(202) 482–2044 or (202) 482–1791, respectively.

SUPPLEMENTARY INFORMATION:

Background

On May 1, 2019, Commerce published in the **Federal Register** a notice of opportunity to request an administrative review of the AD order on CTL plate from Taiwan for the POR.[1] Commerce received a timely request from ArcelorMittal USA LLC, Nucor Corporation, and SSAB Enterprises, LLC (collectively, the petitioners), in accordance with section 751(a) of the Tariff Act of 1930, as amended (the Act), and 19 CFR 351.213(b), to conduct an administrative review of this AD order for 19 companies.[2]

On July 15, 2019, Commerce published in the **Federal Register** a notice of initiation with respect to these companies.[3] On October 8, 2019, the petitioners timely withdrew their request for an administrative review for all 19 companies.[4]

Rescission of Administrative Review

Pursuant to 19 CFR 351.213(d)(1), Commerce will rescind an administrative review, in whole or in part, if the parties that requested a review withdraw the request within 90 days of the date of publication of the notice of initiation of the requested review. The petitioners withdrew their request for review before the 90-day deadline, and no other party requested an administrative review of this order. Therefore, we are rescinding the administrative review of the AD order on CTL plate from Taiwan covering the period May 1, 2018, through April 30, 2019, in its entirety.

Assessment

Commerce will instruct U.S. Customs and Border Protection (CBP) to assess antidumping duties on all appropriate entries. Because Commerce is rescinding this administrative review in its entirety, the entries to which this administrative review pertained shall be assessed at rates equal to the cash deposit of estimated antidumping duties required at the time of entry, or withdrawal from warehouse, for consumption, in accordance with 19 CFR 351.212(c)(1)(i). Commerce intends to issue appropriate assessment instructions directly to CBP 15 days after the date of publication of this notice in the **Federal Register**.

Notification to Importers

This notice serves as the only reminder to importers of their responsibility, under 19 CFR 351.402(f)(2), to file a certificate regarding the reimbursement of antidumping duties prior to liquidation of the relevant entries during this review period. Failure to comply with this requirement may result in the presumption that reimbursement of antidumping duties occurred and the subsequent assessment of double antidumping duties.

Notification Regarding Administrative Protective Orders

This notice serves as the only reminder to parties subject to administrative protective order (APO) of their responsibility concerning the disposition of proprietary information disclosed under APO in accordance with 19 CFR 351.305(a)(3). Timely written notification of the return or destruction of APO materials or conversion to judicial protective order is hereby requested. Failure to comply with the regulations and the terms of an APO is a sanctionable violation.

Notification to Interested Parties

This notice is published in accordance with sections 751(a)(1) and 777(i)(1) of the Act and 19 CFR 351.213(d)(4).

Dated: October 24, 2019.

James Maeder,

Deputy Assistant Secretary for Antidumping and Countervailing Duty Operations.

[FR Doc. 2019–23772 Filed 10–30–19; 8:45 am]

BILLING CODE 3510–DS–P

[1] *See Antidumping or Countervailing Duty Order, Finding, or Suspended Investigation; Opportunity To Request Administrative Review,* 84 FR 18479 (May 1, 2019).

[2] *See* Petitioners' Letter, ''Carbon and Alloy Steel Cut-To-Length Plate from Taiwan—Petitioner's Request for 2018/2019 Administrative Review,'' dated May 31, 2019.

[3] *See Initiation of Antidumping and Countervailing Duty Administrative Reviews,* 84 FR 33739 (July 15, 2019).

[4] *See* Petitioners' Letter, ''Carbon and Alloy Steel Cut-To-Length Plate from Taiwan—Petitioner's Withdrawal of Review Request for 2018/2019 Administrative Review,'' dated October 8, 2019.

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No. 191016–0064]

Request for Comments on FIPS 186–5 and SP 800–186

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

ACTION: Notice; request for comments.

SUMMARY: The National Institute of Standards and Technology (NIST) requests comments on Federal Information Processing Standard (FIPS) 186–5, Digital Signature Standard. FIPS 186–5 specifies four techniques for the generation and verification of digital signatures that can be used for the protection of data: The Rivest-Shamir Adelman Algorithm (RSA), the Digital Signature Algorithm (DSA), the Elliptic Curve Digital Signature Algorithm (ECDSA), and the Edwards curve Digital Signature Algorithm (EdDSA). Elliptic curves recommended for government use with ECDSA and EdDSA are specified in draft NIST Special Publication (SP) 800–186, Recommendations for Discrete-Logarithm Based Cryptography: Elliptic Curve Domain Parameters. We are also requesting comments on draft SP 800–186.

