(HTS) heading 9902.51.11); and (2) for worsted wool fabric with average fiber diameters of 18.5 microns or less (HTS heading 9902.51.12). On August 6, 2002, President Bush signed into law the Trade Act of 2002, which includes several amendments to Title V of the Act. On December 3, 2004, the Act was further amended pursuant to the Miscellaneous Trade Act of 2004, Public Law 108–429. The 2004 amendment included authority for the Department to allocate a TRQ for new HTS category, HTS 9902.51.16. This HTS category refers to worsted wool fabric with average fiber diameter of 18.5 microns or less. The amendment provided that HTS 9902.51.16 is for the benefit of persons (including firms, corporations, or other legal entities) who weave such worsted wool fabric in the United States that is suitable for making men's and boys' suits. The TRQ for HTS 9902.51.16 provided for temporary reductions in the import duties on 2,000,000 square meters annually for 2005 and 2006. The amendment requires that the TRQ be allocated to persons who weave worsted wool fabric with average fiber diameter of 18.5 microns or less, which is suitable for use in making men's and boys' suits, in the United States. On August 17, 2006, the Act was further amended pursuant to the Pension Protection Act of 2006, Public Law 109–280, which extended the TRQ for HTS 9902.51.16 through 2009. The Senate-passed Emergency Economic Stabilization Act of 2008 extending the TRQ for HTS 9902.51.16 through 2014.

On October 24, 2005, the Department adopted final regulations establishing procedures for allocating the TRQ. *See* 70 FR 61363; 19 CFR 335. In order to be eligible for an allocation, an applicant must submit an application on the form provided at *http://otexa.ita.doc.gov/wooltrq/wool_fabric.htm* to the address listed above by 5 p.m. on October 21, 2011 in compliance with the requirements of 15 CFR 335. Any business confidential information that is marked business confidential will be kept confidential and protected from disclosure to the full extent permitted by law.

Dated: September 14, 2011.

Kim Glas,

Deputy Assistant Secretary for Textiles and Apparel.

[FR Doc. 2011–24257 Filed 9–20–11; 8:45 am]

BILLING CODE 3510–DS–P

DEPARTMENT OF COMMERCE

International Trade Administration

Request for Comments on World Health Organization Pandemic Influenza Preparedness Framework

AGENCY: International Trade Administration, Department of Commerce.

ACTION: Notice and request for comments.

SUMMARY: The International Trade Administration invites submission of comments from the public and relevant industries on influenza surveillance and response, including implementation of the World Health Organization Pandemic Influenza Preparedness Framework (*http://apps.who.int/gb/ebwha/pdf_files/WHA64/A64_8-en.pdf*) and additional planning for future possible pandemic influenza.

DATES: Written comments must be submitted on or before October 21, 2011. Comments should be no more than 15 pages. Business-confidential information should be clearly identified as such.

ADDRESSES: You may submit comments by any of the following methods:

E-mail: Vaccines@trade.gov.

Fax: (202) 482–0975 (*Attn.:* Jane Earley).

Mail or Hand Delivery/Courier: Jane Earley, U.S. Department of Commerce, Office of Health and Consumer Goods, Room 1015, 1401 Constitution Avenue, NW., Washington, DC 20230.

FOR FURTHER INFORMATION CONTACT: For questions on the submission of comments, please contact Jane Earley by phone at (202) 482–6241 or Andrea Cornwell at (202) 482–0998.

SUPPLEMENTARY INFORMATION: Written comments are sought in light of the approval of the World Health Organization (WHO) Pandemic Influenza Preparedness Framework by WHO Member States at the World Health Assembly and the need for the U.S. Government to participate in discussions and activities to plan for future pandemics. The facts and information obtained from written submissions will be used to inform the participation of the United States Department of Commerce in the interagency process to prepare for United States participation in international pandemic preparedness discussions and activities, following the May 2011 approval of the WHO Pandemic Influenza Preparedness Framework. The written submissions will be shared with other interested U.S. Government agencies, as needed, during the interagency process.

This agency previously requested comments on international pandemic influenza preparedness via the **Federal Register** on September 14, 2010; 75 FR 55776–55777.

The Department of Commerce invites comments from civil society organizations as well as pharmaceutical and medical technology industries and other interested members of the public on a number of issues regarding pandemic influenza preparedness and response.

