Comments Received in Response to:

Request for Comments on Draft Revision of the Applicability Clause of FIPS 180-4, Secure Hash Standard

From: Alexey Bagaev <bagalex@msn.com>
Sent: Tuesday, August 26, 2014 12:38 PM
To: internal-hash
Subject:Comment on draft revision to the Applicability Clause of FIPS 180

For last day for comments regarding secure hash functions I strongly recommend to exclude SHA-1 hash function from FIPS 180-4 compliant hash functions due to highly untrusted security algorithm. I know, that this algorithm is integrated in 96% of currently available commercial and over non-government solutions. But will you accept it, if all cryptographic communication solutions based on this technology can be easily (in a millisecond) altered by unknown ‘third party’? - I DON’T.

Thank you for your time.

NIST RESPONSE: The comment does not directly apply to the Revised Applicability Clause of FIPS 180-4, which simply acknowledges that FIPS 202 specifies valid options for secure hash functions. Moreover, NIST has already developed and implemented an appropriate policy for the use of SHA-1, based on the latest security information, as described in NIST Special Publication 800-131A.