. Well, let me just—to the point just made, Senator, I have confirmed, personally, with the CEO of Go Daddy, that we are investigating this, and we will investigate this particular thing you just referred to——

Senator BURNS. OK.

Dr. TWOMEY.—in—within our compliance terms.

To come to your point about budget, the demands on—for the coordination of the DNS to do the sorts of compliance work we're talking about just in this conversation, to do many of the things that Christine has already raised, and to be able to support the large growth of the DNS, has—does require additional resources. We have moved to increase that budget. That budget process is done, Senator, through a very bottom-up process. We have a process of—where we have a strategic plan that the community develops. Behind that strategic plan, we then develop—there's an operational plan the community all responds on, project by project, and, at the end of that process, it's actually then calculated how much does it cost us to do all these things the community wants us to do? And that's the process which has actually driven the increase in the budget, as a reaction back to the things that people want to do.

The budget is not a huge amount of money. For this coming financial year, it is budgeted for about $33 million. So, that's for the coordination of all of these factors coming out of that community process.

I'm very, very conscious of the need for accountability on that, and for transparency, and we do have, I think, a very accountable and transparent process. I wonder if I might just comment on that.

One of the things that I'm very conscious of, as the President of ICANN, is, I think, as an organization, we are actually very transparent. But, at the moment, we're suffering a little bit of being transparent, like credit card agreements are transparent—everything's there, but it's not necessarily easy for people to understand what's there. And I think that's one of our great tasks, going forward. We need to make it not only transparent, but more easy for people to understand what's in the material and what's being put forward. And that's one of our very high priorities this coming year.

So, there's a distinction, I think, between being transparent and being accessible, and accessibility is one of our challenges, at the moment.

Senator BURNS. Well, it seems to me that the matter of transparency has surfaced here, and I guess that would—I could follow-up—the leverage that the registrars have with regard to the proc-

ess of ICANN and also with regard to their budget, do they have any leverage in that?

Dr. TWOMEY. Well, Senator, it's a good question. The registrars, 2 years ago—well, 18 months ago—constituted the—by far, the greatest contribution to the ICANN budget. And, at the time, they themselves asked us to make an effort to rebalance their contribution to ensure that the registrees made more contributions. So, in the discussions with the registrees concerning their contracts, we have actually moved to change the financial flow so that there is more contribution, then, from the registrees. We have frozen any increases from the registrars on any sort of per-transaction basis, and, indeed, we'd look at—they've got proposals in front of us of being able to change that and amend it, and we are open to alternative sources of revenue. If the registrars put forward to us different views, we'd decrease their contributions further, as well. So, we are very open to their input about ensuring we have a widely balanced budget and sources of revenue, and we've been working toward that, quite specifically.

The registry agreements, including the dot-com agreement, have terms in there specifically coming out of that conversation, to shift the balance of contribution.

Senator BURNS. Thank you, Mr. Chairman.

The CHAIRMAN. Mr. Chairman, if I may——

Senator SMITH. Yes, of course.

The CHAIRMAN. For your information, I've just had a discussion with Senator Smith. You know, at times we run into subjects we need to know a lot more about. And we've had a little habit of calling just for listening sessions. I think, assuming the management doesn't change around here after this new period we're going to go through here——

[Laughter.]

The CHAIRMAN.—I would want to hold a listening session and get people to come in and just tell us what their function is and how they view this arrangement, and how much they think we ought to be involved, or ought not to be involved. We ought to do some listening on this one before we really react.

Ms. Jones, I appreciate your comments, and I'm sure that Dr. Twomey wants to have some counter-comments. But we used that process in approaching the communications bill, and it worked very well. And I would like to hold a listening session early next year, if that's agreeable to you, Mr. Chairman.

Senator SMITH. Yes, I would heartily agree with that as a need, and certainly, I think we should consult Chairman-in-waiting, Senator Pryor.

[Laughter.]

Senator SMITH. But obviously it's the kind of thing that we all look for more knowledge on.

The CHAIRMAN. Well, I have a feeling Senator Inouye would agree.

Thank you very much. I must go to another meeting.

Senator SMITH. OK. Thank you, Senator.

Senator Pryor?

Senator PRYOR. Thank you, Mr. Chairman.

Dr. Twomey—is that how you pronounce your name—Twomey? I would like to—I don't know if you heard my last series of questions with the previous panel, but I'd like to ask you about the dot-xxx domain. And I would like to understand what happened. You know, my impression was that dot-xxx had a lot of support, that a lot of folks here in this country and around the world thought it was a good idea, could be a good development. But it didn't happen. So, I'd like to hear ICANN's version of the facts there and what happened.

Dr. TWOMEY. Senator, ICANN put out, as part of the process for introducing more competition among the gTLD space, a round of so-called "sponsored top-level domains," top-level domains that are sponsored by a community or a particular grouping for the use of their own community. We received ten applications. One of those applications was for dot-xxx for the community of responsible adult-content providers, as they put it. That—our processes of—included the posting of these agreements, the posting of the comments, and allowed for a lot of public comment on those consultations. It also allows for comments from our various supporting organizations, and, very importantly, allows for—in our bylaws, for the advice of public—for the provision of public policy advice from the Governmental Advisory Committee on which there are over a hundred governments participating.

As the process continued with those various registries, particularly dot-xxx, we received a lot of public comments. We received, I would say, over 100,000 comments from various—online comments from various members of different associations in the United States against the dot-xxx. We received various comments from people in favor of it. And we did receive requests from governments—not just the United States, but a number of other governments—asking for more time to allow governments to consider the implications of the application. We had a meeting in March this year in Wellington, New Zealand, and in that meeting the Governmental Advisory Committee put forward some advice concerning public-policy issues.

The Board eventually made a decision based on a number of issues that—the reasons for those decisions were made public for each of the Board Members. It's not one comprehensive set of reasons. But not in a majority—not in a unanimous sense, but in a majority sense, most of the Board Members decided that the contract, as put before us by the applicant—and at the time when the applicant asked us, the applicant not only put forward to us a redraft of the contract, but said, "Please vote on this now"—the majority of the board, on the basis of that contract, felt that they could not proceed, a number of us feeling that some of the provisions in the contract were not enforceable.

So, that's the sort of formal status of the process that was followed. It has a lot to do with the nature of the contractual language put forward by the applicant, and a lot to do with the timing of the request for actually proceeding with that vote.

Senator PRYOR. Well, that may actually go to Senator Stevens' previous point about, maybe we need to know more about this. And maybe this also illustrates one of the problems, at least from the outside looking in, with ICANN, is that there's not a lot of trans-

parency there, and—at least that's the perception. And you all go through this process, and you're in New Zealand, and you make this decision, and I guess I don't know what it means that parts of the contract are not enforceable. What does that mean, "parts of the contract are not enforceable"?

Dr. TWOMEY. There were aspects of the contract language that was put forward that some Members of the Board—and I should let the record speak for itself, Senator. I mean, I—the Senate—the record of the ICANN Board meeting is available publicly, and the decision was available publicly. And the actual wordings of individual Board Members on their rationale for decisionmaking is there, available. I—and they felt that certain parts of the—being able to—certain language related to enforcing all public—all relevant public policy from all relevant countries was, sort of, language that some of them found it difficult to consider that was enforceable under the contract. I give that as an example, but I should point back to the record. We actually—and we can—I can—I'm happy to come back to you in writing to point out the—that record, point out the reasons given by the Board Members who were voting.

Senator PRYOR. Yes, I'd like for you to do that.

[The documents from the March 25–31, 2006 meeting in Wellington, New Zealand are available at *http://www.icann.org/en/meetings/wellington/*].

You said that you had about 100,000 negative responses from inside the U.S. Do you know, were those generated by groups or were those just——

Dr. TWOMEY. They were generated by groups, the—groups like the American Family Association and others.

Senator PRYOR. OK. And apparently some asked for more time, as well. Has ICANN decided to give this more time, or have you just—is this a flat rejection?

Dr. TWOMEY. There was extensive period of time additionally given to this particular application, at that request. And we're—it was the applicant who, themselves, said, "Please move forward with this vote. Please, we'd like you to move it to the vote now and make a decision, one way or the other," when that decision was made.

Senator PRYOR. Has there been any follow-up with the applicant to see if they want to make another run at this?

Dr. TWOMEY. The applicant has—the process is not completed, because we do have two rounds of—two processes for review available to the applicant, both a review committee of the Board and then an independent review panel, an independent arbitrator.

Senator PRYOR. Have that——

Dr. TWOMEY. And then——

Senator PRYOR. Has the applicant requested review?

Dr. TWOMEY. They have requested—they have requested a review—the review is underway—but those two mechanisms are still available to the applicant.

Senator PRYOR. OK.

Mr. Chairman, that's all I have right now. I may have some more in writing, but I know we're trying to get to a vote here in a few minutes.

Senator SMITH. Well, thank you very much, Senator Pryor. And I'll also have some written questions, because of the vote.

But I do want to ask one, and if you can answer as briefly as possible so I can hear your answers, I would appreciate it. As you all know, in 2005 the current dot-com registry operator won a competitive bid process to continue to operate the dot-net domain registry. And, with that, the prices have fallen, or at least, for dot-net, dropped from $6 to 3.50 through the end of 2006. At the same time, lots of security measures, I believe, have been put into the system including infrastructure investments. The competitive model seemed to work in dot-net, but now, the proposed dot-com registry contract apparently removes all of that and puts in automatic price increases. And I'm just wondering if that's defensible, if that's the right thing.

Dr. TWOMEY. Senator, I assume that question is to myself, but I'll make two observations. I think you're actually confusing two agreements. The dot-net agreement is the one you're referring to, which——

Senator SMITH. Correct.

Dr. TWOMEY. All right. The dot-com agreement—if your question is going to the question of rebidding—the dot-com agreement process of whether it could be rebid or not was decided in 2000 and 2001 by discussions by then-ICANN Board Members, the DOC, and VeriSign, and that was a whole set of discussions involving, if you like, breaking up the control that VeriSign had on dot-com, dot-net, and dot-org, where dot-org was rebid so that VeriSign could not rebid, dot-net was rewritten such that dot-net could be rebid and VeriSign could be one of the bidders, and dot-com was agreed would continue under dot-com's—under VeriSign's control. That was actually in the 2001 contract.

As the contracts come up for renewal or rediscussion now, the ICANN Board does not have any legal freedom to be able to change the provision that was in the—already agreed in the 2001 set of arrangements agreed with the Department of Commerce, VeriSign, and the then-ICANN Board. So, the point you're—the point you're—it's just to distinguish between those two contracts.

Senator SMITH. Correct. Well, thank you for that.

I guess the question that a lot of people are asking now, though, is, what's wrong with bidding out the dot-com? And why not let VeriSign win it, if they can, with a competitive bid?

Dr. TWOMEY. Well, apart from the question that—the legal difficulties that we have already under contract, with that particular question, I think there's a second question that the ICANN Board is taking very seriously about its responsibilities for both competition and also security and stability. The introduction of new gTLDs, introduction of new TLDs available to compete with dot-com, we think, is a very important part of implementing competition. The second point we should make very clear is the introduction of new registrars has been a key part of the competition for registrants. We now have nearly 800 registrars, and it's the competition amongst registrars that have reduced prices significantly to the end users.

Indeed, the changes in pricing we saw in dot-net have not, on the whole, been passed through to registrants. The registrars them-

selves have taken the benefit of those price reductions, not the registrants. And that's the nature of the structure of the market, with registrars traditionally competing separately.

