Federal Communications Commission
Washington, D.C. 20554

May 2, 2013

Via Electronic Mail

Mr. Alfred Lee
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue N.W., Room 4725
Washington, DC 20230

Dear Mr. Lee:

Please find attached the comments of the Federal Communications Commission's Chief Economist in Docket No. 130206115-3115-01, "Incentives to Adopt Improved Cybersecurity Practices." We appreciate the opportunity to comment.

Please feel free to contact me at (202) 418-2031 or by e-mail at steve.wildman@fcc.gov if you have any questions about this submission.

Sincerely,

Steven S. Wildman, PhD
Chief Economist, FCC

Comments of
FCC Chief Economist
Department of Commerce Docket Number 130206115-3115-01
"Incentives to Adopt Improved Cybersecurity Practices"

The FCC welcomes the opportunity to respond to the Department of Commerce's Notice of Inquiry (NOI) on incentives to adopt improved cybersecurity practices.[1] Economic forces affect the private sector's incentives to adopt cybersecurity practices and individual and organizational incentives shape public sector performance in this regard as well. Effective responses to cybersecurity threats will depend largely on developing a deeper understanding of the factors influencing the decisions that individuals and organizations make regarding threats to cybersecurity. We offer the following observations and suggestions:

Examine Existing Incentives. First, we agree with the Department of Commerce that it is important to examine carefully existing incentives in current government and private sector programs, including public-private partnerships. A better understanding of which incentives have worked, which have not, and what experience-based insights tells us might lead to improvement, should be further developed and widely shared across agencies and sectors. This effort should include exploration of applying principles and strategies successfully employed to facilitate public and private efforts in the service of other public interest goals. Following are examples of three FCC initiatives relevant to this perspective.

- **Public-Private Partnerships.** Where coordination may otherwise be difficult to achieve, public-private partnerships can provide opportunities for Federal agencies to foster beneficial coordination efforts by industry stakeholders. An example is the FCC's longstanding work with the Communications Security, Reliability and Interoperability Council (CSRIC),[2] an FCC federal advisory committee, with members from the private sector, Federal/state/local/tribal/territorial governments, and academia that has considerable expertise in cybersecurity. During the CSRIC III, chartered March 2011 to March 2013, CSRIC members developed botnet remediation best practices and recommendations and delivered a Final Report, *U.S. Anti-Bot Code of Conduct (ABCs) for Internet Service Providers (ISPs) – Barrier and Metric Considerations.*[3] Appendix 3, *Guide to Barriers and Code Participation*, provides guidance to ISPs in implementing the ABCs for ISPs, identifies potential barriers[4] to implementation, and recommends strategies for overcoming them. Although these barriers were identified and the recommendations were developed to facilitate implementation of best practices to reduce the spread of bots, the analytical construct and recommendations for overcoming implementation barriers are extensible. These recommendations may serve as a model for efforts to promote effective participation in the Cybersecurity Framework program as

[1] *See* http://www.ntia.doc.gov/files/ntia/publications/cybersecurity_noi_03282013.pdf.

[2] *See* http://www.fcc.gov/encyclopedia/communications-security-reliability-and-interoperability-council-iii.

[3] *See* http://www.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG7_Report_March_%202013.pdf.

[4] The barriers are distinguished as: (1) Technology Barriers, (2) Consumer and Market Barriers, (3) Operational Barriers, (4) Financial Barriers, and (5) Legal, Regulatory, or Policy Barriers.

participating companies will likely encounter implementation barriers similar to those identified in the CSRIC Final Report. For participating companies, direct benefits of participation in the ABCs for ISPs would include better protection for critical information and data, a bigger return on investments in cybersecurity, the reputational benefits of complying with widely accepted practices, and the opportunity to rely on self-regulation in place of the more direct Federal oversight than otherwise might be required.[5] Collectively, participating companies and the nation's economy would benefit from reduced informational asymmetries and the added security realized as the fraction of business partners employing best practices increases.