The Department of Commerce invites written submissions on the following topics:

1. *Implementation of the WHO Pandemic Influenza Preparedness Framework.*

2. *Operations of the Global Influenza Surveillance and Response System.*

3. *Other matters related to prevention, planning and response whose resolution will be integral for the effective operation of a global influenza pandemic response.*

4. *Other matters that are related to the substance contained in 1–3, above.*

Upon receipt of the written submission, representatives from the Department of Commerce will consider them and share them, as needed, with other interested U.S. Government agencies and departments. Entities making submissions may be contacted for further information or explanation and, in some cases, meetings with individual submitters may be requested.

Dated: September 15, 2011.

James Rice,

Acting Director, Office of Health and Consumer Goods, International Trade Administration.

[FR Doc. 2011–24205 Filed 9–20–11; 8:45 am]

BILLING CODE 3510–DR–P

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

National Telecommunications and Information Administration

DEPARTMENT OF HOMELAND SECURITY

[Docket No. 110829543–1541–01]

Models To Advance Voluntary Corporate Notification to Consumers Regarding the Illicit Use of Computer Equipment by Botnets and Related Malware

AGENCIES: U.S. Department of Commerce, National Institute of

Standards and Technology; U.S. Department of Commerce, National Telecommunications and Information Administration; and U.S. Department of Homeland Security, National Protection and Programs Directorate.

ACTION: Request for Information.

SUMMARY: The U.S. Department of Commerce and U.S. Department of Homeland Security are requesting information on the requirements of, and possible approaches to creating, a voluntary industry code of conduct to address the detection, notification and mitigation of botnets.[1] Over the past several years, botnets have increasingly put computer owners at risk. A botnet infection can lead to the monitoring of a consumer's personal information and communication, and exploitation of that consumer's computing power and Internet access. Networks of these compromised computers are often used to disseminate spam, to store and transfer illegal content, and to attack the servers of government and private entities with massive, distributed denial of service attacks. The Departments seek public comment from all Internet stakeholders, including the commercial, academic, and civil society sectors, on potential models for detection, notification, prevention, and mitigation of botnets' illicit use of computer equipment.

DATES: Comments are due on or before 5 p.m. EDT, November 4, 2011.

ADDRESSES: Written comments may be submitted by mail to the National Institute of Standards and Technology at the U.S. Department of Commerce, 1401 Constitution Avenue, NW., Room 4822, Washington, DC 20230. Submissions may be in any of the following formats: HTML, ASCII, Word, rtf, or pdf. Online submissions in electronic form may be sent to *Consumer_Notice_RFI@nist.gov.* Paper submissions should include a compact disc (CD). CDs should be labeled with the name and organizational affiliation of the filer and the name of the word processing program used to create the document. Comments will be posted at *http://www.nist.gov/itl/.*

FOR FURTHER INFORMATION CONTACT: Jon Boyens, National Institute of Standards and Technology, 100 Bureau Drive, Mail Stop 8930, Gaithersburg, MD 20899, *jon.boyens@nist.gov.* Please direct media inquires to NIST's Office of Public Affairs at (301) 975–NIST.

SUPPLEMENTARY INFORMATION:

Background

The U.S. Department of Commerce (Commerce) recently issued a ''Green Paper'' [2] that suggests that voluntary codes of conduct [3] developed through a multi-stakeholder process can significantly advance efforts to protect the Internet from the growing security threats. One of the policy recommendations put forth was for Commerce to expand its role of working with multiple stakeholders to facilitate and promote the use of voluntary codes of conduct. Though the responses to the Green Paper are still being analyzed, it is clear that this facilitating role in the area of codes of conduct is seen as vital to advancing industry efforts in specific areas.

The U.S. Department of Homeland Security (DHS) has played an essential role in building cybersecurity educational programs for consumers. DHS's educational programs emphasize that every Internet consumer has a role to play in securing cyberspace and in ensuring the safety of ourselves, our families, and our communities online. DHS has a variety of outreach programs; most notable from a consumer perspective are the National Cybersecurity Awareness Month and Campaign. Each October DHS hosts events to encourage consumers to follow a few simple steps to keep themselves safe online. The Awareness Campaign ''Stop. Think. Connect.'' is a year-round program that helps consumers become more aware of growing threats and arms them with tools to protect themselves.

While security risks on the Internet exist in many areas, one current widely exploited threat comes from 'botnets.' Through this Request for Information and any follow-on work, the two Departments aim to reduce the harm that botnets inflict on the nation's computing environment.