So, the question of competition, we think, is very much about an introduction of new gTLDs. The Board has also thought very carefully about the position put to the—by the various registries of their need for certainty for capital investment, for the sorts of investments that security and other demands are making upon them. And while the board has not moved to reduce the provisions in the contract which allow us to intervene in the case of people breaching security arrangements and being able to move against them, the board has come down, on balance, to say there is—they are persuaded by the need to have certainty for capital investment as being an important part of ensuring security and stability.

Senator SMITH. And is that what justifies the automatic price increases?

Dr. TWOMEY. Well, that's what's justifying the renewals.

Ms. JONES. Mr. Chairman, may I be heard briefly on that point?

Senator SMITH. Yes.

Ms. JONES. I'm happy to hear the commitment to additional infrastructure spending, but I think the point is, if there is going to be a presumptive renewal and an automatic price increase built into this contract, there should be some price justification. And to your point about the dot-net agreement, when that was competitively bid, the price didn't increase by 7 percent, the price decreased. And that goes to a lot of reasons, not just because of economies of scale, but also because what we're talking about are commodity products—bandwidth and hosting and all of the things that all of us buy and all of us have to spend money on. We do it, too, with our system and our networks. The costs of all of it—you know—because when you buy a laptop today it costs you one-tenth of what it cost 10 years ago. Prices go down. And so, put aside for a minute the economies of scale, because we know that VeriSign built this huge system that's magnificently scalable, and we all admire them for it. Put that aside for a minute. Even if we didn't take that into consideration, we still know that commodity pricing goes down. And so, there is simply no reason, that we can see, to build in a price increase; and if they're going to build in a price increase, tell us why.

Senator SMITH. What's the justification?

Ms. JONES. Why do you need the price increase, and why is it so difficult to say it?

Senator SMITH. I mean, you've said my question better than I did. But, I mean, I've been in the commodity business, myself, and, frankly, economies of scale and commodity pricing, such that where there is competition, it doesn't warrant these kinds of increases. But, Mr. Silva, maybe you have another view of that.

Mr. SILVA. Senator, I'd like to follow up on that, if I may.

Ms. Jones is a very good attorney, and she's representing her client very well. OK? But she's not a technologist. OK? We're not talking about commodity hardware here. OK? We're talking about massively scalable databases. OK? These are very complex. Moving data in a disaster-recovery scenario from one place to another is

significantly more complicated in a database that size. Significantly more.

So, dot-net prices did go down during the rebid process. It's a different animal. It's a much smaller zone. It's a much smaller problem, quite frankly. OK?

Now, I will point out that consumers never saw one red cent of that reduction in price. OK? Registrars maintained the same prices that they were before the price reduction from the registry.

Now, let's—so, first of all, there's no automatic price increase at 7 percent. OK? What there is, is the possibility of a price increased based on the security and stability needs that we have at the time. So, let me——

Senator SMITH. And who will approve the increase?

Mr. SILVA. Well—OK, so there is the—all right, so let's think about what happened prior to Katrina. OK? The Army Corps of Engineers, for a number of years, attempted to justify cost increases to reinforce the levees around New Orleans. OK? For a number of years. Sometimes they got some funding, sometimes they didn't, but they probably never got all of the funding that they wanted.

Now, when a hurricane started forming out in the tropics, and started heading in that direction—OK?—they probably would have gotten all the funding that they wanted at that time. The problem is, it would have been too late. OK?

We constantly probe and penetrate our systems, and know where their weaknesses are, know where their scalability is, and know where it's about to fail. We know better than anyone when we have to make that investment, sometimes 3 or 4 years out. Sometimes it has to be made in 6 months, sometimes it has to be made in 3 months. OK?

So, there are also consensus policies that are built into the agreement—OK?—which continually change the raising of the bar for the security standards. OK? This is a very fluid requirement. And if we take—for example, 2 years ago, when I worked on the NRIC Council, OK, on cybersecurity, we made 150 recommendations for what companies ought to do to reinforce cybersecurity. The following year, we made 250. OK? We will never know, at any snapshot in time, what that number's going to be, or what it's going to equate to. But we have increased capacity 10,000 times. We have 10,000 times the capacity today that we had in 2000. OK? And that still is not enough. OK? And I can't predict to you what it's going to be in 2012. OK? But in terms of cost justification—OK?—this is really—this really boils down to security and stability. When we need to spend the money, we need to spend the money. OK? And we can't go to our competitors and ask them for permission to spend it.

Senator SMITH. Well, please be clear, I'm not saying the price increase is justified or not. I'm simply inquiring, because I want to make the point to you that this is one of the areas of concern. Usually when you have just one provider, you have a potential monopoly, and that requires regulation. I'm not a regulator.

Mr. SILVA. Right.

Senator SMITH. But I am saying that with a monopoly, without regulation, there has got to be some sort of market test, and I think people are going to be looking to you to justify these levels

of increases. And it may be entirely warranted. I'm not making a judgment on that. But it is an area of real concern.

Mr. SILVA. Right. So, I think, in this particular case—OK?—that is what is built into the agreement, is a cap on the amount that they can, in fact, be raised. OK? So, for 7 years they weren't raised at all. OK? Not at all. OK? Even though the number of registrations grew at a specific rate—OK?—the threats and the volume of traffic that we see, just in normal traffic—OK?—security issues aside, the security issues are so phenomenally higher, in terms of the volume of activity that we see, over what we register as new names—OK?—6 months ago—or, excuse me—so, 8 months ago, I would have told you that, yes, you know, it's perfectly reasonable, we could probably forecast out a couple of years what we would need. And then all of a sudden January came, and we got hit with an attack ten times larger than anything we would have expected. And I can tell you right now that when I briefed the Department of Homeland Security, and when I held a classified briefing with the Senate Intelligence Committee on exactly what this threat meant, not only to our system, but to their systems—OK?—they took this very seriously. National Infrastructure Protection Plan calls for private industry to make significant investments where they control critical infrastructure. We plan on making those critical investments. And basically that's what these provisions are for, so that when all of a sudden Windows Vista™ comes out—and experts have said that that could as much as double the amount of DNS traffic—we're able to respond to it in a timely fashion.

Senator SMITH. I wish we had more time to go on with this, but I'm going to miss a vote if I don't adjourn this hearing. I, again, apologize for my delay, and I thank my colleagues for proceeding, out of respect for your time. We thank you for your contribution to this hearing. And we have more to learn and more to do, because this is an enormously important topic.

So, with that, we thank you and we're adjourned.

[Whereupon, at 11:30 a.m., the hearing was adjourned.]

A P P E N D I X

PREPARED STATEMENT OF HON. GORDON H. SMITH, U.S. SENATOR FROM OREGON

I call to order this hearing of the Senate Subcommittee on Trade, Tourism, and Economic Development.

Today's hearing considers Internet governance and the future of ICANN.

In 1997, the Secretary of Commerce was directed by the President to privatize the management of the domain name system in a manner that increases competition and facilitates international participation in its management.

Soon thereafter the Department of Commerce signed an official Memorandum of Understanding recognizing ICANN—the Internet Corporation for the Assignment of Names and Numbers, as the new, not-for-profit corporation to manage the domain name system.

Under the terms of the MOU, ICANN has the authority to:

1. Set policy for, and direct the allocation of, the IP addresses that underlie each domain name.
2. Oversee the operation of an authoritative root server system,
3. Set the policies for determining how new top level domains would be added to the root system; and
4. Coordinate the assignment of the Internet technical parameters needed to maintain the universal connectivity of the Internet.

The MOU between the Department of Commerce and ICANN expires on September 30, 2006 among controversy in the international community.

Some are suggesting that no single government should have a preeminent role in relation to the Internet and are calling for further internationalization of Internet governance.

This would be a mistake. The current system for management of the domain name system works. The Secretary of Commerce should maintain oversight of ICANN so that ICANN can continue to manage the day-to-day operation of the Internet's domain name and addressing system and remain responsive to all Internet stakeholders worldwide.

Today's hearing will examine the management and governance of ICANN, including the future of the Domain Name System, recent concerns expressed regarding the current ICANN-VeriSign settlement agreement, and privacy issues surrounding the "WHOIS" database.

I thank all of our witnesses for rearranging their schedules to appear before the Subcommittee and look forward to your testimony.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DANIEL K. INOUYE TO JOHN M.R. KNEUER

Question 1. As part of the settlement of a long-running dispute between ICANN and VeriSign, the ICANN Board of Directors approved a new dot-corn agreement with VeriSign. Under this settlement, VeriSign will be in charge of the dot-com registry until 2012 (with a presumption that the agreement will be renewed beyond that date), and will be able to raise domain registration fees by 7 percent in four of the next 6 years. Critics of the settlement assert that the agreement is anti-competitive, giving VeriSign a virtually permanent monopoly over the lucrative dot-com registry, while also enabling VeriSign to raise registration fees without justification.

Many critics of the settlement agreement argue that the presumptive renewal clause would allow VeriSign to hold on to the dot-com registry in perpetuity. How do you see ICANN holding the registry operator accountable without the strong leverage of awarding the contract to a competing operator?

Answer. Over the course of the past 6 months, I and other Commerce Department officials have met with a number of interested stakeholders including registrars, Internet service providers, and search engine companies with interests in or concerns about the .com Registry Agreement. The concerns have largely focused on the impact on competition of the proposed price increase for registrations permitted by the new agreement and the terms for future renewals of the new .com Registry Agreement. The Commerce Department has sought the advice of the Antitrust Division of the Justice Department on the competition concerns raised.

It is also important to note that other interested stakeholders have advocated that the renewal terms of the proposed agreement benefit the security and stability of the Internet domain name system. We have also consulted with those Federal agencies with expertise in the areas of security and stability on this matter.

Based on the information that we have gathered, I am confident that any decision made by the Department will appropriately balance all of these interests to ensure the continued stability and security of the Internet domain name system and of promoting the consumer benefits of a competitive marketplace.

Question 2. One of ICANN's primary missions is to promote competition. How does a presumptive renewal clause promote competition?

Answer. As noted above, the Department is reviewing the proposed new agreement in its entirety to ensure both the continued stability and security of the Internet domain name system and of promoting the consumer benefits of a competitive marketplace.

Question 3. Cybersecurity is a critical mission that all organizations struggle with. How can ICANN ensure that the registry operators are making the necessary security enhancements to guarantee the stability of the domain name system? How can ICANN hold a registry operator accountable?

Answer. Cybersecurity standards are developed by various industry organizations, such as the Internet Engineering Task Force (IETF), ISO, and IEEE, and adherence to the various standards is voluntary for the most part. While ICANN is not a standards organization, it promotes the adoption of industry standards through its agreements with registry operators to comply with these standards. Registry agreements address the technical performance obligations, including compliance with the various industry-developed standards, security requirements and outage reporting that all registry operators must meet. In addition each registry agreement contains a service level agreement which clearly sets forth the registry operator's obligation for failure to meet the technical performance specifications.

Question 4. Assuming that NTIA approves the settlement agreement, what mechanisms would ICANN have available to ensure that it has meaningful control over the service quality or conduct of registry operators?

Answer. Like any commercial agreement between private sector parties, the proposed new .com Registry Agreement contains enforcement provisions. It also contains quality of service commitments that ICANN can enforce under the terms of the agreement.

Question 5. The settlement agreement allows VeriSign to raise domain registration fees by 7 percent in four out of 6 years without having to provide a justification. Do you believe that a registry operator should be required to publicly justify any price increases?

If no—Why not? Doesn't a registry operator enjoy a monopoly over the pricing for a specific top-level domain?

If yes—What concerns do you have with the VeriSign settlement that would allow it to increase prices by 7 percent four out of 6 years without having to provide a justification? How is such a clause *not* anticompetitive?

Answer. The domain name marketplace is not a regulated one. Prices are set based on negotiations between private sector parties. The price cap for .com registrations and price adjustments permitted under the proposed new .com Registry Agreement were negotiated by ICANN and VeriSign.

