4558 Shetland Green Rd
Alexandria, VA 22312
800-522-6948
inquiries@RNTFnd.org

28 October 2021

Response to Request for Public Comment
Bureau of Industry and Security, Office of Technology Evaluation,
U.S. Department of Commerce

Re: Risks in the Information and Communications Technology Supply Chain
Federal Register Docket Number 210910-0181, Document Number 2021-20229

We are responding to your request for comment, particularly in the areas of:

- "…risks posed by supply chains' reliance on digital products that may be vulnerable to failures or exploitation,"
- "… other capabilities necessary to produce or supply… information communications technology (ICT) hardware," and
- "…specific policy recommendations important for ensuring a resilient supply chain for the ICT industrial base. Such recommendations may include… addressing risks due to vulnerabilities in digital products relied on by supply chains."

Positioning, navigation, and timing (PNT) services are necessary to the ICT hardware supply chain in two very different ways.

First, PNT services directly support the production of ICT hardware. They underpin all transportation systems for production and most logistics systems. They are also essential to many supervisory control and data acquisition (SCADA) systems used in manufacturing, materials processing, management of electrical power grids, and other industrial functions.

Second, PNT services are needed for much ICT hardware to function. Examples include digital land mobile radios, navigation devices, surveying equipment, and wireless network equipment. Therefore, extant PNT service is needed to make production of this ICT hardware worthwhile. As one example of such ICT devices and their use of PNT, enclosure (1) discusses telecom network reliance on Global Positioning System (GPS) signals and the consequences of disruptions.

America’s acute over-reliance on highly vulnerable GPS signals for PNT services poses a major risk to production and use of ICT devices.

We urge the federal government in the strongest possible terms to comply with the requirements of the National Timing Resilience and Security Act of 2018 and establish one or more national alternatives/ backups for GPS signals.

ICT Supply Chain Vulnerabilities and Risks Related to Reliance on GPS for PNT

Most all PNT service in the United States is sourced directly or indirectly from GPS.

The nation’s over-dependence on GPS for PNT across all critical infrastructure sectors has resulted in Department of Homeland Security officials in the Obama administration calling it “a single point of failure” for America.

PNT service from GPS is highly vulnerable to a wide variety of threats. The level of risk from each of these threats is a matter of subjective evaluation and changes over time as technology and global relations develop. That said, all the various threats are widely acknowledged and have been documented by the government. When the cumulative risk from all threats is considered, the need for prompt action is clear and cannot be avoided.

Enclosure (2) discusses each of the following threats:

- Denial of service (jamming) due inadvertent or intentional interference with GPS’ exceptionally weak signals.
- Signal deception (spoofing) resulting in hazardously misleading information to users and/or insertion of false data to systems and records.
- Denial of service due to interference from severe solar activity (coronal mass ejections). This could last several days.
- Damage, disabling, or destruction of GPS satellites and systems from:
    - Cyberattack
    - Kinetic or directed energy attack
    - Debris
    - Coronal mass ejection

Note: Other nations, most notably China, Russia, and Iran, have one or more terrestrial systems that provide PNT services to complement and backup those they receive from space. Thus, the consequences of disrupted space based PNT signals are much greater for the U.S. This makes disrupting GPS signals a much more attractive option for our adversaries than it would be if America had a domestic PNT capability independent of space.

Recommended Actions to Reduce Risks Related to Reliance on GPS and Improve ICT Supply Chain Security:

The President's National Space-based Positioning, Navigation, and Timing Advisory Board has long advocated a holistic approach to protecting GPS signals and users. It involves:

- Protecting GPS signals through active frequency management. This includes sufficient laws and regulations, interference detection, and enforcement resources.
- Toughening users by encouraging adoption of more resilient equipment and, when appropriate, requiring its use.
- Augmenting GPS signals with other PNT sources

Active management of a holistic approach to PNT resilience by the federal government is urgently needed. Executive Order 13905 (20 February 2020), "Strengthening National Resilience Through Responsible Use of Positioning, Navigation, and Timing Services," took some steps toward implementing such an approach. These are necessary but far from sufficient.

While the administration is making some efforts to protect signals from interference and to encourage "toughened" more resilient receivers, nothing is underway to establish one or more augmenting or alterative PNT sources to work alongside and reinforce GPS. This despite numerous studies and several decisions by the federal government to do so (see enclosure 3).

Like GPS, alternatives should include systems that are wireless, easily accessed and adopted, and reach all parts of the nation. This will:

- Provide users alternative PNT during local and widespread GPS disruptions.
- Help stabilize and validate GPS services when used in the same receiver. This will improve overall PNT utility for current and future applications.
- Help protect GPS signals and satellites by making them less attractive targets.

