ATIS – RNTF
GNSS Stationary Timing Receiver Resilience Workshop
User Needs, Wants and the State of the Market

http://atis.org/trr

Booz Allen Hamilton facility
8283 Greensboro Drive, McLean Virginia
April 17, 2018

Corporate Support from

Booz | Allen | Hamilton and SPIRENT

Workshop Purpose

Stimulate use of more resilient Global Navigation and Satellite System (GNSS) receivers, including antennas, specifically focusing on stationary precision timing receivers.

Workshop Goals & Products

1) Identify GNSS timing receiver system (including antenna) resiliency needs within the United States telecom, electric power and financial service industries. Product will be a list, by industry, of potential threats against which resiliency is desired.
2) Identify the state of the market and the state of technology for resilience to these threats. Products will be the lists of threats from Goal 1, with each threat annotated as to whether a countering technology is available on the market now, not available on the market but the technology exists, or the technology does not exist. Also included will be an indication as to the degree to which a countering technology may be effective against the threat.
3) Discuss a roadmap for providing reliable information to industry stakeholders on specifics of receiver resilience capabilities that stakeholders require. Products will be a list of ideas to be further explored and a consensus of whether or not a follow-on workshop is desirable.

The Working Group is inviting representatives of timing users from the electric grid, financial and telecommunications industry, as well as from timing receiver manufacturers to participate in this event, and from companies and organizations that might do testing. If you know of a good representative from one of these areas, or would like to attend yourself, please complete the registration application on the ATIS website listed above.

Workshop organizers are interested in ideas in advance of the workshop for potential threats to GNSS timing systems against which receivers might have resiliency features. The following is a preliminary list to which we would like contributions from users. Please send all input and ideas to the link on the ATIS website above.

Potential threats include:

I. System issues
   a. Compliance and response to basic issues: leap seconds, reference date field roll-overs, etc.
   b. Errors and failures: data fields with impossible numbers, clock data errors (think UTC off by 13 micros), on-board clock failures
   c. Compliance with Interface Specification documents such as IS-GPS-200H (ensures receivers will be able to operate with future allowed changes to signals)
   d. Poor processing of multiple GNSS signals (modernized GPS signals), and how this processing is done

II. Out of Band Interference

III. Jamming (unintentional and intentional)
   a. Antenna design
   b. Signal processing to mitigate effects
   c. Holdover capabilities

IV. Spoofing Detection and Resistance
   a. Spoofing detection alone, with alerts
   b. Various levels of resistance from simple and inexpensive to complex and expensive
   c. Use of better clocks or alternate signals to detect/resist/mitigate