Disclosure

We intend to disclose the calculations performed to parties in this proceeding within five days after public announcement of the amended preliminary determination, in accordance with 19 CFR 351.224(b).

International Trade Commission Notification

In accordance with section 733(f) of the Act, we will notify the International Trade Commission of our amended preliminary determination.

Notification to Interested Parties

This amended preliminary determination is issued and published pursuant to sections 733(d) and 777(i) of the Act and 19 CFR 351.224(e).

Dated: June 12, 2023.

Lisa W. Wang,

Assistant Secretary for Enforcement and Compliance.

Appendix—Scope of the Investigation

The products within the scope of the investigation are file folders consisting primarily of paper, paperboard, pressboard, or other cellulose material, whether coated or uncoated, that has been folded (or creased in preparation to be folded), glued, taped, bound, or otherwise assembled to be suitable for holding documents. The scope includes all such folders, regardless of color, whether or not expanding, whether or not laminated, and with or without tabs, fasteners, closures, hooks, rods, hangers, pockets, gussets, or internal dividers. The term ''primarily'' as used in the first sentence of this scope means 50 percent or more of the total product weight, exclusive of the weight of fasteners, closures, hooks, rods, hangers, removable tabs, and similar accessories, and exclusive of the weight of packaging.

Subject folders have the following dimensions in their folded and closed position: lengths and widths of at least 8 inches and no greater than 17 inches, regardless of depth.

The scope covers all varieties of folders, including but not limited to manila folders, hanging folders, fastener folders, classification folders, expanding folders, pockets, jackets, and wallets.

Excluded from the scope are:

- mailing envelopes with a flap bearing one or more adhesive strips that can be used permanently to seal the entire length of a side such that, when sealed, the folder is closed on all four sides;
- binders, with two or more rings to hold documents in place, made from paperboard or pressboard encased entirely in plastic;
- binders consisting of a front cover, back cover, and spine, with or without a flap; to be excluded, a mechanism with two or more metal rings must be included on or adjacent to the interior spine;
- non-expanding folders with a depth exceeding 2.5 inches and that are closed or closeable on the top, bottom, and all four sides (*e.g.,* boxes or cartons);
- expanding folders that have (1) 13 or more pockets, (2) a flap covering the top, (3) a latching mechanism made of plastic and/or metal to close the flap, and (4) an affixed plastic or metal carry handle;
- folders that have an outer surface (other than the gusset, handles, and/or closing mechanisms, if any) that is covered entirely with fabric, leather, and/or faux leather;
- fashion folders, which are defined as folders with all of the following characteristics: (1) plastic lamination covering the entire exterior of the folder, (2) printing, foil stamping, embossing (*i.e.,* raised relief patterns that are recessed on the opposite side), and/or debossing (*i.e.,* recessed relief patterns that are raised on the opposite side), covering the entire exterior surface area of the folder, (3) at least two visible and printed or foil stamped colors (other than the color of the base paper), each of which separately covers no less than 10 percent of the entire exterior surface area, and (4) patterns, pictures, designs, or artwork covering no less than thirty percent of the exterior surface area of the folder;
- portfolios, which are folders having (1) a width of at least 16 inches when open flat, (2) no tabs or dividers, and (3) one or more pockets that are suitable for holding letter size documents and that cover at least 15 percent of the surface area of the relevant interior side or sides; and
- report covers, which are folders having (1) no tabs, dividers, or pockets, and (2) one or more fasteners or clips, each of which is permanently affixed to the center fold, to hold papers securely in place.

Imports of the subject merchandise are provided for under Harmonized Tariff Schedule of the United States (HTSUS) category 4820.30.0040. Subject imports may also enter under other HTSUS classifications. While the HTSUS subheading is provided for convenience and customs purposes, the written description of the scope of the investigation is dispositive.

[FR Doc. 2023–13014 Filed 6–16–23; 8:45 am]

BILLING CODE 3510–DS–P

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No.: 220208–0264]

National Cybersecurity Center of Excellence (NCCoE) Cybersecurity for the Water and Wastewater Sector: A Practical Reference Design for Mitigating Cyber Risk in Water and Wastewater Systems

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

ACTION: Notice.

