subject to this review. For any individually examined respondent whose weighted-average dumping margin is above *de minimis* (*i.e.,* 0.50 percent), the Department will calculate importer- (or customer)-specific assessment rates for merchandise subject to this review. Where the respondent reported reliable entered values, the Department calculated importer- (or customer)-specific *ad valorem* rates by aggregating the dumping margins calculated for all U.S. sales to the importer- (or customer) and dividing this amount by the total entered value of the sales to the importer- (or customer).[14] Where the Department calculated an importer- (or customer)-specific weighted-average dumping margin by dividing the total amount of dumping for reviewed sales to the importer- (or customer) by the total sales quantity associated with those transactions, the Department will direct CBP to assess importer- (or customer)-specific assessment rates based on the resulting per-unit rates.[15] Where an importer- (or customer)-specific *ad valorem* or per-unit rate is greater than *de minimis,* the Department will instruct CBP to collect the appropriate duties at the time of liquidation. Where either the respondent's weighted average dumping margin is zero or *de minimis,* or an importer (or customer-) specific *ad valorem* or per-unit rate is zero or *de minimis,* the Department will instruct CBP to liquidate appropriate entries without regard to antidumping duties.[16]

For merchandise whose sale/entry was not reported in the U.S. sales database submitted by an exporter individually examined during this review, but that entered under the case number of that exporter (*i.e.,* at the individually-examined exporter's cash deposit rate), the Department will instruct CBP to liquidate such entries at the PRC-wide rate. Additionally, if the Department determines that an exporter under review had no shipments of the subject merchandise, any suspended entries that entered under that exporter's case number will be liquidated at the PRC-wide rate.[17]

[14] *See* 19 CFR 351.212(b)(1).

[15] *Id.*

[16] *See Antidumping Proceedings: Calculation of the Weighted-Average Dumping Margin and Assessment Rate in Certain Antidumping Duty Proceedings; Final Modification,* 77 FR 8101, 8103 (February 14, 2012).

[17] *See Non-Market Economy Antidumping Proceedings: Assessment of Antidumping Duties,* 76 FR 65694 (October 24, 2011), for a full discussion of this practice.

Cash Deposit Requirements

The following cash deposit requirements will be effective upon publication of these final results of review for shipments of the subject merchandise from the PRC entered, or withdrawn from warehouse, for consumption on or after the publication date, as provided by section 751(a)(2)(C) of the Act: (1) For the companies listed above the cash deposit rate will be their respective rate established in the final results of this review; (2) for previously investigated PRC and non-PRC exporters not listed above that have separate rates, the cash deposit rate will continue to be the exporter-specific rate published for the most recent period; (3) for all PRC exporters of subject merchandise which have not been found to be entitled to a separate rate, the cash deposit rate will be the rate for the PRC-wide entity (*i.e.,* 165.04 percent); and (4) for all non-PRC exporters of subject merchandise which have not received their own rate, the cash deposit rate will be the rate applicable to the PRC exporter that supplied that non-PRC exporter. These deposit requirements, when imposed, shall remain in effect until further notice.

Disclosure

We intend to disclose the calculations performed for these final results within five days of publication of this notice in the **Federal Register** in accordance with 19 CFR 351.224(b).

Notification to Importers Regarding the Reimbursement of Duties

This notice also serves as a final 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 could result in the Department's presumption that reimbursement of antidumping duties occurred and the subsequent assessment of double antidumping duties.

Notification Regarding Administrative Protective Orders (APO)

This notice also serves as a reminder to parties subject to APO of their responsibility concerning the return or destruction of proprietary information disclosed under APO in accordance with 19 CFR 351.305, which continues to govern business proprietary information in this segment of the proceeding. 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 terms of an APO is a violation which is subject to sanction.

This notice of the final results of this antidumping duty administrative review is issued and published in accordance with sections 751(a)(1) and 777(i) of the Act and 19 CFR 351.213 and 19 CFR 351.221(b)(5).

Dated: July 5, 2017.

Carole Showers,

Executive Director, Office of Policy, performing the duties of the Deputy Assistant Secretary for Enforcement and Compliance.

Appendix—List of Topics Discussed in the Issues and Decision Memorandum

[FR Doc. 2017–14611 Filed 7–11–17; 8:45 am]

BILLING CODE 3510–DS–P

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket Number 170627596–7596–01]

Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure: Workforce Development

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

ACTION: Notice; Request for Information (RFI).

SUMMARY: Executive Order 13800, ''Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure'' (the ''Executive Order''), directs the Secretary of Commerce, in conjunction with the Secretary of Homeland Security, and in consultation

with other Federal Departments and Agencies, to assess the scope and sufficiency of efforts to educate and train the American cybersecurity workforce of the future, including cybersecurity-related education curricula, training, and apprenticeship programs, from primary through higher education; and provide a report to the President with findings and recommendations regarding how to support the growth and sustainment of the Nation's cybersecurity workforce in both the public and private sectors. The National Institute of Standards and Technology (NIST) is seeking information on the scope and sufficiency of efforts to educate and train the Nation's cybersecurity workforce and recommendations for ways to support and improve that workforce in both the public and private sectors.

