| Friday, Sep 21, 2018 .... | • Site visit to a U.S. OEM (*e.g.*: Oceaneering or GE Wellstream—TBD).
• Mission participants lunch.
• One group meeting with another oil company (*e.g.*: Shell—TBD).
• Evening Departure (**). |

(**) As an option, trade mission participants may stay over the weekend and attend at least one day of the Rio Oil and Gas Trade Show that will take place from September 24–27, 2018. There is no additional costs to the participation fee for the optional trade show participation. There is free transportation offered by the show organizers to and from the conference grounds. All additional costs that TM participants will have do not apply to the TM participation fee.

Participation Requirements

Recruitment for the mission will begin immediately and conclude no later than July 30, 2018. All parties interested in participating in the trade mission must complete and submit an application package for consideration by the Department of Commerce. All applications must be submitted before July 30, 2018. The Department of Commerce will evaluate all applications and inform applicants of selection decisions as soon as possible after this application deadline.

Applications received after July 30, 2018, will be considered only if space and scheduling constraints permit.

Fees and Expenses

After a company or organization has been selected to participate in the mission, a payment to the Department of Commerce in the form of a participation fee is required. The participation fee for the Trade Mission will be $2,010 for a small or medium-sized firm (SME), and $2,320 for large firms. The fee for each additional firm representative (large firm or SME/trade organization) is USD $750.00.

Participants selected for the Trade Mission will be expected to pay for the cost of all personal expenses, including, but not limited to, international travel, lodging, meals, transportation, communication, and incidentals, unless otherwise noted. In the event that the Mission is cancelled, no personal expenses paid in anticipation of a Trade Mission will be reimbursed. However, participation fees for a cancelled Trade Mission will be reimbursed to the extent they have not already been expended in the anticipation of the Mission.

Participants will be able to take advantage of U.S. Government rates for hotel rooms. Business or entry visas may be required to participate in the mission. Applying for and obtaining such visas will be the responsibility of the mission participant. Government fees and processing expenses to obtain such visas are not included in the participation fee. However, the Department of Commerce will provide instructions to each participant on the procedures required to obtain necessary business visas.

Timeframe for Recruitment and Application

Mission recruitment will be conducted in an open and public manner, including publication in the **Federal Register**, posting on the Commerce Department trade mission calendar (*http://export.gov/trademissions*) and other Internet Web sites, press releases to general and trade media, direct mail, notices by industry trade associations and other multiplier groups, and publicity at industry meetings, symposia, conferences, and trade shows.

Recruitment for the mission will begin immediately and conclude no later than July 30, 2018. Applications received after July 30, 2018, will be considered only if space and scheduling constraints permit.

Contacts

Regina Cunha, Senior Commercial Specialist, U.S. Department of Commerce, Address: U.S. Consulate General. Avenida Presidente Wilson 147. Centro, Rio de Janeiro. Brazil. Tel.: # +55 21 38232416, Email: *regina.cunha@trade.gov*.

Rodrigo Correa, Commercial Assistant, U.S. Department of Commerce, Address: U.S. Consulate General. Avenida Presidente Wilson 147. Centro, Rio de Janeiro. Brazil. Tel.: # +55 21 38232406, Email: *rodrigo.correa@trade.gov*.

Stefan Popescu, Commercial Specialist, CS Toronto, Tel: 1 416–595–5412 x223, *Stefan.Popescu@trade.gov*.

Connie Irrera, Commercial Specialist, CS Montreal, Tel: 1 514–908–3662, *Connie.Irrera@trade.gov*.

Julius Svoboda, Senior Oil & Gas Trade Specialist, U.S. Department of Commerce, Address: 1401 Constitution Ave., Tel.: +1–202–482–5430, Email: *Julius.Svoboda@trade.gov*.

Frank Spector,
Senior Advisor for Trade Missions.
[FR Doc. 2017–16082 Filed 7–31–17; 8:45 am]
BILLING CODE 3510–DR–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 a meeting of a multistakeholder process on Internet of Things Security Upgradability and Patching on September 12, 2017.

DATES: The meeting will be held on September 12, 2017, from 10:00 a.m. to 4:00 p.m., Eastern Time. See **SUPPLEMENTARY INFORMATION** for details.

ADDRESSES: The meeting will be held at the American Institute of Architects, 1735 New York Ave. NW., Washington, DC 20006.

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

---

[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.*

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 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.

After reviewing these comments, NTIA announced that the next multistakeholder process on cybersecurity would be on IoT security upgradability and patching.[5] The first meeting of a multistakeholder process on this topic was held on October 19, 2016.[6] Subsequent meetings were held on January 31, 2017,[7] April 26, 2017,[8] and July 18, 2017.[9]

The matter of patching vulnerable systems is now an accepted part of cybersecurity.[10] 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.[11]

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.

Stakeholders have identified four distinct work streams that could help foster better security across the ecosystem, and focused their efforts in four working groups addressing both technical and policy issues.[12] The main objectives of the September 12, 2017, meeting are to discuss stakeholder comments on draft working group documents and, where possible, to finalize working group documents. More information about stakeholders' work is available at: *https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security.*

Time and Date: NTIA will convene a meeting of the multistakeholder process on Internet of Things Security Upgradability and Patching on September 12, 2017, from 10:00 a.m. to 4:00 p.m., Eastern Time. The meeting date and time are 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.

