| Company | 2014 *Ad Valorem* rate |
|---|---|
| Hyundai Steel Company Ltd | 0.23 percent *ad valorem* (*de minimis*). |

**Disclosure**

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

**Assessment Rates**

In accordance with 19 CFR 351.212(b)(2), the Department intends to issue assessment instructions to U.S. Customs and Border Protection (CBP) 15 days after the date of publication of these final results to liquidate shipments of subject merchandise produced by DSM and Hyundai Steel entered, or withdrawn form warehouse, for consumption on or after January 1, 2014, through December 31, 2014, without regard to CVDs because a *de minimis* subsidy rate was calculated for each company.

**Cash Deposit Instructions**

The Department also intends to instruct CBP to collect cash deposits of zero percent on shipments of the subject merchandise produced and/or exported by DSM and Hyundai Steel entered or withdrawn from warehouse, for consumption on or after the date of publication of the final results of this review. For all non-reviewed firms, we will instruct CBP to collect cash deposits of estimated countervailing duties at the most recent company-specific or all-others rate applicable to the company. These cash deposit requirements, when imposed, shall remain in effect until further notice.

**Return or Destruction of Proprietary Information**

This notice also serves as a 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/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 these final results in accordance with sections 751(a)(1) and 777(i)(1) of the Act.

Dated: September 12, 2016.

**Ronald K. Lorentzen,**

*Acting Assistant Secretary for Enforcement and Compliance.*

**Appendix**



[FR Doc. 2016–22403 Filed 9–16–16; 8:45 am]

**BILLING CODE 3510–DS–P**

## DEPARTMENT OF COMMERCE

### National Telecommunications and Information Administration

### Multistakeholder Process on Internet of Things Security Upgradability and Patching

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

**ACTION:** Notice of open meeting.

**SUMMARY:** The National Telecommunications and Information Administration (NTIA) will convene meetings of a multistakeholder process concerning Internet of Things Security Upgradability and Patching. This Notice announces the first meeting, which is scheduled for October 19, 2016.

**DATES:** The meeting will be held on October 19, 2016, from 10:00 a.m. to 4:00 p.m., Central Daylight Time.

**ADDRESSES:** The meeting will be held in the Trinity Ballroom at the Renaissance Austin Hotel, 9721 Arboretum Boulevard, Austin, Texas 78759.

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

**SUPPLEMENTARY INFORMATION:**

*Background:* In March of 2015 the National Telecommunications and Information Administration issued a Request for Comment to ''identify substantive cybersecurity issues that affect the digital ecosystem and digital economic growth where broad consensus, coordinated action, and the development of best practices could substantially improve security for organizations and consumers.'' [1] We received comments from a range of stakeholders, including trade associations, large companies, cybersecurity startups, civil society organizations and independent computer security experts.[2] The comments recommended a diverse set of issues that might be addressed through the multistakeholder process, including cybersecurity policy and practice in the emerging area of Internet of Things (IoT).

In a separate but related matter in April 2016, NTIA, the Department's Internet Policy Task Force, and its Digital Economy Leadership Team sought comments on the benefits, challenges, and potential roles for the government in fostering the advancement of the Internet of Things.'' [3] Over 130 stakeholders responded with comments addressing many substantive issues and

[1] U.S. Department of Commerce, Internet Policy Task Force, Request for Public Comment, Stakeholder Engagement on Cybersecurity in the Digital Ecosystem, 80 FR 14360, Docket No. 150312253–5253–01 (Mar. 19, 2015), *available at: https://www.ntia.doc.gov/files/ntia/publications/cybersecurity_rfc_03192015.pdf.*

[2] NTIA has posted the public comments received at *https://www.ntia.doc.gov/federal-register-notice/2015/comments-stakeholder-engagement-cybersecurity-digital-ecosystem.*

[3] U.S. Department of Commerce, Internet Policy Task Force, Request for Public Comment, Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things, 81 FR 19956, Docket No. 160331306–6306–01 (April 5, 2016), *available at: https://www.ntia.doc.gov/federal-register-notice/2016/rfc-potential-roles-government-fostering-advancement-internet-of-things.*

opportunities related to IoT.[4] Security was one of the most common topics raised.

Many commenters emphasized the need for a secure lifecycle approach to IoT devices that considers the development, maintenance, and end-of-life phases and decisions for a device. On August 2, 2016, after reviewing these comments, NTIA announced that the next multistakeholder process on cybersecurity would be on IoT security upgradability and patching.[5]

The matter of patching vulnerable systems is now an accepted part of cybersecurity.[6] Unaddressed technical flaws in systems leave the users of software and systems at risk. The nature of these risks varies, and mitigating these risks requires various efforts from the developers and owners of these systems. One of the more common means of mitigation is for the developer or other maintaining party to issue a security patch to address the vulnerability. Patching has become more commonly accepted, even for consumers, as more operating systems and applications shift to visible reminders and automated updates. Yet as one security expert notes, this evolution of the software industry has yet to become the dominant model in IoT.[7]

To help realize the full innovative potential of IoT, users need reasonable assurance that connected devices, embedded systems, and their applications will be secure. A key part of that security is the mitigation of potential security vulnerabilities in IoT devices or applications through patching and security upgrades.

