From: Martin, Suzanne
To: securityRFC2015
Cc: Andrew Hoog
Subject: WRITTEN RESPONSES TO RIN 0660-XC108 (Sections (h) and (k)) Stakeholder Engagement on Cybersecurity in the Digital Ecosystem
Date: Thursday, May 07, 2015 3:57:58 PM

National Telecommunications and Information Administration
[Docket No. 150312253–5253–01]
RIN 0660–XC018 Stakeholder Engagement on Cybersecurity in the Digital Ecosystem

(h) Trusted Downloads. Internet users often download content and applications online without clear assurance of the security of the site. Are there best practices and existing standards that providers of online applications and downloadable tools can adopt to ensure consumer protection without impacting innovation or business models?

I am Andrew Hoog, CEO and co-founder of a mobile security company called NowSecure. Since 2009, we have been focused on securing mobile devices, apps and enterprises. We believe it is critical to build a strong, industry-wide foundation of best practices, tools and analytics to foster and maintain a high degree of trust in the mobile marketplace.

Were all apps developed according to best security practices -- which includes ensuring apps properly handle sensitive data, addressing issues surrounding caching and logging, and dealing with problems specific to iOS and Android, and more -- the mobile ecosystem would be much more secure. Unfortunately, security is too often a secondary concern for both app developers and app marketplaces. Our recent research showed that almost 50% of mobile apps have at least one high risk security flaw and 60% transmit data insecurely over the network.

Downloadable apps that can provide insights into what organizations and what countries a device is communicating with and show which apps may be sending data insecurely go a long way toward educating users about what their device is really doing. An app that tells users when security vulnerabilities have been discovered in apps on their devices would provide actionable intelligence about how to remediate their risks. Tools like these are needed to help consumers learn about mobile security and how to protect their devices because the leading app marketplaces are not doing enough to make sure the apps they offer pass basic security tests. For a broader, more comprehensive understanding of the threats facing mobile users, its paramount to leverage existing analytics to identify the top vulnerabilities facing users worldwide. At NowSecure we track these vulnerabilities globally and make the real-

time view publically available here to benefit both individuals and security analysts.

(k) Managed Security Services: Requirements and Adoption. Managed security services (MSS) allow many firms, particularly small- and medium-sized businesses, to secure themselves without acquiring expensive in-house expertise, yet there are obstacles preventing seamless market cooperation and accountability between clients and vendors. How can a common understanding of security needs by stakeholders enable faster and more efficient adoption to improve security without sacrificing accountability?

I am Andrew Hoog, CEO and co-founder of a mobile security company called NowSecure. Since 2009, we have been focused on securing mobile devices, apps and enterprises.

What's currently lacking in the mobile space is a common industry approach to standards, disclosure, remediation and education of both individuals and enterprises. Because the mobile world simply moves faster and increasingly affects more users worldwide than traditional computing (a recently discovered Samsung vulnerability potentially affected 200 million devices), responsible disclosure must be carried out on a more accelerated timeline. In turn, developers need to respond by issuing more timely fixes. Developers must also incorporate best practices and security testing into their development cycles, which would prevent many of the most common vulnerabilities from arising in the first place. Enterprises need to explore multiple security tools (software, security apps, intelligence and analytics) and implement intelligent mobile security policies. Individuals must learn how to use apps securely and take charge of their own data. Wireless network providers must recognize they have a role to play in protecting their users' data.

Increasing availability of user device security data, as can be seen here, will provide a more transparent view of vulnerabilities, leading to the ability of individuals and enterprises of any size to harness the power of analytics to prevent issues rather than just managing security as a remediation effort.

The app stores can't be expected to address mobile security issues on their own. Only when all stakeholders in the mobile arena begin to take responsibility for improving the state of security will we approach the common understanding needed to advance mobile security worldwide.