Nevertheless, the Commerce Department is aware of the concerns raised primarily by the registrar community about the impact of a price increase on their industry. We have been in consultation with the Antitrust Division on this issue and will be guided by its advice in any final decision the Department makes.

Question 6. Do you think it is reasonable for a registry operator to explain to ICANN their reasons for a price increase, and then have ICANN approve or reject such a proposal accordingly?

What criteria is used to evaluate price increases? Specifically, under what circumstances would an automatic price increase without justification be acceptable?

Answer. As noted above, the domain name marketplace is not a regulated one. Prices are set based on negotiations between private sector parties. To introduce

government price regulation would be a significant departure from the *status quo* and massive introduction of government regulations that does not currently exist into a private marketplace.

Question 7. I understand the Department of Justice's Antitrust Division was asked to review the settlement agreement. Can you share with us the Division's concerns? How are these concerns being addressed? Were there recommendations or suggestions made that are not being implemented or considered?

Answer. During its review of the proposed new .com Registry Agreement, the Commerce Department has sought the advice of the Antitrust Division of the Justice Department regarding the impact on competition of the proposed price increase for registrations permitted by the new agreement and the terms for future renewals of the revised new .com Registry Agreement. The Antitrust Division has been gathering information from the parties, interested stakeholders, and others on these issues, to provide its analysis and advice to the Department on any competition issues that may be raised by the proposed agreement. We expect to rely on this advice to evaluate the potential impact on competition of this agreement.

Question 8. Are you open to bringing together the different stakeholders in order to arrive at a solution that will satisfy the different parties and still ensure the promotion of competition?

Answer. In addition to its consultation with the Department of Justice's Antitrust Division regarding the competition issues raised by the proposed new .com Registry Agreement, I and other Commerce Department and Antitrust Division officials have met with a number of interested stakeholders, including registrars, Internet service providers, search engine companies, among others, with interests in or concerns about the agreement. The Commerce Department has also heard from a number of stakeholders advocating the benefits of the new agreement for the security and stability of the Internet domain name system. We have also heard from Members of Congress on both sides of the issue. Commerce Department and Antitrust Division officials have been gathering information from proponents and opponents of the agreement and I am confident that this information will be taken into consideration in any final decision that is made.

Question 9. Transparency has long been a concern with ICANN. Many critics argue that the ICANN Board operates behind closed doors, even though the organization is charged with developing consensus through a "bottom-up" approach. Can you comment on ICANN's transparency issues? How has this improved over the years? How can the organization continue to improve?

Answer. The Department has long considered transparency to be a fundamental principle to ICANN's overall mission and function. The current Memorandum of Understanding (MOU) was structured to ensure that ICANN becomes a sufficiently stable, transparent, representative, and sustainable management organization capable of handling the important tasks associated with the technical management of the Internet domain name system into the future. This MOU also contains specific provisions intended to improve transparency, efficiency, and timeliness in the consideration and adoption of policies. While ICANN has made several improvements in its decisionmaking and policy development processes, as well as in internal reviews and evaluations of these processes, I believe ICANN is mindful of the need for continual improvement. The Department's recent public consultation process has revealed strong support from a majority of interested stakeholders for a more specific focus on transparency and accountability in ICANN's internal procedures and decision-making processes.

Question 10. The ICANN Board has proposed new contract agreements for the operators of dot-biz, dot-info, and dot-org. The contracts for dot-biz and dot-info are not up for renewal until next year and dot-org isn't to be renewed until 2009. The public was not aware that negotiations were taking place until ICANN posted the proposed agreements for public comment. Can you comment on ICANN's transparency in developing the proposed agreements for the dot-biz, dot-info, and dot-org top-level domains (TLDs)?

One element of the newest proposal is to allow for differential pricing of domain names. Can you explain the public policy rationale behind allowing a registry to apply a differential pricing scheme for specific domain names?

Is there concern that a registry could limit free speech by charging an unreasonable fee to register a domain name critical of political party, public figure, or issue?

Answer. The proposed new registry agreements for the .biz, .org, and .info top level domains are commercial agreements between private sector parties. As I understand it, under the terms of the existing agreements, the parties can mutually agree to amend or enter into new agreements. The Department of Commerce has not examined the pricing provisions of these agreements. ICANN has posted all

three agreements for comments from interested stakeholders. I expect ICANN will fully consider the interests of all interested stakeholders as it negotiates these agreements.

Question 11. Last year NTIA urged ICANN to reject the creation of a dot-xxx top level domain. Under pressure from the U.S. Government, and much to the consternation of the international community as a result, ICANN ultimately rejected the dot-xxx domain. Can you describe NTIA's involvement in rejecting the creation of a dot-xxx top level domain?

Answer. In June 2005, the ICANN Board of Directors approved the initiation of negotiations between ICANN staff and ICM Registry, the applicant for the .xxx domain. Beginning in July 2005, ICANN's Governmental Advisory Committee (GAC) began to raise questions regarding the procedure followed by the Board in reviewing the application and its rationale for entering into contract negotiations. On August 11, 2005, then-NTIA Assistant Secretary Michael D. Gallagher sent a letter to ICANN's Chairman of the Board requesting that ICANN take into consideration all comments it received during its consideration of this application (see letter to Dr. Vinton Cerf, attached).

In response to the GAC's request for additional information and requests from other governments, ICANN released its comprehensive Evaluation Report on all of the sponsored top level domain applications in November 2005. The ICANN Board elected to defer consideration of the .xxx application pending a review of the Report by the GAC.

The GAC considered the report and additional information during its March 2006 meeting in Wellington, New Zealand prior to the ICANN Board meeting there. The GAC conveyed its views and concerns to the Board through a communiqué. As part of the process in developing that communiqué, I sent a letter dated March 20, 2006, to the GAC Chairman expressing concerns about ICANN's ability to obtain the public policy benefits promised by the applicant absent enforceable contract terms in the proposed .xxx Registry Agreement (see letter to Mr. Sharil Tarmizi, attached).

On May 10, 2006, the ICANN Board of Directors made a final decision to disapprove the pending application from ICM Registry to manage the proposed .xxx top level domain.

ATTACHMENTS

U.S. DEPARTMENT OF COMMERCE—THE ASSISTANT SECRETARY FOR COMMUNICATIONS AND INFORMATION
Washington, D.C., August 11, 2005

Dr. VINTON CERF,
Senior Vice President, Technology Strategy,
MCI
Ashburn, VA.

Dear Dr. Cerf:

I understand that the Board of Directors of the Internet Corporation for Assigned Names and Numbers (ICANN) is scheduled to consider approval of an agreement with the ICM Registry to operate the .xxx top level domain (TLD) on August 16, 2005. I am writing to urge the Board to ensure that the concerns of all members of the Internet community on this issue have been adequately heard and resolved before the Board takes action on this application.

Since the ICANN Board voted to negotiate a contract with ICM Registry for the .xxx TLD in June 2005, this issue has garnered widespread public attention and concern outside of the ICANN community. The Department of Commerce has received nearly 6,000 letters and e-mails from individuals expressing concern about the impact of pornography on families and children and opposing the creation of a new top level domain devoted to adult content. We also understand that other countries have significant reservations regarding the creation of a .xxx TLD. I believe that ICANN has also received many of these concerned comments. The volume of correspondence opposed to creation of a .xxx TLD is unprecedented. Given the extent of the negative reaction, I request that the Board will provide a proper process and adequate additional time for these concerns to be voiced and addressed before any additional action takes place on this issue.

It is of paramount importance that the Board ensure the best interests of the Internet community as a whole are fully considered as it evaluates the addition of this new top level domain. Thank you for your attention to this matter.

Sincerely,

MICHAEL D. GALLAGHER.

cc: Dr. Paul Twomey

U.S. DEPARTMENT OF COMMERCE—THE ASSISTANT SECRETARY FOR COMMUNICATIONS AND INFORMATION
Washington, D.C., March 20, 2006

Mr. SHARIL TARMIZI,
Senior Advisor, Office of the Chairman,
Malaysian Communications and Multimedia Commission;
Chair, Government Advisory Committee of ICANN,
Selangor Darul Ehsan, Malaysia.

Dear Mr. Tarmizi,

Pursuant to the ICANN Government Advisory Committee (GAC) meeting in Vancouver in November 2005, the Department of Commerce has undertaken an analysis of the proposed .xxx Registry Agreement to determine whether its provisions reflect the commitments made by ICM Registry. As you will recall, the ICM Registry presentation to the GAC outlined in some detail the anticipated public interest benefits of its application for the .xxx top level domain.

The attached assessment indicates that the key commitments offered by ICM Registry to the GAC are not reflected in the provisions of the proposed .xxx Registry Agreement. In your capacity as GAC Chair and GAC liaison to the ICANN Board, NTIA would appreciate your sharing this information with both the GAC and the Board prior to the Wellington, New Zealand meeting.

Sincerely,

JOHN M.R. KNEUER,
Acting Assistant Secretary.

cc: Mr. Paul Twomey.

Omissions in the Proposed .xxx Registry Agreement

In its application, supporting materials, and presentation to the Governmental Advisory Committee in November 2005, ICM Registry (ICM) promised certain public interest benefits as part of its bid to operate the .xxx domain. These promises, however, have not been included in the proposed .xxx Registry Agreement negotiated with ICANN, and thus, ICM is not obligated to provide these public interest benefits. Section 8.12 of the .xxx Registry Agreement provides in pertinent part: "This Agreement (including its Appendices, which form a part of it) constitutes the entire agreement of the parties hereto pertaining to the operation of the TLD and supersedes all prior agreements, understandings, negotiations and discussions, whether oral or written, between the parties on that subject." Thus, if ICM is not required to provide the public interest benefits by the terms of its registry agreement, it is not obligated to do so.

Below is a sample of the ICM promises that do not appear in the proposed .xxx Registry Agreement:

To Form a Nonprofit Policy Development Entity to Create Rules for .xxx. In the .xxx application, ICM stated that it formed a nonprofit Canadian entity (International Foundation for Online Responsibility (IFFOR)) to develop rules and policies to govern a new .xxx domain. ICM Application, Part B, at 2–5, 7–13. The proposed .xxx Registry Agreement does not require ICM to form or maintain this nonprofit entity or to abide by any .xxx rules it would establish. Instead, the proposed .xxx Registry Agreement delegates all policy development authority for .xxx to ICM. In fact, the proposed .xxx Registry Agreement provides that the IFFOR Board will not be created until the day that the agreement is signed and will not be in place until 90 days after signing. See .xxx Registry Agreement, Appendix S. Moreover, IFFOR is not a party to the proposed .xxx Registry Agreement.

To Require .xxx Registrants to adhere to Best Business Practices as a condition of .xxx registration. ICM promised that IFFOR would develop rules to this effect (ICM Application, at 3, 16). There is no requirement to do so in the proposed .xxx Registry Agreement and IFFOR is not a party to this agreement.

To Require all .xxx Registrations to be ICRA Labeled. In its presentation to the ICANN Government Advisory Committee, November 29, 2005, ICM promised that it would require all .xxx registrations to be labeled according to the Internet Content Ratings Association (ICRA) ratings to permit filtering of content. ICM further

promised that any website that points to a .xxx site must also be ICRA labeled. There is no provision in the proposed .xxx Registry Agreement that would obligate 1CM to require such labeling.

To Safeguard Children Online. ICM promised that IFFOR would sponsor the development of technology tools and education programs for parents. (ICM Application, at 3, 16; The Sponsored .xxx TLD Proposals: Executive Summary for the ICANN Board, at 2). ICM also promised that IFFOR would fund the participation of independent advocates for children (ICM Letter to ICANN, October 9, 2004, at 17). These promises are not reflected in ICM's obligations in the proposed .xxx Registry Agreement and IFFOR is not a party to this agreement.