DATES: Comments on FIPS 186–5 and SP 800–186 must be received on or before January 29, 2020.

ADDRESSES: The drafts of FIPS 186–5 and SP 800–186 are available for review and comment on the NIST Computer Security Resource Center website at *http://csrc.nist.gov and at www.regulations.gov.* Comments on FIPS 186–5 may be sent electronically to *FIPS186-comments@nist.gov* with ''Comment on FIPS 186'' in the subject line or submitted via *www.regulations.gov.* Comments on SP 800–186 may be sent electronically to *SP800–186-comments@nist.gov* with ''Comment on SP 800–186'' in the subject line. Written comments may also be submitted by mail to Information Technology Laboratory, ATTN: FIPS 186–5 and SP 800-186 Comments, National Institute of Standards and Technology, 100 Bureau Drive, Mail Stop 8930, Gaithersburg, MD 20899–8930.

Relevant comments received by the deadline will be published electronically at *http://csrc.nist.gov/* and *www.regulations.gov* without change or redaction, so commenters should not include information they do not wish to be posted (*e.g.,* personal or confidential business information). Comments that contain profanity, vulgarity, threats, or other inappropriate language or content will not be posted or considered.

FOR FURTHER INFORMATION CONTACT: Dr. Dustin Moody, National Institute of Standards and Technology, 100 Bureau Drive, Mail Stop 8930, Gaithersburg, MD 20899–8930, email: *Dustin.Moody@nist.gov,* phone: (301) 975–8136.

SUPPLEMENTARY INFORMATION: FIPS 186 was initially developed by NIST in collaboration with the National Security Agency (NSA), using the NSA-designed Digital Signature Algorithm (DSA). Later versions of the standard approved the

use of ECDSA, developed by Certicom, and RSA, developed by Ron Rivest, Adi Shamir and Len Adelman. The American Standards Committee (ASC) on Financial Services, X9, developed standards specifying the use of both ECDSA and RSA; the standards included 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) 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 American National Standard (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 public concerns that there could be an unknown weakness in these curves. NIST is not aware of any vulnerabilities to attacks on these curves when they are implemented correctly and used as described in NIST standards and guidelines.

Advances in the understanding of elliptic curves within the cryptographic community have led to the development of new elliptic curves and algorithms, and their designers claim that they offer better performance and are easier to implement in a secure manner than previous versions. In 2014, NIST's 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.'' *See https://www.nist.gov/sites/default/files/documents/2017/05/09/VCAT-Report-on-NIST-Cryptographic-Standards-and-Guidelines-Process.pdf.*

In June 2015, NIST hosted a 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 on the development, standardization, and adoption of new elliptic curves.

In October 2015, NIST solicited comments on the elliptic curves and signature algorithms specified in FIPS 186–4 (80 FR 63539). The comments noted the broad use of the NIST prime curves and ECDSA within industry, but many commenters called for the standardization of new elliptic curves and signature algorithms.

As a result of this input, NIST is proposing updates to its standards on digital signatures and elliptic curve cryptography to align with existing and emerging industry standards. As part of these updates, NIST is proposing to adopt two new elliptic curves, Ed25519 and Ed448, for use with EdDSA. EdDSA is a deterministic elliptic curve signature scheme currently specified in the Internet Research Task Force (IRTF) RFC 8032, Edwards-Curve Digital Signature Algorithm. NIST further proposes adopting a deterministic variant of ECDSA; this variant is currently specified in RFC 6979, Deterministic Usage of the Digital Signature Algorithm and Elliptic Curve Digital Signature Algorithm. Finally, based on feedback received on the adoption of the current elliptic curve standards, the draft standards deprecate curves over binary fields due to their limited use by industry.

