Statement of Scott Totzke

Senior Vice President, BlackBerry Security Group

Research In Motion

before the

Subcommittee on Communications and Technology of

the House Committee on Energy and Commerce

on

"Cybersecurity: The Pivotal Role of Communications Networks"

March 7, 2012

Chairman Walden, Ranking Member Eshoo, and Members of the Subcommittee, my name is Scott Totzke and I am the Senior Vice President of BlackBerry Security at Research In Motion. I am pleased to appear before you today to speak on the issue of cybersecurity.

Research In Motion (RIM), a global leader in wireless innovation, revolutionized the mobile industry with the introduction of the BlackBerry® solution in 1999. Today, BlackBerry products and services are used by millions of customers around the world to stay connected to the people and content that matter most throughout their day. Founded in 1984 and based in Waterloo, Ontario, RIM operates globally in the Americas, Europe, the Middle East, Africa and Asia-Pacific. There are more than 630 carriers and distribution partners offering BlackBerry products and services in over 175 countries around the world. More than 90% of the Fortune 500, as well as countless government agencies, are among our customers. We have a longstanding relationship with the federal government. RIM is proud to serve the U.S. Congress,

the Department of Defense, and the Department of Homeland Security, just to name a few of our valued federal customers.

Mobile communications face similar security risks as non-mobile communications. Several of the same types of threats and attack techniques that have existed on traditional computing platforms can impact smartphone users as the power, ubiquity, and computing capabilities of smartphones have increased over the last few years. Most users have yet to realize the applicability of both existing and emerging threats to what is essentially just a smaller and more mobile computing platform than they already use in their home or office.

As with any computer security solution, a mobile solution must take into consideration what applications the smartphone will need to run, what data it will need to send, receive, and store as well as the regulations with which the organization must comply. While the challenges and security concerns are constant regardless of whether the computer is mobile, mobility requires additional considerations due to the constraints of the platform relative to a desktop PC (in terms of screen size, computing power, battery life, and network capacity) and the ubiquity of mobile smartphone use across diverse populations. An effective and comprehensive mobile security solution must therefore provide protection by preventing unauthorized access to the smartphone and its data, to data in transit over the wireless network, and to the corporate network using features that are built into the platform in order to properly account for these inherent limitations. While technology vendors can provide components of these solutions, it is equally important that, as a mobile technology industry, we help government, enterprises, and consumers understand the risks involved with all types of online activities.

The topic of cybersecurity is becoming increasingly predominant in discussions related to the worldwide growth of mobile data and communications for consumers and enterprises. At its core, cybersecurity means protecting and securing our networks from all forms of attacks and ensuring that these networks continue to operate in times of crisis. For governments and enterprises this is best done through the application of a cybersecurity policy that enhances the safety of an organization, its partners, and its customers, thereby minimizing the risk of exposure and possible exploitation and maintaining valuable brand credibility. The cumulative measures

that individuals and organizations take to protect their network assets (personal computers, mobile phones, servers, and so on) are generally known as cyber defense. To understand the impact of cybersecurity and cyber defense in the global conversation, and most relevant to this Subcommittee, we must understand the value of security in mobile communications.

RIM focuses on designing secure and efficient solutions for enterprises and consumers. A longtime innovator and leader in mobile communications, RIM has a history of integrating security features into its products and firmly believes that security technologies are an important foundation for a digital economy. Furthermore, RIM's position is that built-in security features are essential to the delivery of any technology that will be used for mobile communications if governments, enterprises, and citizens are to benefit from a consistent foundation of security. RIM has also built in features that allow for data to be encrypted and protected from unauthorized access, to limit and control access to information on the smartphone by third party applications and to remotely erase sensitive information in the case where a smartphone is lost or stolen. These controls can all be centrally managed by the BlackBerry Enterprise Solution, which is designed to give large and small organizations the ability to balance individual and enterprise use of BlackBerry smartphones while protecting the privacy of their corporate and employee information.

