This document is scheduled to be published in the Federal Register on 01/11/2018 and available online at **https://federalregister.gov/d/2018-00322**, and on **FDsys.gov**

Billing Code: 3510-60-P

DEPARTMENT OF COMMERCE

National Telecommunications and Information Administration

[Docket No. 180103005-8005-01]

RIN 0660-XC040

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 Department of Commerce (Department) is requesting comment on a draft Report about actions to address automated and distributed threats to the digital ecosystem as part of the activity directed by Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure." Through this Notice, the Department seeks broad input and feedback from all interested stakeholders—including private industry, academia, civil society, and other security experts—on this draft Report, its characterization of risks and the state of the ecosystem, the goals laid out, and the actions to further these goals.

DATES: Comments are due on or before 5 p.m. Eastern Time on February 12, 2018.

ADDRESSES: Written comments may be submitted by email to *counter_botnet@list.commerce.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: Executive Order 13800 on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure called for "resilience against botnets and other automated, distributed threats."[1] The Order directed the Secretary of Commerce, together with the Secretary of Homeland Security, to "lead an open and transparent process to identify and promote action by appropriate stakeholders" with the goal of "dramatically reducing threats perpetrated by automated and distributed attacks (e.g., botnets)."[2]

The Departments of Commerce and Homeland Security worked jointly on this effort through three approaches—hosting a workshop, publishing a request for comment, and initiating an inquiry through the President's National Security Telecommunications Advisory Committee (NSTAC)—all aimed at gathering a broad range of input from experts and stakeholders, including private industry, academia, and civil society. The Departments worked in consultation with the Departments of Defense, Justice, and State, the Federal Bureau of Investigation, the sector-specific agencies, the Federal Communications Commission, and Federal Trade

[1] Exec. Order 13800, 82 Fed. Reg. 22,391 (May 11, 2017).

[2] *Id.*

Commission, as well as other interested agencies. These activities all contributed to the information gathering process for developing a draft Report.

The draft Report, published on January 5, 2018, and available at https://www.ntia.doc.gov/report/2018/report-president-enhancing-resilience-internet-and-communications-ecosystem-against, characterizes the status of the Internet and communications ecosystem, and offers a positive vision of the future. The Departments determined that the opportunities and challenges in working toward dramatically reducing threats from automated, distributed attacks can be summarized in six principal themes.

1. **Automated, distributed attacks are a global problem.** The majority of the compromised devices in recent botnets have been geographically located outside the United States. Increasing the resilience of the Internet and communications ecosystem against these threats will require coordinated action with international partners.
2. **Effective tools exist, but are not widely used.** The tools, processes, and practices required to significantly enhance the resilience of the Internet and communications ecosystem are widely available, if imperfect, and are routinely applied in selected market sectors. However, they are not part of common practices for product development and deployment in many other sectors for a variety of reasons, including (but not limited to) lack of awareness, cost avoidance, insufficient technical expertise, and lack of market incentives.
3. **Products should be secured during all stages of the lifecycle.** Devices that are vulnerable at time of deployment, lack facilities to patch vulnerabilities after discovery, or remain in service after vendor support ends make assembling automated, distributed threats far too easy.

4. **Education and awareness is needed.** Knowledge gaps in home and enterprise customers, product developers, manufacturers, and infrastructure operators impede the deployment of the tools, processes, and practices that would make the ecosystem more resilient.
5. **Market incentives are misaligned.** Perceived market incentives do not align with the goal of "dramatically reducing threats perpetrated by automated and distributed attacks." Market incentives motivate product developers, manufacturers, and vendors to minimize cost and time to market, rather than to build in security or offer efficient security updates. There has to be a better balance between security and convenience when developing products.
6. **Automated, distributed attacks are an ecosystem-wide challenge.** No single stakeholder community can address the problem in isolation.

