From: Barker, Elaine B. (Fed)
To: Foti, James (Fed)
Subject: Re: Announcement text for your two pubs
Date: Thursday, February 14, 2019 1:01:51 PM
Attachments: sp800-131 draft v2.17.docx

Here's version 17 with some editorial fixes and accepting the markup. We still need to fix the references to FIPS 140 and SP 800-56B.

Elaine

From: "Foti, James (Fed)" <james.foti@nist.gov>
Date: Thursday, February 14, 2019 at 8:57 AM
To: "Elaine. Gov" <elaine.barker@nist.gov>
Subject: RE: Announcement text for your two pubs

Actually, could you please send me the latest version of 800-131A Rev 2? (I see v2.16 from 12/19/18 in NIKE.) Thanks for already sending me 800-56B Rev. 2.

Jim

From: Barker, Elaine B. (Fed)
Sent: Thursday, February 14, 2019 8:27 AM
To: Foti, James (Fed) <james.foti@nist.gov>
Subject: Re: Announcement text for your two pubs

Announcement for SP 800-131A, Rev 2:

NIST announces the publication of SP 800-131A, Revision 2, *Transitioning the Use of Cryptographic Algorithms and Key Lengths*. This Recommendation provides guidance for transitions to the use of stronger cryptographic keys and more robust algorithms by federal agencies when protecting sensitive, but unclassified information. These transitions are meant to address the challenges posed by new cryptanalysis, the increasing power of classical computing technology, and the potential emergence of quantum computers. This revision includes a strategy and schedule for retiring the use of the Triple Data Encryption Algorithm (TDEA) specified in SP 800-67, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*.

Announcement for SP 800-56B:

NIST announces the publication of SP 800-56B, Revision 2, *Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography*. This Recommendation specifies key-transport and key-agreement schemes using the RSA cryptographic algorithm. This revision 1) approves additional key sizes for key establishment, 2) removes provisions for using the Triple Data Encryption Algorithm (TDEA) specified in SP 800-67, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, and 3) removes the KTS-KEM-KWS key-transport scheme that was

included in previous versions of this Recommendation. In addition, the key derivation methods required for the key-agreement schemes have been moved to SP 800-56C, *Recommendation for Key-Derivation Methods in Key-Establishment Schemes*.

From: "Foti, James (Fed)" <james.foti@nist.gov>
Date: Wednesday, February 13, 2019 at 3:28 PM
To: "Elaine. Gov" <elaine.barker@nist.gov>
Subject: Announcement text for your two pubs

Hi Elaine-

If possible, could you please send me some draft announcement text for both 800-131A Rev. 2 and 800-56B Rev. 2? I'm on vacation all next week and would like to sent it to Isabel Van Wyk before I leave, so that she can work on writing the CSRC Updates and GovDelivery notices while I'm gone.

But, if you can't get them to me just yet, that's ok. Just trying to line things up while I can, and while she has some availability.

Thanks,
Jim

Jim Foti | IT Security Specialist | Computer Security Division | csrc.nist.gov
P:301.975.8018 | jfoti@nist.gov
NIST | 100 Bureau Drive, Stop 8930 | Bldg. 222, Room B349 | Gaithersburg, MD 20899-8930