



1200 G Street, NW  
Suite 500  
Washington, DC 20005

P: +1 202-628-6380  
W: [www.atis.org](http://www.atis.org)

November 29, 2018

The Honorable Karen Dunn Kelley  
Under Secretary for Economic Affairs  
**Department of Commerce**  
1401 Constitution Avenue, NW  
Washington, D.C. 20230

Karen Van Dyke  
Principal Technical Advisor  
**Department of Transportation**  
55 Broadway  
Cambridge, MA 02142

The Honorable Claire Grady  
Under Secretary for Management  
**Department of Homeland Security**  
245 Murray Lane, SW  
Washington, D.C. 20528

Rear Admiral Douglas Fears  
**National Security Council**  
Eisenhower Executive Office Building  
Washington, D.C. 20504

The Honorable Patrick Shanahan  
Deputy Secretary of Defense  
**Department of Defense**  
1010 Defense Pentagon  
Washington, D.C. 20301

Art Ray  
**National Security Council**  
Eisenhower Executive Office Building  
Washington, D.C. 20504

Dana Deasy  
Chief Information Officer  
**Department of Defense**  
6000 Defense Pentagon  
Washington, D.C. 20301

Scott Pace  
Executive Secretary  
**National Space Council**  
300 E. Street SW  
Suite 5R30  
Washington, D.C. 20546

The Honorable Jeffrey Rosen  
Deputy Secretary  
**Department of Transportation**  
1200 New Jersey Avenue, SE  
Washington, D.C. 20590

Suzette Kent  
Administrator of the Office of Electronic  
Government  
**Office of Management and Budget**  
725 17th Street, NW  
Washington, D.C. 20503

Dear Recipient:

The Alliance for Telecommunications Industry Solutions (ATIS) SYNC Committee is writing to request Federal Government action to mitigate the impacts of GPS vulnerability to the public. Below are recommendations for governmental action from attendees of the GNSS Stationary Timing Receiver Resilience Workshop sponsored by ATIS and the Resilient Navigation and Timing Foundation on April 17, 2018.

## **About ATIS SYNC**

ATIS is a global standards development and technical planning organization that develops and promotes worldwide technical and operations standards for information, entertainment, and communications technologies. ATIS' diverse membership includes key stakeholders from the Information and Communications Technologies (ICT) industry – wireless and wireline service providers, equipment manufacturers, broadband providers, software developers, consumer electronics companies, public safety agencies, and internet service providers. ATIS is also a founding partner and the North American Organizational Partner of the Third Generation Partnership Project (3GPP), the global collaborative effort that has developed the Long-Term Evolution (LTE) and LTE-Advanced wireless specifications.

Nearly 600 industry subject matter experts work collaboratively in ATIS' open industry committees and incubator solutions programs, which includes SYNC. ATIS SYNC develops and recommends standards and prepares technical reports related to telecommunications network technology pertaining to network synchronization interfaces. GPS vulnerability has been a focus of the SYNC committee activities for the last several years. A technical report, [ATIS-0900005, GPS Vulnerability](#), was issued September 2017.

## **About the Workshop**

About 40 timing and synchronization experts attended the workshop. The primary objective of the workshop was to explore challenges to the adoption of better, more resilient GPS/GNSS (Global Positioning System/Global Navigation Satellite Systems) receivers that would enhance our critical infrastructure and enhance the system to become more secure by mitigating disruptions like jamming, spoofing, and GNSS anomalies. The Department of Defense (DoD) has taken an appropriately aggressive approach to protect itself against GPS vulnerability and threats. During the workshop, there was significant input that a critical effort is needed to support the civilian community. In particular, a core recommendation was that the Federal Government take on an active role by designating a “prime” in efforts to protect the public on this issue.

There was also common agreement that timing and synchronization are essential to almost all critical infrastructure. In this context, the general view of the group was that there is a need to enhance communication to leaders in industry and government and stress the importance of GPS/GNSS signals, including their vulnerability, used for synchronization and timing. Such an increase in awareness would mitigate risk to our critical infrastructure.