Responses to this RFI—which will be posted at *https://nist.gov/nice/cybersecurityworkforce*—will inform the assessment and report of the Secretaries of Commerce and Homeland Security to the President.

DATES: Comments must be received by 5 p.m. Eastern time on August 2, 2017.

ADDRESSES: Online submissions in electronic form may be sent to *cybersecurityworkforce@nist.gov.* Please include the subject heading of ''Cybersecurity Workforce RFI''. Attachments to electronic comments will be accepted in Microsoft Word or Excel, or Adobe PDF formats only. Written comments may be submitted by mail to Cybersecurity Workforce RFI, National Institute of Standards and Technology, 100 Bureau Drive, Stop 2000, Gaithersburg, MD 20899. Comments containing references, studies, research, and other empirical data that are not widely published should include copies or electronic links of the referenced materials.

All submissions, including attachments and other supporting materials, will become part of the public record and subject to public disclosure. Sensitive personal information, such as account numbers or Social Security numbers, or names of other individuals, should not be included. Submissions will not be edited to remove any identifying or contact information. Do not submit confidential business information, or otherwise sensitive or protected information. Please do not submit additional materials. All comments received in response to this RFI will be made available at *https://nist.gov/nice/cybersecurityworkforce* 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 will not be posted or considered.

FOR FURTHER INFORMATION CONTACT: For questions about this RFI, contact: Danielle Santos at 301–975–5048 or *Danielle.Santos@nist.gov.* Please direct media inquiries to the NIST Public Affairs Office at 301–975–2762 or *Jennifer.huergo@nist.gov.*

SUPPLEMENTARY INFORMATION: Executive Order 13800 of May 11, 2017, ''Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,'' directs the Secretary of Commerce and the Secretary of Homeland Security to consult with the Secretaries of Defense, Labor, and Education, the Director of the Office of Management and Budget, and other agencies identified jointly by the Secretary of Commerce and the Secretary of Homeland Security, in conducting an assessment and making recommendations regarding the nation's cybersecurity workforce.[1] Specifically, these departments are to:

(A) ''jointly assess the scope and sufficiency of efforts to educate and train the American cybersecurity workforce of the future, including cybersecurity-related education curricula, training, and apprenticeship programs, from primary through higher education; and''

(B) ''within 120 days of this order, provide a report to the President through the Assistant to the President for Homeland Security and Counterterrorism, with findings and recommendations regarding how to support the growth and sustainment of the Nation's cybersecurity workforce in both the public and private sectors.'' [2]

The Commerce Department's National Institute of Standards and Technology is soliciting comments from the public that will aid the Department of Commerce (DOC) and the Department of Homeland Security (DHS) in preparing the assessment and report to the President. For the purposes of this RFI, ''education and training'' of the American cybersecurity workforce does not include general workforce cybersecurity awareness efforts. Rather, ''education and training'' refers to curriculum- or practicum-based programs to increase the effectiveness of the workforce addressing cybersecurity challenges. As the Executive Order states, comments are sought on the cybersecurity workforce in both the private and public sectors.

NIST may conduct workshops to gain further public input to the assessment and recommendations regarding the cybersecurity workforce. Information will be made available at *https://nist.gov/nice/cybersecurityworkforce.*

This RFI does not address additional aspects of the cybersecurity workforce that are included in the Executive Order.

Request for Information

Given the nature and importance of the Executive Order, NIST requests information from the public about current, planned, or recommended education and training programs aimed at strengthening the U.S. cybersecurity workforce.

Respondents are encouraged—but are not required—to respond to each question and to present their answers after each question. The following questions cover the major areas about which NIST seeks comment. They are not intended to limit the topics that may be addressed. Respondents may address related topics and may organize their submissions in response to this RFI in any manner. Responses may include estimates; please indicate where the response is an estimate.

All responses that comply with the requirements listed in the **DATES** and **ADDRESSES** sections of this RFI will be considered.

Comments containing references, studies, research, and other empirical data that are not widely published should include copies or electronic links of the referenced materials. Do not include in comments or otherwise submit proprietary or confidential information, as all comments received in response to this RFI will be made available publicly at *https://nist.gov/nice/cybersecurityworkforce.* Comments that contain profanity, vulgarity, threats, or other inappropriate language will not be posted or considered.

General Information

1. Are you involved in cybersecurity workforce education or training (*e.g.,* curriculum-based programs)? If so, in what capacity (including, but not limited to: Community college or university faculty or administrator; official with a non-profit association focused on cybersecurity workforce needs; manufacturer or service company that relies on cybersecurity employees; cybersecurity curriculum developer; cybersecurity training institute; educator in a primary grade school; government agency that provides

[1] Exec. Order No. 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, 82 FR 22391 (May 16, 2017).

[2] *https://www.federalregister.gov/d/2017-10004.*

funding for cybersecurity education; or student or employee enrolled in a cybersecurity education or training program)? *Note:* Providing detailed information, including your specific affiliation is optional and will be made publicly available. Commenters should not include information they do not wish to be posted (*e.g.,* personal or confidential business information) and are strongly encouraged not to include Personally Identifiable Information in their submissions.

