Cash Deposit Rates Pursuant to Remand Redetermination.''

Dated: October 8, 2015.

Paul Piquado,

Assistant Secretary for Enforcement and Compliance.

Appendix: Revised Antidumping Duty Cash Deposit Rates Pursuant To Remand Redetermination

Exporter	Producer	Revised AD cash deposit rate (%)
BEIJING SAI LIN KE HARDWARE CO., LTD	XUZHOU GUANG HUAN STEEL TUBE PRODUCTS CO., LTD.	69.2
BENXI NORTHERN PIPES CO., LTD	BENXI NORTHERN PIPES CO., LTD	69.2
DALIAN BROLLO STEEL TUBES LTD	DALIAN BROLLO STEEL TUBES LTD	69.2
GUANGDONG WALSALL STEEL PIPE INDUSTRIAL CO. LTD.	GUANGDONG WALSALL STEEL PIPE INDUSTRIAL CO. LTD.	69.2
HENGSHUI JINGHUA STEEL PIPE CO., LTD	HENGSHUI JINGHUA STEEL PIPE CO., LTD	69.2
HULUDAO STEEL PIPE INDUSTRIAL CO	HULUDAO STEEL PIPE INDUSTRIAL CO	69.2
JIANGSU GUOQIANG ZINC-PLATING INDUSTRIAL CO., LTD.	JIANGSU GUOQIANG ZINC–PLATING INDUSTRIAL CO., LTD.	69.2
JIANGYIN JIANYE METAL PRODUCTS CO., LTD	JIANGYIN JIANYE METAL PRODUCTS CO., LTD	69.2
KUNSHAN HONGYUAN MACHINERY MANUFACTURE CO., LTD.	KUNSHAN HONGYUAN MACHINERY MANUFACTURE CO., LTD.	69.2
KUNSHAN LETS WIN STEEL MACHINERY CO., LTD	KUNSHAN LETS WIN STEEL MACHINERY CO., LTD	69.2
QINGDAO XIANGXING STEEL PIPE CO., LTD	QINGDAO XIANGXING STEEL PIPE CO., LTD	69.2
QINGDAO YONGJIE IMPORT & EXPORT CO., LTD	SHANDONG XINYUANGROUP CO., LTD	69.2
RIZHAO XINGYE IMPORT & EXPORT CO., LTD	SHANDONG XINYUAN GROUP CO., LTD	69.2
SHANGHAI METALS & MINERALS IMPORT & EXPORT CORP.	BENXI NORTHERN PIPES CO., LTD	69.2
SHENYANG BOYU M/E CO., LTD	BAZHOU DONG SHENG HOT-DIPPED GALVANIZED STEEL PIPE CO., LTD.	69.2
SHIJIAZHUANG ZHONGQING IMP & EXP CO., LTD	BAZHOU ZHUOFA STEEL PIPE CO. LTD	69.2
TIANJIN BAOLAI INT'L TRADE CO., LTD	TIANJIN JINGHAI COUNTY BAOLAI BUSINESS AND INDUSTRY CO. LTD.	69.2
TIANJIN NO. 1 STEEL ROLLED CO., LTD	TIANJIN HEXING STEEL CO., LTD	69.2
TIANJIN NO. 1 STEEL ROLLED CO., LTD	TIANJIN RUITONG STEEL CO., LTD	69.2
TIANJIN NO. 1 STEEL ROLLED CO., LTD	TIANJIN YAYI INDUSTRIAL CO	69.2
TIANJIN XINGYUDA IMPORT & EXPORT CO., LTD	TANGSHAN FENGNAN DISTRICT XINLIDA STEEL PIPE CO., LTD.	69.2
TIANJIN XINGYUDA IMPORT & EXPORT CO., LTD	TIANJIN LIFENGYUANDA STEEL GROUP	69.2
TIANJIN XINGYUDA IMPORT & EXPORT CO., LTD	TIANJIN LITUO STEEL PRODUCTS CO	69.2
TIANJIN XINGYUDA IMPORT & EXPORT CO., LTD	TIANJIN XINGYUNDA STEEL PIPE CO	69.2
WAH CIT ENTERPRISE	GUANGDONG WALSALL STEEL PIPE INDUSTRIAL CO. LTD.	69.2
WAI MING (TIANJIN) INT'L TRADING CO., LTD	BAZHOU DONG SHENG HOT-DIPPED GALVANIZED STEEL PIPE CO., LTD.	69.2
WEIFANG EAST STEEL PIPE CO., LTD	WEIFANG EAST STEEL PIPE CO., LTD	69.2
WUXI ERIC STEEL PIPE CO., LTD	WUXI ERIC STEEL PIPE CO., LTD	69.2
WUXI FASTUBE INDUSTRY CO., LTD	WUXI FASTUBE INDUSTRY CO., LTD	69.2
ZHANGJIAGANG ZHONGYUAN PIPE-MAKING CO., LTD	ZHANGJIAGANG ZHONGYUAN PIPE-MAKING CO., LTD	69.2
PRC-WIDE ENTITY		85.55