To build a botnet, intruders exploit security flaws in the hardware and/or software used by individual consumers, and they install malicious software that connects the consumer's computer into a remotely controlled network of many computers. Once compromised, the owners of these computers are put at risk. Criminals have the ability to access personal information stored on the computer and communications made with the computer. Criminals can exploit this information for identity theft, privacy violations, and other crimes, as well as utilize the impacted users' computing power and Internet access. Networks of these compromised computers are often used to disseminate spam, store and transfer illegal content, and attack the servers of government and private entities with distributed denial of service attacks. Researchers suggest an average of about 4 million new botnet infections occur every month.[4]

The Departments are concerned about the potential economic impact of botnets and the problems they cause to computer systems, businesses, and consumers. To address these problems, it is necessary to stop botnets from propagating and to remove or mitigate the malicious software (malware) where installed. Companies and consumers may be able to voluntarily address some of these issues, but to fully address the problem, they will need to work together to clean and better protect computers. This will require voluntary efforts on many fronts, including better standards and procedures to secure systems.

One strategy that security experts suggest has been successful in stemming the tide of botnets has been for private sector entities to voluntarily and timely detect and notify end-users that their machines have been infected. This voluntary notification has mostly, though not always, come from the user's Internet Service Provider (ISP), which has contact information for the end-user and a pre-existing relationship. Once a service provider has detected a likely end-user security problem, it can inform the Internet user of the steps the user can take to address the problem. For example, last year in Australia, the Internet Industry Association in conjunction with the Minister for Broadband, Communications and the Digital Economy launched a voluntary code of practice for Australian ISPs to ensure consistent notification and remediation of consumer computer problems created by botnets. Once notified of a botnet infection, the consumer is sent to a website with information to help clean up his or her

[1] *Botnets* are collections of compromised computers that are remotely controlled by a malevolent party, as defined by the National Research Council's Committee on Improving Cybersecurity Research in the United States, *Toward a Safer and More Secure Cyberspace,* at 40 (2007).

[2] *See, e.g., Cybersecurity, Innovation and the Internet Economy* at *http://www.nist.gov/itl/upload/Cybersecurity_Green-Paper_FinalVersion.pdf.*

[3] A Code of Conduct in business is typically a written set of industry-wide voluntary practices designed to spur a community to operate in a uniform and predictable manner.

[4] *See, McAfee Quarterly Threat Report 2nd Quarter 2011: http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q2–2011.pdf.*

computer.[5] Germany [6] and Japan [7] have begun similar efforts. Several U.S. companies seem to be engaged in similar types of practices, though without a code of conduct in place, and standards organizations [8] have been discussing standards for botnet detection. Last December the Federal Communication Commission's (FCC's) Communications Security, Reliability and Interoperability Council (CSRIC) Working Group (WG) 8 recommended 24 Best Practices to address botnet protection for end-users as well as for the network.[9] The Best Practices cover several areas including prevention, detection, notification and mitigation, and identified means to address externalities such as privacy concerns. The Best Practices identified are primarily for use by ISPs that provide direct service to end-users on residential broadband networks. However, they may apply to other end-users and networks as well. The Internet Engineering Task Force also has developed a draft ''Recommendation for the Remediation of Bots in ISP Networks.'' [10]

Incentives and Voluntary Approaches

To promote voluntary best practices in botnet detection, notification and mitigation, one suggestion has been to provide companies that take action with certain types of liability protection in order to foster greater marketplace certainty. Another suggestion is to encourage ISPs to send consumer support queries to a centralized consumer resource center that could be supported by a wide number of players.[11] Such a resource center could reduce the burden on corporate customer support centers by pooling resources. The center could aid consumers by, for example, providing certain no-cost means of support, as well as information on other means for expedited support. This center could also be used to facilitate information sharing and research that could lead to better botnet detection. Moreover, as a ''condition of sponsorship'' private sector entities could be required to adopt an agreed upon set of practices.

There are many different ways that such a resource center could be created, including some that help encourage innovation in preventative security models and/or directly aid consumers in cleaning their machines. Below are three very broad scenarios proposed to help focus comment on possible voluntary approaches:

A. *Private-Sector Run and Supported*—Under this scenario, the private sector would create, run, and fund a resource center to inform and educate consumers who have been notified that their equipment may be infected by a botnet. This service could be run by a new or existing non-profit or for-profit entity depending on the needs and the model created.

B. *Public/Private Partnership*—Under this scenario, the government and private sector would work together to create a resource to inform and educate consumers who have been notified that their equipment may be infected by a botnet. These services could be provided through a non-profit or quasi-governmental entity depending on the needs and the model created.

