assembly or boom assembly. Forklifts are material handling vehicles with a working attachment, usually a fork, lifted along a vertical guide rail with the operator seated or standing on the chassis behind the vertical mast. Vertical mast lifts are person and material lifting vehicles with a working attachment, usually a platform, lifted along a vertical guide rail with an operator standing on the platform. Mobile self-propelled cranes are material handling vehicles with a boom attachment for lifting loads of tools or materials that are suspended on ropes, cables, and/or chains, and which contain winches mounted on or near the base of the boom with ropes, cables, and/or chains managed along the boom structure. The scope also excludes motor vehicles (defined as a vehicle driven or drawn by mechanical power and manufactured primarily for use on public streets, roads, and highways, but does not include a vehicle operated only on a rail line pursuant to 49 U.S.C. 30102(a)(7)) that incorporate a scissor arm assembly or boom assembly. The scope further excludes vehicles driven or drawn by mechanical power operated only on a rail line that incorporate a scissor arm assembly or boom assembly. The scope also excludes: (1) Rail line vehicles, defined as vehicles with hi-rail gear or track wheels, and a fixed (non-telescopic) main boom, which perform operations on rail lines, such as laying rails, setting ties, or other rail maintenance jobs; and (2) certain rail line vehicle subassemblies, defined as chassis subassemblies and boom turntable subassemblies for rail line vehicles with a fixed (non-telescopic) main boom.

Certain mobile access equipment subject to this investigation is typically classifiable under subheadings 8427.10.8020, 8427.10.8030, 8427.10.8070, 8427.10.8095, 8427.20.8020, 8427.20.8090, 8427.90.0020 and 8427.90.0090 of the Harmonized Tariff Schedule of the United States (HTSUS). Parts of certain mobile access equipment are typically classifiable under subheading 8431.20.0000 of the HTSUS. While the HTSUS subheadings are provided for convenience and customs purposes only, the written description of the merchandise under investigation is dispositive.

Appendix II

List of Topics Discussed in the Issues and Decision Memorandum

I. Summary
II. Background
III. Period of Investigation
IV. Scope of Investigation
V. Adjustment Under Section 777A(f) of the Act
VI. Adjustment to Cash Deposit Rate For Export Subsidies
VII. Changes Since the *Preliminary Determination*
VIII. Discussion of the Issues

Issues Related to Dingli

Comment 1: Should China to the United States Ocean Freight Surrogate Values (SVs) be Revised
Comment 2: Should World to Brazil Ocean Freight SVs be Revised
Comment 3: Should Commerce Multiply the Value of Marine Insurance to Cover 110 percent of the Total Value of the Goods Shipped
Comment 4: Should Commerce Include Research and Development Expenses in General and Administrative Expenses for Further Manufacturing
Comment 5: Should Commerce Reject Dingli's Submission of Untimely New Factual Information
Comment 6: Should Commerce Make Revisions to its SVs for Dingli's Inputs for the Final Determination
Comment 7: Should Commerce Value Certain Inputs that Include Alloy and Non-Alloy Harmonized Tariff Schedule Headings Based on a Simple Average of SVs
Comment 8: Whether Commerce's Application of the Cohen's-d Test to Dingli's U.S. Sales is Unsupported by Substantial Evidence and Controlling Law

Issues Related LGMG

Comment 9: Should Commerce Revise its SVs for LGMG's Inputs for the Final Determination
Comment 10: Should Commerce Apply Circumstance of Sale Adjustments to Certain LGMG Sales for the Final Determination

Issues Related to Dingli and LGMG

Comment 11: Should Commerce Deduct Section 301 Duties from U.S. Sales Prices in Calculating Dingli's and LGMG's Dumping Margin

Issues Related to Skyjack Inc. (Skyjack)

Comment 12: Whether Skyjack is Entitled to a Separate Rate

IX. Recommendation

[FR Doc. 2022–03660 Filed 2–18–22; 8:45 am]
BILLING CODE 3510–DS–P

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket Number: 220210–0045]

Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management

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

ACTION: Notice; request for information.