The proposed digital signature algorithms are included in the draft FIPS 186–5, Digital Signature Standard. NIST-recommended elliptic curves, previously specified in FIPS 186–4 Appendix D, are now included in the draft SP 800–186, Recommendations for Discrete-Logarithm Based Cryptography: Elliptic Curve Domain Parameters. Both documents are available for review and comment on the NIST Computer Security Resource Center website at *http://csrc.nist.gov/* as well as *www.regulations.gov.*

Noting increased industry adoption of ECDSA within security products, the draft FIPS 186–5 proposes the removal of the DSA. DSA was initially the only approved signature algorithm in the Digital Signature Standard when FIPS 186 was originally published in 1994 (59 FR 26208). Industry adoption of DSA was limited, and subsequent versions of FIPS 186 added other signature algorithms that are in broad use within products and protocols, including ECDSA and RSA-based signature algorithms. At this time, NIST is not aware of any applications where DSA is currently broadly used. Furthermore, recent academic analysis observed that implementations of DSA may be vulnerable to attacks if domain parameters are not properly generated. These parameters are not commonly verified before use. The removal of DSA from FIPS 186–5 would prohibit use of DSA for generating digital signatures, while legacy use of DSA to verify existing signatures would be allowed.

Draft FIPS 186–5 includes other updates intended to maintain normative references within the standard, as well as updates to technical content based on current cryptographic research. RSA digital signature schemes based on ANS X9.31, *Digital Signatures Using Reversible Public Key Cryptographic for the Financial Services Industry,* are no longer referenced in FIPS 185–5, as that standard is no longer being maintained by the Accredited Standards Committee on Financial Services, X9. RSA digital signature schemes based on Public-Key Cryptography Standard (PKCS) #1, RSA Cryptography Standard, is also specified in IETF RFC 8017, and the draft FIPS 186–5 approves the use of implementations of either or both of these standards, along with some additional requirements.

Request for Comments

NIST is seeking public comments on the proposed revisions to the digital signature algorithms specified in draft FIPS 186–5. NIST further invites public comments on the related elliptic curve specifications in draft NIST SP 800–186.

As part of this request, NIST seeks public feedback on the variants and parameters specified for EdDSA in draft FIPS 186–5. The draft revisions include a variant known as Pre-hash EdDSA. NIST seeks input on the need for this variant in cryptographic products and protocols. Furthermore, NIST seeks input on the allowed hash functions specified for use with EdDSA.

In addition to EdDSA, Draft FIPS 186–5 includes a second deterministic signature algorithm which is a variant of ECDSA. As referenced in the draft FIPS 186–5, recent security research has found that implementations of these deterministic signature algorithms may be vulnerable to certain kinds of side-channel or fault injection attacks. NIST seeks comments on the suitability of these algorithms for broad use in security products and protocols, and comments on the need for any additional guidance for implementors.

NIST also requests comments on the set of recommended and allowed elliptic curves included in draft NIST SP 800–186. In particular, NIST requests feedback on the use of these curves by industry, and industry's need for additional elliptic curve specifications to meet security or customer requirements.

Finally, NIST requests comments on the proposal to remove DSA from FIPS 186–5. In particular, NIST seeks comments on applications where DSA is being used, security considerations

around its use, and the need for a deprecation plan rather than an immediate removal.

Authority: 44 U.S.C. 3553(f)(1), 15 U.S.C. 278g–3.

Kevin A. Kimball,

Chief of Staff.

[FR Doc. 2019–23742 Filed 10–30–19; 8:45 am]

BILLING CODE 3510–13–P

COMMODITY FUTURES TRADING COMMISSION

Agency Information Collection Activities Under OMB Review

AGENCY: Commodity Futures Trading Commission.

ACTION: Notice.

SUMMARY: In compliance with the Paperwork Reduction Act of 1995 (PRA), this notice announces that the Information Collection Request (ICR) abstracted below has been forwarded to the Office of Management and Budget (OMB) for review and comment. The ICR describes the nature of the information collection and its expected costs and burden.

DATES: Comments must be submitted on or before December 2, 2019.

ADDRESSES: Comments regarding the burden estimate or any other aspect of the information collection, including suggestions for reducing the burden, may be submitted directly to the Office of Information and Regulatory Affairs (OIRA) in OMB within 30 days of this notice's publication by either of the following methods. Please identify the comments by ''Margin Requirements for Uncleared Swaps for Swap Dealers and Major Swap Participants, Comparability Determinations With Margin Requirements, OMB Control No. 3038–0111.''

- *By email addressed to: OIRAsubmissions@omb.eop.gov* or
- *By mail addressed to:* the Office of Information and Regulatory Affairs, Office of Management and Budget, Attention Desk Officer for the Commodity Futures Trading Commission, 725 17th Street NW, Washington DC 20503.