Establishing a backup capability for GPS timing signals is required by statute.

The National Timing Resilience and Security Act (NTRSA) of 2018 requires establishment of a terrestrial backup capability for GPS timing, along with any other systems (space-based or terrestrial) as determined by a technology demonstration program. The Act required this be in place by December 2020.

No monies have been appropriated by Congress to fund such a project. Neither did the Trump administration request any funds.

In its first budget submission the Biden administration did not request any funds and went so far as to propose repeal of the NTRSA.

To the best of our knowledge, nearly three years after its passage, the executive branch has taken no action to comply with NTRSA.

NOTE: For a timing system to serve mobile users independent of GPS, it must also provide a basic level of location information. Thus, complying with NTRSA will support timing and, at a basic level, location information to support production and use of a wide variety of ICT devices.

Our Top Recommendation: Comply with the law. - Establish one or more timing backup capabilities for GPS as required by NTRSA.

The resulting timing and location information will greatly improve the resilience, reliability, and safety of all supply chains and ICT devices that access the new capability.

While establishing such a capability may seem to be a formidable and expensive task for any federal agency, it need be neither.

As was made clear in a recent Department of Transportation report on an alternate PNT technology demonstration program, the needed technologies are mature and available. Also, the government can access the services these technologies provide through commercial contracts. This will speed implementation by obviating the need for an expensive and cumbersome government capital acquisition program and can minimize total costs to the government.

Enclosure (4) is our white paper “A Resilient National Timing Architecture.” It discusses in some detail how NTRSA could be relatively quickly and inexpensively implemented.

Mr. Dana A. Goward
President, RNT Foundation

U.S. Telecommunications Networks' Dependence on GPS Timing

A Case Study of Critical Dependency

Most 4G and 5G networks utilize Time Division Duplex (TDD) transmitters and have a critical timing requirement of 1.5 micro-second UTC time alignment. This is a 3GPP industry standard.

In almost all cases, network applications obtain timing directly from GPS, or from network sources such as PTP that can be ultimately traced back to GPS.

Telecommunications networks include a large number of oscillators and clocks that are continually synchronized with GPS. These do not provide time. During short GPS disruptions they hold time to keep their part of the network in sync with the rest.

As an illustrative example, a delivery driver uses a GPS jammer to keep from being tracked by his employer. Along his route he stops at a traffic light that happens to be near a telecom base station. When the base station loses its GPS signal, its oscillator will hold timing and keep the station in the network long enough for the light to change and the driver to move away.

The tens of thousands of oscillators and clocks used throughout the nation's telecom networks vary greatly in cost, quality, and the amount of time they can stay synced with others during a GPS outage. The vast majority of these devices are inexpensive oscillators that can holdover for a few minutes. Some are able to hold sync for an hour or more, and a few are expensive grand master clocks that can hold good time for more than a day.

The organic development of the telecommunications industry in the United States, along with the many networks that have been combined due to mergers and consolidations, means that there is no standard architecture for networks and equipment. The exact number, location, and performance of oscillators and clocks is nearly unknowable.

Thus, it is not possible to predict the exact sequence of network failure during a widespread GPS disruption. On a macro level, though, we do know that:

- Within five minutes or so of the disruption, inexpensive oscillators will drift out of the required 1.5 micro-second alignment. This will cause associated equipment to shut down, taking it out of its network.
- The number of oscillators and clocks drifting out of sync will progressively increase during the course of the outage. More and more of the network will be disabled.

- Most networks will be almost entirely disabled if the disruption lasts 24 hours.

One of the most effective methods of protecting GPS satellites and signals is to establish GPS alternatives and make them widely and easily available. This will “take the bullseye off of GPS” making it a much less attractive target for those who would do America harm.

It will also facilitate the roll-out of 5G, autonomy, intelligent transportation systems, and other next-generation applications and capabilities, while making the nation more resilient to the impact of GPS disruptions.

The RNT Foundation white paper “A Resilient National Timing Architecture” available at www.RNTFnd.org/Library describes how such alternatives could be easily and inexpensively established.

This white paper was endorsed by telecom CEOs and senior executives on the National Security Telecommunications Advisory Committee in their May 2021 report to President Biden. In it they recommended he begin funding such an architecture.

The imperative for GPS alternatives was also the subject of letters to members of Congress in May 2021 from the Alliance for Telecommunications Solutions. Those letters urged funding of positioning, navigation, and timing backups for GPS.