To Combat Child Pornography. ICM promised that IFFOR would provide funding and tools to combat online child pornography and to prohibit child pornography in the .xxx domain as defined by international law. (ICM Application, at 3; ICM Letter to ICANN, August 15, 2005, at 2; ICM's Responses to Evaluators' Questions, Question 2). This promise is not reflected in ICM's obligations in the proposed .xxx Registry Agreement and IFFOR is not a party to the agreement.

To Implement a WHOIS Compliance Program. In its application (ICM Application, at 20–21), ICM promised to document false and inaccurate WHOIS data and to implement additional verification processes. This promise is not reflected in ICM's obligations in the proposed .xxx Registry Agreement.

To Provide Funds for Global Child Initiatives. ICM promised to give IFFOR $10 per .xxx domain name so that IFFOR can make some of this funding available for global child advocacy community targeted especially to eradicate child pornography. (ICM Memorandum to the ICANN Board of Directors, November 2, 2004, revised December 7, 2004, at 5). ICM also promised that IFFOR would provide grants to developing countries in the area of child online protection. (ICM's Responses to Evaluators' Questions, Question 7). There is no obligation in the proposed .xxx Registry Agreement for ICM to fund IFFOR or for IFFOR to provide this kind of financial assistance to child advocacy groups or developing countries. Moreover, IFFOR is not a party to the .xxx Registry Agreement.

To Prohibit Child Exploitation including Requiring Proof of Age of Actors Portrayed in Content in .xxx Domain. In its presentation to ICANN's Board, April 3, 2005, ICM promised that this prohibition would appear as part of its registration agreement with .xxx domain name holders. There is no obligation in the proposed .xxx Registry Agreement to this effect.

To Promote Responsible Marketing Practices by Requiring .xxx Registrants to Agree to Combat SPAM and Not Use Malicious Codes and Technologies (i.e., Spoofing) and other Illegal and Questionable Marketing Practices. ICM Presentation to ICANN, April 3, 2005; White Paper, Thinking Outside the Porn Box, Annex B, ICM's Intentions. There is no obligation in the proposed .xxx Registry Agreement to this effect.

Response to Written Questions Submitted by Hon. Daniel K. Inouye to Christine N. Jones

Question 1. Many of the concerns about the proposed VeriSign-ICANN agreement are coming from other registrars. The transfer of the dot-com registry to VeriSign would affect other registry services as a whole. How do the presumptive renewal and guaranteed price increases included in the proposed agreement concern registrars?

Answer. In the current environment, allowing .com prices to increase without cost justification is anti-competitive. .Com still has considerable market power making up 75 percent of all registered gTLD domain names and 80 percent of the ongoing market share. The price increases allowed in the proposed agreement will net VeriSign over $1 Billion in incremental revenue based on current growth projections, all of which will be passed on directly to consumers, registrars' customers.

VeriSign has repeatedly stated that it needs these additional funds to ensure the stability and security of the .com DNS. We have no problem with that, but ask then that at the very least VeriSign be required to demonstrate that need when requesting all price increases, and be required to invest a significant portion of the additional funds in the .com DNS infrastructure.

We explain our concerns with the presumptive renewal in our response to the next question.

Question 2. Would the proposed agreement possibly hinder ICANN's ability to become an autonomous body by relinquishing a substantial amount of control over the dot-com registry?

Answer. If ICANN's mission continues to include ensuring the security and stability of the Internet's Domain Name System (DNS), then yes.

The .com DNS is arguably the most important element of the Internet DNS. Yet the proposed agreement basically hands the responsibility of the security and stability of the .com DNS entirely over to VeriSign, leaving ICANN very little recourse if there are problems. The form of presumptive renewal being proposed in the agreement allows VeriSign to breach it, even repeatedly, with little more than financial penalties as long as they cure the breaches. There is also no requirement for VeriSign to invest in the .com DNS infrastructure.

However, under the current agreement, the conditions of presumptive renewal would allow ICANN to make a determination as to VeriSign's continued ability to manage the .com DNS and to provide a substantial service to the Internet community (Section 25.B). Breaches of the agreement and its service level requirements in particular, would certainly be a factor in that determination. The current agreement also required VeriSign to make substantial investments in the DNS infrastructure it was contracted to manage, $200 million to be exact.

.Com is too important to simply assume that giving VeriSign a perpetual renewal without conditions will be incentive enough to ensure they continue operating it responsibly, or that they will make the necessary infrastructure investments to ensure stable and secure operations. ICANN, at a minimum, must allow itself an out to re-bid .com if VeriSign fails to continue to meet the conditions as stated in 25.B of its current agreement, and must require VeriSign to make substantial investments in the .com DNS infrastructure.

Question 3. What concerns would the reduced control over the dot-com registry and its security measures raise for the registrar community?

Answer. The reduced control, as a result of the strengthened form of presumptive renewal, demonstrates an assumption that ICANN is making—that VeriSign will continue to qualify as registry operator for .com and will continue to invest in its infrastructure appropriately. .Com is too important to make such assumptions regardless of VeriSign's past performance. Investment requirements, cost justifications for price increases, and the potential for eventual re-bid would be far more motivating and provide the Internet community better assurance of reliable performance of its most important gTLD.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DANIEL K. INOUYE TO HON. JON LEIBOWITZ*

Question 1. What effect would the lack of competition and price controls have on competition in the marketplace?

Answer. Your question raises important issues about the effects of anticompetitive conduct and, as I understand it, specifically relates to the competitive effects of the proposed settlement agreement between ICANN and VeriSign, Inc. (the "VeriSign Settlement Agreement" or "Agreement").

Generally, consumers benefit from unfettered competition in the marketplace. Consequently, the FTC seeks to prevent business practices that restrain competition—including agreements among competitors to limit competition, attempts to monopolize an industry through unfair or exclusionary practices, and anticompetitive mergers and acquisitions. However, each case requires a careful evaluation of the challenged business practice.

In regard to the competitive implications of the VeriSign Settlement Agreement, the Department of Commerce (DOC) and the Department of Justice (DOJ) are both already considering this issue. Pursuant to agreements among DOC, VeriSign, and ICANN, the VeriSign Settlement Agreement is subject to DOC' s approval. DOC has consulted with interested stakeholders about the Agreement and has sought DOJ' s advice on its competitive effects. I am aware that Senators Hatch and Leahy have sent letters to the Secretary of Commerce highlighting the goal of open competition and the importance of DOJ' s guidance with respect to whether the VeriSign Settlement Agreement has any potential anticompetitive effects. I understand that DOC and DOJ are analyzing the competitive implications of the Agreement and assessing its effects on both stakeholders within the ICANN community and on American consumers.

---

*The written testimony submitted for the September 20, 2006 hearing reflects the views of the Federal Trade Commission ("FTC" or "Commission"). However, my responses to these post-hearing questions reflect my own views and do not necessarily reflect the views of the Commission or of any other Commissioner.

Question 2. What concerns do the lack of justification behind the guaranteed price increases raise for you?

Answer. Again, my understanding is that your question relates to the VeriSign Settlement Agreement, which DOC and DOJ are currently reviewing.

Question 3. Worldwide attention is focused on ICANN and its role in Internet governance. Many nations frustrated over the slow progress toward ICANN autonomy are proposing individual governance of the Internet. How would the proposed VeriSign agreement affect the road toward autonomy for ICANN?

Answer. As your question aptly points out, we need to strike the right balance to ensure that ICANN's passage to autonomy progresses as quickly as possible—but also responsibly. To this end, DOC has a Joint Project Agreement with ICANN to facilitate the transition of the domain name system to the private sector. Pursuant to this agreement, DOC advises ICANN on how to improve its transparency and accountability. It also monitors whether ICANN effectively considers competition interests in top-level domain management decisions. As part of its periodic review process, DOC will evaluate relevant factors, including, if necessary, the effects of the VeriSign Settlement Agreement, when considering when to complete the privatization of the domain name system.

Question 4. If ICANN does not make strides toward the goals of transparency, bottom-up management, representation, and stability in a more timely manner than it has, how do you think this could effect the progress made at the World Summit on the Information Society?

Answer. I agree that transparency, bottom-up management, representation, and stability are important goals for ICANN to pursue and could help instill increased confidence in ICANN on the international stage. One key to ensuring transparency and stability is ensuring continued access to WHOIS databases, as the Commission advocated in its testimony on September 20, 2006.

I am aware that the international community is focused on ICANN and Internet governance as a result of discussions in the World Summit on Information Society—and that relevant stakeholders—including DOC, the Department of State, and ICANN—are working hard to try to satisfy all relevant interests. As to a specific assessment of the progress ICANN has made, DOC continues to monitor ICANN's progress in achieving the important goals you have identified.

Question 5. How would an unstable political environment affect domain name system (DNS) security and stability?

Answer. Preserving the security and stability of the Internet is critical. One issue that the FTC advocates as a means of preserving the security and stability of the Internet is continued access to WHOIS domain name registration data. An unstable political environment could lead to a decision not to provide WHOIS data to law enforcement and to the public. This would have extremely negative consequences for consumers in the United States and elsewhere, who want agencies like ours to bring actions against Internet malefactors that attempt to defraud them or that threaten their privacy.

Response to Written Questions Submitted by Hon. Daniel K. Inouye to Ken Silva

This submission is respectfully submitted on behalf of Mr. Silva in response to the questions posed by the Senate Commerce Committee following the hearing on September 20, 2006.

For purposes of background to its responses, VeriSign provides the following brief summary of the operation of the Internet and the functional distinctions between domain name registries and domain name registrars.

Background

The Internet is a network of interconnected computers and computer networks. Every computer connected directly to the Internet has a unique address. These addresses, which are known as Internet Protocol ("IP") numbers, are necessary for computers to "communicate" with each other over the Internet. An example of an IP number might be: 98.27.241.30. Because IP numbers can be cumbersome and difficult for Internet users to remember or to use, the IP number system has been overlaid with a more "user-friendly" system of domain names: the Internet domain name system, or "DNS". This overlay associates a unique alpha-numeric character string—or domain name—with a specific IP number.

Internet domain names consist of a string of "domains" separated by periods. "Top-level" domains, or "TLDs," are found to the right of the period and include (among others) ".com," ".gov," ".net," and ".biz," which are sometimes referred to as

"generic" TLDs (also known as "gTLDs"). Other top-level domains are referred to as country code TLDs (also known as "ccTLDs"), and are represented by two-letter abbreviations for each country, such as ".uk" (United Kingdom) and ".ca" (Canada), and .eu (Europe). gTLDs are functionally equivalent to ccTLDs. There are approximately 250 top-level domains, which are administered and operated by numerous entities, both in and outside of the United States.[1]

"Second-level" domains (SLDs) are those domains immediately to the left of the top-level domain, such as "senate" in the domain name "senate.gov.", or "aol" in "aol.com." There are approximately 100 million second-level domains currently registered within the various TLDs.

Because domain names are essentially "addresses" that allow computers connected to the Internet to communicate with each other, each domain name must be unique, even if it differs from another domain name by only one character (*e.g.*, "uscourts.com" is different from "uscourt.com" or "us-courts.com"). A given domain name, therefore, can be registered to only one entity.

VeriSign acts as the "registry" for domain names registered in the .com gTLD in accordance with a written agreement with ICANN and through its cooperative agreement with the U.S. Department of Commerce. Among the other services VeriSign performs as the "registry" for the .com gTLD, VeriSign maintains the definitive directory that associates registered domain names in this gTLD with the corresponding IP numbers of their respective domain name servers. The domain name servers, in turn, direct Internet queries to resources such as websites and e-mail systems. Under the DNS architecture, one given domain name is essentially associated by domain name servers with one IP number or distinct computer.

