were produced and/or exported by Conduit, Prolamsa, or Ternium.

Additionally, because the Department determined that Lamina y Placa and Mueller had no shipments of the subject merchandise, any suspended entries that entered under those companies' case numbers (*i.e.,* at those companies' rates) will be liquidated at the all-others rate effective during the period of review consistent with the Department's practice.[13]

Cash Deposit Requirements

The following cash deposit requirements will be effective upon publication of the notice of final results of administrative review for all shipments of subject merchandise entered, or withdrawn from warehouse, for consumption on or after the publication of the final results of this administrative review, as provided by section 751(a)(2) of the Act: (1) The cash deposit rates for Conduit, Maquilacero, Prolamsa, Regiopytsa, and Ternium will be the rates established in the final results of this administrative review; (2) for merchandise exported by producers or exporters not covered in this administrative review but covered in a prior segment of the proceeding, the cash deposit rate will continue to be the company-specific rate published for the most recent period; (3) if the exporter is not a firm covered in this review, a prior review, or the original investigation, but the producer is, the cash deposit rate will be the rate established for the most recent period for the producer of the merchandise; and (4) the cash deposit rate for all other producers or exporters will continue to be 32.62 percent, the all-others rate established in the investigation.[14] These cash deposit requirements, when imposed, shall remain in effect until further notice.

Notification to Importers

This notice 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 Secretary's presumption that reimbursement of antidumping duties occurred and the subsequent assessment of doubled antidumping duties.

[13] For a full discussion of this clarification, *see Antidumping and Countervailing Duty Proceedings: Assessment of Antidumping Duties,* 68 FR 23954 (May 6, 2003).

[14] *See Final Determination of Sales at Less Than Fair Value: Circular Welded Non-Alloy Steel Pipe from Mexico,* 57 FR 42953 (September 17, 1992).

Administrative Protective Order

This notice also serves as a reminder to parties subject to administrative protective orders (APO) of their responsibility concerning the return or destruction of proprietary information disclosed under APO in accordance with 19 CFR 351.305(a)(3), which continues to govern business proprietary information in this segment of the proceeding. Timely written notification of the return/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.

We are issuing and publishing this notice in accordance with sections 751(a)(1) and 777(i)(1) of the Act and 19 CFR 351.213(h).

Dated: June 6, 2017.

Ronald K. Lorentzen,

Acting Assistant Secretary for Enforcement and Compliance.

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

[FR Doc. 2017–12187 Filed 6–12–17; 8:45 am]

BILLING CODE 3510–DS–P

DEPARTMENT OF COMMERCE

International Trade Administration

[A–533–840]

Certain Frozen Warmwater Shrimp From India: Correction to the Initiation Notice of the 2016–2017 Antidumping Duty Administrative Review

AGENCY: Enforcement and Compliance, International Trade Administration, Department of Commerce.

FOR FURTHER INFORMATION CONTACT: Manuel Rey, Enforcement and Compliance, International Trade Administration, U.S. Department of Commerce, 1401 Constitution Avenue NW., Washington, DC 20230; telephone: (202) 482–5518.

SUPPLEMENTARY INFORMATION:

Background

On April 10, 2017, the Department of Commerce (the Department) published in the **Federal Register** notice of its initiation of the 2016–2017 administrative review of the antidumping duty order on certain frozen warmwater shrimp from India.[1] The period of review is February 1, 2016, through January 31, 2017. Subsequent to the publication of the initiation of this segment of the proceeding in the **Federal Register**, we identified inadvertent errors in the *Initiation Notice:.*

- First, the Department omitted from the *Initiation Notice* the following companies for which a review was requested: MTR Foods; Royale Marine Impex Pvt. Ltd.; and Sagar Foods.[2]
- Second, we initiated the review for Hindustan Lever, Ltd., a company for which no review was requested.[3]
- Third, we initiated the review on duplicate companies.[4]
- Finally, we made typographical errors in the name of several companies.[5]

The Department is hereby correcting the *Initiation Notice* to address these errors. This correction to the notice of initiation of administrative review is issued and published in accordance

[1] *See Initiation of Antidumping and Countervailing Duty Administrative Reviews,* 82 FR 17188 (April 10, 2017) (*Initiation Notice*).

