Communications Daily
The authoritative news source for communications regulation
A service of WARREN COMMUNICATIONS NEWS

## ATIS Makes GNSS Vulnerability Recommendations Amid GPS Vulnerabilities

ATIS recommended government take more actions to ensure GPS and global navigation satellite system security, amid vulnerabilities. They **are**: establish a positioning, navigation and timing (PNT) program for civilian infrastructure; publish GPS disruption analysis; develop a self-assessment tool that helps organizations and individuals discover how and where they use and depend on PNT; monitor for GPS/GNSS disruptions; and enhance efforts to enforce spectrum violations. ATIS' Sync committee suggestions stemmed from an April GNSS Stationary Timing Receiver Resilience Workshop, "and represent the views of government, industry and GPS/GNSS users," **said** ATIS CEO Susan Miller Wednesday. The suggestions were sent to DOD, the Commerce, Homeland Security and Transportation departments, the National Security Council, National Space Council and Office of Management and Budget. Putting the recommendations "into action will speed development of solutions to mitigate the risks to the systems that are the critical backbone for precision timing for so many industries," Miller said, and is part of ongoing work. The FCC last month approved U.S. nonfederal devices accepting signals from Europe's Galileo GNSS system, though Commissioner Jessica Rosenworcel raised security concerns (see **1811150028**). During the federal government's closure Wednesday, her office and the FCC didn't comment. Trimble didn't comment, and Garmin referred our query to the GPS Innovation Alliance. That group "strongly" backs "enhanced enforcement against spectrum violations and welcome[s] efforts that facilitate the sharing of information, raise awareness and collaboration of stakeholders to improve the resilience of critical systems," said Executive Director David Grossman.