A copy of all comments submitted to OIRA should be sent to the Commodity Futures Trading Commission (the ''Commission'') by either of the following methods. The copies should refer to ''OMB Control No. 3038–0111.''

- *By mail addressed to:* Christopher Kirkpatrick, Secretary of the Commission, Commodity Futures Trading Commission, Three Lafayette Centre, 1155 21st Street NW, Washington, DC 20581;
- By Hand Delivery/Courier to the same address; or
- Through the Commission's website at *http://comments.cftc.gov.* Please follow the instructions for submitting comments through the website.

A copy of the supporting statement for the collection of information discussed herein may be obtained by visiting *http://RegInfo.gov.*

All comments must be submitted in English, or if not, accompanied by an English translation. Comments will be posted as received to *http://www.cftc.gov.* You should submit only information that you wish to make available publicly. If you wish the Commission to consider information that you believe is exempt from disclosure under the Freedom of Information Act, a petition for confidential treatment of the exempt information may be submitted according to the procedures established in § 145.9 of the Commission's regulations.[1] The Commission reserves the right, but shall have no obligation, to review, pre-screen, filter, redact, refuse or remove any or all of your submission from *http://www.cftc.gov* that it may deem to be inappropriate for publication, such as obscene language. All submissions that have been redacted or removed that contain comments on the merits of the ICR will be retained in the public comment file and will be considered as required under the Administrative Procedure Act and other applicable laws, and may be accessible under the Freedom of Information Act.

FOR FURTHER INFORMATION CONTACT: Lauren Bennett, Special Counsel, Division of Swap Dealer and Intermediary Oversight, Commodity Futures Trading Commission, (202) 418–5290 or *lbennett@cftc.gov.*

SUPPLEMENTARY INFORMATION:

Title: Margin Requirements for Uncleared Swaps for Swap Dealers and Major Swap Participants; Comparability Determinations With Margin Requirements (OMB Control No. 3038–0111). This is a request for an extension and revision of a currently approved information collection.

Abstract: Section 731 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (''Dodd-Frank Act''),[2] amended the Commodity Exchange Act (''CEA''), 7 U.S.C. 1 *et seq.,* to add, as section 4s(e) thereof, provisions concerning the setting of initial and variation margin requirements for swap dealers (''SDs'') and major swap participants (''MSPs'').[3] Each SD and MSP for which there is a Prudential Regulator, as defined in section 1a(39) of the CEA,[4] must meet margin requirements established by the applicable Prudential Regulator, and each SD and MSP for which there is no Prudential Regulator (''Covered Swap Entities'' or ''CSEs'') must comply with the Commission's regulations governing margin on all swaps that are not centrally cleared.

With regard to the cross-border application of the Commission's margin rules, section 2(i)[5] of the CEA provides the Commission with express authority over activities outside the United States relating to swaps when certain conditions are met. Section 2(i) of the CEA provides that the provisions of the CEA relating to swaps that were enacted by the Wall Street Transparency and Accountability Act of 2010 (including any rule prescribed or regulation promulgated under that Act), shall not apply to activities outside the United States unless those activities (1) have a direct and significant connection with activities in, or effect on, commerce of the United States or (2) contravene such rules or regulations as the Commission may prescribe or promulgate as are necessary or appropriate to prevent the evasion of any provision of the CEA that was enacted by the Wall Street Transparency and Accountability Act of 2010.

On May 31, 2016, the Commission published a final rule addressing the cross-border application of its margin requirements for uncleared swaps applicable to CSEs.[6] As described below, the adopting release for the Final Rule contained a collection of information regarding requests for comparability determinations, which was previously included in the proposing release, and for which the Office of Management and Budget (''OMB'') assigned OMB control number 3038–0111, titled ''Margin Requirements for Uncleared Swaps for Swap Dealers and Major Swap Participants; Comparability Determinations With Margin Requirements.'' In addition, the adopting release included two additional information collections regarding non-netting jurisdictions[7] and

[1] 17 CFR 145.9.

[2] Public Law 111–023, 124 Stat. 1376 (2010).

[3] 7 U.S.C. 6s(e).

[4] 7 U.S.C. 1a(39).

[5] 7 U.S.C. 2(i).

[6] 81 FR 34818 (May 31, 2016).

[7] As used in the adopting release, a ''non-netting jurisdiction'' is a jurisdiction in which a CSE cannot conclude, with a well-founded basis, that the netting agreement with a counterparty in that

Continued