The ultimate objective of the multistakeholder process is to foster a market offering more devices and systems that support security upgrades through increased consumer awareness and understanding. Enabling a thriving market for patchable IoT requires common definitions so that manufacturers and solution providers have shared visions for security, and consumers know what they are purchasing. Currently, no such common, widely accepted definitions exist, so many manufacturers struggle to effectively communicate to consumers the security features of their devices. This is detrimental to the digital ecosystem as a whole, as it does not reward companies that invest in patching and it prevents consumers from making informed purchasing choices.

The immediate goal of this process will be to develop a broad, shared definition or set of definitions around security upgradability for consumer IoT, as well as strategies for communicating the security features of IoT devices to consumers. One initial step will be to explore and map out the many dimensions of security upgradability and patching for the relevant systems and applications. A goal will be to design and explore definitions that are easily understandable, while being backed by technical specifications and organizational practices and processes. A final step will be to develop a strategy to share these definitions throughout the broader development community, and ultimately with consumers. This may include raising awareness in the consumer space to help consumers understand security options and drive market forces.

Stakeholders will determine the shape of the conversation and the process. NTIA has announced that the scope of the discussion will be around consumer devices, but stakeholders will ultimately determine which technologies, sectors, and applications will be discussed in the process, and covered by the resulting definitions and framework.

While we anticipate a technical discussion in the process of exploring security upgrades, NTIA does not expect this discussion to develop new technical standards. This multistakeholder process is not a formal standards development process. Stakeholders may wish to use existing standards in their discussion and definitions, or may wish to call for new standards or standards processes as part of their recommendations.

Stakeholders will determine the exact nature of the outcome of this process. Because it is unlikely that a one-size-fits-all solution will be feasible in this dynamic space, stakeholders will need to determine how to scope and organize the work through sub-groups or other means. Success of the process will be evaluated by the extent to which stakeholders embrace and implement the consensus findings within their individual practices or organizations, and work to promulgate them throughout the community. Although the stakeholders determine the outcome of the process, it is important to note that the process will not result in a new law or regulation.

*Matters to Be Considered:* The October 19, 2016, meeting will be the first in a series of NTIA-convened multistakeholder discussions concerning IoT security upgradability and patching. Subsequent meetings will follow on a schedule determined by those participating in the first meeting. Stakeholders will engage in an open, transparent, consensus-driven process to understand the range of issues in security upgradability, and develop a set of definitions useful to both industry and consumers. The multistakeholder process will involve hearing and understanding the perspectives of diverse stakeholders, including a range of IoT manufacturers, solution providers, security experts, and consumer advocates.

The October 19, 2016, meeting is intended to bring stakeholders together to share the range of views on security upgradability and patching, and to establish more concrete goals and structure of the process. The objectives of this first meeting are to: (1) Briefly review the importance of patching and the challenges in the existing ecosystem; (2) briefly share different perspectives on existing technologies and practices; (3) engage stakeholders in a discussion of key security upgrade dimensions, features, and concerns; (4) engage stakeholders in a discussion of logistical issues, including internal structures such as a small drafting committee or various working groups, and the location and frequency of future meetings; and (5) identify concrete goals and stakeholder work following the first meeting.

The main objective of further meetings will be to encourage and facilitate continued discussion among stakeholders to build out a mapping of the range of issues, and develop a consensus view of a consolidated set of potential definitions. Discussions will also cover best practices for sharing security information with consumers. This discussion may include circulation of stakeholder-developed strawman drafts and discussion of the appropriate scope of the initiative. Stakeholders may also agree on procedural work plans for the group, including additional meetings or modified logistics for future meetings. NTIA suggests that stakeholders consider setting clear deadlines for a working draft and a phase for external review of this draft,

[4] NTIA has posted the public comments received at *https://www.ntia.doc.gov/federal-register-notice/2016/comments-potential-roles-government-fostering-advancement-internet-of-things.*

[5] NTIA, *Increasing the Potential of IoT through Security and Transparency* (Aug. 2, 2016), *available at: https://www.ntia.doc.gov/blog/2016/increasing-potential-iot-through-security-and-transparency.*

[6] *See, e.g.* Murugiah Souppaya and Karen Scarfone, *Guide to Enterprise Patch Management Technologies, Special Publication 800–40 Revision 3,* National Institute of Standards and Technology, NIST SP 800–40 (2013) *available at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf.*

[7] Bruce Schneier, *The Internet of Things Is Wildly Insecure—And Often Unpatchable,* Wired (Jan. 6, 2014) *available at: https://www.schneier.com/blog/archives/2014/01/security_risks_9.html.*

before reconvening to take account of external feedback.