Patrick Diamond

Dr. Patrick Diamond — Dr. Marc Weiss — Mr. Dana A. Goward

About the Authors

Dr. Pat Diamond is CTO and Founder of K2Mobile. He serves on both the Sync Committee of the Alliance for Telecommunications Solutions, and the President’s Space-based Positioning, Navigation, and Timing Advisory Board.

Dr. Marc Weiss is a theoretical physicist consulting on time and frequency issues. He served for forty years at the National Institute of Standards and Technology and is a member of the Sync Committee of the Alliance for Telecommunications Industry Solutions.

Mr. Dana A. Goward is the President of the Resilient Navigation and Timing Foundation. He serves on the President’s Space-based Positioning, Navigation, and Timing Advisory Board, and is a Senior Adviser to Space Command’s Purposeful Interference Response Team.

Enclosure 2

Risks to the Global Positioning System

According to the Department of Homeland Security, the risk to a given system is the product of its **vulnerability** to damage, the **likelihood** of an adverse event, and the **impact** or magnitude of the resulting damage or adverse consequences.

Value of GPS

Before addressing the individual threats, it is appropriate to discuss how to view the impact of its loss.

Several studies have been done to assess the economic impact of GPS and the resulting damage if it were to be disabled. Most acknowledge up front the difficulty of putting a number to a critical utility that underpins all of society. One compared it to trying to estimate the value of the electrical grid.

A 2019 attempt by RTI in a study for the Department of Commerce estimated the negative impact of a prolonged GPS disruption to be about $1B a day, for the sectors and applications they examined.

While this seems a substantial number it represents only about a 2% reduction in daily GDP. Given the exceptionally broad reliance of networks many other technologies on GPS, the true impact is undoubtedly much higher.

A 2012 estimate by Boston Consulting Group found the value of just GPS location services in the U.S. to increased productivity and savings to be $3T/year. This is more than $8B/day.

Likely the best approach is that taken by author Greg Milner in "Pinpoint," his book about GPS. In response to the question about the value of GPS he says 'What's the value of oxygen?'

A prolonged disruption of GPS services is a near-existential threat to the U.S. It would devastate our economy and greatly reduce America's place in the world.

The following general comments and assessments are based upon likely effects on the ICT supply chain.

Denial of Service - Jamming

Vulnerability – Generally Very High (varies by receiver)

GPS signals are exceptionally weak. Weaker than the "cosmic hum" made by the sun and stars. Thus, receivers must search for coded GPS signals in the radio frequency "noise floor." This means that almost any additional radio noise on or near GPS frequencies can disrupt the functioning of many or most receivers.

Receiver technology (hardware and software) is available that can make receivers much less subject to interference. Few users employ such equipment due to its much greater cost.

Likelihood –

Very High (Local)

Numerous reports of GPS jamming have appeared in U.S. media. While we know of no systematic studies within the U.S., a sampling by the European Union's Strike3 project found almost 500,000 incidents of interfering signals. About 10% of these were deemed to be deliberate interference.

Low to Medium (Wide Area)

Virtually every terrorist organization and nation state has access to inexpensive, easy to use equipment able to disrupt GPS signals over broad areas. U.S. law enforcement has very little capability to locate and terminate even strong jamming signals. Even if the U.S. had such capability, red-teaming has developed scenarios in which one or more relatively powerful jammers would be difficult to locate and stop.

Military electronic warfare equipment is exceptionally powerful. As one example, Russia reportedly has nuclear powered electronic warfare satellites in orbit that could easily deny GPS signals to the entire planet.

Impact –

Low to Very High (Local)

The great majority of jamming events are unintentional, short range, and transitory. These have little to no measurable impact on the nation or economy, and no attempt has ever been made, to our knowledge, to estimate the aggregate impact of what are likely hundreds of thousands of minor incidents per year.

Yet the potential impact is very high. As one example, a jamming incident in 2019 nearly resulted in a passenger aircraft impacting a mountain near Sun Valley, ID. During the early stages of a jamming incident many receivers will continue to try to function and display false information. This appears to be what happened in this incident reported to the NASA safety system. But for the intervention of a distant air traffic controller, it is likely the aircraft would have crashed killing all aboard.

Very High (Wide Area)

Wide area jamming is most likely to be intentional and malicious. It has the potential to disable reception across areas ranging from entire metropolitan areas to continents. Depending upon duration, the impacts could be exceptionally damaging. See "value of GPS" above.

