RESILIENT NAVIGATION and TIMING FOUNDATION

Emergency Services Sector (Law Enforcement, EMS & Incident Management)

Use of Positioning, Navigation and Timing (PNT) Services

These comments are based upon public and private assertions made by representatives of this Critical Infrastructure/Key Resource (CI/KR) sector and PNT subject matter experts that have examined such issues. Some members of CI/KR sectors might not provide public comment out of a desire to avoid disclosing vulnerabilities and/or proprietary information. Therefore, the RNT Foundation is providing this response for the public record "on their behalf." See explanatory notes at the end of this document.

GPS PNT services have been integrated into virtually every technology and are a critical to nearly every facet of life in America. As such, their impact on one sector very much impacts another. For example, the transportation and communications sectors both rely heavily on GPS, and all sectors rely heavily on transportation and communications. The comments in this response try to address only the ways in which GPS/ PNT services are uniquely used by this sector.

These comments have been structured to respond as directly as possible to the questions posted in the Federal Register (***bold italics*** below).

(a) A brief description of your application(s) of positioning, navigation, and timing services;

Sidebar: As a general matter, this sector depends upon PNT in much the same way as other sectors, though uses are often much more often likely to result in the immediate and direct saving or loss of life and/or property, prevention or prosecution of crime, etc. PNT use by the Transportation Systems, Communications, and Information Technology sectors are especially key.

Tracking – Tracking devices are used to overtly monitor offenders as an alternative to confinement. They are also used to covertly track the movements of suspected criminals and terrorists as a part of on-going investigations.

Common Operational Pictures – Routine operations and responses to incidents are coordinated and made much more effective through the use of "blue force tracking" and displaying locations in common operational picture.

GPS Jamming and Spoofing –

By Friendly Forces – Some law enforcement agencies have the ability to jam cell phone and GPS frequencies as a method of denying their adversaries the ability to communicate, detonate weapons, etc.[1]

By Hardened Adversaries – The FBI has issued an advisory that GPS jammers have become a favorite tool of organized crime and provided several examples of its use in major thefts.[2] These groups include international criminal networks such as drug cartels[3]. An ad hoc survey near a US international airport showed 25-30% of trucks had GPS

[1] http://www.washingtonpost.com/wp-dyn/content/article/2009/01/31/AR2009013101548.html
[2] https://info.publicintelligence.net/FBI-CargoThievesGPS.pdf
[3] http://www.rx-360.org/LinkClick.aspx?fileticket=PDU23r9W9IM%3D&tabid=209

jammers.[4] These drivers were obviously trying to avoid being tracked, but it was not possible to determine whether it was to facilitate other criminal activity or evade surveillance for another reason. Relatively simple jamming technology, and more complex spoofing technology, are readily available to both criminal and terrorist organizations and pose a significant threat to homeland and national security.

By "Unintentional" Adversaries - The FCC has advised that use of "personal privacy devices" and other equipment that disrupt GPS signals is increasing in the United States. Individuals using such devices have disrupted airport landing systems[5], cargo cranes at ports[6], and cell phone signals[7]. While their intentions are often non-criminal (one employer was trying to improve workplace safety), their acts are. They also have the potential to cause disruptions that directly lead to the loss of life, property damage, or severe negative economic consequences.

(b) the positioning, navigation, and/or timing performance required for a complementary PNT capability to support operations during a disruption of GPS that could last for longer than a day,

To qualify as a "complementary" system, a new PNT capability would need to:

1. **Provide very wide area, precise, wireless location and timing services.** The timing signal would need to be synchronized with UTC (and therefore GPS, when in it is in operation) and location information would have to correspond to that obtained from GPS as closely as possible.
2. **Have features and/or capabilities not available with GPS.** Without such it would be a "duplicate" or "redundant" service, vice "complementary." Desired features for special-purpose users, such as First Responders and the military, include a signal that is usable under foliage, underground (i.e., garages), indoors and that has a robust, security-capable, data channel for differential corrections and other information.
3. **Likely remain functioning in situations when GPS is disrupted.** The complementary system should have different signal characteristics, and therefore different failure modes, than GPS. These include a signal that is terrestrial based, high power and in a frequency band far distant from that of GPS.

