Register on Thursday, October 2, 2008 (73 FR 57336).

The Council's Research Steering Committee (Committee) will address a range of issues including a briefing on the status of NMFS' Cooperative Research Program activities and funding. The Committee also will review preliminary work of the NEFMC's 5-year research priorities. The Committee will re-examine, and possibly revise, the evaluation criteria for cooperative research priorities subject to review by the Committee as well as review a small number of cooperative research project final reports. The Committee will also discuss the use of a workshop format to conduct future Committee management reviews. Finally, the Committee will discuss outstanding issues related to the Council's research set-aside programs if time allows. The Committee may consider other topics at their discretion.

Although non-emergency issues not contained in this agenda may come before this group for discussion, those issues may not be the subject of formal action during this meeting. Action will be restricted to those issues specifically listed in this notice and any issues arising after publication of this notice that require emergency action under section 305(c) of the Magnuson-Stevens Act, provided the public has been notified of the Council's intent to take final action to address the emergency.

Special Accommodations

This meeting is physically accessible to people with disabilities. Requests for sign language interpretation or other auxiliary aids should be directed to Paul J. Howard, Executive Director, at (978) 465–0492, at least 5 days prior to the meeting date.

Authority: 16 U.S.C. 1801 *et seq.*

Dated: October 6, 2008.

Tracey L. Thompson,

Acting Director, Office of Sustainable Fisheries, National Marine Fisheries Service.

[FR Doc. E8–23941 Filed 10–8–08; 8:45 am]

BILLING CODE 3510–22–S

DEPARTMENT OF COMMERCE

National Telecommunications and Information Administration

Docket Number: 0810021307–81308–01

Enhancing the Security and Stability of the Internet's Domain Name and Addressing System

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

ACTION: Notice of Inquiry

SUMMARY: The Department of Commerce (Department) notes the increase in interest among government, technology experts and industry representatives regarding the deployment of Domain Name and Addressing System Security Extensions (DNSSEC) at the root zone level. The Department remains committed to preserving the security and stability of the DNS and is exploring the implementation of DNSSEC in the DNS hierarchy, including at the authoritative root zone level. Accordingly, the Department is issuing this notice to invite comments regarding DNSSEC implementation at the root zone.

DATES: Comments are due on November 24, 2008.

ADDRESSES: Written comments may be submitted by mail to Fiona Alexander, Associate Administrator, Office of International Affairs, National Telecommunications and Information Administration, U.S. Department of Commerce, 1401 Constitution Avenue, N.W., 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 website 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:

Background. The Domain Name and Addressing System (DNS) is a critical component of the Internet infrastructure and is used by almost every Internet protocol-based application to associate human readable computer hostnames with the numerical addresses required to deliver information on the Internet. It is a hierarchical and globally distributed system in which distinct servers maintain the detailed information for their local domains and pointers for how to navigate the hierarchy to retrieve information from other domains. The accuracy, integrity, and availability of the information supplied by the DNS are essential to the operation of any system, service or application that uses the Internet.

The DNS was not originally designed with strong security mechanisms to ensure the integrity and authenticity of the DNS data. Over the years, a number of vulnerabilities have been identified in the DNS protocol that threaten the accuracy and integrity of the DNS data and undermine the trustworthiness of the system. Technological advances in computing power and network transmission speeds have made it possible to exploit these vulnerabilities more rapidly and effectively.[1]

Development of the DNSSEC Protocol. To mitigate the long-recognized vulnerabilities in the DNS, the Internet Engineering Task Force (IETF), using the same open standards process employed to develop the core DNS protocols, has developed a set of protocol extensions to protect the Internet from certain DNS related attacks: DNSSEC.[2] DNSSEC is 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. It is designed to offer protection against forged (''spoofed'') DNS data, such as that created by DNS cache poisoning, by providing: (1) validation that DNS data is authentic; (2) assurance of data integrity; and (3) authenticated denial of existence.[3] DNSSEC does not provide any confidentiality for, or encryption of, the DNS data itself. The DNSSEC protocol also does not protect against denial of service (DoS) attacks or other attacks against the name server itself.[4]

The DNSSEC protocol is designed to allow for deployment in discrete zones within the DNS infrastructure without requiring deployment elsewhere, as DNSSEC is an opt-in technology. Signing of any individual zone or domain within the hierarchy does not

