ECKERT SEAMANS
ATTORNEYS AT LAW

AUGUST 28, 2014

UTILITIES AND TELECOMMUNICATIONS ALERT

FCC SEEKS COMMENT ON CYBERSECURITY BEST PRACTICES

In light of the many recent well-publicized cybersecurity attacks on U.S. companies, the Federal Communications Commission ("FCC" or "Commission") is seeking comments from businesses regarding the effectiveness of cybersecurity best practices initially recommended in March 2012. Although implementation of these best practices are currently voluntary, they may foreshadow future regulatory obligations—just as the Commission's involvement with Net Neutrality began with the aspirational principles in its Internet Policy Statement and evolved into its current fight to assert binding rulemaking authority over network management techniques. With respect to cybersecurity, effective advocacy at this critical point can help ensure that the Commission proceeds in a manner that best aligns with the interests of your organization.

The best practices in question were initially developed and adopted by the Commission's third Communications Security, Reliability and Interoperability Council ("CSRIC III"), a federal advisory committee comprised of leaders from the private sector, academia, engineering, non-profit organizations, and government partners. As some time has passed since their adoption, the Commission would now like public comment on the use of these best practices from ISPs and other members of the Internet community. Comments are due by September 26, 2014. The full text of the public notice can be found here.

As noted above, the CSRIC III cybersecurity best practices are not currently required. Companies are free to adopt them on a voluntary basis. However, they focus on combating major cybersecurity threats that companies need to address for their own protection irrespective of the Commission's involvement.

Specifically, the CSRIC III cybersecurity best practices address: (1) botnet attacks; (2) Internet route hijacking; and (3) domain name fraud. The term **botnet** typically refers to a network of compromised computers whose security defenses have been breached and which are now controlled by a third party. It has been estimated that as many as two million personal computers in the US are incorporated into botnets. These botnets in turn can be used to launch what is known as a distributed denial-of-service ("DDoS") attack, in which the combined computers of the botnet submit as many requests as possible to a single Internet computer or service to overwhelm it and prevent it from servicing legitimate requests from other users. Similar to a hacker's use of a botnet, **Internet route hijacking** and source-address spoofing allows a hacker to transmit information that appears to come from a more legitimate IP address, which then facilitates a wide variety of other hacking attacks. Finally**, domain name fraud** refers to various techniques used to generate illicit revenue by manipulating businesses and other entities into buying, listing or converting an Internet domain name.

With respect to these cybersecurity threats, the Commission's public notice specifically seeks responses to the following questions as they relate to the CSRIC III best practices cited above:

1. What progress have stakeholders made in implementing the recommendations?
2. What barriers have stakeholders encountered in implementing the recommendations?
3. What significant success stories or breakthroughs have been achieved in implementing the recommendations?
4. What are stakeholders' views and/or plans for full implementation of the recommendations?
5. How effective are the recommendations at mitigating cyber risk when they have been implemented? Given the experiences gained in the past two years, are there alternatives to full implementation that could be more effective than full implementation at mitigating cyber risk risks posed by botnets, Domain Name System ("DNS") vulnerabilities, routing infrastructure vulnerabilities, and source address spoofing? On what basis do stakeholders believe that these alternatives are more effective than the CSRIC III recommendations? Do stakeholders undertake qualitative or quantitative evaluations of the effectiveness of these various approaches, or both?

This public notice is part of a larger trend of increased focus on cyber-security and data-privacy matters not only by the FCC but other federal regulatory agencies as well. As the Commission has yet to impose binding regulatory requirements, this public comment period represents a great opportunity to help shape the conversation before the Commission at a relatively early stage in its examination of these issues.

As noted previously, parties that wish to provide a comment must do so by September 26, 2014. If you have any additional questions regarding the above or if you are interested in further advocacy with respect to these issues, please contact Earl Comstock (ecomstock@eckertseamans.com) at 202.659.6627 or Rob Gastner (rgastner@eckertseamans.com) at 202.695.6674.

This Utilities and Telecommunications Alert is intended to keep readers current on matters affecting businesses and is not intended to be legal advice.