STATEMENT

Of

JOHN J. OLSEN
SENIOR VICE PRESIDENT AND CHIEF INFORMATION OFFICER
METROPCS COMMUNICATIONS, INC.

Before the

SUBCOMMITTEE ON COMMUNICATIONS AND TECHNOLOGY
COMMITTEE ON ENERGY & COMMERCE
UNITED STATES HOUSE OF REPRESENTATIVES

On

CYBERSECURITY: THE PIVOTAL ROLE OF COMMUNICATIONS NETWORKS

March 7, 2012

Thank you, Chairman Walden and Ranking Member Eshoo. It is an honor to appear before you and your colleagues on the Communications and Technology Subcommittee today. I hope that you will find my testimony to be informative and helpful as Congress debates the appropriate role of the Federal government in the important area of cybersecurity and private sector communications networks.

My name is John J. Olsen. I am the Senior Vice President and Chief Information Officer for MetroPCS Communications, Inc. I have nearly 30 years of experience in the information technology and communications fields. Prior to joining MetroPCS in April 2006, I served as the Chief Technology Officer at a heath care technology company, as a Vice President of Systems Development and then as a Vice President of Information Technology Engineering at another major wireless and wireline telecommunications provider, and as the Chief Information Officer at a large business network solutions provider. Before that, I held a number of positions managing information technology for a large electric and gas utility. I began my career as a Director of Management Information Systems for the U.S. Air Force School of Aerospace Medicine.

MetroPCS is headquartered in Richardson, Texas, and is a leading provider of unlimited wireless communications services for a flat-rate on a no annual contract basis. We currently are the fifth largest facilities-based wireless provider in the United States based on number of subscribers served, and we operate networks covering approximately 100 million people. As of December 31, 2011, MetroPCS had over 9.3 million subscribers.

As a leading innovator in the wireless industry, MetroPCS was the first provider in the United States to launch a 4G LTE commercial network in 2010, the first to launch a dual mode

4G LTE/CDMA phone and the first carrier to provide a dual mode 4G LTE/CDMA handset using the Android operating system. MetroPCS currently offers consumers 4G LTE services in the following major metropolitan areas: Atlanta, Boston, Dallas-Fort Worth, Detroit, Jacksonville, Las Vegas, Los Angeles, Miami, New York City, Orlando, Philadelphia, Sacramento, San Francisco and Tampa. And with MetroUSA$^{(SM)}$, MetroPCS customers can use their service in areas throughout the United States covering a population of over 280 million people through roaming agreements MetroPCS has reached with other carriers.

MetroPCS also owns and operates approximately 160 retail stores, but the majority of our customers purchase their service plans and phones and pay their bill through thousands of independent MetroPCS dealers, of which a substantial portion are minority or women owned businesses. Consumers also can purchase MetroPCS services through Amazon.com as well as online through our own website.

To support our business and our customers, we use four IT networks for our business and communications network operations. All four networks are critically important to maintaining our ability to provide reliable services to our customers and safeguarding proprietary customer and corporate information. I am responsible for three of the company’s IT networks: M-Net, SOA-Net and V-Net. The other network, OD-Net, is operated by our engineering group.

The M-Net (or Metro Net) is used to interconnect our corporate office, regional offices and retail stores. The network carries encrypted subscriber data, email and provides Internet connectivity and data from point-of-sale terminals located in our retail stores. The SOA-Net is the Service Oriented Architecture layer that is mainly used to integrate transactions, including billing, payment processing and customer activations and deactivations, and allows our different vendors and systems to interact with each other. The SOA-Net resides within the Amdocs data center. The V-Net (or vender net) is the point-to-point vendor network that is mainly used for vender transactions that are not integrated through SOA-Net or which do not interact with the Amdocs billing system. The OD-Net or Operational Data Network is the IT network that connects the facilities and backhaul of our communications network.

All four of MetroPCS' IT networks utilize Multiprotocol Label Switching (MPLS) circuits from two large, well-known and highly reputable national service providers based in the United States. The MetroPCS IT network equipment, including hardware, routers, switches, firewalls, intrusion prevention systems and wireless access points, are made by a major, well-recognized reputable vendor based in the United States.

MetroPCS also operates a separate WiFi network in each of its retail stores for customers and employees to use for demonstrations and other purposes. However, each is a stand-alone private network that does not connect to any of the other MetroPCS networks.

Security of these critical networks and the customer and personal information transmiting over these networks is very important to MetroPCS. To secure these networks, MetroPCS maintains a comprehensive "risk-based" information security program built on industry best practices covering people, process and technology. The foundation for the program includes standards such as COBIT (Control Objectives for Information and Related Technology), ISO 27001 (an international standard for information security management) as well as other compliance-related standards. MetroPCS uses a combination of hardware, software and services to secure its IT networks.

Our security program directives are driven by a formal “governance” function ensuring that the program is aligned based on defined organizational risk tolerance levels. Other program component highlights include centralized policy management, security awareness, training, internal and third-party monitoring, physical protections, threat identification and vulnerability management as well as intrusion prevention.