[1] *See*, National Research Council, The National Academies, *Signposts in Cyberspace: The Domain Name System and Internet Navigation* 154 (2005)(*Signposts*), http://books.nap.edu/catalog.php?record__id=11258#toc (last checked September 29, 2008); Department of Homeland Security, National Security Division, and National Institute of Standards and Technology, National Vulnerability Database, Vulnerability Summary for CVE-2008–1447 (Original release date July 08, 2008; last revised September 17, 2008) available at http://web.nvd.nist.gov/view/vuln/detail?vuln Id=CVE-2008–1447 (last checked September 23, 2008) (This site provides a list of most recent advisories regarding DNS vulnerabilities including DNS spoofing, cache poisoning, etc., and includes links to tools and solutions).

[2] The DNSSEC protocol has been under development since the 1990s with the latest revision approved by the IETF in 2005. RFC 4033 and its companion documents RFCs 4034 and 4035 update, clarify and refine the security extensions previously defined orginally in RFC 2535 and its predecessors. *Id.*, *Signposts*, at 154; *see also*, S. Rose and R. Chandramouli, ''Challenges in Securing the Domain Name System,'' Institute of Electrical and Electronics Engineers (IEEE) Security and Privacy Journal, Vol. 4, No. 1, 84 (Tom Karygiannis, Rick Kuhn, and Susan Landau eds., Jan./Feb. 2006)(Challenges), http://www.antd.nist.gov/pubs/Rose-Challenges%20in%20Securing%20DNS.pdf.

[3] R. Arends *et al.*, DNS Security Introduction and Requirements, Internet Engineering Task Force (IETF) Request for Comment (RFC) 4033 (March 2005)(RFC 4033), http://www.ietf.org/rfc/rfc4033.txt (last checked September 24, 2008).

[4] *Id.*

obligate or force any entity operating a zone elsewhere in the DNS hierarchy to deploy. In addition, end users systems only receive DNSSEC signed information if they request it.

Proponents of DNSSEC assert that widespread deployment of the protocol would mitigate many of the vulnerabilities currently associated with the DNS, increasing the security and integrity of the Internet DNS in a scalable fashion.[5] Ubiquitous deployment of DNSSEC would also enable authentication of the hierarchical relationship between domains to provide the highest levels of assurance. Thus, to realize the greatest benefits from DNSSEC, there needs to be an uninterrupted chain of trust from the zones that choose to deploy DNSSEC back to the root zone.[6]

Ubiquitous deployment of DNSSEC throughout the Internet landscape would require action by a broad range of entities supporting the operation of the DNS infrastructure including, for example, domain name registrars, top level domain (TLD) registry operators and the operators or managers for sub-domains or enterprise networks, Internet service providers (ISPs), software vendors, and others.[7] Additionally, software will need to be developed, servers will need to be configured to support DNSSEC, and users' systems will need to be configured to look for the authenticating signatures.

Current DNSSEC Deployment Status. To date, deployment of DNSSEC has been somewhat piecemeal. At present, only a small number of country code top level domain (ccTLD) operators (*e.g.*, .se [Sweden], .pr [Puerto Rico], .bg [Bulgaria], and .br [Brazil]) have deployed DNSSEC.[8] In addition, the operators of several generic TLDs (including .org and .gov) have publicly announced their intention to do so.[9] A number of second-level domain operators have also signed their zones, such as nist.gov.[10]

Some argue that DNSSEC deployment has been delayed because without a signed root, early deployments operate as ''islands of trust'' with no established chain of trust above them in the DNS hierarchy connecting them to other signed zones.[11] Without a common, shared ''trust anchor,''[12] these early deployers and others that wish to deploy DNSSEC must be able to manage not only their own trust anchors or ''keys,'' but also the trust anchors for other signed domains within the DNS hierarchy.[13] The technical and procedural challenges presented by this ''key management'' dilemma need to be overcome to facilitate DNSSEC deployment.[14]

Due to the complexities involved in managing trust anchors in the absence of a signed root, alternative mechanisms such as ''trust anchor repositories'' (TARs) are also being developed.[15] TARs are just one type of alternative available today. It is not clear what other alternatives for key management may be currently under development or could be developed in the future.[16]

