Wireless Innovation Forum Spectrum Sharing Committee Releases Two New Security Related Technical Specifications for the 3550-3700 MHz Band

CBRS Operational Security and CBRS Communications Security address various security issues including cybersecurity, threat models, Public Key Infrastructure policies, and more

For Immediate Release

Washington, DC, 25 August 2016 – The Wireless Innovation Forum (WInnForum), a non-profit international industry association dedicated to driving the future of radio communications and systems worldwide, today announced the public availability of two new reports that address security issues related to the 3550-3700 MHz, or Citizens Broadband Radio Service (CBRS) band. The reports, “CBRS Operational Security Technical Specification” and “CBRS Communication Security Technical Specification,” were produced by its Spectrum Sharing Committee’s (SSC) Security Working Group, led by Charles Clancy a founder of Federated Wireless. They are available publicly here: http://groups.winnforum.org/Specifications.

“Security design for the CBRS ecosystem is a critical ingredient in preparing the band for commercial use,” said Greg Billock (Google NASDAQ: GOOGL), chair of the Communications Task Group which prepared the Communications Security (COMSEC) document. “These specifications represent the outcome of productive and enthusiastic participation from industry and government parties. Congratulations on this milestone to the Forum members and observers, who have all spent so much time fine-tuning designs for this critical area of CBRS operation."

The overall security concept for the 3550-3700 MHz CBRS includes operational security of the Citizens Broadband Service Devices (CBSDs), Spectrum Access Systems (SASs) and Environmental Sensing Capabilities (ESCs). Operations security (OPSEC) is a military discipline that enables mission success by preventing inadvertent compromise of sensitive or classified activities, capabilities, or intentions at the tactical, operational and strategic levels. This is distinct from the operational security of the CBRS, which encompasses a wider range of security disciplines, including cybersecurity. Cybersecurity includes protection of data in transit and at rest from attack through communications security, physical security, personnel security, and supply chain risk management.

The OPSEC document addresses both requirements to preserve incumbent operations security as required by the Federal Communications Commission (FCC) for operation in the 3550-3700 MHz CBRS band and operational security of the CBRS, with the exception of the policies described in the COMSEC. Policies described in the COMSEC document are part of the Public Key Infrastructure (PKI) which governs communications within the Citizens Broadband Radio Service ecosystem and provides authentication and authorization for messages exchanged within the SAS ecosystem as part of the protocols described in the SAS-CBSD Technical Reports and the SAS-SAS Technical Reports.

The OPSEC document provides an overview of regulatory requirements and thread models, including ESC requirements, protection zone activation, exclusion/protection zone activation obfuscation, authorization limiting, obfuscating incumbent episodes, public release of CBSD registration information, and channel availability lists – incumbent frequency obfuscation.

“We are pleased that the Spectrum Sharing Committee members were able to keep the momentum moving for commercialization of the 3.5 GHz band with the release of these two important security reports,” said Kurt Schaubach, CTO of Federated Wireless (a subsidiary of Allied Minds LSE: ALM). “It is critical to have the security principles in place as we proceed towards the conclusion of the certification process for our Spectrum Access System and Environmental Sensing Capability. The WInnForum continues to help shepherd the advent of shared spectrum which will be a true disruptor in the future of wireless networks.”

The COMSEC document overviews elements of the PKI such as the actors and structure, and includes the transport security protocol, blacklisting information and security procedures and best practices.

Announced in February 2015 (http://groups.winnforum.org/d/do/7966), the SSC was specifically formed to develop the solutions and standards that will encourage rapid development of the CBRS ecosystem, protect incumbent operations, and benefit all potential stakeholders in the band. The SSC benefits from participation of a broad based group that includes wireless carriers, network equipment manufacturers, potential SAS Administrators, satellite operators, existing 3650-3700 MHz band licensees, and other parties with an interest in the 3550 MHz band. The committee has formed multiple sub-groups/task groups; participation in these work groups and task groups currently encompasses some 120 participants from over 40 different organizations. Work products from the committee can be found here: http://groups.winnforum.org/ssc-work-products.

Supported by platinum sponsors Google, Motorola Solutions, Finmeccanica and Thales, WInnForum has several working groups focusing on projects related to Software Communications Architecture (SCA) and Spectrum Innovation. Visit http://www.WirelessInnovation.org to learn more. Individuals or organizations wishing to participate in WInnForum Working Groups should contact Lee Pucker at Lee.Pucker@WirelessInnovation.org.

###

About the Wireless Innovation Forum

Established in 1996, The Wireless Innovation Forum (SDR Forum Version 2.0) is a non-profit mutual benefit corporation dedicated to advocating for spectrum innovation, and advancing radio technologies that support essential or critical communications worldwide. Members bring a broad base of experience in Software Defined Radio (SDR), Cognitive Radio(CR) and Dynamic Spectrum Access (DSA) technologies in diverse markets and at all levels of the wireless value chain to address emerging wireless communications requirements. To learn more about The Wireless Innovation Forum, its meetings and membership benefits, visit www.WirelessInnovation.org.

Editorial Contacts

Lee Pucker, 604-828-9876, Lee.Pucker@wirelessinnovation.org or
Stephanie Hamill, 970-290-9543 or Stephanie.Hamill@wirelessinnovation.org