SUMMARY: The National Institute of Standards and Technology (NIST) is seeking information to assist in evaluating and improving its cybersecurity resources, including the ''Framework for Improving Critical Infrastructure Cybersecurity'' (the ''NIST Cybersecurity Framework,'' ''CSF'' or ''Framework'') and a variety of existing and potential standards, guidelines, and other information, including those relating to improving cybersecurity in supply chains. NIST is considering updating the NIST Cybersecurity Framework to account for the changing landscape of cybersecurity risks, technologies, and resources. In addition, NIST recently announced it would launch the National Initiative for Improving Cybersecurity in Supply Chains (NIICS) to address cybersecurity risks in supply chains. This wide-ranging public-private partnership will focus on identifying tools and guidance for technology developers and providers, as well as performance-oriented guidance for those acquiring such technology. To inform the direction of the NIICS, including how it might be aligned and integrated with the Cybersecurity Framework, NIST is requesting information that will support the identification and prioritization of supply chain-related cybersecurity needs across sectors. Responses to this RFI will inform a possible revision of the Cybersecurity Framework as well as the NIICS initiative.

DATES: Comments in response to this notice must be received by April 25, 2022. Submissions received after that date may not be considered.

Comments may be submitted by any of the following methods:

Electronic submission: Submit electronic public comments via the Federal e-Rulemaking Portal.

1. Go to *www.regulations.gov* and enter NIST–2022–0001 in the search field,
2. Click the ''Comment Now!'' icon, complete the required fields, and
3. Enter or attach your comments.

Electronic submissions may also be sent as an attachment to *CSF-SCRM-RFI@nist.gov* and may be in any of the following unlocked formats: HTML; ASCII; Word; RTF; or PDF. Please submit comments only and include your name, organization's name (if any), and cite ''NIST Cybersecurity RFI'' in all correspondence. Comments containing references, studies, research, and other empirical data that are not widely published should include copies of the referenced materials. Please do not submit additional materials.

Comments received by the deadline may be posted at *www.regulations.gov* and *https://www.nist.gov/cyberframework.* All submissions, including attachments and other supporting materials, may become part of the public record and may be subject to public disclosure. NIST reserves the right to publish relevant comments publicly, unedited and in their entirety. Personal information, such as account numbers or Social Security numbers, or names of other individuals, should not be included. Do not submit confidential

business information, or otherwise sensitive or protected information. Comments that contain profanity, vulgarity, threats, or other inappropriate language or content will not be considered.

FOR FURTHER INFORMATION CONTACT: For questions about this RFI contact: *CSF-SCRM-RFI@nist.gov* or Katherine MacFarland, National Institute of Standards and Technology, 100 Bureau Drive, Stop 2000, Gaithersburg, MD 20899; (301) 975–3359. Direct media inquiries to NIST's Office of Public Affairs at (301) 975–2762. Users of telecommunication devices for the deaf, or a text telephone, may call the Federal Relay Service, toll free at 1–800–877–8339.

Accessible Format: NIST will make the RFI available in alternate formats, such as Braille or large print, upon request by persons with disabilities.

SUPPLEMENTARY INFORMATION: The NIST Cybersecurity Framework consists of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to reduce cybersecurity risks. It is used widely by private and public sector organizations in and outside of the United States and has been translated into multiple languages, speaking to its success as a common resource.

The Cybersecurity Framework was last updated in April 2018. Much has changed in the cybersecurity landscape in terms of threats, capabilities, technologies, education and workforce, and the availability of resources to help organizations to better manage cybersecurity risk. That includes an increased awareness of and emphasis on cybersecurity risks in supply chains, including a decision to launch NIICS. With those changes in mind, NIST seeks to build on its efforts to cultivate trust by advancing cybersecurity and privacy standards and guidelines, technology, measurements, and practices by requesting information about the use, adequacy, and timeliness of the Cybersecurity Framework and the degree to which other NIST resources are used in conjunction with or instead of the Framework. Further, to inform the direction of the NIICS, including how it might be aligned and integrated with the Cybersecurity Framework, NIST is requesting information that will support the identification and prioritization of supply chain-related cybersecurity needs across sectors.

Following is a non-exhaustive list of possible topics that may be addressed in any comments. Comments may address topics in the following list, or any other topic believed to have implications for the improvement of the NIST Cybersecurity Framework or NIST's cybersecurity guidance regarding supply chains. NIST will consider all relevant comments in the development of the revised Framework and guidance regarding supply chains.

Use of the NIST Cybersecurity Framework

1. The usefulness of the NIST Cybersecurity Framework for aiding organizations in organizing cybersecurity efforts via the five functions in the Framework and actively managing risks using those five functions.

2. Current benefits of using the NIST Cybersecurity Framework. Are communications improved within and between organizations and entities (*e.g.,* supply chain partners, customers, or insurers)? Does the Framework allow for better assessment of risks, more effective management of risks, and/or increase the number of potential ways to manage risks? What might be relevant metrics for improvements to cybersecurity as a result of implementation of the Framework?

