From: Dworkin, Morris J. (Fed)
To: Foti, James (Fed)
Subject: Re: Stateful Hash-Based Signatures (HBS): Request for Public Comments
Date: Monday, February 4, 2019 11:15:08 AM

Thanks, looks good.

MD

> On Feb 4, 2019, at 9:46 AM, Foti, James (Fed) <james.foti@nist.gov> wrote:
>
> Hi Morrie-
> Nikki Keller just sent out the GovDelivery notice, too. See below.
> Jim
>
> ---
>
> **From:** NIST Computer Security Division <csrc.nist@service.govdelivery.com>
> **Sent:** Monday, February 4, 2019 9:44 AM
> **To:** Foti, James (Fed) <james.foti@nist.gov>
> **Subject:** Stateful Hash-Based Signatures (HBS): Request for Public Comments
>
> In June 2018, NIST requested public feedback on plans to standardize either one or both of the LMS and XMSS stateful hash-based signature (HBS) schemes, as developed by the Internet Engineering Task Force (IETF). The general consensus was that both stateful HBS schemes should be standardized by NIST.
>
> Therefore, **NIST is now announcing its intent to standardize on both schemes: LMS and XMSS**. Because stateful hash-based signatures are prone to misuse, NIST seeks input on the following questions:
>
> - How should NIST's specification characterize the applications for which such signatures are, or are not, appropriate?
> - What requirements and guidance for protecting against misuse should NIST include beyond what is provided in the IETF specifications?
>
> **Comments may be sent to** pqc-comments@nist.gov with the subject line "stateful HBS comments" **by April 1, 2019.** See the Request for Public Comments link below for additional details and background information.
>
> Request for Public Comments:
> https://csrc.nist.gov/news/2019/stateful-hbs-request-for-public-comments
>
> Stateful Hash-Based Signatures Project:
> https://csrc.nist.gov/projects/stateful-hash-based-signatures
>
> ---
>
> NIST Applied Cybersecurity Division
> NIST Computer Security Division
> webmaster-csrc@nist.gov (Attn: Stateful Hash-Based Signature Team)
> Notification Sent By: N. Keller, NIST Computer Security Division
>
> ---

Questions? Contact Us

STAY CONNECTED:

SUBSCRIBER SERVICES:

Manage Preferences | Unsubscribe | Help

If you have questions or problems with the subscription service, please contact subscriberhelp.govdelivery.com. Technical questions? Contact inquiries@nist.gov. (301) 975-NIST (6478).

This service is provided to you at no charge by National Institute of Standards and Technology (NIST). 100 Bureau Drive, Stop 1070 · Gaithersburg, MD 20899 · 301-975-6478

GovDelivery logo