C. *Government Run and Supported*—Under this scenario, the government would create a centralized resource to inform and educate consumers who have been notified that their equipment may be infected by a botnet. These centralized services would be provided by a government agency with some substantive input from the private sector, perhaps through a Federal Advisory Committee.

Request for Information. Recognizing the seriousness of the threat from, and potential harm caused by, botnets, Commerce and DHS are issuing this Request for Information to solicit information on: the need for a voluntary code of conduct for consumer notifications on botnets; how private entities might help prevent and identify botnets and certain types of malware on systems and networks; how to mitigate and notify users about botnets—on systems and networks; how to help promote incentives for companies to participate in voluntary notification efforts; and how to help build related resources in the United States for ISPs or other entities to notify consumers.

The questions below are to assist in framing the issues and should not be construed as a limitation on comments. The Departments invite comment on the full range of issues that may be presented by this Request for Information. Comments that contain references, studies, research and other empirical data that are not widely published should include copies of the referenced materials with the submitted comments.

A. General Questions on Practices To Help Prevent and Mitigate Botnet Infections

(1) What existing practices are most effective in helping to identify and mitigate botnet infections? Where have these practices been effective? Please provide specific details as to why or why not.

(2) What preventative measures are most effective in stopping botnet infections before they happen? Where have these practices been effective? Please provide specific details as to why or why not.

(3) Are there benefits to developing and standardizing these practices for companies and consumers through some kind of code of conduct or otherwise? If so, why and how? If not, why not?

(4) Please identify existing practices that could be implemented more broadly to help prevent and mitigate botnet infections.

(5) What existing mechanisms could be effective in sharing information about botnets that would help prevent, detect, and mitigate botnet infections?

(6) What new and existing data can ISPs and other network defense players share to improve botnet mitigation and situational awareness? What are the roadblocks to sharing this data?

(7) Upon discovering that a consumer's computer or device is likely infected by a botnet, should an ISP or other private entity be encouraged to contact the consumer to offer online support services for the prevention and mitigation of botnets? If so, how could support services be made available? If not, why not?

(8) What should customer support in this context look like (*e.g.,* web information, web chat, telephone support, remote access assistance, sending a technician, *etc.*) and why?

(9) Describe scalable measures parties have taken against botnets. Which scalable measures have the most impact in combating botnets? What evidence is available or necessary to measure the impact against botnets? What are the

---

[5] See, the icode Web site: *http://icode.net.au.* This is the site used for notification. It also has links to historical information about its founding.

[6] See, Anti-Botnet Advisory Center: *https://www.botfrei.de/en/index.html.*

[7] See, Cyber Clean Center: *https://www.ccc.go.jp/en_ccc/.*

[8] *See, e.g.,* IETF related Best Current Practice: *http://tools.ietf.org/html/draft-ietf-opsec-current-practices-07#section-2.8.*

[9] *See, e.g., Internet Service Provider (ISP) Network Protection Practices* at *http://transition.fcc.gov/pshs/docs/csric/CSRIC_WG8_FINAL_REPORT_ISP_NETWORK_PROTECTION_20101213.pdf.* The FCC has announced the creation of a new Working Group under the auspices of the reconstituted CSRIC. As we move forward with this process, we will coordinate with stakeholders and the nation's independent telecommunications regulator to ensure that we are not duplicating any efforts for industry or government.

[10] *See http://tools.ietf.org/id/draft-oreirdan-mody-bot-remediation-03.html.*

[11] *See, e.g.,* Maxim Weinstein, *Stop Badware Comments to the Department of Commerce Cybersecurity Green Paper,* July 29, 2011 at *http://www.nist.gov/itl/upload/StopBadware_response-to-DOC-Cybersecurity-Green-Paper.pdf.*

challenges of undertaking such measures?

B. Effective Practices for Identifying Botnets

(10) When identifying botnets, how can those engaged in voluntary efforts use methods, processes and tools that maintain the privacy of consumers' personally identifiable information?

(11) How can organizations best avoid ''false positives'' in the detection of botnets (*i.e.,* detection of behavior that seems to be a botnet or malware-related, but is not)?

(12) To date, many efforts have focused on the role of ISPs in detecting and notifying consumers about botnets. It has been suggested that other entities beyond ISPs (such as operating system vendors, search engines, security software vendors, *etc.*) can participate in anti-botnet related efforts. Should voluntary efforts focus only on ISPs? If not, why not? If so, why and who else should participate in this role?

