WG 4: Network Security Best Practices

Co-Chair – Rodney Joffe, Sr., NeuStar
Co-Chair – Rod Rasmussen, Internet Identity
FCC Liaison – Kurian Jacob

Description: This Working Group will examine and make recommendations to the Council regarding best practices to secure the Domain Name System (DNS) and routing system of the Internet during the period leading up to the successful global implementation of the Domain Name System Security Extensions (DNSSEC) and Secure BGP (Border Gateway Protocol) extensions.
DNS is the directory system that associates a domain name with an IP (Internet Protocol) address. In order to achieve this translation, the DNS infrastructure makes hierarchical inquiries to servers that contain this global directory. As DNS inquiries are made, their IP packets rely on routing protocols to reach their correct destination. BGP is the protocol utilized to identify the best available paths for packets to take between points on the Internet at any given moment. This foundational system was built upon a distributed unauthenticated trust model which was sufficient for the early period of the Internet.

These foundational systems are vulnerable to compromise through operator procedural mistakes as well as through malicious attacks that can suspend a domain name or IP address's availability, or compromise their information and integrity. While there are formal initiatives under way within the IETF which has been chartered to develop Internet technical standards and protocols that will improve this situation significantly, global adoption and implementation will take some time. This Working Group will examine vulnerabilities within these areas and recommend best practices to better secure these critical functions of the Internet during the interval of time preceding deployment of more robust, secure protocol extensions.

Duration:
1. DNS Security Best Practices - September 12, 2012
2. Routing Security Best Practices – March 6, 2013