For technological reasons, the uniqueness requirements of the DNS architecture described above, mandate that there can only be one entity that operates any TLD registry that maintains the authoritative database of domain names registered in a particular TLD. *Accordingly, there can be only one registry operator for .com.*

A domain name is created by an individual or organization that registers the domain name and thereby includes it in the registry's master database. The individual or organization that registers a specific domain name is a "registrant." Registrants do not have direct access to the VeriSign registry. Instead, prospective registrants must register domain names through any one of over 800 private companies located in the United States and throughout the world that are accredited by, and enter into a Registrar Accreditation Agreement with ICANN to act as domain name "registrars" for the second-level domain names in the .com gTLD. While there can be only one registry for each TLD, there are hundreds of registrars and thousands of resellers around the world who sell these domain name registrations to end users.

Registrars, not registries, sell domain names to registrants, or consumers. There are no restrictions by ICANN or the government upon the price for which registrars sell domain name services to consumers.[2] Nearly all domain name registrars that provide domain registration services for the .com gTLD also provide domain name registration services for other gTLDs and ccTLDs. For example, according to its website, *GoDaddy.com,* one of the largest Internet domain name registrars, offers prospective registrants the ability to register SLDs in 29 gTLDs and ccTLDs in addition to the .com gTLD. Domain name registrars set their own prices for domain name registration services and the prices registrants are charged by domain name registrars to register a domain name within the same TLD vary widely.

Registrars provide direct services to registrants and prospective registrants, such as processing domain name registrations. The VeriSign registry has no contractual or other relationship with a registrant. This means that VeriSign has no information as to the identity of a registrant. Conversely, registrars have a contractual relationship with registrants and keep all information regarding the registrants.

Regardless of the price paid for a domain by an end user to a Registrant, the name works the same technically on the Internet. The Registries who operate these top level domains are responsible for ensuring that queries from around the world to that domain are answered ("resolved") when executed. The volume of these queries is dictated by the growth of online users around the world and their increased usage of the Internet. Over the last decade, the number of users and usage of the Internet has grown at a pace that far outstrips the corresponding growth in the number of domain names registered worldwide. The ease of use for a user going online (*i.e.,* access to broadband and wireless devices that are Internet-enabled), access to online content in non-English languages, and the meaningfulness of content online are the key drivers of Internet usage. Even during the historical slowing of domain name registration sales during the "bust" of the Internet bubble, usage continued to increase.

Question 1. Security is a significant concern of stakeholders and Internet users at large. How do you address concerns about the registrar's lack of a disaster recovery plan?

Answer. The lack of effective disaster recovery for registrars, along with the absence of registrar security requirements, is a cause for serious concern. Historically, in the absence of stringent security requirements for registrars as part of their ICANN Accreditation Agreements, registries, such as VeriSign, have been the safety net for registrar security deficiencies. Under the current structure of ICANN Registrar Accreditation Agreements, registrars have no incentive to, and do not, invest in the security or stability of the DNS. Accordingly, the work of insuring the operational security and stability of the DNS falls to registries in general, and VeriSign in particular for .com, through continued and significant investment beyond that required in current contracts.

In light of the lack of infrastructure investments by registrars, VeriSign supports adding requirements to the ICANN Registrar Accreditation Agreements of registrars to fill the security and stability void in those agreements and to establish obligations in the Registrar Accreditation Agreements that provide ICANN with the ability to address security and stability issues (for example through a flexible Consensus Policy provision such as that currently provided for in Section 3.1 of the proposed .com Registry Agreement). The Registrar Accreditation Agreement is not part of the proposed .com Registry Agreement.

Since the question above explicitly deals with the disaster recovery systems of Registrars, we have provided, below, answers related to the contractual requirement of data escrow/disaster recovery, which is a core component to ensure proper disaster recovery.

Registrars maintain all personal end-user data related to the sale of a domain name which is needed to fully recover the ownership of domain. The registries maintain all data related to the technical elements of the domain's status and location on the Internet, but no personal data. The Registrar Accreditation Agreement, to which all ICANN-accredited registrars are parties with ICANN, includes a contractual requirement that the registrar maintain an escrow of the registrar specific data related to their registrations. (Registrar Accreditation Agt., Sect. 3.4).[3]

A similar obligation exists for the registry operator in the .com registry agreement to maintain registry level data as noted above (but no personal data). In particular, the registry operator is required to establish at its expense a data escrow or mirror site for registry data compiled by the registry operator. (Registry Agt., Sect. 3.1(c)(i)).[4] Further specific details of this extensive, structured mirror site obligation are set forth in Appendix 1 and Appendix 2 to the .com Registry Agreement. In summary, the obligation requires that the registry operator establish an escrow account to deposit a complete set of all data identified in section 3.1(c)(i) of the .com Registry Agreement to the data escrow provider on a daily and weekly basis. The data is verified by the escrow provider for completeness, accuracy, and format accuracy to avoid any risk of a failure to restore due to data corruption. In addition, the schedule, content, format, and procedure for escrow may be changed by ICANN as conditions warrant or through establishment of Consensus Policies. The intent of the mirror site obligation is to encapsulate registry operations and identified data into a single escrow file available to a third party for escrow storage and recovery.[5]

VeriSign is compliant with all requirements to provide updates in escrow (as explained more fully in response to *Question 3*). Through a time-proven process, it has a verifiable record of delivering completeness, correctness and integrity of the data within each escrow file. VeriSign completes daily and weekly deposits of reports and meta-data for all .com domain names.

Further, VeriSign has a demonstrated record of compliance with its escrow obligations and of continual monitoring of related issues. For example, VeriSign switched providers of its escrow services in December 2005 because it became apparent that most large gTLD registrars were using the same offsite data storage provider which was regarded as a possible single point of failure in the system. VeriSign believed that this circumstance created a risk to the community at large and, therefore, initiated a community discussion of this risk, and proposed a transition in its service to an alternate provider to eliminate the overlap. The new provider was reviewed and approved by ICANN before the transition was made.

As explained more fully in response to *Question 3* below, the proposed .com Registry Agreement also includes other substantial, detailed requirements to ensure the secure and stable operation of the .com registry, including thorough oversight by and accountability to ICANN. For example, the proposed .com Registry Agreement expressly adds the further contractual requirement that the registry operator take those steps necessary to protect all personal data from loss, misuse, unauthorized

disclosure, alteration or destruction and includes monthly data reporting requirements, together with ICANN audits of such reporting. (Registry Agt., Sect. 3.1(c)(ii)).

Question 2. Does VeriSign have a plan to address these security concerns?

Answer. As explained above, VeriSign acts as the "registry" (not the registrar) for domain names registered in the .com gTLD in accordance with a written agreement with ICANN. Accordingly, as explained in response to *Question 1*, VeriSign does not have control over any of the 800 registrars or their disaster recovery plans or security or stability deficiencies.

However, the work of ensuring security and stability to make up for this gap falls to the registries. VeriSign regularly conducts failure mode analyses on all of the .com registry systems. This includes testing to insure the mitigation of risks occurring due to possible failures in hardware and software, the network layer, security systems, facility-related issues, and environmental factors. As a financially sound, U.S.-based, public company, with robust technical capabilities, VeriSign has a carefully developed plan for data recovery, including provisions for DNS restoration and data retrieval, and provisions to facilitate system reconstitution.

VeriSign believes that the best place to address registrar security concerns is through the addition of contractual obligations to the Registrar Accreditation Agreements of registrars, such as the inclusion of flexible Consensus Policy language such as the provision currently included in Section 3.1 of the proposed .com Registry Agreement, which gives ICANN the power to address security and other issues. Topics for such policies and discussions could include registrar business continuity, disaster recovery and periodic accreditation compliance audit.

Question 3. Under the proposed agreement VeriSign has no accountability to ICANN regarding security measures. How will VeriSign ensure the safety of the DNS?

Answer. The premise of this question is not based on the facts of the proposed .com Registry Agreement as the proposed Agreement not only provides substantial accountability to ICANN for insuring the security and stability of the registry and DNS, it increases the accountability over what is currently called for in existing registry agreements that have controlled the operation of the registry during the preceding 8 years. Under the preceding agreements, VeriSign has maintained 100 percent availability of the .com TLD for 8 years, an unparalleled record in Internet security and stability.

Under the proposed .com Registry Agreement, VeriSign is contractually obligated to maintain 100 percent availability of the DNS systems for the .com gTLD. (Registry Agt., (Sect. 3.1(d)(ii), App. 7, Sect. 7). In order to meet this obligation, VeriSign must take all steps necessary to maintain the secure and stable operation of the DNS. In fact, numerous provisions of the proposed agreement are specifically directed to insuring compliance with this contractual obligation, including by placing particular and detailed obligations on the registry operator and providing for ongoing ICANN oversight. The following provisions of the proposed agreement, for example, are cumulative in their requirements:

VeriSign is obligated to meet detailed functional and performance specifications incorporated into the contract in the form of Appendix 7. (Registry Agt., Sect. 3.1(d)(ii)). These contract requirements were established by experts and standards bodies within the Internet community in order to create a secure and stable DNS. The registry operator also is required to maintain technical and operational records, for inspection and audit by ICANN, sufficient to insure compliance with these specifications. (*Id.*).[6]

The proposed agreement further provides a process for changes in the contractual operational specification or policies affecting the registry through the development of Consensus Policies by ICANN, and the Internet community, during the existence of the agreement. This process for the adoption of Consensus Policies is expressly intended to allow for the continual monitoring and updating of policies affecting the registry in order to insure ongoing security and stability in response to changing conditions. (Registry Agt., Sect. 3.1(b)). Pursuant to such provisions, for example, contractual operational specifications on the registry operator may be changed during the term of the contract as necessary to meet changing conditions affecting the security or stability of the DNS or registry database. (Id.). Moreover, unlike the existing .com Registry Agreement, or the Registrar Accreditation Agreements, the proposed agreement adds important flexibility to the process for adopting Consensus Policies by allowing the process itself to be changed during the term of the contract consistent with the requirements of ICANN's Bylaws.[7]

Similarly, the proposed .com Registry Agreement provides procedures for ICANN to adopt, on an emergency basis, new policies necessary to maintain the stability or security of the DNS. (Registry Agt., Sect. 3.1(a)(i)). The precondition for the exer-

cise of this power by ICANN is the determination of the ICANN Board that the change is necessary to maintain the security or stability of the DNS. (*Id.*).[8] This process is an additional oversight and accountability mechanism of substantial breadth.

Therefore, neither the process for the adoption of Consensus Policies, nor the contractual specifications intended to address security and stability, are frozen in place by the contract. Instead, the proposed agreement specifically allows for monitoring and changing requirements on the registry operator as necessary to address the changing requirements for the security or stability of the DNS. (Registry Agt., Sect. 3.1(b)(ii)). These flexible procedures provide extraordinary oversight and accountability, including to address new security and stability concerns.

The proposed .com Registry Agreement also substantially expands ICANN's oversight, and VeriSign's accountability to ICANN, over changes in registry services or new services introduced by the registry operator, prior to such changes being implemented. Such oversight includes reviews of changing services by DNS experts and public review and comment periods. (Registry Agt., Sect. 3.1(d)(iv)). This process for assessing changes in registry services has been used by ICANN as a model for other new registry agreements, including .net and .mobi, among others. There is no comparable process in the existing .com Registry Agreement.

