777(i)(1) of the Tariff Act of 1930, as amended, and 19 CFR 351.213(d)(4).

Dated: June 2, 2010.

John M. Andersen,

Acting Deputy Assistant Secretary for Antidumping and Countervailing Duty Operations.

[FR Doc. 2010–13862 Filed 6–8–10; 8:45 am]

BILLING CODE 3510–DS–S

DEPARTMENT OF COMMERCE

National Telecommunications and Information Administration

[Docket No. 100603240–0240–01]

Availability of Testing and Evaluation Report and Intent To Proceed With the Final Stages of Domain Name System Security Extensions Implementation in the Authoritative Root Zone

AGENCY: National Telecommunications and Information Administration, Department of Commerce.

ACTION: Notice.

SUMMARY: The Department of Commerce's National Telecommunications and Information Administration (NTIA) announces the availability of the Domain Name System Security Extensions (DNSSEC) testing and evaluation report and NTIA's intent to proceed with the final stages of DNSSEC deployment in the authoritative root zone. As part of this notice, NTIA is providing a public review and comment period on the testing and evaluation report and the commencement of the final stage of the DNSSEC deployment before taking any action.

DATES: Comments must be submitted by June 21, 2010.

ADDRESSES: Written comments may be submitted by mail to Fiona Alexander, Associate Administrator, Office of International Affairs, National Telecommunications and Information Administration, US Department of Commerce, 1401 Constitution Avenue, NW., Room 4701, Washington, DC 20230. Written comments may also be sent by facsimile to (202) 482–1865 or electronically via electronic mail to *DNSSEC@ntia.doc.gov.* Comments will be posted on NTIA's Web site at *http://www.ntia.doc.gov/DNS/DNSSEC.html.*

FOR FURTHER INFORMATION CONTACT: For further information about this notice, please contact Ashley Heineman at (202) 482–0298 or *aheineman@ntia.doc.gov.*

SUPPLEMENTARY INFORMATION: The Domain Name and Addressing System (DNS) is a distributed hierarchical system that converts domain names (*e.g.*, *http://www.ntia.doc.gov*) into the numerical Internet Protocol (IP) addresses (*e.g.*, 170.110.225.155). The accuracy, integrity, and availability of the information supplied by the DNS is essential to the operation of any system or service that uses the Internet.

However, the DNS was not originally designed with strong security mechanisms, and technological advances have made it easier to successfully exploit vulnerabilities. Such exploits include distributing false DNS information and improperly re-directing Internet users to bogus Web sites.

To mitigate these vulnerabilities, the Internet Engineering Task Force (IETF),[1] using the same open standards process used to develop the core DNS protocols, developed a set of protocol security extensions known as DNSSEC. DNSSEC was designed to support authentication of the source and integrity of information stored in the DNS using public key cryptography and a hierarchy of digital signatures.

On October 9, 2008, NTIA issued a Notice of Inquiry (NOI) seeking input from the community regarding DNSSEC implementation at the Root Zone.[2] NTIA received many comments in response to the NOI. The comments NTIA received from the Internet community indicated that DNSSEC should be implemented at the Root Zone level as soon as practically possible in a manner that maintains the security and stability of the DNS. Thus, NTIA, in conjunction with the National Institute for Standards and Technology (NIST), announced in June 2009 that it would work with the Internet Corporation for Assigned Names and Numbers (ICANN) and VeriSign to deploy DNSSEC at the authoritative root zone of the Internet.[3] Subsequently, these parties initiated work on DNSSEC deployment including the development of detailed documentation and consultation with experts within the Internet technical community.[4]

Prior to NTIA providing authorization to proceed with the final stages of deployment, ICANN and VeriSign agreed to document and evaluate all DNSSEC testing and implementation efforts taken at the authoritative root zone and submit a final report to NTIA for its review and approval.[5]

On May 31, 2010, ICANN and VeriSign submitted their testing and evaluation report.[6] With the submission of the testing and evaluation report, ICANN and VeriSign also formally requested NTIA authorization to proceed with the final stages of DNSSEC deployment at the authoritative root zone. NTIA and NIST have reviewed the testing and evaluation report and conclude that DNSSEC is ready for the final stages of deployment at the authoritative root zone. NTIA hereby announces its intent to authorize the final stages of deployment, which include the publication of the root DNSSEC trust anchor[7] and the distribution of a DNSSEC validatable root zone with an anticipated completion date of July 15, 2010.

Review and Comment Period:

Before NTIA takes any action to authorize the final stage of DNSSEC deployment at the authoritative root zone, NTIA seeks public comment on the intended action. NTIA welcomes comments from the public relevant to the DNSSEC testing and evaluation report and/or NTIA's notice of intent to proceed with the final stages of DNSSEC deployment at the authoritative root zone. Comments must be submitted by June 21, 2010.

Dated: June 3, 2010.

Lawrence E. Strickling,

Assistant Secretary for Communications and Information.

[FR Doc. 2010–13893 Filed 6–8–10; 8:45 am]

BILLING CODE 3510–60–P

[1] The IETF is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual. For more information see *http://www.ietf.org.*

[2] Enhancing the Security and Stability of the Internet's Domain Name and Addressing System, 73 FR 59,608 (Oct. 9, 2008), available at *http://www.ntia.doc.gov/frnotices/2008/FR_DNSSEC_081009.pdf.* The Root Zone is the top-level DNS zone in a Domain Name System (DNS) hierarchy.

[3] NTIA Press Release, June 8, 2009, available at *http://www.ntia.doc.gov/press/2009/OIA_DNSSEC_090603.html.*

[4] This documentation is available at *http://www.root-dnssec.org/documentation.*

[5] VeriSign's and ICANN's roles with regards to root zone management are pursuant to the Cooperative Agreement and IANA Functions Contract respectively.

[6] This report is available at *http://www.ntia.doc.gov/DNS/DNSSEC_05282010.html.*

[7] In cryptography, a trust anchor is an authoritative entity represented via a public key and associated data. It is used in the context of public key infrastructures, digital certificates and DNSSEC.