C. Reviewing Effectiveness of Consumer Notification

(13) What baselines are available to understand the spread and negative impact of botnets and related malware? How can it be determined if practices to curb botnet infections are making a difference?

(14) What means of notification would be most effective from an end-user perspective?

(15) Should notices, and/or the process by which they are delivered, be standardized? If so, by whom? Will this assist in ensuring end-user trust of the notification? Will it prevent fraudulent notifications?

(16) For those companies that currently offer mitigation services, how do different pricing strategies affect consumer response? Are free services generally effective in both cleaning computers and preventing re-infection? Are fee-based services more attractive to certain customer segments?

(17) What impact would a consumer resource center, such as one of those described above, have on value-added security services? Could offers for value-added services be included in a notification? If not, why not? If so, why and how? Also, how can fraudulent offers be prevented in this context?

(18) Once a botnet infection has been identified and the end-user does not respond to notification or follow up on mitigating measures, what other steps should the private sector consider? What type of consent should the provider obtain from the end-user? Who should be responsible for considering and determining further steps?

(19) Are private entities declining to act to prevent or mitigate botnets because of concerns that, for example, they may be liable to customers who are not notified? If so, how can those concerns be addressed?

Best Practices for Consumer Notification

(20) Countries such as Japan, Germany, and Australia have developed various best practices, codes of conduct, and mitigation techniques to help consumers. Have these efforts been effective? What lessons can be learned from these and related efforts?

(21) Are there best practices in place, or proposed practices, to measure the effectiveness of notice and educational messages to consumers on botnet infection and remediation?

D. Incentives To Promote Voluntary Action To Notify Consumers

(22) Should companies have liability protections for notifying consumers that their devices have been infected by botnets? If so, why and what protections would be most effective in incentivizing notification? If not, why not? Are there other liability issues that should be examined?

(23) What is the state-of-practice with respect to helping end-users clean up their devices after a botnet infection? Are the approaches effective, or do end-users quickly get re-infected?

(24) What agreements with end-users may need modification to support a voluntary code of conduct?

(25) Of the consumer resource scenarios described above, which would be most effective at providing incentives for entities to participate? Are there other reasons to consider one of these approaches over the others?

(26) If a private sector approach were taken, would a new entity be necessary to run this project? Who should take leadership roles? Are the positive incentives involved (cost savings, revenue opportunity, *etc.*) great enough to persuade organizations to opt into this model?

(27) If a public/private partnership approach were taken, what would be an appropriate governance model? What stakeholders should be active participants in such a voluntary program? What government agencies should participate? How could government agencies best contribute resources in such a partnership?

(28) If a government-run approach were taken, what government agencies should play leading roles?

(29) Are there other approaches aside from the three scenarios suggested above that could be used to create a consumer resource and to incentivize detection, notification, and mitigation of botnets?

(30) Are there other positive incentives that do not involve creation of an organized consumer resource that could encourage voluntary market-based action in detection, notification, and mitigation of botnets?

Willie E. May,

Associate Director for Laboratory Programs/ Principal Deputy, Department of Commerce.

Lawrence E. Strickling,

Assistant Secretary for Communications and Information, Department of Commerce.

Rand Beers,

Under Secretary, National Protection and Programs Directorate, Department of Homeland Security.

[FR Doc. 2011–24180 Filed 9–20–11; 8:45 am]

BILLING CODE 3510–13–P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

RIN 0648–XA713

Endangered Species; File Nos. 16526, 16323, 16436, 16422, 16438, 16431, 16507, 16547, 16375, 16442, 16482, and 16508.

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

ACTION: Notice; receipt of applications.

SUMMARY: Notice is hereby given that NMFS has received twelve applications applying in due form for permits to take Atlantic sturgeon (*Acipenser oxyrinchus oxyrinchus*) for purposes of scientific research.

DATES: Written, telefaxed, or e-mail comments must be received on or before October 21, 2011.

ADDRESSES: The application and related documents are available for review by selecting ''Records Open for Public Comment'' from the *Features* box on the Applications and Permits for Protected Species (APPS) home page, *https://apps.nmfs.noaa.gov,* and then selecting associated File No. from the list of available applications.

These documents are also available upon written request or by appointment in the offices listed in **SUPPLEMENTARY INFORMATION**.

Written comments on this application should be submitted to the Chief, Permits and Conservation Division, Office of Protected Resources, NMFS, 1315 East-West Highway, Room 13705,