For example, before a change in registry services may be implemented by the registry operator, including the introduction of new services, information regarding the service and potential security and stability implications must be provided to ICANN. ICANN thereafter has the right to review the service, including by seeking advice by experts on whether the service might have implications for the security or stability of the DNS. ICANN further has the right to submit the proposed change to a standing panel of experts to conduct a more detailed analysis of the service prior to its adoption by the registry operator. The panel consists of 20 persons expert in the design, management and implementation of complex systems and standards-protocols utilized in the Internet infrastructure and DNS. In the event the proposed change is submitted to the standing panel, the panel shall invite public comment on the proposed change. If it is determined that the proposed change creates a reasonable risk of an adverse affect on security or stability, the registry operator will not implement the change.

The proposed .com Registry Agreement further requires a twice annual security and stability review by ICANN of issues regarding security and stability affecting the registry. (Registry Agt., Sect.3.1(g)). This requirement does not exist in the current agreement.

The proposed .com Registry Agreement requires the registry operator to establish at its expense a data escrow or mirror site policy for registry data compiled by the registry operator. (Registry Agt., Sect. 3.1(c)(i)). The operator is required regularly to deposit into the escrow all registry data. The proposed agreement also expressly requires the registry operator to take steps to protect all personal data from loss, misuse, unauthorized disclosure, alteration or destruction. (Registry Agt., Sect. 3.1(c)(ii)).

In addition to these contractual provisions providing accountability, VeriSign also engages in other briefings and security activities with ICANN and the Internet community. Currently, VeriSign partners with Department of Homeland Security, National Security Administration and other governmental parties regularly to brief these agencies on the stability and security of the overall DNS and to give timely updates and detailed information regarding attacks and their impact on the Internet infrastructure. VeriSign considers this sharing of information and coordination of data important to the overall stability of the DNS.

VeriSign's technical staff further participates, including by holding key positions in Internet standards and security groups, including Root Server System Advisory Committee (RSSAC), Security and Stability Advisory Committee (SSAC), Internet Engineering Task Force (IETF), Internet Security Alliance (ISA), Information Technology—Information Sharing and Analysis Center (IT–ISAC), National Infrastructure Protection Center (NIPC), Network Reliability and Interoperability Council (NRIC) and National Security Telecommunications Advisory Committee (NSTAC). Such open forums enable discussion and development of critical design considerations for changes to the architecture of the DNS and Internet, both at the root level and the interoperability of third-party systems and applications. VeriSign staff has authored numerous RFCs that define the myriad of standards, features, and best practices of DNS management, security and operations. Through one of these organizations, the IETF, for example, VeriSign has initiated, shaped and refined the standards for DNS Security Extensions, an important issue in shaping future Internet security.

Therefore, the proposed agreement provides multiple, cumulative requirements on the registry operator to insure the stability and security of the registry, provide oversight by ICANN, and ensure accountability to ICANN.

Question 4. How will VeriSign justify the costs of improvements to security systems without accountability to ICANN?

Answer. As explained in response to *Question 3* above, the proposed .com Registry Agreement provides multiple, cumulative requirements on the registry operator to insure the stability and security of the registry, provide oversight by ICANN, and ensure accountability to ICANN. The proposed agreement explicitly requires VeriSign to meet detailed specifications and other obligations designed to insure a secure and stable .com registry. VeriSign has served as the operator of the .com registry since its beginnings in 1992. During this period, VeriSign established an unparalleled record in operating a secure and stable registry. The proposed .com Registry Agreement not only contractually obligates VeriSign to continue to meet that standard, the proposed agreement explicitly provides for increased oversight by ICANN and the Internet community, through Consensus Policies and other provisions, to insure that the operator continues to meet, as it has in the past, the changing requirements for security and stability for the registry and DNS.

VeriSign has been a leader in Internet and DNS security throughout its tenure as the operator of the .com registry. It has participated in industry boards that have helped establish the security and stability requirements for the Internet and DNS. VeriSign also has participated in government reviews with the Department of Homeland Security and National Security Administration, among other governmental security organizations, aimed at developing a coordinated security strategy for the Internet.

From the founding of the DNS through today, VeriSign has invested hundreds of millions of dollars in creating a secure DNS infrastructure, including as the volume of Internet traffic has grown 10,000-fold during just the years 2000 through present. No other operator has ever created or run a registry of this magnitude.

The express terms of the proposed .com Registry Agreement establish substantial and detailed accountability for the operation of the .com registry. Moreover, under the proposed agreement, VeriSign is contractually obligated to maintain 100 percent availability of the DNS systems for the .com gTLD. (Registry Agt., (Sect. 3.1(d)(ii), App. 7, Sect. 7). In order to meet this obligation, VeriSign must take all steps necessary to maintain the secure and stable operation of the DNS. In fact, numerous provisions of the proposed agreement are specifically directed to insuring compliance with this contractual obligation, including by placing particular and detailed obligations on the registry operator and providing for ongoing ICANN oversight as explained in response to *Question 3.* Further, VeriSign's consistent performance since the founding of the DNS, a record spanning more than a decade, establishes beyond any reasonable doubt that VeriSign is motivated to continue to invest in and maintain a secure and stable .com registry, a necessity to meet its performance obligations under the .com Registry Agreement.

ICANN has carefully considered the issue of improvements to security and stability and the methods to insure investment. Cost-based price regulation is complex, costly, and inefficient in the context of preemptive investment in the security and stability of the DNS. As a result, regulators have been moving away from such strict, command-and-control regulation. Such regulation would be particularly harmful in light of the need for preemptive investment in the security and stability of the DNS. The type of investment that needs to be made is critical and often unpredictable until after the consequences of an attack are known. The type of work that needs to be done requires strategic, critical, and preemptive investment that if delayed or derailed by cost justification assessment models would come too late to have an effect. Setting a reasonable price cap that allows for some limited price flexibility, together with the extensive price protections in place in the agreement, strikes the right balance between providing the incentive and flexibility needed for efficient, ongoing, investment to protect security and stability while protecting consumers.

As explained more fully in response to *Question 5,* those price protections include among others, the prohibition on VeriSign from discriminating in price among registrars or their customers, the requirement that VeriSign give registrars 6 months' notice of proposed price increases,[9] and the requirement to allow registrations for terms up to 10 years. This provision was included in the proposed .com Registry Agreement specifically to allow registrants to lock in current prices for up to 10 years and thereby avoid the impact of any proposed price increase even if the registrant choose not to avail themselves of competitive alternatives. (Registry Agt., Sect. 7.3(f)).[10]

ICANN has adopted this carefully considered framework as its model for registry operator agreements. In fact, this model already has been implemented with respect to the 2005 .net Registry Agreement, over a year ago, and the .mobi Registry Agreement.

Question 5. According to the provisions of the proposed agreement, VeriSign can increase prices up to 7 percent in most years, resulting in an overall price increase of up to 31 percent in 6 years. The proposed agreement includes presumptive renewal and guaranteed price increases in most years. How does VeriSign respond to claims of creating a monopoly environment?

Answer. VeriSign appreciates the opportunity to clear up some misconceptions about the effects of the proposed .com Registry Agreement on competition. This agreement has been subject to an extensive and thorough competitive review by the Department of Commerce with the assistance of the Antitrust Division of the Department of Justice. VeriSign and ICANN have worked in concert with these Departments. As a result, the proposed agreement is one which promotes the security and stability of the Internet by providing the incentives and contractual feasibility to make necessary investments in the .com infrastructure. Additionally, the proposed agreement includes specific provisions providing for increased oversight by ICANN of services provided by the registry, including the adoption of a more efficient consultative process with clearer guidelines to allow VeriSign to introduce changes to or new registry services that can benefit the Internet community and the public, while allowing ICANN to review any security, stability and competitive affects of such services prior to their introduction.

Price Increases: It is important to recognize that VeriSign does not set the prices that consumers and businesses pay for domain name registrations. Those prices are set by hundreds of independent domain name registrars, some of whom charge as much as $35 for a domain name, while paying VeriSign, the registry operator, only $6 to provide for operation of the domain name on the Internet. VeriSign's price to registrars for registering .com domain names has been contractually frozen at $6 since 1999. The new .com agreement provides VeriSign some limited flexibility to raise prices at the registry level but it does so under conditions that are tailored to protect registrars and their customers by leveraging important market forces.

The .com registry requires substantial investment in infrastructure, and the demands on that infrastructure are ever increasing, due to rapidly increasing use of the Internet and the growing and more sophisticated attacks on Internet security that were described at the hearing.[11] As explained above, VeriSign has invested hundreds of millions of dollars in creating a secure DNS infrastructure, including while the volume of Internet traffic has grown 10,000-fold during just the years 2000 through present. As the registry operator, VeriSign must bear the entire burden of those investments, and the only source of funding is the .com registry fees. A freeze on those fees would chill incentives and jeopardize the ability to fund needed investments.

The proposed .com Registry Agreement balances the interest in removing inflexible price controls against the needs of registrars by strictly limiting the amount and rate of price increases by VeriSign as well as providing additional safeguards. Thus, VeriSign will only be permitted to increase the price of .com registrations by a maximum of 7 percent and only in four of the six years of a contract term. Thus, by the end of 2012, and assuming VeriSign actually takes the maximum price increases permitted by the agreement, the cost of a .com domain name registration to registrars would be only $7.86.

Other provisions of the agreement also operate to provide safeguards for consumers. While there can only be one operator of the .com or any other TLD registry, there is competition among numerous TLD registries for the business of domain name registrants. There are over 250 TLD registries worldwide. Most domain name registrants can choose among many generic TLDs (gTLDs) such as .com, .biz, .info, .org, .net, and others, and also have choices from among country code TLDs (ccTLDs) such as .de, .uk, .jp, .us and many others—including the recently introduced .eu for registrants with activity anywhere in the European Union. Many domain registrars promote these different TLDs as competitive alternatives for their customers. If registrars view .com as unduly expensive, they can use pricing and promotion to steer registrants to other TLDs. Building on such competitive facts, provisions of the proposed .com Registry Agreement leverage competitive market forces to protect consumers.

First, the proposed .com Registry Agreement expressly prohibits VeriSign from discriminating in price among registrars or their customers. (Registry Agt., Sect. 7.3(e)).[12] VeriSign cannot charge a higher price for renewals of a .com domain name registration than it charges for a new registration. It cannot charge U.S. registrants/registrars a higher price than it charges foreign registrants/registrars. Seventy five

percent of the growth in Internet usage is occurring outside the U.S. and it is estimated that over 60 percent of all domain name registrations come from non-U.S. registrants. More than half the domain names worldwide are registered in TLDs other than .com. Thus, the ongoing competition to attract new registrants to .com—particularly in foreign countries, where .com lags behind ccTLDs and where the overwhelming growth in Internet use and domain name registration is occurring—will force VeriSign to set its prices for *all* registrants at a level dictated by competitive forces worldwide. At the same time, increasing competition from search, keywords and new Internet navigation methods constrain domain name pricing.

Second, the proposed .com Registry Agreement includes a provision requiring VeriSign to give registrars 6 months' notice of proposed price increases, and to allow registrations for terms up to 10 years at the existing price. This provision was included in the agreement specifically to allow registrants to lock in current prices for up to 10 years and thereby avoid the impact of a proposed price increase even if they choose not to avail themselves of competitive alternatives. (Registry Agt., Sect. 7.3(f)). [13]

Therefore, while VeriSign for technical reasons must be the sole operator of the .com registry, it is not a "monopoly" in terms of competitive choices to consumers. The provisions of the .com Registry Agreement gradually relax the 8-year freeze on VeriSign's pricing, but set strict caps on future price increases and include terms that in any circumstances would prevent VeriSign from charging a supracompetitive price for domain name registrations.