Implementing DNSSEC at the Root. The hierarchical nature of the DNS structure (*e.g.*, root zone, top level domains, sub-domains) and the trust anchor framework required for security-aware resolvers to validate a signed response arguably make DNSSEC deployment at the root level (*i.e.*, ''signing'' of the root) an important step to achieve optimal benefits from the protocol. Signing the root would provide a single trust anchor at the top of the hierarchy upon which the DNS infrastructure could depend. Proponents contend this would simplify the validation process for those who have already deployed DNSSEC, while providing an incentive for possible broader deployment by others across the DNS domain space by removing one of the primary deterrents (the lack of a single trust anchor) to adoption.[17]

Support among the DNS community for implementation of DNSSEC at the root level has progressively grown over the years, as threats to the DNS have emerged. Several organizations have publicly indicated their support for signing the root zone.[18] Various Internet entities have undertaken a number of test-bed and pilot project initiatives to assess the technical feasibility and issues associated with signing of the root zone. Some notable examples include:

Internet Corporation for Assigned Names and Numbers (ICANN) DNSSEC testing demo (https://ns.iana.org/dnssec/status.html)

VeriSign DNSSEC Root testbed (https://webroot.verisignlabs.com/)

[5] *Id.*, at 6.

[6] *See Signposts*, *supra* note 1 at 158.

[7] *See e.g.*, Challenges, *supra* note 2, at 86-87. The Department recognizes that the ultimate success of DNSSEC would also require a widespread education campaign among end-users and DNSSEC awareness would have to be integrated into application and operating system software and development.

[8] To check which TLDs that have deployed DNSSEC, *see* University of Southern California Los Angeles, ''SecSpider: the DNSSEC Monitoring Project'' (UCLA SecSpider), http://secspider.cs.ucla.edu (last checked September 19, 2008) (each TLD zone can be looked up separately using this tool); Carolyn Duffy Marsan, Network World, ''Feds Tighten Security on .GOV'' (September 22, 2008), http://www.networkworld.com/news/2008/092208-government-web-security.html?page=1 (last checked September 25, 2008).

[9] Public Interest Registry, '' .ORG Becomes First Generic Top Level Domain to Start DNSSEC Implementation'' (July 21, 2008), http://pir.org/index.php?db=content/News&tbl=Press&id=9 (last checked September 24, 2008); Executive Office of the President, Office of Management and Budget, Memorandum for Chief Information Officers, Securing the Federal Government's Domain Name System Infrastructure (August 22, 2008), http://www.whitehouse.gov/omb/memoranda/fy2008/m08-23.pdf (last checked September 24, 2008).

[10] *See* UCLA SecSpider, *supra* note 8, (second level zones may also be looked up using this tool).

[11] R. Arends, *et al.*, Protocol Modifications for the DNS Security Extensions, Internet Engineering Task Force (IETF) Request for Comment (RFC) 4035 (March 2005)(RFC 4035), http://www.ietf.org/rfc/rfc4035.txt (last checked September 25, 2008) (This document defines the concept of a signed zone and lists requirements for a zone signature).

[12] As defined in RFC 4033, a ''Trust Anchor'' is ''a configured DNSKEY RR or RR hash of a DNSKEY RR. A validating security-aware resolver uses this public key or hash as a starting point for building the authentication chain to a signed DNS response.'' Further, ''presence of a trust anchor also implies that the resolver should expect the zone to which the trust anchor points to be signed.'' *See* RFC 4033, *supra* note 3.

[13] *See* RFC 4035, *supra* note 11.

[14] *See* Challenges, *supra* note 2 at 85-86.

[15] TARs allow a trusted third party to collect, authenticate, and manage the required keys on behalf of a group of DNSSEC users. For additional information on TARs, *see*, Sparta Inc., Shinkuro Inc., and National Institute of Science and Technology, ''Statement of Needed Internet Capability: Trust Anchor Repositories'' (June 9, 2008), http://www.dnssec-deployment.org/tar/tarpaper.pdf (last checked September 24, 2008). In April 2008, the Board of Directors of the Internet Corporation for Assigned Names and Numbers (ICANN) authorized the creation and maintenance of an Interim TAR to act as a registry of DNSSEC trust anchors for top level domains. *See*, Minutes of the Special Meeting of the ICANN Board of Directors (April 30, 2008), http://www.icann.org/en/minutes/minutes-30apr08.htm (last checked September 24, 2008).