Place: The meeting will be held at the American Institute of Architects, 1735 New York Ave. NW., Washington, DC 20006. 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. 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 the meeting. The meeting 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 the meeting. There will be an opportunity for stakeholders viewing the webcast to

[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.*

[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] NTIA, Notice of Multistakeholder Process on Internet of Things Security Upgradability and Patching Open Meeting (Sept. 15, 2016), *available at: https://www.ntia.doc.gov/federal-register-notice/2016/10192016-meeting-notice-msp-iot-security-upgradability-patching.*

[7] NTIA, Notice of 01/31/2017 Meeting of the Multistakeholder Process on Internet of Things Security Upgradability and Patching (January 11, 2017), available at *https://www.ntia.doc.gov/federal-register-notice/2017/notice-01312017-meeting-multistakeholder-process-internet-things.*

[8] NTIA, Notice of 04/26/2017 Meeting of the Multistakeholder Process on Internet of Things Security Upgradability and Patching, available at *https://www.ntia.doc.gov/federal-register-notice/2017/notice-04262017-meeting-multistakeholder-process-internet-things.*

[9] NTIA, Notice of 07/18/2017 Meeting of the Multistakeholder Process on Internet of Things Security Upgradability and Patching, available at *https://www.ntia.doc.gov/federal-register/2017/notice-07182017-iot-security-virtual-meeting.*

[10] *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.*

[11] 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.*

[12] Documents shared by working group stakeholders are *available at: https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security.*

participate remotely in the meeting through a moderated conference bridge, including polling functionality. Access details for the meeting are 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.

Dated: July 27, 2017.

Kathy D. Smith,

Chief Counsel, National Telecommunications and Information Administration.

[FR Doc. 2017–16155 Filed 7–31–17; 8:45 am]

BILLING CODE 3510–60–P

DEPARTMENT OF COMMERCE

National Telecommunications and Information Administration

Community Broadband Workshop

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

ACTION: Notice of Open Meeting.

SUMMARY: The National Telecommunications and Information Administration (NTIA), through the BroadbandUSA program, will hold a Technical Assistance Workshop to share information and help communities build their broadband capacity and utilization. The workshop will present in-depth sessions on planning and funding broadband infrastructure projects. The session on planning will explore effective business and partnership models. The session on funding will explore available funding options and models, including federal funding.

DATES: The Technical Assistance Workshop will be held on Tuesday, September 19, 2017, from 8:30 a.m. to 12:30 p.m., Eastern Daylight Time.

ADDRESSES: The meeting will be held in Charleston, West Virginia at the Law Firm of Jackson Kelly PLLC, 500 Lee Street East, Suite 1600, Rooms A and B, Charleston, WV 25301.

FOR FURTHER INFORMATION CONTACT: Giselle Sanders, National Telecommunications and Information Administration, U.S. Department of Commerce, Room 4889, 1401 Constitution Avenue, NW., Washington, DC 20230; telephone: (202) 482–7971; email: *gsanders@ntia.doc.gov.* Please direct media inquiries to NTIA's Office of Public Affairs, (202) 482–7002; email: *press@ntia.doc.gov.*

SUPPLEMENTARY INFORMATION: NTIA's BroadbandUSA program provides expert advice and field-proven tools for assessing broadband adoption, planning new infrastructure, and engaging a wide range of partners in broadband projects. BroadbandUSA convenes workshops on a regular basis to bring stakeholders together to discuss ways to improve broadband policies, share best practices, and connect communities to other federal agencies and funding sources for the purpose of expanding broadband infrastructure and adoption throughout America's communities. The Charleston workshop will explore two specific topics for broadband infrastructure: Planning and funding.

The Charleston workshop will feature subject matter experts from NTIA's BroadbandUSA broadband program. The first session will explore key elements required for planning successful broadband projects. The second session will explore funding models, including federal programs that fund broadband infrastructure projects.

The Charleston workshop will be open to the public. Pre-registration is requested, and space is limited. NTIA will ask registrants to provide their first and last names and email addresses for both registration purposes and to receive any updates on the workshop. If capacity for the meeting is reached, NTIA will maintain a waiting list and will inform those on the waiting list if space becomes available. Meeting updates, changes in the agenda, if any, and relevant documents will also be available on NTIA's Web site at *https://www2.ntia.doc.gov/notice-09192017-workshop.*

The public meeting is physically accessible to people with disabilities. Individuals requiring accommodations, such as language interpretation or other ancillary aids, are asked to notify Giselle Sanders at the contact information listed above at least five (5) business days before the meeting.

Dated: July 27, 2017.

Kathy D. Smith,

Chief Counsel, National Telecommunications and Information Administration.

[FR Doc. 2017–16154 Filed 7–31–17; 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 August 31, 2017.

ADDRESSES: Comments regarding the burden estimate 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 this notice's publication by either of the following methods. Please identify the comments by ''OMB Control No. 3038–0081''.

• *By email addressed to: OIRAsubmissions@omb.eop.gov* or

• *By mail addressed 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.

A copy of all comments submitted to OIRA should be sent to the Commodity Futures Trading Commission (the ''Commission'') by either of the following methods. The copies should refer to ''OMB Control No. 3038–0081''.

• *By mail addressed to:* Christopher Kirkpatrick, Secretary of the Commission, Commodity Futures Trading Commission, Three Lafayette Centre, 1155 21st Street NW., Washington, DC 20581;

• *By Hand Delivery/Courier to the same address;* or

• Through the Commission's Web site at *http://comments.cftc.gov.* Please follow the instructions for submitting comments through the Web site.

A copy of the supporting statement for the collection of information discussed herein 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.* You should submit only information that you wish to make available publicly. If you wish the Commission to consider information that you believe is exempt from disclosure under the Freedom of Information Act, a petition for confidential treatment of the exempt information may be submitted according to the procedures established in § 145.9 of the Commission's regulations.[1] The

---

[1] 17 CFR 145.9.