[2] Because the Department received timely review requests for these companies, we now correct the *Initiation Notice* to initiate reviews for them.

[3] The Department did not receive a review request for this company; therefore, it should not have been included in the *Initiation Notice.* As a result, we now correct the *Initiation Notice* to remove this company name.

[4] These companies are as follows: Edhayam Frozen Foods Private Limited; Kadalkanny Frozen Foods; Kader Exports Private Limited; Kader Investment and Trading Company Private Limited; Kay Kay Exports (Kay Kay Foods); Liberty Frozen Foods Private Limited; Liberty Oil Mills Ltd.; Nila Sea Foods Exports; Satya Seafoods Private Limited; Universal Cold Storage Private Limited; and Usha Seafoods. These companies were either: (1) found in a previous segment of this proceeding to be part of a collapsed entity (*i.e.,* treated as a single entity for purposes of calculating antidumping duty rates); For (2) considered to be a name variation (*i.e.,* ''also known as'') of another company for which the Department also received a review request. Therefore, we have removed the duplicated instance of the names of these companies.

[5] The following names involved typographical errors: Exporter Coreline Exports Falcon Marine Exports Limited/K.R. Enterprises, Sprint Exports Pvt. Ltd. Sri Sakkthi Cold Storage, and Amarsagar Seafoods Exports Private Limited. The correct individual company names are Exporter Coreline Exports, Falcon Marine Exports Limited/K.R. Enterprises, Sprint Exports Pvt. Ltd., Sri Sakkthi Cold Storage, and Amarsagar Seafoods Private Limited.

with sections 751(a) and 777(i)(1) of the Tariff Act of 1930, as amended.

Dated: June 8, 2017.

Gary Taverman,

Deputy Assistant Secretary for Antidumping and Countervailing Duty Operations.

[FR Doc. 2017–12186 Filed 6–12–17; 8:45 am]

BILLING CODE 3510–DS–P

DEPARTMENT OF COMMERCE

National Telecommunications and Information Administration

[Docket No. 170602536–7536–01]

RIN 0660–XC035

Promoting Stakeholder Action Against Botnets and Other Automated Threats

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

ACTION: Notice, request for public comment.

SUMMARY: The National Telecommunications and Information Administration (NTIA), on behalf of the Department of Commerce (Department), is requesting comment on actions that can be taken to address automated and distributed threats to the digital ecosystem as part of the activity directed by the President in Executive Order 13800, ''Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.'' Through this Request for Comments (RFC), NTIA seeks broad input from all interested stakeholders—including private industry, academia, civil society, and other security experts—on ways to improve industry's ability to reduce threats perpetuated by automated distributed attacks, such as botnets, and what role, if any, the U.S. Government should play in this area.

DATES: Comments are due on or before 5 p.m. Eastern Time on July 13, 2017.

ADDRESSES: Written comments may be submitted by email to *counter_botnet_RFC@ntia.doc.gov.* Written comments also may be submitted by mail to the National Telecommunications and Information Administration, U.S. Department of Commerce, 1401 Constitution Avenue NW., Room 4725, Attn: Evelyn L. Remaley, Deputy Associate Administrator, Washington, DC 20230. For more detailed instructions about submitting comments, see the ''Instructions for Commenters'' section of **SUPPLEMENTARY INFORMATION**.

FOR FURTHER INFORMATION CONTACT: Megan Doscher, tel.: (202) 482–2503, email: *mdoscher@ntia.doc.gov*, or Allan Friedman, tel.: (202) 482–4281, email: *afriedman@ntia.doc.gov*, National Telecommunications and Information Administration, U.S. Department of Commerce, 1401 Constitution Avenue NW., Room 4725, Washington, DC 20230. Please direct media inquiries to NTIA's Office of Public Affairs, (202) 482–7002, or at *press@ntia.doc.gov.*

SUPPLEMENTARY INFORMATION:

Background: The open and distributed nature of the digital ecosystem has led to unprecedented growth and innovation in the digital economy. However, it has been accompanied by risks that threaten to undermine that very ecosystem. These risks take many forms online, with different combinations of threats, vulnerabilities, and affected parties from those in the physical world. The President has directed the Departments of Commerce and Homeland Security to jointly lead an open and transparent process to identify and promote action by appropriate stakeholders to improve the resilience of the Internet and communications ecosystem and to encourage collaboration with the goal of dramatically reducing threats perpetrated by automated and distributed attacks.[1] This RFC focuses on automated, distributed attacks that affect large sets of victims, and that put the broader network and its users at risk. These types of attacks have been a concern since the early days of the Internet,[2] and were a regular occurrence by the early 2000s.[3] Automated and distributed attacks, particularly botnets due to their ability to facilitate high-impact disruption, form a threat that is bigger than any one company or sector. Botnets are used for a variety of malicious activities, but distributed denial of service (DDoS) attacks, which can overwhelm other networked resources, are a critical threat and developing collaborative solutions to prevent and mitigate these attacks is a priority. As new scenarios emerge, including those exploiting a new generation of connected devices (so called ''Internet of Things'' (IoT) devices), there is an urgent need for coordination and collaboration across a diverse set of ecosystem stakeholders.

As part of this effort, the Department will also host a public workshop at the National Institute of Standards and Technology's National Cybersecurity Center of Excellence on July 11–12, 2017, entitled, ''Enhancing Resilience of the Communications Ecosystem.'' Outputs from this workshop will also help to guide implementation activities related to the President's Executive Order. More information about the workshop will be available on the NIST Web site at: *www.nist.gov.*

The Federal government has worked with stakeholders in the past to address new threats as they arise. Previous efforts include the White House-led Industry Botnet Group [4] (which led to an Anti-Botnet Code of Conduct [5]), the Communications Security, Reliability and Interoperability Council's (CSRIC) reports on ISP Network Protection Practices [6] and Remediation of Server-Based DDoS Attacks,[7] as well as the active and ongoing work by the Department of Justice and its many partners on attacking and ''sink-holing'' the infrastructure supporting these threats.[8] These initiatives, and others like them, underscore the need for active collaboration between the public and private sectors.

The Department has played an important role in facilitating engagement around cybersecurity between public policy interests and the innovative force of the private sector. The Department was tasked to work with industry to develop a framework

[1] *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,* Exec. Order 13800, 82 FR 22391 (May 11, 2017).

[2] *See generally United States* v. *Morris,* 928 F.2d 504 (2d Cir. 1991) (discussing one of the first known computer worms to spread across the Internet).

[3] *See* Nicholas C. Weaver, *Warhol Worms: The Potential for Very Fast Internet Plagues, Int'l Computer Science Inst.* (Aug. 15, 2001), *http://www1.icsi.berkeley.edu/~nweaver/papers/warhol/warhol.html.*

[4] U.S. Dep't of Commerce, *White House Announces Public-Private Partnership Initiatives to Combat Botnets* (May 30, 2012), *http://2010-2014.commerce.gov/news/press-releases/2012/05/30/white-house-announces-public-private-partnership-initiatives-combat-b.html.*

[5] Working Group 7—Botnet Remediation, Communications Security, Reliability and Interoperability Council III, *Final Report, U.S. Anti-Bot Code of Conduct (ABC) for Internet Services Providers (ISPs),* Barrier and Metric Considerations (Mar. 2013), *https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG7_Report_March_%202013.pdf.*

[6] Working Group 8, Communications Security, Reliability and Interoperability Council I, *Final Report, Internet Service Provider (ISP) Network Protection Practices* (Dec. 2010), *http://transition.fcc.gov/pshs/docs/csric/CSRIC_WG8_FINAL_REPORT_ISP_NETWORK_PROTECTION_20101213.pdf.*

[7] Working Group 5, Communications Security, Reliability and Interoperability Council IV Working Group 5, *Final Report, Remediation of Server-Based DDoS Attacks* (Sept. 2014), *https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG5_Remediation_of_Server-Based_DDoS_Attacks_Report_Final_(pdf)_V11.pdf.*

[8] *See, e.g.,* U.S. Dep't of Justice, *Avalanche Network Dismantled in International Cyber Operation* (Dec. 5, 2016), *https://www.justice.gov/opa/pr/avalanche-network-dismantled-international-cyber-operation.*