Strict price controls are strongly disfavored as a matter of public policy. Even in cases where firms have dominant market shares, and their market position stems in part from governmental grants, price controls are often eschewed. [14] Given the competitive forces at work, allowing VeriSign some carefully limited pricing flexibility is plainly in the public interest, especially given that unlike most contracts, the .com Registry Agreement allows ICANN, through the adoption of Consensus Policies, to change the operational performance requirements for the registry, or require it to provide new services.

Presumptive Renewal: The renewal provisions of the proposed .com Registry Agreement are virtually identical to the renewal provisions in the existing agreement, which were approved by the Department of Commerce in 2001. Both require renewal absent a material breach of the agreement or other circumstances not present here. The existing agreement also specifically provides that this presumptive renewal provision "shall be included in any renewed Registry Agreement." Consistent with renewal models in other infrastructure industries, presumptive renewal is representative of the renewal model ICANN is pursuing in its registry agreements generally, as set out in the .net and .mobi agreements.

The 2001 .com Registry Agreement provides that the agreement "shall be" renewed absent a material breach of the agreement. (2001 Registry Agt., Sect. 25). [15] With respect to the provision concerning a breach of the registry agreement, the existing and proposed agreements contain minor differences. Unlike the existing agreement, the proposed agreement provides that a neutral arbitrator must determine that the registry operator is in breach of the agreement before such a dispute over contractual performance may be the basis for denying renewal. This change is designed to protect VeriSign from the potential loss of its investment in the registry based on a good faith disagreement as to whether particular conduct may be within the scope of the agreement, or the possible use of a claim of breach to extract concessions under the contract. Disagreements regarding the interpretation of the registry agreement have arisen between ICANN and VeriSign from time to time in the past. The change is thus necessary to resolve potential uncertainties in performance of the registry agreement. Certainty in the operation of the registry is necessary to allow ongoing investment in the DNS infrastructure.

The proposed .com Registry Agreement also allows VeriSign an opportunity to cure a breach, which is a standard term of commercial contracts, especially important to contractual certainty in a changing environment for contractual performance such as the Internet. The same clause has been adopted for this same reason in other registry agreements, such as the .net and .mobi Registry Agreements.

Accordingly, there has been no loss of a previously existing opportunity for competitive bidding to replace VeriSign as the operator of the .com registry in the absence of material and uncured breach by VeriSign.

The right to renewal of the .com agreement so long as VeriSign lives by its terms is an enforceable contract right that VeriSign already has. Such a provision is critical in order to allow the registry operator to make the ongoing and substantial investment in the DNS infrastructure necessary to its stability and security.

Despite the claims from self-interested opponent registrars, the proposed .com Registry Agreement does not make any significant change in VeriSign's existing

contractual rights to retain its role as the .com registry operator so long as it is performing in accord with the requirements of the agreement. The explicit terms of the existing agreement require that it be renewed upon its expiration and that the renewal agreement include a similar provision.

Presumptive renewal, or a renewal expectancy, is a common feature of contracts, licenses and franchises that involve long-term investments for some public purpose. Such terms are used in varying ways in broadcast, cable, satellite and other communications licenses, utility franchises and other similar agreements. Without a renewal expectancy, a firm would find it difficult to justify making substantial investments that would take a long time to recoup. With only a 6-year contract term, and with capped prices, an economically rational registry operator would think long and hard about investing millions of dollars in new infrastructure and systems to meet emerging security threats or to respond to increased demand caused by new Internet business models, such as the substantial (and largely unremunerated) demands caused by domain name speculators and pay-per-click advertising businesses. A rational registry operator that did not have a secure renewal expectancy might well defer such investments, particularly toward the end of the contract term, and then promise to make them as part of a renewal bid. Such a framework would undermine the security and stability of the DNS. Moreover, renewal expectancy provides distinct benefits for consumers in the form of quality of service as well as a minimized risk of service disruption due to an arbitrary change in an underlying operator that has provided satisfactory levels of service.

VeriSign has been a highly reliable steward of the .com registry for over 8 years. It has provided unmatched reliability under the most demanding conditions—unlike the problems experienced by firms operating even much smaller and less demanding registries. Competition from other TLD registries will continue to force VeriSign to keep .com competitive. It would be short-sighted to destroy the renewal expectancy, there is no competitive reason to do so, and it would be a violation of the express terms of the existing registry agreement.

Question 6. How will the exclusion of competition affect pricing elsewhere in the Internet registry market?

Answer. As the answer to *Question 5* demonstrates, the .com agreement will not exclude competition. There can be only one registry for the .com TLD or for each of the other more than 250 registries worldwide. The proposed .com Registry Agreement, therefore, will neither eliminate any competition that would otherwise have existed nor will it create monopoly power. Rather it carefully regulates the terms, including the price, on which VeriSign can provide domain name registrations and other registry services to registrars. Within the constraints of the proposed agreement, VeriSign's pricing will continue to be affected by the competitive pricing and service offerings of other competitive registries, particularly as VeriSign seeks to assist registrars in penetrating growing geographic markets in Asia, Europe, Latin America and the rest of the world, and as the registry competes for new domain name registrations in addition to renewal registrations, which must be priced in a nondiscriminatory manner. Likewise, innovative services from VeriSign will stimulate competition from those other registries and benefit domain name registrars and registrants in the U.S. and around the world.

Question 7. What strength is there to the VeriSign claims that not renewing its contract will be a detriment to DNS security?

Answer. Currently, .com is under constant attack from hackers who realize the economic devastation that would result if businesses that use the Internet to conduct business via IP-based transactions (banks, brokerage houses, stock exchanges, online commerce) were to lose the ability to connect to one another via the Internet. For example, NASD, the London Stock Exchange, Chase Bank and Citibank run on .com name servers. Additionally, all of the agencies reliant upon .gov sites are reliant upon .com as the resolution provider for all .gov names is routed through a .com server. In February 2005, the World Bank Operations and Policy Department issued a paper which outlined the development of capital markets and eFraud. The paper reviewed several case studies of fraud perpetrated upon various financial systems around the word. The common component of the study reveals that the world's economic models more and more heavily rely upon IP-based transactions. While hackers attempt to penetrate these institutions at various levels, including the private hardware and software of banks, it is important to note that malicious attacks against the core infrastructure providers of the DNS are the most malicious way to attack the broadest segment of the financial institutions of this country. Financial institutions are just one example of a meaningful U.S. business sector reliant upon the stability of the DNS.

As explained in response to *Question 5,* due to the large ongoing investments currently required in the development and maintenance of the DNS infrastructure, such uncertainty would negatively impact the willingness of registry operators to make the investments necessary to guarantee a secure and stable registry, especially toward the end of a registry term.

The express terms of the existing 2001 .com Registry Agreement require renewal. More specifically, Section 25 of the agreement explicitly provides that the agreement "shall be" renewed (absent a material breach of the agreement, which is not present here) and that this renewal clause shall be included in the renewal agreement. A failure to comply with the renewal terms would constitute a breach of the registry contract contrary to law. Equally fundamental, a failure to comply with such terms, which are included in other registry agreements as well as the 2001 .com Registry Agreement, would interject damaging uncertainty into the performance of such agreements.

Furthermore, only VeriSign has demonstrated an ability to operate in a secure and stable manner a registry of the magnitude of the .com registry, as explained above. ICANN explicitly adopted such a finding in November 2005.[16] Unlike any other registry operator, VeriSign has operated the .Com registry, the largest Internet registry, at 100 percent availability (with no interruption of service) for the last 8 years. Thus, there would be inherent risks to the security and stability of the DNS in failing to renew the agreement (as its express terms require) and transitioning the operation of the registry to a new and necessarily untested operator.

Endnotes

[1] Examples of TLDs available around the world include: .info, .org, com, .travel, .mil, .us, .biz, .net, info, .name, .bz, .jp, eu, .uk, .de, .kr, .mobi, .asia, .museum, .pro, .jobs, .edu, .gov. Norid, the .no registry, has a complete list of worldwide domains at *http://www.norid.no/domenenavnbaser/domreg.html*.

[2] For example, registrars today offer a .com domain for prices from $1.99 to $1,000 within packages and as stand alone sales. Domain name registrations are accepted by Registrars from end-users for terms of 1 (one) year to one-hundred (100) years. The registrars differentiate themselves from one another based upon value added services, customer service and some compete upon price. Regardless of the registrar model, the registry wholesale price for a .com name, as set in the ICANN contract with VeriSign is currently $6.00. This is the "wholesale" rate. The average "retail" rate charged for a .com domain today is $21.00.

[3] The Registrar Accreditation Agreement provides as follows:

> "3.6 *Data Escrow.* During the Term of this Agreement, on a schedule, under the terms, and in the format specified by ICANN, Registrar shall submit an electronic copy of the database described in Subsection 3.4.1 to ICANN or, at Registrar's election and at its expense, to a reputable escrow agent mutually approved by Registrar and ICANN, such approval also not to be unreasonably withheld by either party. The data shall be held under an agreement among Registrar, ICANN, and the escrow agent (if any) providing that (1) the data shall be received and held in escrow, with no use other than verification that the deposited data is complete, consistent, and in proper format, until released to ICANN; (2) the data shall be released from escrow upon expiration without renewal or termination of this Agreement; and (3) ICANN's rights under the escrow agreement shall be assigned with any assignment of this Agreement. The escrow shall provide that in the event the escrow is released under this Subsection, ICANN (or its assignee) shall have a nonexclusive, irrevocable, royalty-free license to exercise (only for transitional purposes) or have exercised all rights necessary to provide Registrar Services."

http://www.icann.org/registrars/ra-agreement-17may01.htm#3.

[4] The .com Registry Agreement Provides as follows:

> "Data Escrow. Registry Operator shall establish at its expense a data escrow or mirror site policy for the Registry Data compiled by Registry Operator. Registry Data, as used in this Agreement, shall mean the following: (1) data for domains sponsored by all registrars, consisting of domain name, server name for each nameserver, registrar id, updated date, creation date, expiration date, status information, and DNSSEC-related key material; (2) data for nameservers sponsored by all registrars consisting of server name, each IP address, registrar id, updated date, creation date, expiration date, and status information; (3) data for registrars sponsoring registered domains and nameservers, consisting of registrar id, registrar address, registrar telephone number, registrar e-mail address, WHOIS server, referral URL, updated date and the name, telephone

number, and e-mail address of all the registrar's administrative, billing, and technical contacts; (4) domain name registrant data collected by the Registry Operator from registrars as part of or following registration of a domain name; and (5) the DNSSEC-related material necessary to sign the .com zone (*e.g.*, public and private portions of .com zone key-signing keys and zone-signing keys). The escrow agent or mirror-site manager, and the obligations thereof, shall be mutually agreed upon by ICANN and Registry Operator on commercially reasonable standards that are technically and practically sufficient to allow a successor registry operator to assume management of the TLD. To this end, Registry Operator shall periodically deposit into escrow all Registry Data on a schedule (not more frequently than weekly for a complete set of Registry Data, and daily for incremental updates) and in an electronic format mutually approved from time to time by Registry Operator and ICANN, such approval not to be unreasonably withheld by either party. In addition, Registry Operator will deposit into escrow that data collected from registrars as part of offering Registry Services introduced after the Effective Date of this Agreement. The escrow shall be maintained, at Registry Operator's expense, by a reputable escrow agent mutually approved by Registry Operator and ICANN, such approval also not to be unreasonably withheld by either party. The schedule, content, format, and procedure for escrow deposits shall be as reasonably established by ICANN from time to time, and as set forth in Appendix 1 hereto. Changes to the schedule, content, format, and procedure may be made only with the mutual written consent of ICANN and Registry Operator (which neither party shall unreasonably withhold) or through the establishment of a Consensus Policy as outlined in Section 3.1(b) above. The escrow shall be held under an agreement, substantially in the form of Appendix 2, as the same may be revised from time to time, among ICANN, Registry Operator, and the escrow agent."