[16] The potential risks and benefits associated with TARs and other alternatives to signing of the root are not the primary focus of this NOI and, accordingly, are addressed only briefly here. However, depending on the comments received in response to this NOI, the Department may consider these issues more fully at a later date.

[17] *See*, Samuel Weiler, Carnegie Mellon University, Information Networking Institute, ''Deploying DNSSEC Without a Signed Root'' (April 2004), http://www.watson.org/~weiler/INI 1999–19.pdf (last checked September 25, 2008) (This document discusses the importance of a signed root from a technical perspective and discusses alternatives if the root is not signed).

[18] The National Academies, *see Signposts*, *supra* note 1, at 158; The European Internet Regional Internet Registry (RIPE), *see* Letter from Axel Pawlik, Managing Director, RIPE Network Coordination Centre to Dr. Vinton Cerf and Paul Twomey, ICANN (June 12, 2007), http://www.ripe.net/ripe/wg/dns/icann-root-signing.pdf (last checked September 24, 2008); Nominet (the .uk registry), *see* Nominet, ''Signing the Root'' (October 2007), http://www.nominet.org.uk/digitalAssets/27762__Signing__the__Root.pdf (last checked September 24, 2008); Public Interest Registry (PIR), *see* Letter from Alexa A.S. Raad, President and CEO, Public Internet Registry to the Honorable Carlos M. Gutierrez, Secretary of Commerce, U.S. Department of Commerce (September 5, 2008).

EP.NET, LLC Root Server Testbed Network (http://www.rs.net/)

These test-beds were established to demonstrate the technical feasibility for signing the root zone on a day-to-day routine basis. However, as they have largely been developed to evaluate technical aspects of signing the root, these test-bed efforts have not addressed or considered certain policy and procedural issues regarding the management of a signed root zone. These policy and procedural issues, especially regarding key management for the root zone, must be resolved before deployment in the root zone to ensure transparency and trustworthiness to the Internet community.

While deployment of DNSSEC at the root has many benefits, it introduces new security requirements. In particular, the cryptographic keys used to protect the root zone must be protected from disclosure. If an unauthorized entity gains access to the keys, it could publish incorrect information in the DNS with DNSSEC extensions falsely indicating the DNS data's integrity and authenticity. This risk can be mitigated through a variety of procedural and technical mechanisms, many of which can be applied in concert. The Department welcomes comments regarding procedural and technical mechanisms available to address such security requirements.

DNSSEC Implementation Models. A DNSSEC signed root zone would represent one of most significant changes to the DNS infrastructure since it was created. Consistent with the *U.S. Principles on the Internet's Domain Name and Addressing System*, the Department is now undertaking a review of the various implementation models to enhance the security and stability of the Internet DNS.[19] The Department recognizes the potential benefits of a DNSSEC signed root and is actively examining various implementation models in coordination with the National Institute of Standards and Technology (NIST) as well as other U.S. Government stakeholders and experts. NIST has been at the forefront of DNSSEC research and deployment domestically.[20] The U.S. Government also recently announced the deployment of DNSSEC throughout the .gov domain.[21] The Department has also been consulting with other relevant stakeholders, including ICANN and VeriSign, Inc., with respect to DNSSEC deployment.[22]

As a fundamental consideration, it is essential that implementation of DNSSEC at the root further ensures the stability and reliability of the root zone management system. All of the DNSSEC root zone deployment models of which the Department is aware would incorporate the elements required for ''signing'' the root into the process flow for management of the authoritative root zone file. At present, the process flow (see diagram at http://www.ntia.doc.gov/DNS/CurrentProcessFlow.pdf) includes the following steps: (1) TLD operator submits change request to the Internet Assigned Numbers Authority (IANA) Functions Operator; (2) the IANA Functions Operator processes the request; (3) the IANA Functions Operator sends a request to the Administrator for verification/authorization; (4) the Administrator sends verification/authorization to the Root Zone Maintainer to make the change; (5) the Root Zone Maintainer edits and generates the new root zone file; and (6) the Root Zone Maintainer distributes the new root zone file to the 13 root server operators. Deployment of DNSSEC in the root zone would introduce new steps into this process flow, but would not necessarily require a change in the existing roles of the various participants in the process.