Signal Deception – Spoofing

Vulnerability – Generally Very High (varies by receiver)

As part of making GPS America's gift to the world, signal characteristics and other information was made publicly available to enable broad adoption and use. This practice has been followed by the providers of equivalent satnav systems referred to as Global Navigation Satellite Systems (GNSS). Making these specifications public knowledge has enabled the signals to be imitated and falsified by an increasingly large number of hackers.

As time has progressed, spoofing equipment has become easier to use, more capable, and less expensive. Once only the province of sophisticated nation states, hobbyists are now able to purchase software defined radios designed for other legitimate purposes that can be easily used to transmit false satnav signals that will deceive many types of receivers. One published paper has shown how, with less than $200 of equipment, signals from all GNSS satellites can be imitated at the same time to misdirect a user.

Receiver technology (hardware and software) is available that can make receivers much less subject to spoofing. Few users employ such equipment due to its much greater cost.

Likelihood – Moderate to High

Spoofing, unlike jamming, is most always a deliberate, premeditated attack with a specific goal. The DHS risk model says that the likelihood of a deliberate attack is the product of the bad actor's capability to conduct the attack and their motivation.

The ready availability of inexpensive, easy to use, highly effective equipment means that bad actors have very high capability.

We have no information on the motivations of bad actors to conduct attacks that would impact the ICT supply chain. It is easy to imagine such motivations, if only to create disruption and terror.

Impact – Moderate to Very High

Spoofing and jamming cargo and delivery vehicles has been shown to be a common criminal tactic in other countries. Nearly 85% of truck hijacking and thefts in Mexico, for example, employed a jamming or spoofing device. Warnings about such events have also been issued by U.S. law enforcement.

Spoofing timing and location could interfere with ICT production related transportation (ex: hijacking trucks, causing air crashes), as well as harming IT, SCADA, and other systems. Impacts would vary greatly depending upon the type and scope of the event

Denial of Service - Severe Solar Activity

Vulnerability – Very High

Coronal mass ejections (CME) can charge the atmosphere and prevent reception of signals from GPS and other GNSS for several days or longer. The system has no resilience to such an event.

Likelihood – Low in any given year, Inevitable over the long term

Powerful CMEs are rare but recurring solar events. The 1859 Carrington Event or the 1921 New York Railway Event, had they happened today, would have certainly caused multi-day GPS disruptions. In 2012 a CME of similar power just missed striking Earth.

Experts at the University Center for Atmospheric Research (UCAR) estimate the probability of a CME or other solar event in the next ten years causing some disruption to GPS service at 35-45%.

UCAR experts estimate the probability of a Carrington-level CME in the next ten years that will disrupt GPS signals for days at 4-12%.

Impact – Very High

See "Impact/Value of GPS" above.

Damage, Disabling, Destruction of Satellites Sufficient to End Service

Attacks on satellites had long been considered unlikely threat vectors because of the difficulty of overcoming US Air Force cyber protections, and, for a physical attack, accessing and damaging enough satellites to impact service. In the past year, though, Space Force media announcements indicate these threats are increasing in severity and likelihood.

Cyberattack

Vulnerability – Low: GPS systems are some of the world's most protected. Ongoing upgrades will make them even more so.

Likelihood – Unknown: A successful attack on GPS operating systems is undoubtedly the "holy grail" for any number of individual and state sponsored hackers. We estimate bad actors' motivation to be high. We hope their capability to overcome the system's cyber protections is non-existent.

Impact – Very High: A cyberattack that damaged or destroyed GPS service, or held it ransom, would have devastating long term impacts to our national security and economy. See "Impact/Value of GPS" above.

Kinetic or directed energy attack

Vulnerability – Very High: GPS satellites have no known inherent defenses nor resilience to such attacks.

Likelihood – Unknown: Recent reports from Space Force, the Defense Intelligence Agency and others indicate that China and Russia have multiple methods to destroy satellites in space. We have no information concerning their desire to do so, or about deterrent measures being taken by the U.S.

Impact – Very High: Very High: Devastating long-term effects on national security and economy. See “Impact/Value of GPS” above.

Destruction by Space Debris

Vulnerability – High: GPS satellites can be maneuvered to avoid debris if it is detected in time. They have no known resilience to impacts.

Likelihood – Low to Moderate: While most of the current concern about space debris is focused on satellites in low earth orbit, 19% of tracked space debris is in medium earth orbit and is a threat to GPS satellites.

Impact – Moderate to Very High: One destroyed GPS satellite would probably require $1B or so to replace. However, if it resulted in a cascading series of debris creating events – the so called Kessler syndrome - many satellites could be destroyed. Worst case, medium earth orbit would become unusable.