Without this level of built-in security, individuals and organizations are left to employ a variety of solutions, including antivirus software, firewalls, and encryption, to help protect personal information on mobile platforms. As an industry, we need to meet the public demand for secure personal and business information, and our communication solutions need to provide built-in security features that allow users to manage their privacy protection easily and consciously. Every security decision is an exercise in risk management and we need to ensure that the technology that users have access to provides a level of transparency and assurance around the protections afforded to them by their mobile solution providers.

RIM also believes that there needs to be more focus on security testing and certification that establishes a baseline for technology vendors. Security is a complex discipline that requires users to make informed decisions about their information. Without an established baseline to

properly gauge the security of a product or network, it is becoming increasingly difficult to make these informed decisions. Vendors that work to certify their mobile solutions through trusted validation programs provide assurance to governments and consumers who would otherwise be unable to verify the security of the mobile technologies they use. BlackBerry products and solutions have already received more security accreditations globally than any other wireless solution and our customers value this level of transparency when it comes to protecting their information. Greater adherence to security standards like FIPS would help customers better understand their personal and professional investments in protecting their information. The assurance that the information of a business, however large or small, established or entrepreneurial, is trusted and suitable for use by some of the most security-conscious organizations in the world is an essential cornerstone in developing trust and confidence in the online economy and its established and emerging brands. As citizens merge their private and business lives on their mobile smartphones, this principle becomes essential to their safety and livelihood.

RIM owns and operates the global BlackBerry Infrastructure (sometimes referred to as the Network Operations Center or NOC) and manages the delivery of wireless messages on various wireless networks sent to and from BlackBerry smartphones. This model simplifies wireless for customers and optimizes protocols for wireless environments by creating a trusted bridge between private networks – the customer's internal network, multiple carrier networks, and RIM's service delivery infrastructure — yet it also ensures that there is a trusted path between all parties that is based on strong, cryptographic, mutual authentication.

The BlackBerry Infrastructure is an integral part of RIM's ability to deliver industry leading push services, security, manageability, and spectral efficiency for RIM's customers and partners. It is designed to efficiently manage the transport of messages between the wireless network and a smartphone and it transfers more than 25 petabytes of data traffic in a month. All messages sent to and from BlackBerry smartphones can be routed through the BlackBerry Infrastructure by default and the BlackBerry Infrastructure is designed to provide a highly secure connection between an organization's network and its smartphones.

Unlike traditional VPN solutions, the BlackBerry solution utilizes built-in, efficient protocols that allow them to authenticate with each other while they transfer data. By building mutual authentication and security directly into the data transfer protocols, the system ensures that every packet contains information that is useful to the end user. This is especially relevant in times of crisis when carriers' network infrastructure can become overwhelmed or are operating at a greatly reduced capacity. The blend of security and spectral efficiency allows BlackBerry smartphone messaging systems to remain fully operational when most in need – an essential element of any mission critical network.

Lastly, the panel has raised concerns regarding two extremely important points related to the evolution of security in the technology and mobility industry that I would like to address.

The first concern is related to information sharing. While there is increased competition between vendors there is also increasing commonality in the components used by many desktop and mobile platforms. This directly translates into an evolving risk of cross platform vulnerabilities, creating a level of shared risk that increases the need for vendors to work together to responsibly disclose and address these concerns. This also means that programs such as RIM's Information Sharing Program (RISP) need to fully engage with public sector groups such as US CERT to ensure the timely and bidirectional flow of critical security information.

The second issue raised is related to supply chain security and the impact it can have on the security and availability of networks. A product that has been modified or created in an unauthorized manner could pose significant risk to the security of our customers' information and to the overall security posture of RIM's BlackBerry Infrastructure, our carrier partner networks, or our customers' networks. RIM has been working for several years to embed network security elements directly into the silicon of our products and into all aspects of our manufacturing processes to ensure that only authentic BlackBerry products are allowed to obtain network services. We believe that this combination of hardware security, operational security in manufacturing facilities, software security, and network security work together to mitigate many of the concerns about "knock off" products or products that have otherwise been tampered with.

We support the Subcommittee's efforts to raise awareness of the wide-reaching impacts of the supply chain security issue.

Chairman Walden and members of the Subcommittee, I would like to thank you once again for the opportunity to provide RIM's perspective on these critical issues.