As a cryptographic key-based system, DNSSEC employs two types of public-private key pairs created for the zone; one is referred to as the Zone Signing Key (ZSK) and the other is referred to as the Key Signing Key (KSK).[23] The private components of these keys are kept secret and are used for signing purposes. The collection of KSK and ZSK public keys published for the root zone is referred to as the root keyset.

Specifically, signing of the root zone would involve three steps:

(1) The signing of the root zone file itself and the creation of the Zone Signing Key (ZSK), which would be performed by the *Root Zone Signer (RZS)*;

(2) The signing of the zone signing keyset and the creation of the Key Signing Key (KSK), which would be performed by the *Root Key Operator (RKO)*; and

(3) Publication of the public key information for propagation throughout the rest of the Internet.[24]

As with other changes to the root zone, the Administrator would be responsible for verifying/authorizing updates to the root keyset.

A number of possible models exist to implement these steps into the existing root zone file management system. Six possible process flow models are presented in Appendix A for consideration and comment; commenters are encouraged to also review the graphic representations of these process flows posted on NTIA's website at http://www.ntia.doc.gov/DNS/DNSSEC.html. The Department recognizes that the six process flow models discussed in the appendix may not represent all of the possibilities available and invites comments below on alternate models, as appropriate.

REQUEST FOR COMMENT:

The Department seeks comments on DNSSEC deployment and a signed root generally, as well as specific details, comments, and evaluations of the various process flow models proposed or other process flow models that may otherwise be technically feasible to implement DNSSEC at the root zone level. Please include an analysis of the risks, benefits, and impacts of each process flow on the DNS security and stability generally. This analysis should include whether there are security weaknesses or strengths with each process flow model, whether there are methods or suggestions that will increase security and efficiency, and/or whether any alternative process flow models exist that may be preferable to those described in the appendix.

Questions on DNSSEC Deployment Generally

- In terms of addressing cache poisoning and similar attacks on the DNS, are there alternatives to DNSSEC

[19] *See U.S. Principles on the Internet's Domain Name and Addressing System*, http://www.ntia.doc.gov/ntiahome/domainname/usdnsprinciples__06302005.htm (last checked September 24, 2008).

[20] National Institute of Standards and Technology (NIST), U.S. Department of Commerce, DNSSEC Project, http://www-x.antd.nist.gov/dnssec/ (last checked September 24, 2008).

[21] Executive Office of the President, Office of Management and Budget, Memorandum for Chief Information Officers, Securing the Federal Government's Domain Name System Infrastructure (August 22, 2008), http://www.whitehouse.gov/omb/memoranda/fy2008/m08-23.pdf (last checked September 24, 2008)(The U.S. Government is requiring deployment of DNSSEC at the TLD level in .gov by January 2009 and in all .gov sub-domains used by Federal agencies by December 2009).

[22] The Department's agreements with ICANN and VeriSign, Inc. provide the process through which changes are currently made to the authoritative root zone file.

[23] *See*, Ramaswamy Chandramouli and Scott Rose, NIST, ''Secure Domain Name System (DNS) Deployment Guide,'' NIST SP 800-81, at 9-3 - 9-5 (May 2006), http://csrc.nist.gov/publications/nistpubs/800–81/SP800–81.pdf (last checked September 24, 2008) (This document provides deployment guidelines for securing DNS at the enterprise level including use of keys and provides a general discussion of the structure of the DNS).

[24] *See generally*, *id.*, at Sections 8 and 9 (These document sections provide a general discussion of zone signing guidelines).

that should be considered prior to or in conjunction with consideration of signing the root?

- What are the advantages and/or disadvantages of DNSSEC relative to other possible security measures that may be available?
- What factors impede widespread deployment of DNSSEC?
- What additional steps are required to facilitate broader DNSSEC deployment and use? What end user education may be required to ensure that end users possess the ability to utilize and benefit from DNSSEC?