   System performance should match that of GPS as closely as possible to ensure continuous support to all the services and applications now used by the Emergency Services sector that rely directly or indirectly upon GPS.

(c) availability and coverage area required for a complementary PNT capability,

Availability. Any system intended to complement GPS should have the same availability as the GPS system.

[4] http://www.gps.gov/governance/advisory/meetings/2014-06/scott.pdf
[5] http://www.fcc.gov/document/32k-penalty-proposed-use-gps-jammer-individual
[6] http://rntfnd.org/2015/02/11/gps-disruption-halts-ports-endangers-ships-us-coast-guard/
[7] http://www.fcc.gov/document/fcc-proposes-29k-fine-employer-jammed-employee-cell-phones

Coverage. As illustrated in the graphic at the end of these comments, a multi-layer model provides the best PNT resiliency. eLoran complements GPS/GNSS' global coverage, provides continental PNT coverage, and complements or enables local PNT coverage.

The system should be as ubiquitous as possible as emergency services are required to operate in every portion of the US, including its navigable waters and Exclusive Economic Zone.

(d) willingness to equip with an eLoran receiver to reduce or prevent operational and/or economic consequences from a GPS disruption,

Note: Our interaction with receiver manufacturers causes us to believe this question to be irrelevant except for the first few years of an eLoran system's operation. Once an eLoran system is in operation and receivers are in wide production, the size, weight, power, and cost (SWAP-C) of the receivers will decrease dramatically. We expect most commercial grade navigation receivers to be "multi-mode", having the capability to receive GPS/GNSS and Loran/eLoran. Many receivers might also include inertial, gyro, CSAC, and/or barometric altimeters. Thus it will not be a matter of a user's "willingness to equip," but rather that the market will be automatically equipping the user. As one manufacturer expressed it: "Except for niche applications, building GPS-only receivers wouldn't make sense."

Emergency services organizations find the ability to navigate in areas not currently accessible without pre-installed infrastructure very appealing. These areas include caves, tunnels, sub-basements and other subterranean areas, urban and natural canyons, other areas without a good view of the sky, and underwater locations.

Also very appealing is the ability to send messages to locations indoors, underground and underwater, and to remote and wilderness areas that have minimal infrastructure. Such a capability could be a valuable safety and command and control feature not available with any system now available. By way of example, if eLoran navigation and communications had been available for emergency services during the wildfires of 2013, it could have provided a guaranteed communications path and navigation tool to direct to safety the 19 firefighters who were lost in Arizona.[8]

(e) current and planned availability of e-Loran capable user equipment,

Loran-C and/or Chayka user equipment is now produced by the governments of China and Russia for internal consumption and use with their national systems. Outside of those countries, Loran-C and eLoran receivers are produced in limited quantities, on demand. RNT Foundation discussions with several large receiver manufacturers have indicated that they would readily pursue development of integrated receivers that include eLoran capability if there were Government support for the provision of eLoran service. The estimated economic order quantity for these vendors is approximately 100,000, although the number of units depends upon the market sector served. Also, once this level of production has been achieved, the size of receivers

[8] http://www.cnn.com/2013/07/01/us/arizona-firefighter-deaths/

will undoubtedly be reduced to be compatible with many mobile devices, and the price per unit will drop dramatically (as was the case with GPS technology).

The US Army has extensive information on this as a result of a recent RFI for 50,000 eLoran receivers.

(f) other non-eLoran PNT technologies or operational procedures, currently available or planned, that could be used during a disruption of GPS for longer than a day.

Sidebar: In 2011, Mr. James Caverly, at that time working for the DHS Office of Infrastructure Protection, reported on the department's "**GPS Critical Infrastructure Timing Study: Usage/Loss Impacts/Backups/Mitigation."** This report has never been made public, to our knowledge. A publicly released presentation based on the report provides information about requirements and backup systems for all critical infrastructure sectors and cites the situation generally as worsening.[9]

We know of no other technologies or operational procedures that could take the place of the unique ways in which GPS is used by the Emergency Services Sector.

Offenders being remotely monitored would have to be taken into physical custody, situational awareness for incident responses would have to be created through voice reports, if radio communications were still functioning, and responders would have to navigate to the scene using maps and relying on voice reports to attempt to avoid congestion and find the quickest route.