.Com Registry Agt., Sect. 3.1(c)(i); *http://www.icann.org/topics/vrsn-settlement/revised-com-agreement-clean-29jan06.pdf.*

[5] *http://www.icann.org/tlds/agreements/verisign/registry-agmt-app1-22sep05.pdf; http://www.icann.org/tlds/agreements/verisign/registry-agmt-app2-22sep05.pdf.*

[6] For example, the .com Registry Agreement provides for reporting and audit with associated penalties:

"Functional and Performance Specifications. Functional and Performance Specifications for operation of the TLD shall be as set forth in Appendix 7 hereto, and shall address without limitation DNS services; operation of the shared registration system; and nameserver operations. Registry Operator shall keep technical and operational records sufficient to evidence compliance with such specifications for at least 1 year, which records ICANN may audit from time to time upon reasonable advance written notice, provided that such audits shall not exceed one per quarter. Any such audit shall be at ICANN's cost."

Registry Agt., Sect. 3.1(d)(ii).

"Monthly Reporting. Within 20 days following the end of each calendar month, Registry Operator shall prepare and deliver to ICANN a report providing such data and in the format specified in Appendix 4. ICANN may audit Registry Operator's books and records relating to data contained in monthly reports from time to time upon reasonable advance written notice, provided that such audits shall not exceed one per quarter. Any such audit shall be at ICANN's cost, unless such audit shall reflect a material discrepancy or discrepancies in the data provided by Registry Operator. In the latter event, Registry Operator shall reimburse ICANN for all costs and expenses associated with such audit, which reimbursement shall be paid together with the next Registry-Level Fee payment due following the date of transmittal of the cost statement for such audit."

Registry Agt., Sect. 3.1(c)(iv).

[7] The provision provides as follows:

"*Consensus Policies.*

(i) At all times during the term of this Agreement and subject to the terms hereof, Registry Operator will fully comply with and implement all Consensus Policies found at *http://www.icann.org/general/consensus-policies.htm,* as of the Effective Date and as may in the future be developed and adopted in accordance with ICANN's Bylaws and as set forth below.

(ii) "Consensus Policies" are those specifications or policies established (1) pursuant to the procedure set forth in ICANN's Bylaws and due process, and (2)

covering those topics listed in Section 3.1(b)(iv) below. The Consensus Policy development process and procedure set forth in ICANN's Bylaws may be revised from time to time in accordance with ICANN's Bylaws, and any Consensus Policy that is adopted through such a revised process and covering those topics listed in Section 3.1(b)(iv) below shall be considered a Consensus Policy for purposes of this Agreement.

(iii) For all purposes under this Agreement, the policies identified at *http://www.icann.org/general/consensus-policies.htm* shall be treated in the same manner and have the same effect as "Consensus Policies."

(A) Consensus Policies and the procedures by which they are developed shall be designed to produce, to the extent possible, a consensus of Internet stakeholders, including the operators of gTLDs. Consensus Policies shall relate to one or more of the following: (1) issues for which uniform or coordinated resolution is reasonably necessary to facilitate interoperability, Security and/or Stability of the Internet or DNS; (2) functional and performance specifications for the provision of Registry Services (as defined in Section 3.1(d)(iii) below); (3) Security and Stability of the registry database for the TLD; (4) registry policies reasonably necessary to implement Consensus Policies relating to registry operations or registrars; or (5) resolution of disputes regarding the registration of domain names (as opposed to the use of such domain names). . . .

[8] That provision states as follows:

"*Preserve Security and Stability.*

ICANN Temporary Specifications or Policies. Registry Operator shall comply with and implement all specifications or policies established by the ICANN Board of Directors on a temporary basis, if adopted by the ICANN Board of Directors by a vote of at least two-thirds of its members, so long as the ICANN Board of Directors reasonably determines that immediate temporary establishment of a specification or policy on the subject is necessary to maintain the Stability or Security (as defined in Section 3.1(d)(iv)(G)) of Registry Services or the DNS ('Temporary Specification or Policies'). Such proposed specification or policy shall be as narrowly tailored as feasible to achieve those objectives. In establishing any specification or policy under this provision, the ICANN Board of Directors shall state the period of time for which the specification or policy is temporarily adopted and shall immediately implement the Consensus Policy development process set forth in ICANN's Bylaws. ICANN shall also issue an advisory statement containing a detailed explanation of its reasons for adopting the temporary specification or policy and why the Board believes the specification or policy should receive the consensus support of Internet stakeholders. If the period of time for which the specification or policy is adopted exceeds 90 days, the ICANN Board shall reaffirm its temporary adoption every 90 days for a total period not to exceed 1 year, in order to maintain such policy in effect until such time as it shall become a Consensus Policy as described in Section 3.1(b) below. If during such 1 year period, the temporary policy or specification does not become a Consensus Policy meeting the standard set forth in Section 3.1(b) below, Registry Operator shall no longer be required to comply with or implement such temporary policy or specification."

[9] "*No price discrimination.* Registry Operator shall charge the same price for Registry Services subject to this Section 7.3, not to exceed the Maximum Price, to all ICANN-accredited registrars (provided that volume discounts and marketing support and incentive programs may be made if the same opportunities to qualify for those discounts and marketing support and incentive programs is available to all ICANN-accredited registrars)." Registry Agt., Sect. 7.3(e).

[10] "*Adjustments to Pricing for Domain Name Registrations.* Registry Operator shall provide no less than 6 months prior notice in advance of any increase for new and renewal domain name registrations and for transferring a domain name registration from one ICANN-accredited registrar to another and shall continue to offer for periods of up to 10 years new and renewal domain name registrations fixed at the price in effect at the time such offer is accepted. Registry Operator is not required to give notice of the imposition of the Variable Registry-Level Fee set forth in Section 7.2(c)." Registry Agt., Sect. 7.3(f).

[11] The Shared Registration System (SRS) is the system maintained by VeriSign as the .com registry operator that allows multiple registrars to register and modify domain names in the registry database. That, however, is only one component of VeriSign's obligations under the .com Registry Agreement. VeriSign also must maintain Domain Name System (DNS) up-time and availability. The DNS is what makes the domain name "work" as a resource or locator on the Internet. Stated another

way, the DNS is what enables you as an Internet user to simply type in a domain name on your computer, such as "verisign.com," and connect it over the Internet to the machine that hosts the proper website. The receipt of DNS queries or "look-ups" for a particular domain name is separate from the SRS or its operation. Were the DNS to fail, the Internet would not work. Were the SRS to fail, traffic would still move over the Internet. Registrars could simply not register new domain names. While domain names may be registered through the SRS and VeriSign receives $6, that fee also must cover resources for processing queries/traffic. Such fee, however, is not based on the volume of queries/traffic received. The explosion of Internet-enabled devices and applications—text messaging, music downloads, VoIP, Blackberries and device-to-device communications—has created exponential growth in Internet traffic far surpassing the increase in users. While users have increased 300 percent since 2000, the volume of traffic on .com and .net has increased 1,900 percent in that same period. Domain name registration has not kept pace.

[12] "*No price discrimination.* Registry Operator shall charge the same price for Registry Services subject to this Section 7.3, not to exceed the Maximum Price, to all ICANN-accredited registrars (provided that volume discounts and marketing support and incentive programs may be made if the same opportunities to qualify for those discounts and marketing support and incentive programs is available to all ICANN-accredited registrars)." Registry Agt., Sect. 7.3(e).

[13] "*Adjustments to Pricing for Domain Name Registrations.* Registry Operator shall provide no less than 6 months prior notice in advance of any increase for new and renewal domain name registrations and for transferring a domain name registration from one ICANN-accredited registrar to another and shall continue to offer for periods of up to 10 years new and renewal domain name registrations fixed at the price in effect at the time such offer is accepted. Registry Operator is not required to give notice of the imposition of the Variable Registry-Level Fee set forth in Section 7.2(c)." Registry Agt., Sect. 7.3(f).

[14] For example, a pharmaceutical company may obtain a patent on a drug that is the sole drug approved by the FDA for a particular indication. An airline may dominate a hub airport due to a lack of gate space or takeoff/landing slots. A franchised cable operator may be the sole provider of broadband Internet access in an area where the local telephone company cannot feasibly provide DSL service. In none of these situations does the government regulate prices.

[15] That provision provides as follows:

> "25. Procedure for Subsequent Agreement
>
> B. ICANN shall consider the Renewal Proposal for a period of no more than 6 months before deciding whether to call for competing proposals from potential successor registry operators for the Registry TLD. During this 6 month period, ICANN may request Registry Operator to provide, and Registry Operator shall provide, additional information concerning the Renewal Proposal that ICANN determines to be reasonably necessary to make its decision. Following consideration of the Renewal Proposal, Registry Operator *shall be awarded* a four-year renewal term unless ICANN demonstrates that: (a) Registry Operator is in material breach of this Registry Agreement, (b) Registry Operator has not provided and will not provide a substantial service to the Internet community in its performance under this Registry Agreement, (c) Registry Operator is not qualified to operate the Registry TLD during the renewal term, or (d) the maximum price for initial and renewal registrations proposed in the Renewal Proposal exceeds the price permitted under Section 22 of this Registry Agreement. The terms of the registry agreement for the renewal term shall be in substantial conformity with the terms of registry agreements between ICANN and operators of other open TLDs then in effect, provided that this Section 25 shall be included in any renewed Registry Agreement unless Registry Operator and ICANN mutually agree to alternative language.
>
> C. In the event that ICANN fails to award a renewal registry agreement to Registry Operator within the 6-month period described above, Registry Operator shall have the right to challenge the reasonableness of that failure under the provisions of Section 15.
>
> D. In the event ICANN does not award Registry Operator a renewal registry agreement according to Subsection 25(B), ICANN shall call for competitive proposals and Registry Operator shall be eligible, to the same extent as similarly situated entities, to submit a proposal in response to such a call and to be considered for such award."

[16] *http://www.icann.org/announcements/announcement-21nov05.htm.*

QUESTIONS SUBMITTED BY HON. DANIEL K. INOUYE TO DR. PAUL TWOMEY*

Question 1. One of ICANN's overarching principles is to create a transparent, "bottom-up" consensus driven system of management. Many critics argue that ICANN has strayed far away from this principle. What response do you have to claims that ICANN does not satisfactorily inform the public of its decisionmaking process, such as, in the case of the dot-biz, dot-org, and dot-info proposed contract agreements?

Question 2. How do you respond to critics who note that ICANN has yet to substantially involve Internet users? For example, the stalled, and ultimately abandoned, attempt to hold open elections.

Question 3. Is the involvement that the NTIA had on the creation of the dot-xxx domain name representative of the decisionmaking process in ICANN?

Question 4. ICANN has been praised for its attention and success in the areas of stability and security of the DNS. However, the proposed agreement with VeriSign and the general evolution of the Internet has raised new concerns. Under the terms of the proposed agreement, ICANN and VeriSign are only required to meet to discuss security every 6 months. Is 6 months often enough to ensure the security of the DNS?

Question 5. The terms of the proposed VeriSign agreement reduces ICANN's power to terminate the agreement. Compared to the 2001 agreement, how does this weaken ICANN's ability to oversee the dot-com registry and maintain the security of the DNS?

Question 6. Do you think that breaking ties with NTIA's governance will make the Internet vulnerable to other governing bodies?

Question 7. How do you address the concerns of those who feel that the MOU should be renewed before the proposed VeriSign agreement is approved or denied in order to address security concerns?

Question 8. The lack of transparency in the ICANN decisionmaking system also extends to the budget. How do you address concerns about a lack of accountability for the ICANN budget?

○

*Response to written questions was not available at the time this hearing went to press.