General Questions Concerning Signing of the Root Zone

- Should DNSSEC be implemented at the root zone level? Why or why not? What is a viable time frame for implementation at the root zone level?
- What are the risks and/or benefits of implementing DNSSEC at the root zone level?
- Is additional testing necessary to assure that deployment of DNSSEC at the root will not adversely impact the security and stability of the DNS? If so, what type of operational testing should be required, and under what conditions and parameters should such testing occur? What entities (*e.g.*, root server operators, registrars, registries, TLD operators, ISPs, end users) should be involved in such testing?
- How would implementation of DNSSEC at the root zone impact DNSSEC deployment throughout the DNS hierarchy?
- How would the different entities (*e.g.*, root operators, registrars, registries, registrants, ISPs, software vendors, end users) be affected by deployment of DNSSEC at the root level? Are these different entities prepared for DNSSEC at the root zone level and /or are each considering deployment in their respective zones?
- What are the estimated costs that various entities may incur to implement DNSSEC? In particular, what are the estimated costs for those entities that would be involved in deployment of DNSSEC at the root zone level?

Operational Questions Concerning Signing of the Root Zone

- The Department recognizes that the six process flow models discussed in the appendix may not represent all of the possibilities available. The Department invites comment on these process flow models as well as whether other process flow model(s) may exist that would implement deployment of DNSSEC at the root zone more efficiently or effectively.
- Of the six process flow models or others not presented, which provides the greatest benefits with the fewest risks for signing the root and why? Specifically, how should key management (public and private key sets) be distributed and why? What other factors related to key management (*e.g.*, key roll over, security, key signing) need to be considered and how best should they be approached?
- We invite comment with respect to what technical capabilities and facilities or other attributes are necessary to be a Root Key Operator.
- What specific security considerations for key handling need to be taken into account? What are the best practices, if any, for secure key handling?
- Should a multi-signature technique, as represented in the M of N approach discussed in the appendix, be utilized in implementation of DNSSEC at the root zone level? Why or why not? If so, would additional testing of the technique be required in advance of implementation?

Dated: October 3, 2008.

Meredith Attwell Baker,

Acting Assistant Secretary for Communications and Information Administration.

Appendix A: Six Possible Process Flow Models

The first three of the process flows described below assign the responsibilities of Root Zone Signer, Root Key Operator, and key publishing among the existing parties to the root zone file management process or to a new, as yet unspecified, third party without materially changing the other pre- existing roles and responsibilities. The fourth model represents a variation of previous models, while changing the current root zone management process flow. The fifth model is also a variation of previous models, while maintaining the current root zone management process flow. The sixth model describes a process flow in which more than one third party, as yet unspecified, are introduced as Root Key Operators, which can be applied to all the previous process flows.

Proposed Process Flow 1 (see diagram at http://www.ntia.doc.gov/DNS/DNSSECproposal1.pdf). In Proposed Process Flow 1, the current root zone file management process outlined previously would remain unchanged except that after the Root Zone Maintainer edits and generates the new root zone file, it would then generate the ZSK and send it to the Root Key Operator. The Root Key Operator would then generate the KSK, sign the root keyset, and transmit the keyset update request to the Administrator. After the Administrator verifies/authorizes the key update request, it would notify the Root Zone Maintainer (in this model serving as the Root Zone Signer), which would sign the root zone file and publish it to the root server operators. Concurrently, the Administrator would also notify the Root Key Operator that the key update request has been verified/authorized and the RKO would then publish the public key information.

In this process flow, the role of Root Zone Signer is assigned to the Root Zone Maintainer. The Root Key Operator responsibilities are assigned to none of the current participants in the root zone file management process. Rather, these duties are assigned to an unspecified third party. This approach involves little change to the current root zone file management process and its existing assignments of roles and responsibilities.

Proposed Process Flow 2 (see diagram at http://www.ntia.doc.gov/DNS/DNSSECproposal2.pdf). Proposed Process Flow 2 is similar to Proposed Process Flow 1 except that in this model, the Root Key Operator is responsible for generating both the Zone Signing Key as well as the Key Signing Key. After creating the ZSK, the Root Key Operator transmits it to the Root Zone Maintainer/Signer, which maintains the ZSK.