Explanatory Notes:

1. The Resilient Navigation and Timing Foundation (RNTF):

RNTF is a scientific and educational 501(c)3 non-profit dedicated to helping protect critical infrastructure through (a) stronger laws and better enforcement against jamming and spoofing of GNSS signals, and (b) encouraging strong, difficult-to-disrupt terrestrial systems to complement and provide additional resilience for GNSS.

Our corporate membership includes providers of a broad spectrum of PNT services from development of GPS satellites, to local and indoor positioning systems, and wide area low frequency systems, and some of the world's leading navigation associations. Individual members are concerned citizens and PNT professionals from academia, industry and government.

2. The Reason We Are Providing These Comments:

Our nation's increasing reliance on GPS location and timing information for a very broad spectrum of technologies represents, in the words of Dr. Brad Parkinson, "… a single point of failure for much of America…" We believe that national effort to provide and encourage adoption of diverse

[9] http://rntfnd.org/wp-content/uploads/James-Caverly-DHS-GPS-PNTTimingStudy-SpaceWeather4-27-111.pdf

sources of location and timing information, provided by both federal and private entities, are essential to our national and economic security.

We believe responses to this request for comment may be limited by individual companies' reluctance to air their vulnerabilities or the perception that they would be revealing proprietary information.

3. How These Comments Were Developed:

The information provided was developed in coordination with our members who have had extensive interaction with the critical infrastructure sector being addressed. Information available in the media, professional discussion sites and other "open sources" has also been included.

4. eLoran:

The request for comment mentions in several places a possible "eLoran" system. Such technology is not generally known in the United States, even though it was developed here.

For purposes of this response, we presume that the eLoran system mentioned is similar to the one in operation in the United Kingdom as recently described in a paper presented to the Institute of Navigation[10]. With appropriate ASF corrections, this system's accuracy has been measured at less than 25 feet for location and less than 50 nanoseconds for timing. While we understand that the Dutch have improved on these results, the underlying system is still eLoran. While most technologists agree that much better performance is possible with further system development, our presumption is that the system the government refers to is the one described in the referenced paper.

5. The Importance of Quickly Implementing a Complementary System for GPS

We are unable to improve upon the 2004 Presidential National Security Directive 39 issued by President Bush and affirmed by President Obama that identified GPS as essential to our national economy and national security, and mandated acquisition of a "back-up" system – though we agree that a more appropriate descriptor would be "complementary" system.

Since 2004 threats to GPS have increased, as have the number of disruptive incidents per day. The threats range from fleeting local disruptions such as might be caused by a private citizen passing by with an illegal "Personal Privacy Device," to a global outage resulting from malicious intervention or simple human error.

