The Internet Corporation for Assigned Names and Numbers

NEWS RELEASE

Brussels ♦ Sydney ♦ Washington ♦ Los Angeles

FOR RELEASE: Immediate

CONTACTS: Brad White
Director of Media Affairs
Ph. +1 202.429.2710
E: brad.white@icann.org

Michele Jourdan
Corporate Affairs Division
Ph. +1 310.301.5831
E: Michele.jourdan@icann.org

ICANN to Work with United States Government and VeriSign on interim solution to core Internet security issue

Immediate security concerns addressed by DNSSEC

Washington, D.C. … June 3, 2009… ICANN will work with the U.S. Department of Commerce's National Telecommunications and Information Administration (NTIA), the National Institute of Standards and Technology (NIST) and VeriSign on the goal of an operationally Signed Root Zone as soon as feasible in 2009.

In a letter agreeing to participate ICANN recognizes the urgency surrounding the issue of electronically signing the Internet's "root zone" but stresses the need for this process to be interim.

"We've been working towards a signed root for more than three years. In fact, ICANN has operated a root zone signing test bed for more than two years. So ICANN is aware of the urgency around signing the root to enhance stability and security" Paul Twomey, President and CEO of ICANN said.

"The ICANN has agreed to work with VeriSign and the Department of Commerce to first test, and then have production deployment of DNS Security Extensions (DNSSEC) before the end of the year without prejudice to any proposals that may be made for long term signing processes" said Twomey.

"There will of course need to be consultations with the Internet technical community as the testing and implementation plans are developed" he added.

The NTIA asked for input from the Internet community in October 2008 on the issue of securing the top level of the domain name system (DNS) from vulnerabilities that threaten the accuracy and integrity of

the DNS data. Vulnerabilities in the existing DNS have become easier to exploit to the extent that malicious parties may be able to distribute false DNS information, and to re-direct Internet users.

Details of the process are still being worked on but discussions between the Department of Commerce and VeriSign and ICANN have identified that VeriSign will manage and have operational responsibility for the Zone Signing Key in the interim arrangement, and that ICANN will manage the Key Signing Key process. ICANN will work closely with VeriSign regarding the operational and cryptographic issues involved.

“This is very important for the global community of Internet users. We will work closely with all participants on this crucial security initiative.” Twomey said.

For more information on DNSSEC deployment, please visit:

http://www.icann.org/en/announcements/dnssec-qaa-09oct08-en.htm

###

About ICANN:

To reach another person on the Internet you have to type an address into your computer - a name or a number. That address has to be unique so computers know where to find each other. ICANN coordinates these unique identifiers across the world. Without that coordination we wouldn't have one global Internet. ICANN was formed in 1998. It is a not-for-profit public-benefit corporation with participants from all over the world dedicated to keeping the Internet secure, stable and interoperable. It promotes competition and develops policy on the Internet’s unique identifiers. ICANN doesn’t control content on the Internet. It cannot stop spam and it doesn’t deal with access to the Internet. But through its coordination role of the Internet’s naming system, it does have an important impact on the expansion and evolution of the Internet. **For more information please visit: www.icann.org.**