Proposed Process Flow 3 (see diagram at http://www.ntia.doc.gov/DNS/DNSSECproposal3.pdf). This model also corresponds closely to Proposed Process Flow 1. However, in this model, the Root Key Operator, both generates the ZSK and signs the root zone file. Thus, after the Root Zone Maintainer generates the root zone file, it would then transmit the file to the Root Key Operator. In turn, the Root Key Operator, after generating the ZSK and the KSK, signing the root keyset, and obtaining verification/authorization from the Administrator, would sign the root zone file and return it to the Root Zone Maintainer for delivery. In this scenario, the Administrator would communicate only with the Root Key Operator with respect to the verification/authorization of the key update request.

Proposed Process Flow 4 (see diagram at http://www.ntia.doc.gov/DNS/DNSSECproposal4.pdf). This model describes a process flow in which the existing roles and responsibilities with respect to the management of the authoritative root zone file are significantly altered.[25] Specifically, under this proposed process flow, existing responsibilities for editing and generating the root zone file that now reside with the Root Zone Maintainer would be transferred to the IANA Functions Operator. In addition, the IANA Functions Operator would also be assigned the responsibilities of Root Zone Signer. The Root Zone Maintainer would continue to be responsible for distributing the now-signed root zone file to the 13 root server operators.

Thus, under this model the process would operate as follows: After receiving a change request from a TLD operator, the IANA Functions Operator would process the request and send a request to the

[25] Under the IANA functions contract with the Department, ICANN submitted a proposal substantially similar to Process Flow 4 for the Department of Commerce's consideration on September 2, 2008. That proposal is pending before the Department. This proposal is available at http://www.ntia.doc.gov/DNS/ICANNDNSSECProposal.pdf.

Administrator for verification/authorization to make the change. Upon receiving verification/authorization, the IANA Functions Operator would then edit and generate a new root zone file. The Root Key Operator function would be physically collocated with the IANA Functions Operator, responsible for generation of the KSK, signing the root keyset, and publishing the public key information. The IANA Functions Operator would also generate the ZSK and sign the root zone file. After signing the root zone file, the IANA Functions Operator would send the signed root zone file to the Root Zone Distributor (formally Root Zone Maintainer), which, in turn, would distribute it to the 13 root server operators. Under this process flow, the Administrator would perform the verification/authorization functions as in the other models.

Proposed Process Flow 5 (see diagram at http://www.ntia.doc.gov/DNS/DNSSECproposal5.pdf). This model maintains the existing roles and responsibilities with respect to the management of the authoritative root zone file.[26] That is, the existing responsibilities for editing and generating the root zone file that now reside with the Root Zone Maintainer would remain the same with the additional/new responsibility of Root Zone Signer and collocating the Root Key Operator function. The Root Zone Maintainer would continue to be responsible for distributing the now-signed root zone file to the 13 root server operators.

Thus, under this model the process would operate as follows: After receiving a change request from a TLD operator, the IANA Functions Operator would process and send a request to the Administrator for verification/authorization to make the change. Upon receiving verification/authorization, the Root Zone Maintainer would then edit and generate a new root zone file. The Root Key Operator responsibility would be physically collocated with the Root Zone Maintainer, responsible for generation of the KSK, signing the root keyset, and publishing the public key information. The Root Zone Maintainer would also generate the ZSK and sign the root zone file. After signing the root zone file, the Root Zone Maintainer would distribute it to the 13 root server operators. Under this process flow, the Administrator would perform the verification/authorization functions as in the other models.

Proposed Process Flow 6 (see diagram at http://www.ntia.doc.gov/DNS/DNSSECproposal6.pdf). The proposed process flow models one through three illustrate the important role played by the Root Key Operator. As presented, they depict the RKO responsibilities as being discharged by a single entity. In process flows four and five, the RKO responsibilities are collocated with either the IANA Functions Operator or the Root Zone Maintainer. However, cryptographic mechanisms exist that theoretically would permit two or more entities to participate in the RKO procedures, known as multi-signature technique, no matter where the RKO responsibilities are located.[27] Such a shared key framework is commonly referred to as an ''M of N'' approach, in which ''M'' is the minimum number of those entities that must participate in order to generate and use the key in question, and ''N'' represents the number of entities that share control of the key. In an M of N approach, only a predetermined subset of the key shares is required to generate a signature. For example, a three (3) of five (5) scheme would include five parties (N) with distinct key shares, but any three (M) of the five parties are required to generate a valid signature.[28]

The M of N approach could theoretically be applied to the KSK, the ZSK, or both. However, increasing the number of participants under this approach increases the complexities of the key management process. Because the ZSK would be used much more frequently than the KSK, Process Flow 6 applies the M of N approach only to management of the KSK. It should be noted that this cryptographic approach could be applied to any of the previous process flow models.