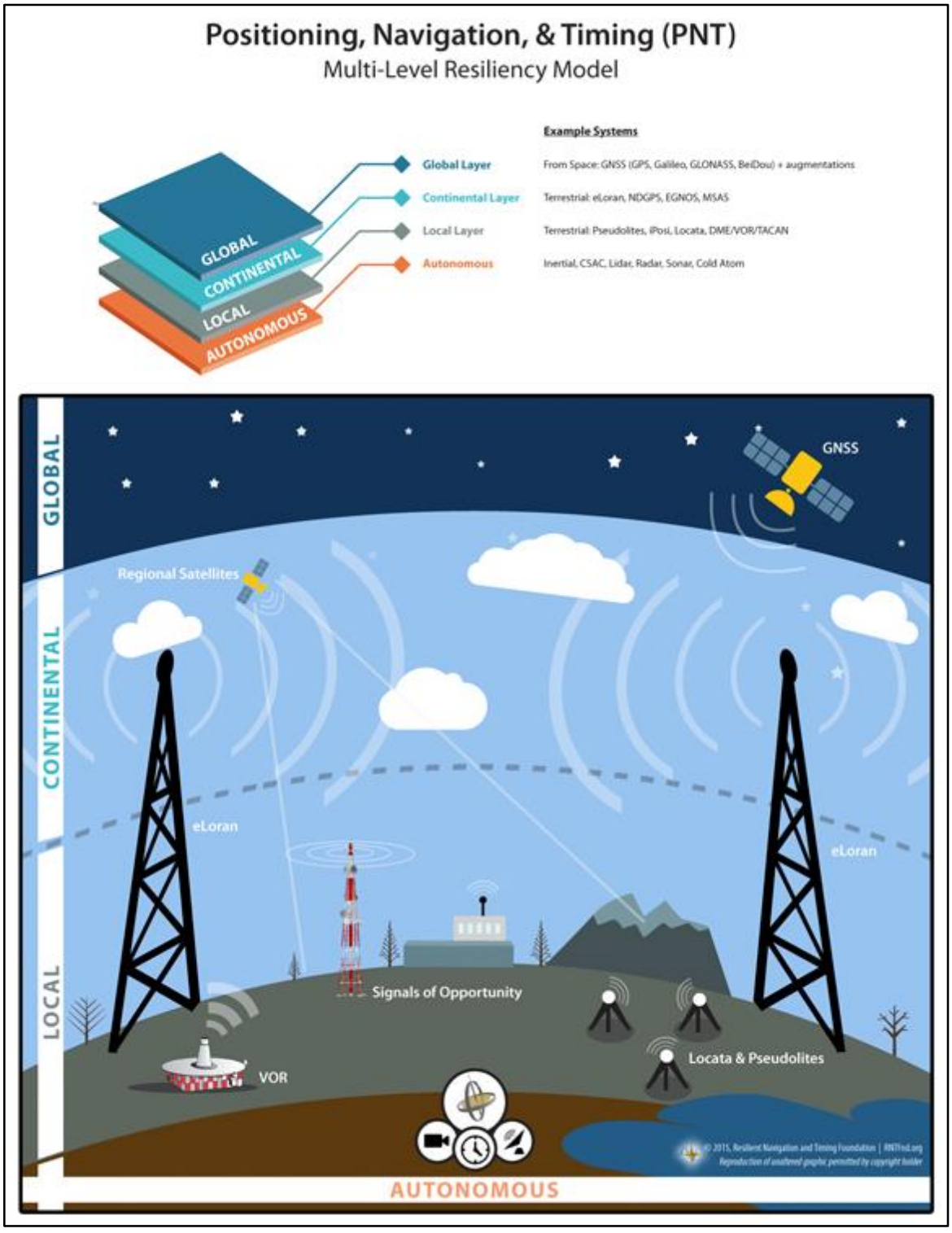
GPS is currently being modernized and made more resilient. It is also being joined by other modern systems, including Galileo (Europe), Beidou (China), QZSS (Japan), INRNSS (India). GLONASS (Russia) is being upgraded over a longer time period to include digitally modulated signals. These have certain resilience features for GPS. These are all positive developments that should be continued in order to improve the overall resilience of our global PNT architecture.

[10] http://rntfnd.org/wp-content/uploads/2015-ION-ITM-Offermans-eLoran-IOC-in-UK-final-4Feb.pdf

In April of last year, GLONASS, the Russian satellite navigation and timing system, experienced two unannounced outages, one of which lasted for eleven hours. If this were to happen to the GPS constellation, unless there were complementary systems, such as other GNSS or eLoran, that users had adopted and which would prevent PNT service disruption, the impact to our critical infrastructure and economy would be widespread and serious.

The larger question, beyond those that the Department of Transportation has posed in the Federal Register, is:

What would happen to our CI/KR, to our nation, and to the daily lives of its citizens, should there be a 24-hour disruption of GPS for any reason?


Positioning, Navigation, & Timing (PNT)
Multi-Level Resiliency Model
Example Systems
GLOBAL
CONTINENTAL
LOCAL
AUTONOMOUS
Global Layer
From Space: GNSS (GPS, Galileo, GLONASS, BeiDou) + augmentations
Continental Layer
Terrestrial: eLoran, NDGPS, EGNOS, MSAS
Local Layer
Terrestrial: Pseudolites, iPosi, Locata, DME/VOR/TACAN
Autonomous
Inertial, CSAC, Lidar, Radar, Sonar, Cold Atom
GLOBAL
CONTINENTAL
LOCAL
GNSS
Regional Satellites
eLoran
eLoran
Signals of Opportunity
VOR
Locata & Pseudolites
AUTONOMOUS