Destruction by Powerful Coronal Mass Ejection

Vulnerability - Unknown: Experts differ and there is no general consensus. Some assert that GPS satellites are designed to withstand a very hostile environment and are over-built to military grade. While acknowledging this probability, others assert the combination of powerful forces emanating from the sun would be such that induced electrical charges and other forces will render satellites inoperable.

Likelihood of “Carrington-like” Event - Low in any given year, Inevitable over the long term: See above discussion of “Severe Solar Activity.”

Impact – Very High: Devastating long-term effects on national security and economy. See “Impact/Value of GPS” above.

Federal Studies and Determinations to Establish GPS Alternatives

Concerns about America's over reliance on GPS began in 1997 with President Clintons' commission on critical infrastructure. This led to a study by the Department of Transportation (DOT) released in 2001. Since then, a number of federal studies and analyses have been done on this topic. The following are among the studies and determinations that are publicly available.

August 2001 – DOT issued the report "Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System." The report addressed a variety of measures, including backup/ alternative systems for each mode of transportation and other critical applications. Issued just days before the attacks of 9/11, policy action to implement the recommendations was delayed for over three years.

December 2004 – In NSPD-39 President Bush mandated the Dept. of Transportation acquire a backup capability for GPS to protect national and economic security.

February 2008 – A DHS press release announced the department would upgrade the Loran-C system to eLoran as the national backup for GPS. – In 2010 Loran service was terminated in the U.S. due to canceled funding

December 2014 – Legislation was signed into law that required preservation of Loran infrastructure until the administration determined a way forward on a GPS backup.

December 2015 – Based upon a multi-department "Tiger Team" study, the Deputy Secretaries of Defense and Transportation wrote to Congress saying they would establish an eLoran system as a backup for GPS.

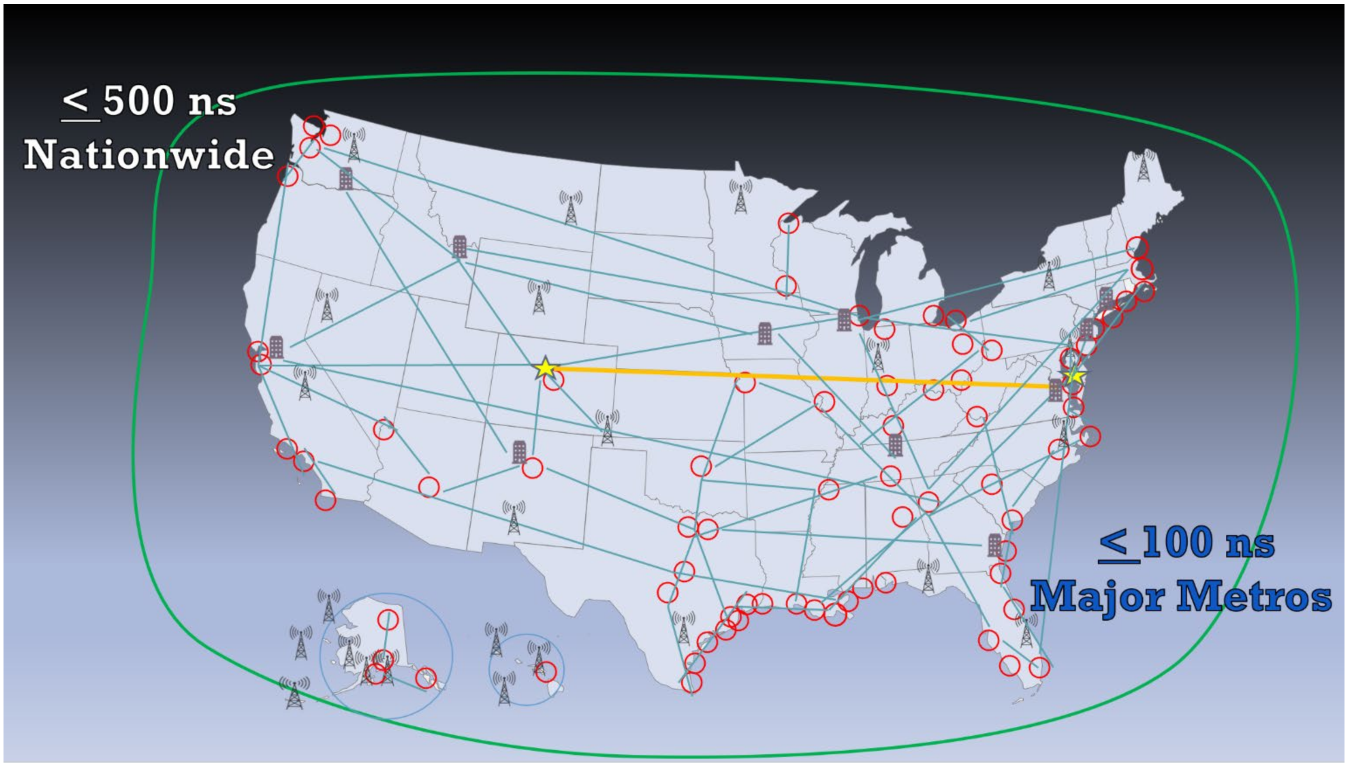
August 2016 – DOT issues report "GPS Dependencies in the Transportation Sector - An Inventory of Global Positioning System Dependencies in the Transportation Sector, Best Practices for Improved Robustness of GPS Devices, and Potential Alternative Solutions for Positioning, Navigation and Timing."