Process Flow 6 depicts the multi-signature technique as applied to Process Flow 1. The N entities would participate in the generation of the KSK key pair, and each would retain a share of the private key. Generating a signature with the KSK, such as signing a new ZSK, would require participation of M key shares.

Process Flow 6 does not propose specific values for either M or N; however, these parameters would need to be resolved prior to implementation of such a framework. This would entail deciding, among other things, (a) how many total RKOs (N) would be technically feasible; (b) what subset of these (M) would be reasonable or appropriate to enable reconstitution of the key; and (c) what other attributes would be necessary from a technical and policy standpoint to carry out this responsibility. The Department invites comments regarding this technique and its application at the root zone level.

[FR Doc. E8–23974 Filed 10–8–08; 8:45 am]

BILLING CODE 3510–60–S

[26] Under the Cooperative Agreement with the Department, VeriSign submitted a proposal substantially similar to Process Flow 5 for the Department of Commerce's consideration on September 23, 2008. That proposal is pending before the Department. This proposal is available at http://www.ntia.doc.gov/DNS/VeriSignDNSSECProposal.pdf.

[27] *See* Tal Rabin, IBM T. J. Watson Research Center, ''A Simplified Approach to Threshold and Proactive RSA'' (1998)(Rabin), http://www.research.ibm.com/security/prsa.ps (last checked September 24, 2008); Adi Shamir, ''How to Share a Secret,'' Communications of the ACM, Volume 22, Issue 11, 612-13 (R. Rivest, eds., Nov. 1979)(discussion of a mathematical model that facilitates dividing a set of data in a certain number pieces that allows the data set to be easily reconstructed); T. Keisler and L. Harn, ''RSA Blocking and Multisignature Schemes with No Bit Expansion,'' Electronic Letters, Volume 26, Issue 18, 1490-91 (Aug. 1990)(describes one example of a multi-signature technique).

[28] *See* Rabin, *supra* note 27; for further information on this technique *see generally*, Elaine Barker, William Barker, William Burr, William Polk, and Miles Smid, NIST, ''Recommendation for Key Management - Part 1: General (revised)'' NIST Special Publication 800–57 Part 1 (May 2006), http:/ /csrc.nist.gov/publications/nistpubs/ 800–57/SP800–57-Part1.pdf (last checked September 24, 2008) (this refers to this class of techniques as ''split knowledge procedures'').

DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

[Docket No. PTO–C–2008–0040]

Performance Review Board (PRB)

AGENCY: United States Patent and Trademark Office.

ACTION: Notice

SUMMARY: In conformance with the Civil Service Reform Act of 1978, 5 U.S.C. 4314(c)(4), the United States Patent and Trademark Office announces the appointment of persons to serve as members of its Performance Review Board.

ADDRESSES: Director, Human Capital Management, Office of Human Resources, United States Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313–1450.

FOR FURTHER INFORMATION CONTACT: Karen Karlinchak at (571) 272–6200.

SUPPLEMENTARY INFORMATION: The membership of the United States Patent and Trademark Office Performance Review Board is as follows:

Margaret J. A. Peterlin, Chair, Deputy Under Secretary of Commerce for Intellectual Property and Deputy Director of the United States Patent and Trademark Office.

Stephen S. Smith, Vice Chair, Chief Administrative Officer, United States Patent and Trademark Office.

John J. Doll, Commissioner for Patents, United States Patent and Trademark Office.

Lynne G. Beresford, Commissioner for Trademarks, United States Patent and Trademark Office.

Wendy R. Garber, Acting Chief Information Officer, United States Patent and Trademark Office.

James A. Toupin, General Counsel, United States Patent and Trademark Office.

Lois E. Boland, Director, Office of Intellectual Property Policy and Enforcement, United States Patent and Trademark Office.

Barry K. Hudson, Chief Financial Officer, United States Patent and Trademark Office.

Jefferson D. Taylor, Director, Office of Governmental Affairs, United States Patent and Trademark Office.

Deborah S. Cohn, Deputy Commissioner for Trademark