## **Recommendations**

Workshop attendees developed a short list of views for use by government, industry, and GPS/GNSS users. Implementing this input would significantly improve the general understanding of the problem and facilitate moving forward to developing solutions to mitigate risk.

- 1. Establish an Assured PNT (Positioning, Navigation and Timing) Program for U.S. Civilian Infrastructure--** As part of its preparatory work, the workshop heard a presentation about the DoD's Assured PNT Program. The Department has recognized GPS vulnerability and is working to harden its equipment and implement alternate PNT sources. Unfortunately, because the vast majority of GPS users are not in the defense/military industries, these civilian users are unable to access and may not benefit from the DoD's investment in Assured PNT. The attendees believed that it is prudent to leverage the DoD

efforts and protect critical infrastructure, transportation systems, and economic security by establishing an Assured PNT program with a single overall federal “prime” to lead its public effort. For example, the existing Department of Homeland Security (DHS) PNT Program Management Office (PMO) could serve this role.

- 2. Publish GPS disruption reports and the government’s analysis** – To improve general awareness and help users protect themselves against future disruptions, the attendees recommended that government make available to the public information on GPS disruptions. It is understood that the Federal Aviation Administration (FAA), U.S. Coast Guard, and others in the Federal Government regularly receive reports of such disruptions; information from these reports should be shared with the public.
- 3. Promote development and use of a PNT maturity model by industries and infrastructure sectors** – Many industries are too reliant on GPS for timing and should assess which complementary PNT or timing systems they should be using. Hence, there is a need to increase awareness among organizational and individual users of the importance of PNT including users’ dependency on it. To that end, it may be beneficial to develop a PNT maturity model, which is a self-assessment tool that helps organizations and individuals discover how and where they use and depend on PNT and where it originates. The government could develop or foster development by industry of a PNT maturity model and encourage its use and maintenance by stakeholders, similar to the Department of Energy’s successful maturity model for cybersecurity.
- 4. Monitor for GPS/GNSS disruptions, interference, and impacts** – The workshop heard from the European Union’s “STRIKE3” project as part of its preparatory activities. With only limited sampling, STRIKE3 has detected hundreds of thousands disruption incidents and categorized them into 300 “jammer families.” Workshop participants were of the view that there could be similar findings in the U.S. and that this information would be useful to the government and the public. Some commenters noted that much “disruption information” was already available from the national security establishment and crowdsourced applications such as “Waze” and only need to be accessed and utilized. A systemized effort in the U.S. to monitor and disseminate valuable data on GPS signal disruption might go a long way to promote the nation’s understanding of the problem, and the ability to educate users about threats and solutions. It also would facilitate enforcement efforts aimed at terminating on-going disruptions and deterring future problems. There have been many concrete instances of GPS disruptions that could have been prevented if this systemized effort was in place.
- 5. Take enforcement action against spectrum violations** – The workshop attendees recommended that the government consider enhancing its enforcement efforts against disruptors of GPS/GNSS signals. Relatively inexpensive, easy to use and easy to maintain equipment is readily available to detect and locate the sources of GPS/GNSS disruptions.

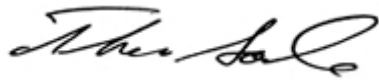
In summary, the above represents the attendees’ highest priority recommendations for governmental action and ongoing dialogue with civilian GPS users to safeguard essential timing and synchronization services. This is by no means an exhaustive list of all input from the

attendees. All the workshop presentations, as well as a summary of their recommendations, can be viewed at <http://atis.org/trr>.

Finally, we want to inform you that ATIS SYNC has initiated discussions to study resilience of GPS receivers and ATIS plans to make information available about this work program as soon it is approved by the committee. ATIS SYNC will be reaching out for input once this work has begun.

If there are any questions, please contact the undersigned.

Sincerely,

A handwritten signature in black ink, appearing to read "Thomas E. Goode". The signature is fluid and cursive, with the first name being the most prominent.

Thomas E. Goode  
ATIS General Counsel