More information about stakeholders' work will be available at: *https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security.*

*Time and Date:* NTIA will convene the first meeting of the multistakeholder process on IoT Security Upgradability and Patching on October 19, 2016, from 10:00 a.m. to 4:00 p.m., Central Daylight Time. Please refer to NTIA's Web site, *https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security*, for the most current information.

*Place:* The meeting will be held in the Trinity Ballroom at the Renaissance Austin Hotel, 9721 Arboretum Boulevard, Austin, Texas 78759. The location of the meeting is subject to change. Please refer to NTIA's Web site, *https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security*, for the most current information.

*Other Information:* The meeting is open to the public and the press on a first-come, first-served basis. Space is limited. To assist the agency in determining space and webcast technology requirements, NTIA requests that interested persons pre-register for the meeting at *https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security.*

The meeting is physically accessible to people with disabilities. Requests for sign language interpretation or other auxiliary aids should be directed to Allan Friedman at (202) 482–4281 or *afriedman@ntia.doc.gov* at least seven (7) business days prior to each meeting. The meetings will also be webcast. Requests for real-time captioning of the webcast or other auxiliary aids should be directed to Allan Friedman at (202) 482–4281 or *afriedman@ntia.doc.gov* at least seven (7) business days prior to each meeting. There will be an opportunity for stakeholders viewing the webcast to participate remotely in the meetings through a moderated conference bridge, including polling functionality. Access details for the meetings are subject to change. Please refer to NTIA's Web site, *http://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security,* for the most current information.

Dated: September 14, 2016.

**Kathy D. Smith,**

*Chief Counsel, National Telecommunications and Information Administration.*

[FR Doc. 2016–22459 Filed 9–16–16; 8:45 am]

**BILLING CODE 3510–60–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 October 19, 2016.

**ADDRESSES:** Comments regarding the burden estimated 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 the notice's publication, by email at *OIRAsubmissions@omb.eop.gov.* Please identify the comments by OMB Control No. 3038–0102. Please provide the Commodity Futures Trading Commission (''CFTC'' or ''Commission'') with a copy of all submitted comments at the address listed below. Please refer to OMB Control No. 3038–0102, found on *http://reginfo.gov.*

Comments may also be mailed 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, or submitted through the Commission's Web site at *http://comments.cftc.gov.* Follow the instructions for submitting comments through the Web site.

Comments may also be mailed to: Christopher Kirkpatrick, Secretary of the Commission, Commodity Futures Trading Commission, Three Lafayette Centre, 1155 21st Street NW., Washington, DC 20581 or by Hand Delivery/Courier at the same address.

A copy of the supporting statements for the collection of information discussed above 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.*

**FOR FURTHER INFORMATION CONTACT:** Melissa D'Arcy, Special Counsel, Division of Clearing and Risk, Commodity Futures Trading Commission, Three Lafayette Centre, 1155 21st Street NW., Washington, DC 20581; (202) 418–5086; email: *mdarcy@cftc.gov,* and refer to OMB Control No. 3038–0102.

**SUPPLEMENTARY INFORMATION:**

*Title:* ''Clearing Exemption for Certain Swaps Entered into by Cooperatives,'' (OMB Control No. 3038–0102). This is a request for extension of a currently approved information collection.

*Abstract:* Section 2(h)(1)(A) of the Commodity Exchange Act requires certain entities to submit for clearing certain swaps if they are required to be cleared by the Commission. Commission regulation 50.51 permits certain cooperatives to elect not to clear certain swaps that otherwise would be required to be cleared, provided that they meet certain conditions. The rule further requires the reporting of certain information if the exemption for cooperatives is elected. This collection pertains to information the Commission needs to monitor use of the cooperative exemption and assess market risk in connection therewith. An agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid OMB control number.

*Burden Statement:* The Commission is revising its estimate of the burden for this collection to reflect the current number of respondents and respondent burden. The respondent burden for this collection is estimated to be as follows:

*Respondents/Affected Entities:* Parties electing the cooperative exemption under Commission regulation 50.51.

*Estimated Number of Respondents:* 25.

*Estimated Average Burden Hours per Respondent:* 1 hour.

*Estimated Total Annual Burden Hours on Respondents:* 25 hours.

*Frequency of Collection:* Annually; on occasion.

There are no capital costs or operating and maintenance costs associated with this collection.

**Authority:** 44 U.S.C. 3501 *et seq.*

Dated: September 14, 2016.

**Robert N. Sidman,**

*Deputy Secretary of the Commission.*

[FR Doc. 2016–22481 Filed 9–16–16; 8:45 am]

**BILLING CODE 6351–01–P**