

Dated: August 25, 2015.

**Julia Harrison,**

Chief, Permits and Conservation Division,  
Office of Protected Resources, National  
Marine Fisheries Service.

[FR Doc. 2015-21390 Filed 8-28-15; 8:45 am]

BILLING CODE 3510-22-P

## DEPARTMENT OF COMMERCE

### National Telecommunications and Information Administration

#### Multistakeholder Process To Promote Collaboration on Vulnerability Research Disclosure

**AGENCY:** National Telecommunications  
and Information Administration,  
Commerce.

**ACTION:** Notice of open meeting.

**SUMMARY:** The National  
Telecommunications and Information  
Administration (NTIA) will convene  
meetings of a multistakeholder process  
concerning the collaboration between  
security researchers and software and  
system developers and owners to  
address security vulnerability  
disclosure. This Notice announces the  
first meeting, which is scheduled for  
September 29, 2015.

**DATES:** The meeting will be held on  
September 29, 2015, from 9:00 a.m. to  
3:00 p.m., Pacific Time. See  
**SUPPLEMENTARY INFORMATION** for details.

**ADDRESSES:** The meeting will be held in  
the Booth Auditorium at the University  
of California, Berkeley, School of Law,  
Boalt Hall, Bancroft Way and Piedmont  
Avenue, Berkeley, CA 94720-7200.

#### 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](mailto:afriedman@ntia.doc.gov). Please direct  
media inquiries to NTIA's Office of  
Public Affairs, (202) 482-7002; email  
[press@ntia.doc.gov](mailto:press@ntia.doc.gov).

#### SUPPLEMENTARY INFORMATION:

*Background:* On March 19, 2015, the  
National Telecommunications and  
Information Administration, working  
with the Department of Commerce's  
Internet Policy Task Force (IPTF),  
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."<sup>1</sup> This  
Request built on earlier work from the  
Department, including the 2011 Green  
Paper *Cybersecurity, Innovation, and  
the Internet Economy*,<sup>2</sup> as well as  
comments the Department had received  
on related issues.<sup>3</sup>

The IPTF asked for suggestions of  
security challenges that an NTIA-  
convened multistakeholder group could  
address, and offered a dozen potential  
topics for explicit feedback.<sup>4</sup> We  
received 35 comments from a range of  
stakeholders, including trade  
associations, large companies,  
cybersecurity startups, civil society  
organizations and independent  
computer security experts.<sup>5</sup> The  
comments highlight a range of issues  
that might be addressed through the  
multistakeholder process and suggest  
various ways in which the group's work  
could be structured.

Of the topics suggested, the challenge  
of collaboration between security  
researchers and system and software  
vendors stands out as a critical issue  
where reaching some consensus on  
shared goals, principles, and practices is  
both feasible and necessary. On July 9,  
2015, after reviewing the comments,  
NTIA announced that the first issue to  
be addressed would be "collaboration  
on vulnerability research disclosure."<sup>6</sup>  
While this is not the first discussion on  
the topic, stakeholders have presented  
the case that the time is right to make  
further progress among ecosystem  
players by achieving consensus and a  
commitment to baseline principles and  
accepted practices.

This issue is commonly referred to as  
the question of "vulnerability  
disclosure." For as long as humans have

<sup>1</sup> 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:  
[http://www.ntia.doc.gov/files/ntia/publications/  
cybersecurity\\_rfc\\_03192015.pdf](http://www.ntia.doc.gov/files/ntia/publications/cybersecurity_rfc_03192015.pdf).

<sup>2</sup> U.S. Department of Commerce, Internet Policy  
Task Force, *Cybersecurity, Innovation, and the  
Internet Economy* (June 2011) (Green Paper),  
available at: [http://www.nist.gov/itl/upload/  
Cybersecurity\\_Green-Paper\\_FinalVersion.pdf](http://www.nist.gov/itl/upload/Cybersecurity_Green-Paper_FinalVersion.pdf).