The Report lays out five complementary and mutually supportive goals that would dramatically reduce the threat of automated, distributed attacks and improve the resilience of the ecosystem. They are:

1. Identify a clear pathway toward an adaptable, sustainable, and secure technology marketplace;
2. Promote innovation in the infrastructure for dynamic adaptation to evolving threats;
3. Promote innovation at the edge of the network to prevent, detect, and mitigate bad behavior;
4. Build coalitions between the security, infrastructure, and operational technology communities domestically and around the world; and
5. Increase awareness and education across the ecosystem.

For each goal, the report suggests supporting activities to be taken by both government and private sector actors. With this Request for Comment, the Department is asking for a response to the issues and goals raised by the draft Report, as well as the proposed approach, current initiatives, and next steps. Following the completion of the comment period, the Department will host a workshop to discuss substantive comments and the way forward for the Report. The workshop will be held February 28 – March 1, 2018 at the National Cybersecurity Center of Excellence (NCCoE). Additional information regarding the workshop, including logistics and registration information, is available at https://csrc.nist.gov/Events/2018/second-botnet-workshop.

Information obtained through this Request for Comment, the NCCoE-hosted workshop, and other stakeholder interactions will be considered for incorporation into the final version of the Report. The final Report is due to the President on May 11, 2018.

Request for Comment

The goal of this Request for Comment is to solicit feedback on the draft Report, its characterization of the challenges, and proposed actions. The Department invites comment on the full range of issues that may be presented by this inquiry, including issues that are not specifically raised in the following questions. Respondents are invited to respond to some or all of the questions below:

1. **The Ecosystem**: Is the Report's characterization of risks and the state of the current Internet and communications ecosystem accurate and/or complete? Are there technical details, innovations, policy approaches, or implementation barriers that warrant new or further consideration?

2. **Goals**: Are the Report's stated goals appropriate for achieving a more resilient ecosystem? Do the actions support the relevant goals? In aggregate, are the actions sufficient to significantly advance the goals?
3. **Stakeholder Roles**: How can specific actions be refined for efficacy and achievability? What actors, inside the Federal government, in the private sector, and across the global community, can be instrumental in the successful accomplishment of these activities? Who should play a leadership role; and where and how? What stakeholders are key to particular successes?
4. **Road map**: What information can help the government and stakeholders delineate a road map for achieving these goals? How should implementation be phased to optimize resources and commitments? Which actions are of highest priority, or offer opportunities for near term progress? Which actions depend on the completion of other actions? Are there known barriers that may inhibit progress on specific actions?
5. **Incentives:** What policies, innovations, standards, best practices, governance approaches, or other activities can promote market-based solutions to the challenges and goals discussed in the report? Are there specific incentive ideas beyond the market-based approaches discussed in the report (e.g., procurement, multistakeholder policy development, R&D, best practices, and adoption & awareness efforts) that demand new consideration or exploration?
6. **Further Activities**: What additional specific actions can improve the resilience of the Internet and communications ecosystem? What partners can drive success for these activities?
7. **Metrics**: How should we evaluate progress against the stated goals?

Instructions for Commenters: The Department invites comment on the full range of issues that may be presented by this inquiry, including issues that are not specifically raised in the above questions. Commenters are encouraged to address any or all of the above questions. Comments that contain references to studies, research, and other empirical data that are not widely available should include copies of the referenced materials with the submitted comments.

Comments submitted by email should be machine-readable and should not be copy-protected. Responders should include the name of the person or organization filing the comment, which will facilitate agency follow up for clarity as necessary, as well as a page number on each page of their submissions. All comments received are a part of the public record and will generally be posted on the NTIA website, *http://www.ntia.doc.gov/,* without change. All personal identifying information (for example, name, address) voluntarily submitted by the commenter may be publicly accessible. Do not submit confidential business information or otherwise sensitive or protected information. The Department will also accept anonymous comments.

Dated: January 5, 2018.

David J. Redl,

Assistant Secretary for Communication and Information, National Telecommunications and Information Administration.

[FR Doc. 2018-00322 Filed: 1/10/2018 8:45 am; Publication Date: 1/11/2018]