December 2018 – The National Timing Resilience and Security Act signed into law. It required establishment of a terrestrial backup system for GPS timing by December 2020.

January 2021 – DOT released and sent Congress the report "Complementary Positioning, Navigation, and Timing (PNT) and GPS Backup Technologies Demonstration." It finds that multiple technologies working together should be used to ensure the nation has the PNT services it needs.

Enclosure 4

16 October 2020



A Resilient National Timing Architecture

DR MARC WEISS, DR PATRICK DIAMOND, MR DANA A. GOWARD

A Resilient National Timing Architecture

"Everyone in the developed world needs precise time for everything from IT networks to communications. Time is also the basis for positioning and navigation and so is our most silent and important utility." *The Hon. Martin Faga, former Asst Secretary of the Air Force and retired CEO, MITRE Corporation*

Executive Summary

Timing is essential to our economic and national security. It is needed to synchronize networks, for digital broadcast, to efficiently use spectrum, for properly ordering a wide variety of transactions, and to optimize power grids. It is also the underpinning of wireless positioning and navigation systems.

America's over-reliance for timing on vulnerable Global Positioning System (GPS) signals is a disaster waiting to happen. Solar flares, cyberattacks, military or terrorist action – all could permanently disable space systems such as GPS, or disrupt them for significant periods of time.

Fortunately, America already has the technology and components for a reliable and resilient national timing architecture that will include space-based assets. This system-of-systems architecture is essential to underpin today's technology and support development of tomorrow's systems.

This paper discusses the need and rationale for a federally sponsored National Timing Architecture. It proposes a phased implementation using Global Navigation Satellite Systems (GNSS) such as GPS, eLoran, and fiber-based technologies. These were selected because they:

- Provide maximum diversity of sources and least common failure modes,
- Are mature, have repeatedly been demonstrated to perform at the required levels, and are ready to deploy,
- Have the potential for further development to increase accuracy, resilience, and cyber security,
- Are already supported, to varying degrees, by existing infrastructure, and
- Require relatively modest investments.

Timing is essential to maintaining our economy and national security. Today's over-reliance on vulnerable GPS satellite signals is a disaster waiting to happen. America already has the technology and components for a reliable and resilient national timing architecture to underpin today's technology, and support development of tomorrow's systems. All that is needed is to bring all the parts together.

I. Imperatives

PNT Essential, GPS Users Threatened

The last ten years have seen ever more sophisticated ways of disrupting satellite-based positioning, navigation, and timing (PNT) services, as well as sharp yearly increases in the number of disruptions reported. Compounding this, the U.S. Federal Communications Commission has recently permitted an operation forecast to interfere with space based PNT for many users.

At the same time thousands of business models are built upon the assumption of continuously available, wide-area, wireless PNT. More and more lives depend upon uninterrupted PNT services. More and more new technologies - aerial drones, autonomous vehicles, intelligent transportation systems - are advancing, often just assuming PNT will be available.

The National PNT Architecture[1] is America's plan for sufficiently robust PNT to ensure national and economic security. Of P, N and T, the "T" is unquestionably foundational. GPS satellites, Loran transmitters, and other wide-area systems are just radios broadcasting time signals from known locations.

Thus, in building a National PNT Architecture, the first and most important step is Timing.

Important and Urgent

Establishing a National Timing Architecture that serves the entire nation has become an increasingly important and urgent task.