[FR Doc. 2015–26601 Filed 10–19–15; 8:45 am]

BILLING CODE 3510–DS–P

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No. 150923882–5882–01]

Federal Information Processing Standard (FIPS) 186–4, Digital Signature Standard; Request for Comments on the NIST-Recommended Elliptic Curves

AGENCY: National Institute of Standards and Technology (NIST), Commerce.

ACTION: Notice and request for comments.

SUMMARY: The National Institute of Standards and Technology (NIST) requests comments on Federal Information Processing Standard (FIPS) 186–4, Digital Signature Standard, which has been in effect since July 2013. FIPS 186–4 specifies three techniques for the generation and verification of digital signatures that can be used for the protection of data: the Rivest-Shamir-Adleman Algorithm (RSA), the Digital Signature Algorithm (DSA), and the Elliptic Curve Digital Signature Algorithm (ECDSA), along with a set of elliptic curves recommended for government use. NIST

is primarily seeking comments on the recommended elliptic curves specified in Appendix D of the FIPS, but comments on other areas of the FIPS will also be considered. FIPS 186–4 is available at *http://dx.doi.org/10.6028/NIST.FIPS.186–4.*

DATES: Comments on FIPS 186–4 must be received on or before December 4, 2015.

ADDRESSES: Comments on FIPS 186–4 may be sent electronically to *FIPS186-comments@nist.gov* with ''Comment on FIPS 186'' in the subject line. Written comments may also be submitted by mail to Information Technology Laboratory, ATTN: FIPS 186–4 Comments, National Institute of Standards and Technology, 100 Bureau Drive, Mail Stop 8930, Gaithersburg, MD 20899–8930.

The current FIPS 186–4 can be found at *http://dx.doi.org/10.6028/NIST.FIPS.186-4.*

Comments received in response to this notice will be published electronically at *http://csrc.nist.gov/,* so commenters should not include information they do not wish to be posted (*e.g.,* personal or confidential business information).

FOR FURTHER INFORMATION CONTACT: Dr. Lily Chen, Computer Security Division, National Institute of Standards and Technology, 100 Bureau Drive, Mail Stop 8930, Gaithersburg, MD 20899–8930, email: *Lily.Chen@nist.gov,* phone: (301) 975–6974.

SUPPLEMENTARY INFORMATION: FIPS 186 was initially developed by NIST in collaboration with the National Security Agency (NSA), using the Digital Signature Algorithm (DSA). Later versions of the standard approved the use of the Elliptic Curve Digital Signature Algorithm (ECDSA) and the Rivest-Shamir-Adleman (RSA) algorithm. American Standards Committee (ASC) X9 developed standards specifying the use of both ECDSA and RSA, including methods for generating key pairs, which were used as the basis for the later versions of FIPS 186.

The ECDSA was included by reference in FIPS 186–2, the second revision to FIPS 186, which was announced in the **Federal Register** (65 FR 7507) and became effective on February 15, 2000. The FIPS was revised in order to align the standard with new digital signature algorithms included in ASC X9 standards. To facilitate testing and interoperability, NIST needed to specify elliptic curves that could be used with ECDSA. Working in collaboration with the NSA, NIST included three sets of recommended elliptic curves in FIPS 186–2 that were generated using the algorithms in the ANS X9.62 standard and Institute of Electrical and Electronics Engineers (IEEE) P1363 standards. The provenance of the curves was not fully specified, leading to recent public concerns that there could be an unknown weakness in these curves. NIST is not aware of any vulnerability in these curves when they are implemented correctly and used as described in NIST standards and guidelines.