SUMMARY: The National Institute of Standards and Technology (NIST) invites organizations to provide letters of interest describing products and technical expertise to support and demonstrate security platforms for the *Cybersecurity for the Water and Wastewater Sector: A Practical Reference Design for Mitigating Cyber Risk in Water and Wastewater Systems* project. This notice is the initial step for the National Cybersecurity Center of Excellence (NCCoE) in collaborating with technology companies to address cybersecurity challenges identified under the *Cybersecurity for the Water and Wastewater Sector: A Practical Reference Design for Mitigating Cyber Risk in Water and Wastewater Systems* project. Participation in the project is open to all interested organizations.

DATES: Collaborative activities will commence as soon as enough completed and signed letters of interest have been returned to address all the necessary components and capabilities, but no earlier than July 20, 2023.

ADDRESSES: The NCCoE is located at 9700 Great Seneca Highway, Rockville, MD 20850. Letters of interest must be submitted to *water_nccoe@nist.gov* or via hardcopy to National Institute of Standards and Technology, NCCoE; 9700 Great Seneca Highway, Rockville, MD 20850. Interested parties can access the letter of interest request by visiting *www.nccoe.nist.gov/projects/securing-water-and-wastewater-utilities* and completing the letter of interest webform. NIST will announce the completion of the selection of participants and inform the public that it is no longer accepting letters of interest for this project at *www.nccoe.nist.gov/projects/securing-water-and-wastewater-utilities.* Organizations whose letters of interest are accepted in accordance with the process set forth in the **SUPPLEMENTARY INFORMATION** section of this notice will be asked to sign an NCCoE consortium Cooperative Research and Development Agreement (CRADA) with NIST. An NCCoE consortium CRADA template can be found at: *https://www.nccoe.nist.gov/publications/other/nccoe-consortium-crada-example.*

FOR FURTHER INFORMATION CONTACT: James McCarthy via telephone at 301–975–0228; by email at *water_nccoe@nist.gov;* or by mail to National Institute of Standards and Technology, NCCoE; 9700 Great Seneca Highway, Rockville, MD 20850. Additional details about the *Cybersecurity for the Water and Wastewater Sector: A Practical Reference Design for Mitigating Cyber Risk in Water and Wastewater Systems* project are available at *https://www.nccoe.nist.gov/projects/securing-water-and-wastewater-utilities.*

SUPPLEMENTARY INFORMATION:

Background: The NCCoE, part of NIST, is a public-private collaboration for accelerating the widespread adoption of integrated cybersecurity tools and technologies. The NCCoE brings together experts from industry, government, and academia under one roof to develop practical, interoperable cybersecurity approaches that address the real-world needs of complex Information Technology (IT) and Operational Technology (OT) systems. By accelerating dissemination and use of these integrated tools and technologies for protecting IT and OT assets, the NCCoE will enhance trust in U.S. IT and OT communications, data, and storage systems; reduce risk for companies and individuals using IT and OT systems; and encourage development of innovative, job-creating cybersecurity products and services.

Process: NIST is soliciting responses from all sources of relevant security capabilities (see below) to enter into an NCCoE Cooperative Research and Development Agreement (CRADA) to provide products and technical expertise to support and demonstrate security platforms for the *Cybersecurity for the Water and Wastewater Sector: A Practical Reference Design for Mitigating Cyber Risk in Water and Wastewater Systems* project. The full project can be viewed at: *www.nccoe.nist.gov/projects/securing-water-and-wastewater-utilities.*

Interested parties can access the request for a letter of interest template by visiting the project website at *www.nccoe.nist.gov/projects/securing-water-and-wastewater-utilities* and completing the letter of interest webform. On completion of the webform, interested parties will receive access to the letter of interest template, which the party must complete, certify as accurate, and submit to NIST by email or hardcopy. NIST will contact interested parties if there are questions regarding the responsiveness of the letters of interest to the project objective or requirements identified below. NIST will select participants who have submitted complete letters of interest on a first come, first served basis within each category of product components or capabilities listed below up to the number of participants in each category necessary to carry out this project. When the project has been completed, NIST will post a notice on the *Cybersecurity for the Water and Wastewater Sector: A Practical Reference Design for Mitigating Cyber Risk in Water and Wastewater Systems* project website at *www.nccoe.nist.gov/projects/securing-water-and-wastewater-utilities* announcing the next phase of the project and informing the public that it will no longer accept letters of interest for this project. There may be continuing opportunity to participate even after initial activity commences. Selected participants will be required to enter into an NCCoE consortium CRADA with NIST (for reference, see **ADDRESSES** section above).

Project Objective: This project will develop example cybersecurity solutions to protect the infrastructure in the operating environments of Water and Wastewater Systems (WWS) sector utilities. The increasing adoption of network-enabled technologies by the sector merits the development of best practices, guidance, and solutions to ensure that the cybersecurity posture of facilities is safeguarded.

