MERCATUS CENTER
GEORGE MASON UNIVERSITY

Public Interest Comment on
Cyber Security Certification Program[1]
July 12, 2010

PS Docket No. 10-93.

The Regulatory Studies Program (RSP) of the Mercatus Center at George Mason University is dedicated to advancing knowledge of the impact of regulation on society. As part of its mission, RSP conducts careful and independent analyses employing contemporary economic scholarship to assess rulemaking proposals from the perspective of the public interest. Thus, this comment on the Federal Communications Commission's (FCC's) Notice of Inquiry does not represent the views of any particular affected party or special interest group, but is designed to assist the commission as it revises its framework for assessing competition in mobile wireless.

1. Introduction

The notice of inquiry seeks comment on whether a cyber security certification program "would create business incentives for providers of communications services to sustain a high level of cyber security culture and practice."[2] Assuming it has legal authority to implement such a program, the Commission should ask itself two questions to help determine whether a certification program is necessary.

First, the Commission should ask itself whether a market failure exists that requires action by the FCC. Are there externalities that might cause under-investment by firms in cyber security? Alternatively, is there an information failure such that firms do not understand the benefits of purchasing a sufficient amount of cyber security? Are communications services providers unable or ill equipped to adopt security standards and ensure vigilant cyber security? Second, even if there is evidence of a market failure, will a certification program be helpful? We see little evidence that these questions can be answered in the affirmative.

2. Is the market failing to provide adequate cyber security?

[1] Prepared by Jerry Brito, senior research fellow, and Tate Watkins, research associate, Mercatus Center at George Mason University. This comment is one in a series of Public Interest Comments from Mercatus Center's Regulatory Studies Program and does not represent an official position of George Mason University.

[2] FEDERAL COMMUNICATIONS COMMISSION, *In the Matter of Cyber Security Certification Program*, PS Docket No. 10-93, Notice of Inquiry (released Apr. 21, 2010) at ¶ 1.

The stated purpose of the notional Commission certification program would be to ensure that "communications services [] sustain a high level of cyber security culture and practice."[3] Before expending resources to establish such a program, the Commission should first ascertain whether in fact there is not already a "high level of cyber security culture and practice" among communications firms. The present Notice of Inquiry acknowledges that the Commission does not know the answer to this question,[4] yet it does not ask for comment on the matter. It simply accepts the National Broadband Plan's recommendation that a voluntary certification program to "create[] market incentives for communications service providers to upgrade their network cybersecurity" is necessary.[5] The Broadband Plan, in turn, does not offer more than conjecture about the state of cyber security practice among communications firms.

There is no evidence that communications and other industries are not able or willing either to create their own cyber security standards and certifications or to adopt existing ones. After all, it is in the interest of communications services providers to provide optimal cyber security to secure their investments and to cater to consumer demand. CIOs and other consumers who value effective information security provision will demand that communications service providers have high levels of protection, giving providers incentive to adhere to cyber security best practices.

Indeed, it seems that the private sector is very concerned about information security. PricewaterhouseCoopers recently surveyed 7,200 executives responsible for IT and security investments in 130 countries and found that "nearly two out of every three respondents (63%) expect spending [on information security] to either increase or stay the same—in spite of the worst economic downturn in decades."[6]

3. Is the market failing to provide adequate cyber security certification?

There are numerous information security standards in existence today, such as the widely recognized ISO 27000 series of standards established by the International Organization for Standardization.[7] These standards offer certification through ISO 27001.[8] There is no evidence that voluntary standards organizations are not already meeting the demand for security certification.

[3] *Id.*,¶ 1.

[4] *Id.*,¶ 7.

[5] FEDERAL COMMUNICATIONS COMMISSION, National Broadband Plan at 321.

[6] PRICEWATERHOUSECOOPERS, *Trial by Fire: What global executives expect of information security*, at 8, *available at* http://www.pwc.com/us/en/it-risk-security/publications/trial-by-fire.jhtml.