> **Current Dependence, Support to New Technology -** While GPS signals were never intended to be the nation's time standard, their low barrier to entry, precision, and wide availability have made them the de facto national reference. At the same time, such wide adoption means their vulnerabilities pose a near-existential threat.
>
> These vulnerabilities are problematic for existing systems and can limit development of PNT-dependent technologies. The following are examples of particularly dependent sectors:

[1] https://www.transportation.gov/pnt/national-positioning-navigation-and-timing-pnt-architecture

- **5G telecommunications** - While many systems appear to have alternate and diverse timing sources and pathways, such as use of the IEEE 1588-2019 Precision Time Protocol (PTP),[2] many, if not most, of these trace back to GPS as the primary reference. Thus, while 5G is moving forward, it is doing so with GPS time being a critical single point of failure.
- **Autonomy** – As remarked by a senior U.S. Department of Transportation official, "No one is going to accept autonomous vehicles without a rock-solid foundation of location and navigation." Drones losing GPS signals and crashing as they are captured by the wind, autonomous vessels being set on the rocks, demonstrations of cars in self-drive mode being forced off the highway by white-hat hackers – all reinforce the notion that reliable and robust PNT is on the critical path to further significant advances in autonomy.
- **Transportation –** Wireless PNT from GPS has been incorporated into every mode of transportation. Without it, every mode would slow, have less capacity, and be more accident prone.
- **Intelligent Transportation Systems (ITS)** – Traffic routing applications such as Waze,™ ride share services like Uber™ and Lyft,™ train/bus arrival notifications, optimized delivery service programs, traffic signal phase and timing coordination - all are early implementations of ITS. In the absence of GPS' wireless PNT none of these would be possible. Many businesses would either cease to exist or require massive retooling and capital investment. Implementation of future ITS features will likewise require robust, resilient, reliable PNT as part of their foundation.
- **Electric Power** - Smart grid technology using synchrophasers for real time control will bring greatly increased safety and efficiency to electrical power distribution. This is unable to move forward, though, without multiple, differently routed Coordinated Universal Time (UTC) time signals to ensure system reliability.
- **Financial Services –** Consumer financial services (ATMs, checking, banking) depend upon GPS' PNT for timestamping transactions and for network synchronization. Financial services regulated by the Security and Exchange Commission use GPS for some applications, but typically also maintain their own internal time "epochs" with suites of clocks to create timestamped event records, fiber, microwave links, etc. While they may be less vulnerable to disruption as a result, the large amounts of money involved make them a more tempting target for malicious PNT disruption.
- **Digital Broadcast & Land Mobile Radios –** GPS' precise timing is used to enable greatly increased use of fixed spectrum in digital radio and television broadcasts, as well as mobile radio networks, over what was available with earlier analog systems. As an example, in their analog form handheld and mobile radios used by security, first responder, military and others were able to support only one transmitter to be

[2] IEEE Standard 1588-2019, Standard for a Precision Clock Synchronization Protocol for Network Measurement and Control Systems https://standards.ieee.org/standard/1588-2019.html

on-air at a time, and one conversation on a frequency. Users had to be careful to push their radio key to talk and say "over" to indicate they were done before releasing the key and freeing up the frequency for a reply. With digital systems leveraging GPS' precise time signals to divide up the conversations into packets, multiple conversations can be had simultaneously on the same frequency.

Existential Contingency – Timing is an essential function for a wide variety of critical infrastructure. No developed nation can afford to risk losing timing.

This has led to many nations beginning to establish more robust and resilient terrestrial timing architectures to complement and backup GNSS. As examples:

- Europe has a well-developed 1588 PTP network infrastructure linking national timing clock suites.
- The United Kingdom is establishing a virtual National Timing Centre with distributed suites of atomic clocks at critical nodes throughout the nation. They are also transmitting precise time from a single eLoran source and appear to be contemplating additional transmitters.
- China has an exceptionally precise 1588 PTP network linking atomic clocks, and a robust Loran time network. Its stated goal of "comprehensive PNT" represents the world's most complete PNT architecture. China has mentioned in a recent publicly available paper that they will be constructing at least three new Loran transmission sites and advancing the capability of their system.[3]
- No information is immediately available about Russian 1588 PTP implementation, though it is clear from their Radionavigation Plan[4] that the Russian variant of Loran will continue to play an important role in national PNT.

Progress in the United States does not appear to be nearly as advanced. Several government departments and labs have distributed clock systems, though they do not appear to be linked in any way to provide national timing resilience. These might, however, have the potential to be incorporated into and benefit the National Timing Architecture. See "Technologies" section below.

Legislation – While progress on system coordination and implementation does not appear well advanced in the U.S. as in some nations, general awareness of the importance of timing resilience has increased. This has resulted in congressional interest and action. The National Timing Resilience and Security Act of 2018,[5] mandates the Department of Transportation establish at least one terrestrial timing system to backup GPS services by December of 2020.