In the fifteen years since FIPS 186–2 was published, elliptic curve cryptography (ECC) has seen slow adoption outside certain communities. Past discussions on this topic have cited several possible reasons for this, including interoperability issues, performance characteristics, and concerns over intellectual property.

In addition, advances in the understanding of elliptic curves within the cryptographic community have led to the development of new elliptic curves and algorithms whose designers claim to offer better performance and are easier to implement in a secure manner. Some of these curves are under consideration in voluntary, consensus-based Standards Developing Organizations.

In 2014, NIST's primary external advisory board, the Visiting Committee on Advanced Technology (VCAT), conducted a review of NIST's cryptographic standards program. As part of their review, the VCAT recommended that NIST ''generate a new set of elliptic curves for use with ECDSA in FIPS 186.''

In June 2015, NIST hosted the technical workshop on Elliptic Curve Cryptography Standards to discuss possible approaches to promote the adoption of secure, interoperable and efficient elliptic curve mechanisms. Workshop participants expressed significant interest in the development, standardization and adoption of new elliptic curves. As a result of this input, NIST is considering the addition of new elliptic curves to the current set of recommended curves in FIPS 186–4. Comments received in response to this solicitation will be used to identify the needs, processes and goals for possible future standards activities.

Request for Comments

NIST requests comments on the following questions regarding the elliptic curves recommended in FIPS 186–4, but comments on other areas of the FIPS will also be considered. The responses to this solicitation will be used to plan possible improvements to the FIPS, including the set of algorithms and elliptic curves specified in the FIPS.

1. Digital Signature Schemes

a. Do the digital signature schemes and key sizes specified in FIPS 186–4 satisfy the security requirements of applications used by industry?

b. Are there other digital signature schemes that should be considered for inclusion in a future revision to FIPS 186? What are the advantages of these schemes over the existing schemes in FIPS 186?

2. Security of Elliptic Curves

a. Do the NIST-recommended curves satisfy the security requirements of applications used by industry?

b. Are there any attacks of cryptographic significance on Elliptic Curve Cryptography that apply to the NIST-recommended curves or other widely used curves?

3. Elliptic Curve Specifications and Criteria

a. Is there a need for new elliptic curves to be considered for standardization?

b. If there is a need, what criteria should NIST use to evaluate any curves to be considered for inclusion?

c. Do you anticipate a need to create, standardize or approve new elliptic curves on an ongoing basis?

4. Adoption

a. Which of the approved digital signature schemes and NIST-recommended curves have been used in practice?

b. Which elliptic curves are accepted for use in international markets?

5. Interoperability

a. If new curves were to be standardized, what would be the impact of changing existing implementations to allow for the new curves?

b. What is the impact of having several standardized curves on interoperability?

c. What are the advantages or disadvantages of allowing users or applications to generate their own elliptic curves, instead of using standardized curves?

6. Performance

a. Do the performance characteristics of existing implementations of the digital signatures schemes approved in FIPS 186–4 meet the requirements of applications used by industry?

7. Intellectual Property

a. What are the desired intellectual property requirements for any new

curves or schemes that could potentially be included in the Standard?

b. What impact has intellectual property concerns had on the adoption of elliptic curve cryptography?

Authority: In accordance with the Information Technology Management Reform Act of 1996 (Pub. L. 104–106) and the Federal Information Security Management Act of 2002 (FISMA) (Pub. L. 107–347), the Secretary of Commerce is authorized to approve 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.

Richard Cavanagh,

Acting Associate Director for Laboratory Programs.

[FR Doc. 2015–26539 Filed 10–19–15; 8:45 am]

BILLING CODE 3510–13–P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

Submission for OMB Review; Comment Request

The Department of Commerce will submit to the Office of Management and Budget (OMB) for clearance the following proposal for collection of information under the provisions of the Paperwork Reduction Act (44 U.S.C. Chapter 35).

Agency: National Oceanic and Atmospheric Administration (NOAA).

Title: Cost-Earnings Survey of American Samoa Longline Fishery.