- **Consumer Complaints.** Like other agencies, the FCC responds to consumer complaints. The Commission is able to track trends in complaints, and occasionally publishes reports on those trends. Such data can be used to alert carriers and service providers to problems, and, if they are unresponsive, to generate reports alerting consumers to problems. These actions (or their potential) create incentives for carriers and service providers to improve practices in order to maintain a positive reputation with consumers and avoid additional regulation. Consumer complaint data might also be used to provide an incentive to improve cybersecurity practices. Recognizing that other businesses and organizations are the most important customers for many carriers and service providers, this approach could be broadened to include complaints from customers of all kinds. This approach can also be seen as an application of principles articulated under the Open Government Directive which requires "concrete measures to implement commitments to transparency, participation, and collaboration."[6]

- **Outage Reporting.** Reporting can also be used to enhance incentives to improve cybersecurity. The FCC employs this strategy to improve communication systems reliability by requiring communications providers to submit outage reports when communications systems are down for specified periods of time. The FCC uses this information to work with communications providers on voluntary initiatives to address trends that appear to be affecting communications reliability. Such reports contribute to informed and reasonable regulatory oversight, and provide an incentive for service providers to minimize outages to protect their reputations and to avoid regulatory intervention.

Study How Private-Sector Initiatives Are Shaped. Second, we recommend more in-depth study of how private sector incentives are shaped, not only by business considerations, but also by law, policies, and other public sector initiatives. Private sector actors respond to incentives that are substantially shaped by the legal and regulatory frameworks governing their sectors. This research would provide valuable context for the study of Federal initiatives discussed immediately above.

---

[5] *Id.*

[6] *See* Sunstein, Cass R., Memorandum for the Heads of Executive Departments and Agencies on Disclosure and Simplification as Regulatory Tools (June 18, 2010), Executive Office of the President; President Barack Obama, Memorandum on Transparency and Open Government (Jan 21, 2009), *available at* http://www.gpoaccess.gov/presdocs./2009/DCPD200900010.pdf; and Office of Management and Budget, Open Government Directive, *available at* http://whitehouse.gov/omb/assets/memoranda_2010/m10-06.pdf.

Include Summary of Academic Literature in the Record. Third, in support of our first two recommendations, we recommend including in the record a robust summary of the academic literature on the incentives available to businesses and individuals as they make cybersecurity decisions. This literature includes discussions of externalities, principal-agent problems, public goods, information asymmetries, reputational effects, information costs, and the nature of human decision making. Armed with appropriate theory and theory-based empirical research, we can work to shape incentives in ways that can help us collectively overcome barriers to implementing effective cybersecurity practices. Examples of relevant academic articles include:

- Cordes, Joseph J., "An Overview of the Economics of Cybersecurity and Cybersecurity Policy," Report, The George Washington University Cyber Security Policy and Research Institute, 2011, *see* http://www.cspri.seas.gwu.edu/Seminar%20Abstracts%20and%20Papers/2011-6%20Economics%20and%20Cybersecurity%20Cordes.pdf.
- Friedman, Allan, "Economic and Policy Frameworks for Cybersecurity Risks," Brookings Center for Technology Innovation, 2011, *see* http://www.brookings.edu/~/media/research/files/papers/2011/7/21%20cybersecurity%20friedman/0721_cybersecurity_friedman.
- Kiely, Matt et al, "Macro-Economic Cyber Security Models," Proceedings of the 2006 Systems and Information Engineering Design Symposium, 2006, *see* http://www.sys.virginia.edu/sieds06/papers/FAfternoonSession6.4.pdf.
- Moore, Tyler, "Introducing the Economics of Cybersecurity: Principles and Policy Options," Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy, National Academy of Sciences, 2010, *see* http://cs.brown.edu/courses/csci1800/sources/lec27/Moore.pdf.
- Moore, Tyler, Richard Clayton, Ross Anderson, "The Economics of Online Crime, Journal of Economic Perspectives," 2009, 23(3): 3-20, *see* http://pubs.aeaweb.org/doi/pdfplus/10.1257/jep.23.3.3.
- Rowe, Brent et al, "Economic Analysis of ISP Provided Cyber Security Solutions," Institute for Homeland Security Solutions, 2011, *see* http://sites.duke.edu/ihss/files/2011/12/Rowe_IHSS_Cyber_Final_ReportFINAL1.pdf.

In conclusion, the FCC supports the efforts of the Department of Commerce to identify and understand the factors that influence the decisions that individuals and organizations make regarding threats to cybersecurity. To that end, we encourage the Department to examine existing incentives, study how private-sector initiatives are shaped, and include a summary of relevant academic literature in the record. We look forward to working with the Department to accomplish the important goals that underlie the NOI.