Critical infrastructure issues in the WWS sector present several unique challenges. Utilities in the sector typically cover a wide geographic area regarding piped distribution networks and infrastructure together with centralized treatment operations. The supporting operational technologies (OT) underpinning this infrastructure are likely reliant on supervisory control and data acquisition (SCADA) systems which provide data transmission across the enterprise, sending sensor readings and signals in real time. These systems also control the automated processes in the production environment which is linked to the distribution network. Additionally, many OT devices are converging upon information technology (IT) capability with the advent of Industrial internet-of-Things (IIoT) devices and platforms, such as cloud-based SCADA and smart monitoring. This project will develop a reference design that demonstrates practical solutions for water and wastewater utilities of all sizes. The reference design will use commercially available products and services to address four WWS cybersecurity challenges: asset management, data integrity, remote access, and network segmentation. The commercial products and services will be integrated into a demonstration of the reference design. The project also initiates a broad discussion with WWS sector stakeholders to identify commercial solution providers.

This project will result in a publicly available NIST Cybersecurity Practice Guide which will include a detailed implementation guide of the practical steps needed to implement a cybersecurity reference design that addresses these challenges.

Requirements for Letters of Interest: Each responding organization's letter of interest should identify which security platform component(s) or capability(ies) it is offering. Letters of interest should not include company proprietary information, and all components and capabilities must be commercially available. Components are listed in section 3 of the *Cybersecurity for the Water and Wastewater Sector: A Practical Reference Design for Mitigating Cyber Risk in Water and Wastewater Systems* project description available at: *www.nccoe.nist.gov/projects/securing-water-and-wastewater-utilities.*

Requested Capabilities

This project will employ products, provided by collaborating vendors, that provide the following cybersecurity capabilities to address the four scenarios described in section 2 of the *Cybersecurity for the Water and Wastewater Sector: A Practical Reference Design for Mitigating Cyber Risk in Water and Wastewater Systems* Project Description.

- *Asset Management:* Asset management capabilities discover and identify physical and virtual assets in the OT environment. These assets may be geographically distributed and may be cloud-based. In addition to network-connected assets, these capabilities should provide a means to discover and identify assets connected by low-bandwidth communications channels and disconnected assets. The asset management capability maintains an inventory of known assets which contains information such asset type, product version, and communication protocols used. Asset management capabilities may provide automation to establish and enforce a baseline security posture.
- *Data Integrity:* Data integrity capabilities protect data and communications within the OT environment against improper modification or destruction. Additionally, these capabilities monitor the OT environment to detect potential integrity violations and generate alerts to initiate any needed responses.
- *Remote Access:* Remote access capabilities provide entities (people and systems) controlled access to OT assets from outside the OT environment. These capabilities authenticate any entity seeking access, allow only explicitly authorized access, control which actions are allowed for each authorized entity, and maintain a record of all actions attempted and completed by each entity.
- *Network Segmentation:* Network segmentation capabilities provide logically isolated network subsets that can be managed more efficiently and

effectively. Segmentation allows for a more detailed level of authorization and access, visibility into network flows among critical assets and infrastructure, and control of device management, and minimizes the potential harm from threats by isolating them to a limited part of the network.

In their letters of interest, responding organizations need to acknowledge the importance of and commit to provide:

1. Access for all participants' project teams to component interfaces and the organization's experts necessary to make functional connections among security platform components.

2. Support for development and demonstration of the *Cybersecurity for the Water and Wastewater Sector: A Practical Reference Design for Mitigating Cyber Risk in Water and Wastewater Systems* project, which will be conducted in a manner consistent with the following standards and guidance: FIPS 200, FIPS 201, SP 800–82 and SP 800–53, the NIST Cybersecurity Framework, and the NIST Privacy Framework.