[7] The ISO 27000 Directory, An Introduction to ISO 27001, ISO 27002....ISO 27008, http://www.27000.org/index.htm.

[8] The ISO 27000 Directory, The ISO27001 Certification Process, http://www.27000.org/ismsprocess.htm.

The National Institute of Standards and Technology have also developed myriad other standards,[9] and the International Society of Automation has developed standard ISA-99 for Industrial Automation and Control System Security.[10] The North American Electric Reliability Corporation also develops standards and common best practices for Critical Infrastructure Protection.[11]

Additionally, the chemical industry has voluntarily developed specific standards for its sector since 2002.[12] Dow describes the initiative as an "industry-wide effort to maintain safe and secure information exchange and operations."[13] Its standards include focusing on risk management and reduction; sharing information within the industry, with other critical infrastructure sectors, and with government; and sector-wide adoption of certain security practices.[14]

The development of both widespread security standards and industry specific ones demonstrate the importance companies and organizations already place on information security. Furthermore, the internationally recognized ISO 27001certification program suggests that it may be superfluous for the FCC to develop a new certification program. Affixing the Commission's name to an existing standard, like the ISO 27001, could raise additional concerns.

4. Would a Commission certification program be helpful?

A potential problem with a Commission certification program is that standards for certification will likely not keep pace with technological advance and emerging threats to information. It is more effective to allow private enterprise to develop protections for rapidly emerging and evolving threats, rather than encouraging them to devote resources to comply with certification standards that may become outdated. Allowing industry the flexibility to develop fluid and responsive security measures will promote innovative discovery that may be hindered by a Commission certification program.

Another concern of such a program is that it may discourage innovation outside the scope of certification. Much as teachers evaluated predominantly by test scores of their students will often "teach to the test," a Commission certification program could encourage communications service providers to concentrate solely on complying with acquiring the certificate, this hindering other security innovations. The Commission

[9] National Institute of Standards and Technology, Computer Security Division, Computer Security Resource Center, Certification & Accreditation, http://csrc.nist.gov/publications/PubsTC.html#Certification & Accreditation.

[10] International Society of Automation, ISA99, Industrial Automation and Control System Security, http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821.

[11] North American Electric Reliability Corporation, Standards: Reliability Standards, http://www.nerc.com/page.php?cid=2|20.

[12] American Chemistry Council, Chemical Sector Cyber Security Program, http://www.americanchemistry.com/s_chemitc/sec_callout.asp?CID=1733&DID=6429.

[13] eBusiness @ Dow, Cyber-Security Standards, http://www.dow.com/ebusiness/elead/cyber.htm.

[14] *Id.*

should be aware of the potential to discourage security innovation outside the bounds of its program by implying, indirectly, that its standards are sufficient.

5. Will a certification program truly be voluntary?

We also wonder whether a Commission certification program will truly be voluntary. If the Commission certifies certain companies, and those companies can market their security as FCC certified, their competitors might be compelled to seek certification as well. Government entities might also begin to incorporate a requirement for certification into contracts. Even a program that is *per se* voluntary, therefore, may become mandatory in practice.

The concern here is that this might encourage service providers to value the acquisition of certification more than the actual provision of security. One can conceive of a firm that develops an innovation that provides greater security to its clients than certified practices, but that may nevertheless be forced to employ certified practices instead. There may even be a reduction of investment in innovation simply because certified practices are perceived as sufficient to attract business.

Conclusion

The communications industry and other sectors have demonstrated the ability and willingness to independently develop cyber security standards, best practices, and certifications. Private firms have great reputational incentive to use high quality and effective cyber security services and products. Participants in the market for communications services already demand secure service. The Commission, therefore, must identify a market failure when it comes to cyber security certification. If no market failure exists, it should consider the necessity of its role in certification.

Even if we assume a market failure, the Commission must ascertain that a cyber security certification program will do more good than harm. These questions, however, are absent from the present NOI. We therefore hope the Commission seeks further information before embarking down the road to certification.