<sup>3</sup> See Comments Received in Response to **Federal  
Register** Notice Developing a Framework for  
Improving Critical Infrastructure Cybersecurity,  
Docket No. 140721609-4609-01, available at:  
[http://csrc.nist.gov/cyberframework/rfi\\_comments\\_  
10\\_2014.html](http://csrc.nist.gov/cyberframework/rfi_comments_10_2014.html).

<sup>4</sup> Request for Public Comment, *supra* note 1.

<sup>5</sup> NTIA has posted the public comments received  
at [http://www.ntia.doc.gov/federal-register-notice/  
2015/comments-stakeholder-engagement-  
cybersecurity-digital-ecosystem](http://www.ntia.doc.gov/federal-register-notice/2015/comments-stakeholder-engagement-cybersecurity-digital-ecosystem).

<sup>6</sup> NTIA, *Enhancing the Digital Economy Through  
Collaboration on Vulnerability Research Disclosure*  
(July 9, 2015), available at: [http://  
www.ntia.doc.gov/blog/2015/enhancing-digital-  
economy-through-collaboration-vulnerability-  
research-disclosure](http://www.ntia.doc.gov/blog/2015/enhancing-digital-<br/>economy-through-collaboration-vulnerability-<br/>research-disclosure).

created software there have been  
software "bugs."<sup>7</sup> Many of these bugs  
can introduce vulnerabilities, leaving  
the users of the systems and software at  
risk. The nature of these risks vary, and  
mitigating these risks requires various  
efforts from the developers and owners  
of these systems. Security researchers of  
all varieties, including academics,  
professionals, and those who simply  
enjoy thinking about security may  
identify these bugs for a number of  
reasons, and in a wide range of contexts.  
How researchers should handle these  
vulnerabilities, and how vendors should  
work with researchers has been the  
matter of active debate for many years,  
since before the turn of the  
millennium.<sup>8</sup> Several points have been  
actively debated. Researchers have  
expressed concerns that vendors do not  
respond in a timely fashion, leaving  
users at risk. Vendors worry about the  
time, expense, and added complexity of  
addressing every vulnerability, as well  
as the risks introduced by potentially  
disclosing vulnerabilities before they  
can be patched or mitigated. Given that  
all good faith actors care about security,  
there is room to find common ground.

The goal of this process is neither to  
replicate past discussions nor duplicate  
existing initiatives. As information  
security is gaining more attention in the  
collective consciousness due to a series  
of high profile cybersecurity incidents  
and disclosed vulnerabilities, more  
firms and organizations are considering  
how to engage with third party  
researchers, just as they are exploring  
other security tools and processes. The  
security community itself has worked to  
promote better collaboration. More  
software vendors and system owners are  
offering "bug bounty" programs that  
reward researchers for sharing  
vulnerability information. In addition to  
enterprises that buy vulnerabilities and  
sell them to vendors, new business  
models have emerged to help  
organizations develop and manage bug  
bounty programs. Leading experts at the  
International Standards Organization  
have developed, and are continuing to  
revise, a formal standard for vendors on  
how to manage incoming vulnerability

<sup>7</sup> See, e.g., Peter Wayner, *Smithsonian Honors the  
Original Bug in the System*, N.Y. Times (Dec. 7,  
1997), available at: [http://www.nytimes.com/  
library/cyber/week/120497bug.html](http://www.nytimes.com/<br/>library/cyber/week/120497bug.html).

<sup>8</sup> For a bibliography of research, proposed  
standards, online discussions and other resources,  
see University of Oulu Secure Programming Group,  
Juhani Eronen & Ari Takanen eds., *Vulnerability  
Disclosure Publications and Discussion Tracking*,  
available at: [https://www.ee.oulu.fi/research/ouspg/  
Disclosure\\_tracking](https://www.ee.oulu.fi/research/ouspg/<br/>Disclosure_tracking) (last visited Aug. 20, 2015).

information.<sup>9</sup> NTIA's process is meant to complement these ongoing developments, as well as existing standards and practices developed by other organizations, by bringing together all relevant stakeholders to find consensus on the overarching goals and principles for successful sharing and handling of vulnerability information. By coming together at this critical juncture, stakeholders can expand norms and expectations for the adoption, adaptation, and innovation of practices and standards.