OMB Control Number: 0648-xxxx.

Form Number(s): None.

Type of Request: Regular (request for a new information collection).

Number of Respondents: 20.

Average Hours per Response: 30 minutes.

Burden Hours: 10.

Needs and Uses: This request is for a new information collection.

The National Marine Fisheries Service (NMFS) proposes to collect information about annual base fishing expenses in the American Samoa longline fishery with which to conduct economic analyses that will improve fishery management in those fisheries; satisfy NMFS' legal mandates under Executive Order 12866, the Magnuson-Steven Fishery Conservation and Management Act (U.S.C. 1801 *et seq.*), the Regulatory Flexibility Act, the Endangered Species Act, and the National Environmental Policy Act; and quantify achievement of the performances measures in the NMFS Strategic Operating Plans. Respondents will include longline fishers in American Samoa and their participation in the economic data collection will be voluntary.

Affected Public: Business or other for-profit organizations.

Frequency: On occasion.

Respondent's Obligation: Voluntary.

This information collection request may be viewed at *reginfo.gov*. Follow the instructions to view Department of Commerce collections currently under review by OMB.

Written comments and recommendations for the proposed information collection should be sent within 30 days of publication of this notice to *OIRA_Submission@omb.eop.gov* or fax to (202) 395–5806.

Dated: October 14, 2015.

Sarah Brabson,

NOAA PRA Clearance Officer.

[FR Doc. 2015–26508 Filed 10–19–15; 8:45 am]

BILLING CODE 3510–22–P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

Submission for OMB Review; Comment Request

The Department of Commerce will submit to the Office of Management and Budget (OMB) for clearance the following proposal for collection of information under the provisions of the Paperwork Reduction Act (44 U.S.C. Chapter 35).

Agency: National Oceanic and Atmospheric Administration (NOAA).

Title: Fishery Products Subject to Trade Restrictions Pursuant to Certification Under the High Seas Driftnet Fishing Moratorium Protection Act.

OMB Control Number: 0648–0651.

Form Number(s): None.

Type of Request: Regular (extension of a currently approved information collection).

Number of Respondents: 60.

Average Hours per Response: 10 minutes.

Burden Hours: 100.

Needs and Uses: This request is for extension of a currently approved information collection.

Pursuant to the High Seas Driftnet Fishing Moratorium Protection Act (Moratorium Protection Act), if certain fish or fish products of a nation are subject to import prohibitions to facilitate enforcement, the National Marine Fisheries Service (NMFS) requires that other fish or fish products from that nation that are not subject to the import prohibitions must be accompanied by documentation of admissibility. A duly authorized official/agent of the applicant's Government must certify that the fish in the shipments being imported into the United States (U.S.) are of a species that are not subject to an import restriction of the U.S. If a nation is identified under the Moratorium Protection Act and fails to receive a certification decision from the Secretary of Commerce, products from that nation that are not subject to the import prohibitions must be accompanied by the documentation of admissibility.

Affected Public: Business or other for-profit organizations.

Frequency: On occasion.

Respondent's Obligation: Mandatory.

This information collection request may be viewed at *reginfo.gov*. Follow the instructions to view Department of Commerce collections currently under review by OMB.

Written comments and recommendations for the proposed information collection should be sent within 30 days of publication of this notice to *OIRA_Submission@omb.eop.gov* or fax to (202) 395–5806.

Dated: October 14, 2015.

Sarah Brabson,

NOAA PRA Clearance Officer.

[FR Doc. 2015–26566 Filed 10–19–15; 8:45 am]

BILLING CODE 3510–22–P

DEPARTMENT OF COMMERCE

National Telecommunications and Information Administration

Membership of the National Telecommunications and Information Administration's Performance Review Board

AGENCY: National Telecommunications and Information Administration, Department of Commerce.

ACTION: Notice of Membership on the National Telecommunications and Information Administration's Performance Review Board.

SUMMARY: In accordance with 5 U.S.C. § 4314(c)(4), the National Telecommunications and Information Administration (NTIA), Department of Commerce (DOC), announces the appointment of those individuals who have been selected to serve as members of NTIA's Performance Review Board. The Performance Review Board is responsible for (1) reviewing performance appraisals and rating of