3. Challenges that may prevent organizations from using the NIST Cybersecurity Framework or using it more easily or extensively (*e.g.,* resource considerations, information sharing restrictions, organizational factors, workforce gaps, or complexity).

4. Any features of the NIST Cybersecurity Framework that should be changed, added, or removed. These might include additions or modifications of: Functions, Categories, or Subcategories; Tiers; Profile Templates; references to standards, frameworks, models, and guidelines; guidance on how to use the Cybersecurity Framework; or references to critical infrastructure versus the Framework's broader use.

5. Impact to the usability and backward compatibility of the NIST Cybersecurity Framework if the structure of the framework such as Functions, Categories, Subcategories, etc. is modified or changed.

6. Additional ways in which NIST could improve the Cybersecurity Framework, or make it more useful.

Relationship of the NIST Cybersecurity Framework to Other Risk Management Resources

7. Suggestions for improving alignment or integration of the Cybersecurity Framework with other NIST risk management resources. As part of the response, please indicate benefits and challenges of using these resources alone or in conjunction with the Cybersecurity Framework. These resources include:

- Risk management resources such as the NIST Risk Management Framework, the NIST Privacy Framework, and Integrating Cybersecurity and Enterprise Risk Management (NISTIR 8286).
- Trustworthy technology resources such as the NIST Secure Software Development Framework, the NIST Internet of Things (IoT) Cybersecurity Capabilities Baseline, and the Guide to Industrial Control System Cybersecurity.
- Workforce management resources such as the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity.

8. Use of non-NIST frameworks or approaches in conjunction with the NIST Cybersecurity Framework. Are there commonalities or conflicts between the NIST framework and other voluntary, consensus resources? Are there commonalities or conflicts between the NIST framework and cybersecurity-related mandates or resources from government agencies? Are there ways to improve alignment or integration of the NIST framework with other frameworks, such as international approaches like the ISO/IEC 27000-series, including ISO/IEC TS 27110?

9. There are numerous examples of international adaptations of the Cybersecurity Framework by other countries. The continued use of international standards for cybersecurity, with a focus on interoperability, security, usability, and resilience can promote innovation and competitiveness while enabling organizations to more easily and effectively integrate new technologies and services. Given this importance, what steps should NIST consider to ensure any update increases international use of the Cybersecurity Framework?

10. References that should be considered for inclusion within NIST's Online Informative References Program. This program is an effort to define standardized relationships between NIST and industry resources and elements of documents, products, and services and various NIST documents such as the NIST Cybersecurity Framework, NIST Privacy Framework, Security and Privacy Controls for Information Systems and Organizations (NIST Special Publication 800–53), NIST Secure Software Development Framework, and the NIST Internet of Things (IoT) Cybersecurity Capabilities Baseline.

Cybersecurity Supply Chain Risk Management

11. National Initiative for Improving Cybersecurity in Supply Chains (NIICS). What are the greatest challenges related to the cybersecurity aspects of supply chain risk management that the NIICS could address? How can NIST build on its current work on supply chain security, including software security work stemming from E.O. 14028, to increase trust and assurance in technology products, devices, and services?

12. Approaches, tools, standards, guidelines, or other resources necessary for managing cybersecurity-related risks in supply chains. NIST welcomes input on such resources in narrowly defined areas (*e.g.* pieces of hardware or software assurance or assured services, or specific to only one or two sectors) that may be useful to utilize more broadly; potential low risk, high reward resources that could be facilitated across diverse disciplines, sectors, or stakeholders; as well as large-scale and extremely difficult areas.

13. Are there gaps observed in existing cybersecurity supply chain risk management guidance and resources, including how they apply to information and communications technology, operational technology, IoT, and industrial IoT? In addition, do NIST software and supply chain guidance and resources appropriately address cybersecurity challenges associated with open-source software? Are there additional approaches, tools, standards, guidelines, or other resources that NIST should consider to achieve greater assurance throughout the software supply chain, including for open-source software?

14. Integration of Framework and Cybersecurity Supply Chain Risk Management Guidance. Whether and how cybersecurity supply chain risk management considerations might be further integrated into an updated NIST Cybersecurity Framework—or whether and how a new and separate framework focused on cybersecurity supply chain risk management might be valuable and more appropriately be developed by NIST.

Alicia Chambers,

NIST Executive Secretariat.