Further, the ongoing validation and improvement of our security program is based on periodic internal and third-party assessments and auditing.

As for the nuts and bolts of our program, we are especially focused on security at the perimeter and use multi-level security technologies to secure our networks, and to prevent unauthorized access from both inside and outside our company. We also conduct regular network security audits and penetration tests. As part of our security program, we have third party vendors conduct regular network security audits and penetration tests. Further, we have standardized on a single provider for the equipment for all of the networks which, in our view, increases the effectiveness of firewalls and encryption which we use extensively. Our networks are also broken up into segments with firewalls between critical segments. For example, there is a firewall, as well as other security measures, between our retail stores and the rest of our networks. Amdocs, which holds our customers’ CPNI, also is firewalled off from the rest of MetroPCS’s IT networks. Our independent dealers also do not have access to MetroPCS’ IT networks. Rather, they connect through our Amdocs billing system using secure sessions.

For the networks that I manage, we have implemented 24 hour monitoring solutions, which includes devices placed within our network to monitor for any kind of malware, intrusion attempts or other unusual activity. We also monitor the devices for performance anomalies and suspicious activity which could be evidence of an attack.

Our monitoring efforts, which are augmented by our cybersecurity partners, can generate hundreds of thousands of alerts a day regarding potential cyber threats, but they are pared down through focused review to just a handful of potential threats that merit attention, which we immediately address.

The OD-Net used by our communications network, which is managed by our engineering group, employs similar technology that we use on the other IT networks. It is important to note that MetroPCS has built a 24/7 Network Operations Center ("NOC") in the Dallas area that monitors every switch and cell site on the communications network as well as the OD-Net. The security for the OD-Net is handled through the NOC.

Of course, MetroPCS has implemented numerous physical security measures to protect its data center and NOC, such as the use of multiple levels of card key and biometric access and security. And, MetroPCS has a second data center for disaster recovery in another region of the country where critical systems are replicated to enable the networks and systems to get back up and running in the event of a localized event in Dallas.

MetroPCS' information security staff also maintains vendor-specific and industry-recognized certifications and organizational memberships. In addition, the information security staff regularly participates in vendor-sponsored symposiums and industry summits and conferences. We are involved in these groups not because we are required to, but because they are a valuable source of knowledge sharing and best practices.

While MetroPCS cannot say definitely that we have never had a cyber intrusion, we are not aware of any significant cyber intrusions or cyber attacks that have been successful at disrupting our IT network.

In light of the significant voluntary measures MetroPCS takes to secure its key IT networks without any government mandate and, to date, has avoided any successful cyber attacks, MetroPCS does not believe that additional government regulations are required or warranted at this time, particularly for private sector communications service providers, such as MetroPCS, that do not provide services to the Federal government or local public safety organizations. Private sector companies like MetroPCS are already well incented to protect their networks because their customers would have a negative reaction to cyber intrusion, especially one that disrupts service on the network or exposes CPNI or customer personal information.

This is particularly true for service providers like MetroPCS who provide services on a month to month basis where customers can terminate service at any monthly renewal without any penalty. This provides a powerful economic incentive to protect customer information. Further, there is substantial retail competition for wireless carriers. If MetroPCS does not provide the level of protection its customers want or demand, its customers can terminate service and activate service with the numerous other facilities and non-facilities based competitors. Moreover, wireless providers do have other reasons to voluntarily undertake these measures. Current Federal regulations like the Federal Communications Commission’s CPNI rules and private sector certifications such as PCI for credit card transactions also force communications service providers to invest in the appropriate tools and practices to detect and deter cyber threats to their networks.

MetroPCS also believes that private market forces are better suited to respond quickly to constantly changing cyber threats. While MetroPCS does not believe additional government regulation is necessary at this time, if regulations are considered, MetroPCS urges that these commercial requirements be flexible and tailored to the size and amount of threat a particular private sector provider may face. Regulatory compliance can be particularly burdensome for competitors such as MetroPCS who compete by maintaining a low cost structure.

MetroPCS does support the enhanced sharing of information regarding cyber threats by the Federal government as long as there is no mandated reporting requirement imposed on the private sector. Unfortunately, even obligations imposed on industry that start out as "voluntary" could evolve into a burdensome mandatory requirement on industry, where the costs far out weigh the benefits. In that light, a Federal government sponsored central clearinghouse for cyber threats could be useful to private sector entities like MetroPCS and our third party vendors that currently waste a great deal of time tracking false threats. While IT security companies collaborate and maintain their own cyber threat databases, there is no central clearinghouse for industry to utilize. Additionally, MetroPCS supports those who advocate immunity from lawsuits for private sector entities if such a clearinghouse is established. Basically, there should be no liability if a private sector company does or does not use the information that may be available in the central clearinghouse.

Overall, any cybersecurity legislation that Congress may consider should focus more on protecting the government's own critical IT systems and networks from cyber threats and sharing critical information with private industry. And while the private sector may be able to help the government in that regard, it should not be used as a means to impose onerous and unwarranted regulations on the private sector.

Thank you again for the opportunity to testify, and I look forward to any questions that you may have.