Growing and Sustaining the Nation's Cybersecurity Workforce

1. What current metrics and data exist for cybersecurity education, training, and workforce developments, and what improvements are needed in the collection, organization, and sharing of information about cybersecurity education, training, and workforce development programs?

2. Is there sufficient understanding and agreement about workforce categories, specialty areas, work roles, and knowledge/skills/abilities?

3. Are appropriate cybersecurity policies in place in your organization regarding workforce education and training efforts and are those policies regularly and consistently enforced?

4. What types of knowledge or skills do employers need or value as they build their cybersecurity workforce? Are employer expectations realistic? Why or why not? Are these expectations in line with the knowledge and skills of the existing workforce or student pipeline? How do these types of knowledge and skills vary by role, industry, and sector, (*e.g.,* energy vs financial sectors)?

5. Which are the most effective cybersecurity education, training, and workforce development programs being conducted in the United States today? What makes those programs effective? What are the goals for these programs and how are they successful in reaching their goals? Are there examples of effective/scalable cybersecurity, education, training, and workforce development programs?

6. What are the greatest challenges and opportunities facing the Nation, employers, and workers in terms of cybersecurity education, training, and workforce development?

7. How will advances in technology (*e.g.,* artificial intelligence, Internet of Things, etc.) or other factors affect the cybersecurity workforce needed in the future? How much do cybersecurity education, training, and workforce development programs need to adapt to prepare the workforce to protect modernized cyber physical systems (CPS)?

8. What steps or programs should be continued, modified, discontinued, or introduced to grow and sustain the Nation's cybersecurity workforce, taking into account needs and trends? What steps should be taken:

i. At the Federal level?

ii. At the state or local level, including school systems?

iii. By the private sector, including employers?

iv. By education and training providers?

v. By technology providers?

Kevin Kimball,

NIST Chief of Staff.

[FR Doc. 2017–14553 Filed 7–11–17; 8:45 am]

BILLING CODE 3510–13–P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric

Administration Proposed Information Collection; Comment Request; West Coast Region Vessel Identification Requirements

AGENCY: National Oceanic and Atmospheric Administration (NOAA), Commerce.

ACTION: Notice.

SUMMARY: The Department of Commerce, as part of its continuing effort to reduce paperwork and respondent burden, invites the general public and other Federal agencies to comment on proposed and/or continuing information collections, as required by the Paperwork Reduction Act of 1995.

DATES: Written comments must be submitted on or before September 11, 2017.

ADDRESSES: Direct all written comments to Jennifer Jessup, Departmental Paperwork Clearance Officer, Department of Commerce, Room 6616, 14th and Constitution Avenue NW., Washington, DC 20230 (or via the Internet at *pracomments@doc.gov*).

FOR FURTHER INFORMATION CONTACT: Requests for additional information or copies of the information collection instrument and instructions should be directed to Shannon Penna, National Marine Fisheries Service (NMFS), West Coast Region (WCR) Long Beach Office, 501 West Ocean Blvd., Suite 4200, Long Beach, CA 90802, (562) 980–4238 or *shannon.penna@noaa.gov.*

SUPPLEMENTARY INFORMATION:

I. Abstract

This request is for extension of a current information collection.

Regulations at 50 CFR 660.704 require that all commercial fishing vessels with permits issued under authority of the National Marine Fishery Service's (NMFS) Fishery Management Plan for United States (U.S.) West Coast Highly Migratory Species Fisheries display the vessel's official number (U.S. Coast Guard documentation number or state registration number). The numbers must be of a specific size and format and located at specified locations. The official number must be affixed to each vessel subject to this section in block Arabic numerals at least 10 inches (25.40 centimeters) in height for vessels more than 25 feet (7.62 meters) but equal to or less than 65 feet (19.81 meters) in length; and 18 inches (45.72 centimeters) in height for vessels longer than 65 feet (19.81 meters) in length. Markings must be legible and of a color that contrasts with the background. The display of the identifying number aids in fishery law enforcement. This requirement does not apply to recreational charter vessels.

II. Method of Collection

The vessels' official numbers are displayed on the vessels.

III. Data

OMB Control Number: 0648–0361.

Form Number(s): None.

Type of Review: Regular submission (extension of a current information collection).

Affected Public: Business or other for-profit organizations.

Estimated Number of Respondents: 1700.

Estimated Time per Response: All but purse seine vessels, 45 minutes; purse seine vessels, 1 hour, 15 minutes.

Estimated Total Annual Burden Hours: 1,325 hours.

Estimated Total Annual Cost to Public: $13,250.

IV. Request for Comments

Comments are invited on: (a) Whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information shall have practical utility; (b) the accuracy of the agency's estimate of the burden (including hours and cost) of the proposed collection of information; (c) ways to enhance the quality, utility, and clarity of the information to be collected; and (d) ways to minimize the burden of the collection of information on respondents, including through the use of automated collection techniques or other forms of information technology.