To: National Telecommunications and Information Administration
In response to "Promoting Stakeholder Action Against Botnets and Other Automated Threats"
Docket No. 180103005–8005–01] RIN 0660–XC040

Feb 11, 2018

This comment focuses on goals, roadmap, incentives and further activities surrounding 'governance, policy and coordination.' On page 20 of the draft report, there is a statement, "real coordination is necessary to fully understand the problem and identify paths to solutions. While the information technology and communications sectors do actively work to understand security risks, sectors often are unable to coordinate well with other sectors. Even though some entities coordinate domestically or regionally, there are few global mechanisms to share information
about threats, solutions, and their adoption and efficacy."

This is absolutely right, and it does not go far enough.

We are co-authors of a forthcoming article, "That was close! Reward Near-Miss Reporting for Cybersecurity," which explores ways in which reward structures could transform what we know about the efficacy of solutions. In particular, we suggest adopting existing US government aviation safety programs (the NASA-run Aviation Safety Reporting System) to cybersecurity.

A draft of the article, with a working title, is available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3081216 .

Standing up a "Cyber Safety Reporting System" should be a milestone in the final document, in support of better understanding how defenses work in operation. In support of and to roadmap that goal, the NTIA should use its convening power to bring together industry, regulators, and enforcement and oversight agencies to work through the challenges laid out that document, including but possibly not limited to:

- Defining accident and near miss
- Running experiments to quantify data collection and processing
- Clarifying regulatory exclusions
- Guidelines for agency judgement
- Statements of agency support

Learning what works and what doesn't by studying the controls that prevent or allow near misses will allow us to focus standards and practices on the controls that stop incidents, and focus research on improving the ones that might be allowing near misses to turn into real incidents.

Lastly, this proposal takes a new tact towards a problem where progress has been challenging, possibly offering a more practical way forward.

Adam Shostack
President, Shostack & Associates
adam@shostack.org/917-391-2168

Steven M. Bellovin
Percy K. and Vida L.W. Hudson Professor of Computer Science, Columbia University
Affiliate faculty at Columbia Law School