Additional details about the *Cybersecurity for the Water and Wastewater Sector: A Practical Reference Design for Mitigating Cyber Risk in Water and Wastewater Systems* project are available at *www.nccoe.nist.gov/projects/securing-water-and-wastewater-utilities.*

NIST cannot guarantee that all the products proposed by respondents will be used in the demonstration. Each prospective participant will be expected to work collaboratively with NIST staff and other project participants under the terms of the NCCoE consortium CRADA in the development of the *Cybersecurity for the Water and Wastewater Sector: A Practical Reference Design for Mitigating Cyber Risk in Water and Wastewater Systems* project. Prospective participants' contribution to the collaborative effort will include assistance in establishing the necessary interface functionality, connection and set-up capabilities and procedures, demonstration harnesses, environmental and safety conditions for use, integrated platform user instructions, and demonstration plans and scripts necessary to demonstrate the desired capabilities. Each participant will train NIST personnel, as necessary, to operate its product in capability demonstrations. Following successful demonstrations, NIST will publish a description of the security platform and its performance characteristics sufficient to permit other organizations to develop and deploy security platforms that meet the security objectives of the *Cybersecurity for the Water and Wastewater Sector: A Practical Reference Design for Mitigating Cyber Risk in Water and Wastewater Systems* project. These descriptions will be public information. Under the terms of the NCCoE consortium CRADA, NIST will support development of interfaces among participants' products by providing IT infrastructure, laboratory facilities, office facilities, collaboration facilities, and staff support to component composition, security platform documentation, and demonstration activities.

The dates of the demonstration of *Cybersecurity for the Water and Wastewater Sector: A Practical Reference Design for Mitigating Cyber Risk in Water and Wastewater Systems* project capability will be announced on the NCCoE website at least two weeks in advance at *https://nccoe.nist.gov/.* The expected outcome will demonstrate how the components of the *Cybersecurity for the Water and Wastewater Sector: A Practical Reference Design for Mitigating Cyber Risk in Water and Wastewater Systems* project architecture can provide security capabilities to mitigate identified risks related to data throughout its lifecycle. Participating organizations will gain from the knowledge that their products are interoperable with other participants' offerings.

For additional information on the NCCoE governance, business processes, and NCCoE operational structure, visit the NCCoE website *https://nccoe.nist.gov/.*

Alicia Chambers,

NIST Executive Secretariat.

[FR Doc. 2023–13043 Filed 6–16–23; 8:45 am]

BILLING CODE 3510–13–P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

[RTID 0648–XD084]

Magnuson-Stevens Fishery Conservation and Management Act Provisions; Atlantic Coastal Fisheries Cooperative Management Act Provisions; General Provisions for Domestic Fisheries; Application for Exempted Fishing Permits

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

ACTION: Notice; request for comments.

SUMMARY: The Assistant Regional Administrator for Sustainable Fisheries, Greater Atlantic Region, NMFS, has made a preliminary determination that an Exempted Fishing Permit application contains all of the required information and warrants further consideration. The Exempted Fishing Permit would allow commercial fishing vessels to fish outside fishery regulations in support of research conducted by the applicant. Regulations under the Magnuson-Stevens Fishery Conservation and Management Act and the Atlantic Coastal Fisheries Cooperative Management Act require publication of this notification to provide interested parties the opportunity to comment on applications for proposed Exempted Fishing Permits.

DATES: Comments must be received on or before July 5, 2023.

ADDRESSES: You may submit written comments by the following method:

- *Email: nmfs.gar.efp@noaa.gov.* Include in the subject line ''NEFSC On-Demand Gear EFP.''

FOR FURTHER INFORMATION CONTACT: Laura Deighan, Fishery Management Specialist, *Laura.Deighan@noaa.gov,* (978) 281–9184.

SUPPLEMENTARY INFORMATION: The NOAA Northeast Fisheries Science Center submitted a complete application for an Exempted Fishing Permit (EFP) to conduct commercial fishing activities that the regulations would otherwise restrict to expand trials of on-demand fishing gear that uses one or no surface buoys and to test the ability of gear marking systems to consistently locate gear. This EFP would exempt the participating vessels from the gear marking requirements at 50 CFR 697.21(b)(2) to allow the use of trawls of more than three traps with no more than one surface marking and § 648.84(b) to allow the use of gillnet gear with no more than one surface marking. Exempted fishing activities would take place between August 21, 2023, and August 20, 2024.

The project is a continuation and expansion of the Center's efforts to trial on-demand fishing systems (also known as ropeless or buoyless) aimed at reducing entanglement risk to protected species, mainly the North Atlantic right whale, in trap/pot and gillnet fisheries. The Center's existing EFP will expire on August 21, 2023, and authorizes gear trials on up to 100 trap/pot vessels. As of March 2023, the Center had collected data from 707 hauls of on-demand gear in Federal waters under its current EFP. Of these, 267 hauls took place in Lobster Management Area (LMA) 3, 164 in LMA 2, and 276 in LMA 1. The Center reported two instances of gear loss or gear conflict. One incident involved a