The goal of this process will be to develop a broad, shared understanding of the overlapping interests between security researchers and the vendors and owners of products discovered to be vulnerable, and establish a consensus about voluntary principles to promote better collaboration. The question of how vulnerabilities can and should be disclosed will be a critical part of the discussion, as will how vendors receive and respond to this information. However, disclosure is only one aspect of successful collaboration. One goal of the overall NTIA process is to promote a digital economy that more strongly emphasizes security and develops community-driven or market-based forces to better and more rapidly secure the digital ecosystem.

Stakeholders will determine the exact nature of the outcome of this process. Since 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. Although the stakeholders determine the outcome of the process, it is important to note that the process will not result in a regulatory policy or new law, nor focus on law enforcement or other non-commercial government use of vulnerability data.

**Matters To Be Considered:** The September 29, 2015, meeting will be the first in a series of NTIA-convened multistakeholder discussions concerning collaboration on vulnerability disclosure. 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 develop voluntary principles guiding the collaboration

between vendors and researchers about vulnerability information. The multistakeholder process will involve hearing and understanding the perspectives of diverse stakeholders, from a wide range of both vendors and researchers, while seeking a consensus that enables collaboration for a more secure digital ecosystem.

The September 29, 2015, meeting is intended to bring stakeholders together to begin to share the range of views on how vulnerability information is shared by researchers, how it is received and used by vendors, and to establish more concrete goals and structure of the process. The objectives of this first meeting are to: (1) Briefly share different perspectives on how vulnerability information is shared, received, and resolved; (2) briefly review perceived challenges in successful collaborations; (3) engage stakeholders in a discussion of high-priority substantive issues stakeholders believe should be addressed; (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 consensus around the principles guiding successful collaboration. This discussion may include circulation of stakeholder-developed straw-man 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 consider a phase for external review of this draft, before reconvening to take account of external feedback.

More information about stakeholders' work will be available at: <http://www.ntia.doc.gov/other-publication/2015/multistakeholder-process-cybersecurity-vulnerabilities>.

**Time and Date:** NTIA will convene the first meeting of the multistakeholder process to promote collaboration on vulnerability research disclosure on September 29, 2015, from 9:00 a.m. to 3:00 p.m., Pacific Time. Please refer to NTIA's Web site, <http://www.ntia.doc.gov/other-publication/2015/multistakeholder-process-cybersecurity-vulnerabilities>, for the most current information.

**Place:** The meeting will be held in the Boardroom in the Booth Auditorium at the University of California, Berkeley, School of Law, Boalt Hall, Bancroft Way and Piedmont Avenue, Berkeley, CA 94720-7200. The location of the meeting is subject to change. Please refer to NTIA's Web site, <http://www.ntia.doc.gov/other-publication/2015/multistakeholder-process-cybersecurity-vulnerabilities>, 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 <http://www.ntia.doc.gov/other-publication/2015/multistakeholder-process-cybersecurity-vulnerabilities>.

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](mailto: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](mailto: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/2015/multistakeholder-process-cybersecurity-vulnerabilities>, for the most current information.

Dated: August 26, 2015.

**Kathy D. Smith,**  
Chief Counsel, National Telecommunications and Information Administration.

[FR Doc. 2015-21500 Filed 8-28-15; 8:45 am]

BILLING CODE 3510-60-P

## DEPARTMENT OF COMMERCE

### Patent and Trademark Office

#### Madrid Protocol

**ACTION:** Proposed collection; comment request.

**SUMMARY:** The United States Patent and Trademark Office (USPTO), as part of its continuing effort to reduce paperwork and respondent burden, invites the

<sup>9</sup>ISO Standard 29147, *Vulnerability Disclosure Overview* (2014), available at: [http://www.iso.org/iso/catalogue\\_detail.htm?csnumber=45170](http://www.iso.org/iso/catalogue_detail.htm?csnumber=45170).