[FR Doc. 2022–03642 Filed 2–18–22; 8:45 am]

BILLING CODE 3510–13–P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

[RTID 0648–XB822]

Western Pacific Fishery Management Council; Public Meetings

AGENCY: National Marine Fisheries Service (NMFS), National Oceanic and Atmospheric Administration (NOAA), Commerce.

ACTION: Notice of public meetings.

SUMMARY: The Western Pacific Fishery Management Council (Council) will hold its American Samoa Fishery Archipelago Fishery Ecosystem Plan (FEP) Advisory Panel (AP), Mariana Archipelago FEP-Commonwealth of the Northern Mariana Islands (CNMI) AP, Mariana Archipelago FEP-Guam AP, Fishing Industry Advisory Committee (FIAC), and the Hawaii Archipelago FEP AP to discuss and make recommendations on fishery management issues in the Western Pacific Region.

DATES: The meetings will be held between March 8 and March 11, 2022. For specific times and agendas, see **SUPPLEMENTARY INFORMATION**.

ADDRESSES: The meetings will be held by web conference via Webex. Instructions for connecting to the web conference and providing oral public comments will be posted on the Council website at *www.wpcouncil.org.* For assistance with the web conference connection, contact the Council office at (808) 522–8220.

FOR FURTHER INFORMATION CONTACT: Kitty M. Simonds, Executive Director, Western Pacific Fishery Management Council; phone: (808) 522–8220.

SUPPLEMENTARY INFORMATION: The American Samoa Archipelago FEP AP will meet on Tuesday, March 8, 2022, from 6 p.m. to 8 p.m., The Mariana Archipelago FEP–CNMI AP will meet on Thursday, March 10, 2022, from 9 a.m. to 11 a.m., the Mariana Archipelago FEP-Guam AP will meet on Thursday March 10, 2022, from 6:30 p.m. to 8:30 p.m., the FIAC will meet on Thursday, March 10, 2022, from 2 p.m. to 5 p.m., and the Hawaii Archipelago FEP AP will meet on Friday, March 11, from 9 a.m. to 12 noon. All times listed are local island times expect for the FIAC which is in Hawaii Standard Time.

Public Comment periods will be provided in the agendas. The order in which agenda items are addressed may change. The meetings will run as late as necessary to complete scheduled business.

Schedule and Agenda for the American Samoa Archipelago AP Meeting

Tuesday, March 8, 2022, 6 p.m.–8 p.m. (American Samoa Standard Time)

1. Welcome and Introductions
2. Review of Last AP Meeting and Recommendations
3. American Samoa (AS) Fishery Issues and Activities
   - A. Bottomfish
     - i. Options for Revising the Territorial Bottomfish Management Unit Species (BMUS)
     - ii. American Samoa Bottomfish Data Workshop
   - B. Council Coordination Committee (CCC) Working Group on Equity and Environmental Justice (EEJ)
   - C. Fishery Biological Opinions (BiOPs) Update
4. 2022 AP Activities Plan
   - A. Update on Sustainable Fisheries Fund Projects
   - B. Catchit Logit (CILI) Update
   - C. Education and Outreach
5. Feedback From The Fleet
   - A. AS Fishermen Observations
   - B. AP Fishery Issues and Activities
6. Public Comment
7. Discussion and Recommendations
8. Other Business

Schedule and Agenda for the Mariana Archipelago-CNMI AP Meeting

Thursday, March 10, 2022, 9 a.m.–11 a.m. (Marianas Standard Time)

1. Welcome and Introductions
2. Review of Last AP Meeting and Recommendations
3. CNMI Fishery Issues and Activities
   - A. Bottomfish
     - i. Options for Revising the Territorial BMUS
     - ii. Fishery BiOPs Update
   - B. Marianas Sanctuary Nomination
   - C. CILI Updates
   - D. CCC Working Group on EEJ
4. 2022 Advisory Panel Activities Plan
   - A. AP Outreach and Education
5. Feedback From The Fleet
   - A. CNMI Fishermen Observations
   - B. AP Fishery Issues and Activities
6. Discussion and Recommendations
7. Other Business

Schedule and Agenda for the Mariana Archipelago-Guam AP Meeting

Thursday, March 10, 2022, 6:30 p.m.–8:30 p.m. (Marianas Standard Time)

1. Welcome and Introductions
2. Review of Last AP Meeting and Recommendations
3. Guam Fishery Issues and Activities
   - A. Bottomfish
     - i. Options for Revising the Territorial BMUS
     - ii. Fishery BiOPs Update