EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

August 22, 2008

M-08-23

MEMORANDUM FOR CHIEF INFORMATION OFFICERS

FROM: Karen Evans
Administrator, Office of E-Government and Information Technology

SUBJECT: Securing the Federal Government's Domain Name System Infrastructure
(Submission of Draft Agency Plans Due by September 5, 2008)

The efficient and effective use of our networks is important to promote a more citizen centered and results oriented government. The Government's reliance on the Internet to disseminate and provide access to information has increased significantly over the years, as have the risks associated with potential unauthorized use, compromise, and loss of the .gov domain space.

Almost every instance of network communication begins with a request to the Domain Name System (DNS) to resolve a human readable name for a network resource (e.g., www.usa.gov) into the technical information (e.g., Internet Protocol address) necessary to actually access the remote resource. This memorandum describes existing and new policies for deploying Domain Name System Security (DNSSEC) to all Federal information systems by December 2009. DNSSEC provides cryptographic protections to DNS communication exchanges, thereby removing threats of DNS-based attacks and improving the overall integrity and authenticity of information processed over the Internet.

Existing Policy
In December 2006, the National Institute of Standards and Technology's (NIST) Special Publication 800-53r1 "Recommended Security Controls for Federal Information Systems" prescribed initial DNSSEC deployment steps necessary for FISMA high and moderate impact information systems.

New Policy
This memorandum addresses two important issues in following through with the existing policy and expanding its scope to address all USG information systems.

A. The Federal Government will deploy DNSSEC to the top level .gov domain by January 2009. The top level .gov domain includes the registrar, registry, and DNS server operations. This policy requires that the top level .gov domain will be DNSSEC signed and processes to enable secure delegated sub-domains will be developed. Signing the top level .gov domain is a critical procedure necessary for broad deployment of DNSSEC, increases the utility of DNSSEC, and simplifies lower level deployment by agencies.

B. Your agency must now develop a plan of action and milestones for the deployment of DNSSEC to all applicable information systems. Appropriate DNSSEC capabilities must

be deployed and operational by December 2009. The plan should follow recommendations in NIST Special Publication 800-81 "Secure Domain Name System (DNS) Deployment Guide," and address the particular requirements described in NIST Special Publication 800-53r1 "Recommended Security Controls for Federal Information Systems."[1]

The plan should report your agency's current level of compliance with the current DNSSEC requirements of NIST Special Publication 800-53r1, and document a plan of action and milestones that assume the scope of the requirement to operate DNSSEC signed zones (SC-20) will be expanded to cover all FISMA information systems (including low impact systems[2]) in revision 3 of NIST Special Publication 800-53. The plan should ensure that all Agency .gov domains are DNSSEC signed by December 2009.

Your agency's draft plan of action and milestones should follow the general outline provided below and be sent to OMB at fisma@omb.eop.gov by September 5, 2008. The draft plans will be reviewed and feedback will be provided. Mutually-agreed upon final plans will be in place by October 24, 2008. Going forward, agency progress to deploy DNSSEC will be tracked and evaluated through annual Federal Information Security Management Act (FISMA) reporting.

Additional Resources

The following resources provide additional technical information and guidance to support your agency's DNSSEC deployment.

- The USG DNSSEC deployment email list: usg-forum@dnssec-deployment.org
- The DNSSEC Deployment Initiative: http://www.dnssec-deployment.org/
- The NIST DNSSEC project: http://www-x.antd.nist.gov/dnssec/
- The Secure Naming Infrastructure Pilot (SNIP): http://www.dnsops.gov/
- The FISMA Implementation Project: http://csrc.nist.gov/groups/SMA/fisma/index.html

DNSSEC Deployment Plan Outline

Section 1 - Enumerate .gov Domains. Enumerate the second level domains beneath .gov operated by your agency (or on behalf of your agency). Only the second level sub-domains need to be listed.

[1] Specific DNSSEC controls are described in SC-8, SC-20, SC-21, and SC-22 of Special Publication 800-53r1. To effectively deploy DNSSEC, your agency should follow recommendations in NIST Special Publication 800-81 "Secure Domain Name System (DNS) Deployment Guide." Procedures for assessing DNSSEC controls are described in NIST's Special Publication 800-53A "Guide for Assessing the Security Controls in Federal Information Systems."

[2] For more information about categorizing information systems by impact level, see Federal Information Processing Standard Publication 199 "Standards for Security Categorization of Federal Information and Information Systems."

Section 2 - Identify Sources of DNS Services. For each domain listed above, describe if your DNS administration and server operation are provided in house, outsourced to a commercial provider (e.g., vendor), or delivered by other means (e.g., provided by another agency).

Section 3 - Describe DNS Server Infrastructure. Document the provider, vendor, or source of DNS server implementations within your agency (e.g., BIND, NSD, Microsoft Advanced Directory, etc.). Include in your estimate the number of such servers per source.

Section 4 - Identify and Address Barriers. Document any perceived technical, contractual or operational barriers impeding deployment of DNSSEC, and milestones for addressing each.

Section 5 – Train and Pilot. Review the activities of the USG Secure Naming Infrastructure Pilot at www.dnsops.gov and plan for your agency will participate in this pilot test bed, as well as associated training workshops.

Section 6 – Plan of Action and Milestones. Document your Agency's plan of action and milestones to fully implement the policies described in this memo. In particular this plan should detail all key activities (e.g., acquisition if necessary, training, test, deployment, operations plans with priority given to citizen services and E-government domains especially those that collect any personally identifiable information) and milestones necessary to achieve the goal of fully operating DNSSEC signed .gov sub-domains by December 2009.