This document is scheduled to be published in the
Federal Register on 04/10/2012 and available online at
http://federalregister.gov/a/2012-08573, and on **FDsys.gov**

Billing Code 3510-13

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

Docket No.: [120224144-2069-01]

Announcing DRAFT Revisions to Federal Information Processing Standard (FIPS) 186-3, Digital Signature Standard (DSS), and Request for Comments.

AGENCY: National Institute of Standards and Technology, Commerce.

ACTION: Notice and Request for Comments.

SUMMARY: The National Institute of Standards and Technology (NIST) requests comments on revisions to Federal Information Processing Standard (FIPS) 186-3, Digital Signature Standard, which was approved in January 2009. The proposed revisions are available at http://csrc.nist.gov/publications/PubsDrafts.html.

DATES: Comments must be received on or before [INSERT DATE 45 DAYS AFTER PUBLICATION OF THIS NOTICE].

ADDRESSES: Written comments may be sent to: Chief, Computer Security Division, Information Technology Laboratory, Attention: Draft Change Notice FIPS 186-3, 100 Bureau Drive, Mail Stop 8930, National Institute of Standards and

Technology, Gaithersburg, MD 20899-8930. Electronic comments may be sent to: fips_186-3_change_notice@nist.gov, with “186-3 Change Notice” in the subject line.

FOR FURTHER INFORMATION CONTACT: Elaine Barker, Computer Security Division, National Institute of Standards and Technology, Gaithersburg, MD 20899-8930, phone: 301-975-2911, email elaine.barker@nist.gov.

SUPPLEMENTARY INFORMATION: FIPS 186, first published in 1994, specified a digital signature algorithm (DSA) to generate and verify digital signatures. Later revisions (FIPS 186-1, FIPS 186-2, and FIPS 186-3, adopted in 1998, 1999 and 2009, respectively) adopted two additional algorithms: the Elliptic Curve Digital Signature Algorithm (ECDSA) and the RSA digital signature algorithm.

NIST is seeking public comment on proposed revisions to FIPS 186-3. This proposed revision:

- Clarifies terms used within the FIPS;
- Allows the use of any random bit/number generator that is approved for use in FIPS-140-validated modules;
- Reduces restrictions on the retention and use of prime number generation seeds for generating RSA key pairs;
- Corrects statements in FIPS 186-3 regarding the generation of the integer *k*, which is used as a secret number in the generation of DSA and ECDSA digital signatures;

- Corrects a typographical error in the processing steps of secret number generation for ECDSA;
- Corrects the wording of the criteria for generating RSA key pairs; and
- Aligns the specification for the use of a salt with RSASSA-PSS digital signatures scheme with Public Key Cryptography Standard (PKCS) #1.

AUTHORITY: In accordance with the Information Technology Management Reform Act of 1996 (Public Law 104-106) and the Federal Information Security Management Act of 2002 (FISMA) (Public Law 107-347), the Secretary of Commerce is authorized to approve Federal Information Processing Standards (FIPS). NIST activities to develop computer security standards to protect Federal sensitive (unclassified) information systems are undertaken pursuant to specific responsibilities assigned to NIST by section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3), as amended by section 303 of FISMA.

E.O. 12866: This notice has been determined not to be significant for the purposes of E.O. 12866.

Dated: March 30, 2012

Willie E. May
<u>Associate Director for Laboratory Programs</u>

[FR Doc. 2012-8573 Filed 04/09/2012 at 8:45 am; Publication Date: 04/10/2012]