Media Release

Communications Security Continues to Improve in the 5G Wireless Era

5G Americas White Paper Details Emerging Security Threats and Safeguards as 5G Wireless Networks Move Towards tions. Today,

5G Americas, the wireless industry trade association and voice of 5G and LTE for the Americas, today published a whitepaper titled *Security Considerations for the 5G Era,* highlighting enhanced security protocols for 5G, as it evolves and matures to address emerging, security threats in the wireless cellular landscape.

The white paper identifies how 5G wireless technology significantly differs from previous generations, as the entire wireless cellular network has been re-architected to use new capabilities such as software-defined networking (SDN), network function virtualization (NFV) for new services, and cloud-native architectures for scalability. The implementation of these elements requires additional encryption, extra defense in edge networks, and sophisticated new protocols to handle the demands of network slicing, multi-access edge computing (MEC), and a disaggregated, radio access network (RAN).

Chris Pearson, President of 5G Americas said, "5G networks are beginning to touch every facet of human life - from work, entertainment, personal and social activities, making security central to this monumental technology. Mobile Network operators and their vendor partners have always and will continue to put security as a top priority for their networks."

Security Considerations for the 5G Era delves into 5G architectures that are designed to close possible security gaps from previous generations of cellular networks, as well as manage new security challenges outside the traditional framework.

This 5G Americas white paper will cover important aspects such as:

- h

David Krauss, Principal Network Architect for Ciena, and leader for the project, said, “Security has been designed and incorporated into 5G standards. A strategic approach is taken related to cloud-native services, open-source software, APIs, SDN, and NFV, which together provide greater overall 5G network security.”

This paper further addresses:

- technology threats that remain in the RAN and how they may be tackled
- detailed 3GPP designs for 5G security capabilities involving confidentiality, integrity, authentication, privacy and isolation
- Network Slicing capabilities that provide greater isolation, privacy, and security across 5G networks
- more highly defined cyber threat intelligence protocols
- Security-as-a-service (“SaaS”) through service-based architecture
- how network operators should address vulnerabilities from interworking with 3G/4G systems, such as 5G short message service (SMS) over non-access stratum (NAS)