---

[3] "High Accuracy Positioning Based on Psuedo-Ranges: Integrated Difference and Performance Analysis of the Loran System" *Sensors* 2020, *20*(16), 4436; https://doi.org/10.3390/s20164436
[4] https://rntfnd.org/wp-content/uploads/CIS-Russia-Radionav-Plan-2019-2024.pdf
[5] Sec 514, S140 "Frank LoBiondo Coast Guard Authorization Act of 2018 https://www.congress.gov/115/bills/s140/BILLS-115s140eas.pdf

This legislation both documents the existential imperative of ensuring non-space-based sources of timing and is a legal imperative in its own right.

II. Considerations

Architectural Considerations

Timing Architecture Goals

Establishment of a National Timing Architecture must:

- Increase time resilience and redundancy across 100% U.S. land area & maritime Exclusive Economic Zone (EEZ),
- Provide trusted time via multiple authenticated, cybersecure sources that can also validate each other,
- Support critical infrastructure and be a basis for commercial enhancement services,
- Provide a solid timing infrastructure upon which new technologies, research, and scientific applications can build,
- Ensure wireless access everywhere across 50 states and the EEZ to 500 nanoseconds or better accuracy relative to UTC,
- Ensure wireless access everywhere in major metro areas to 100 nanoseconds or better accuracy relative to UTC,
- Provide Network Access Points (NAPs) in metro areas with 100 nanoseconds or better accuracy relative to UTC for further network distribution/use,
- Ensure critical users have access to a minimum of three sources of timing (for redundancy & voting) relative to their required accuracies, and
- Ensure operational reliability is maintained to a “five 9’s” level of performance.

Characteristics

Redundancy - One of the more important principles of systems engineering and architecture is redundancy of critical systems. And the more critical the system, the more important redundancy. In the most important instances triplication is required.

From a concise on-line discussion:

In many safety-critical[6] systems, such as fly-by-wire and hydraulic systems in aircraft, some parts of the control system may be triplicated[7] which is formally termed triple modular redundancy (TMR). An error in one component may then be out-voted by the other two. In a triply redundant system, the system has three sub-components, all three of which must fail before the system fails. Since each one rarely fails, and the sub components are expected to fail independently, the probability of all three failing is calculated to be extraordinarily small; often outweighed by other risk factors, such as human error. Redundancy may also be known by the terms "majority voting systems"[8] or "voting logic".[9]

The safety-critical nature of timing services means that the National Timing Architecture must be a hybrid network, or system of systems.

Diversity – Ensuring that the major timing sources in the architecture are as different from each other as possible will help avoid common vulnerabilities, threats, and failure modes. It will also help safety-critical users maximize triple modular redundancy.

Coordinated Universal Time (UTC) – Relative time is often sufficient for synchronization of networks and in many other applications. However, UTC with the government's imprimatur (by the National Institute of Standards and Technology (NIST) and the United States Naval Observatory (USNO)) must be the basis from which the National Timing Architecture provides absolute time across the nation.

Responsibility for Sources – The architecture must provide multiple diverse pathways for users to access and maintain time. Responsibility for providing these sources will vary. For example, the responsibility to establish and maintain UTC, as well as the GPS satellite constellation, is clearly that of the federal government. Holdover clocks, when needed or appropriate, are clearly the responsibility of users. Responsibility for other portions of the architecture will be the subject of policy decisions.

---

[6] A safety-critical system (SCS) or life-critical system is a system whose failure or malfunction may result in one of the following outcomes:

- death or serious injury to people
- loss or severe damage to equipment/property
- environmental harm

[7] Redundancy Management Technique for Space Shuttle Computers, IBM Research

[8] R. Jayapal (2003-12-04). "Analog Voting Circuit Is More Flexible Than Its Digital Version". elecdesign.com. Archived from the original

[9] *"The Aerospace Corporation | Assuring Space Mission Success". Aero.org. 2014-05-20*

Requirements

Current Dependence, Support to New Tech – Available literature[10] indicates that the following are representative of national requirements:

- **5G telecommunications** - Requires 1.1 microseconds accuracy relative to UTC for Radio Synchronization and overall network latency.[11]
- **Autonomy** – Still in development and expected to vary by platform. Requirements for lane keeping in vehicles are expected to range from 5 to 10 centimeters. This will likely exceed what can be reliably provided by infrastructure and require on-vehicle sensors/ augmentation. Establishment of the national timing architecture will still be key to provide a solid foundation upon which innovators can build.
- **Transportation –** Requirements vary by application. For consumer-level applications, 100 nanoseconds timing and ten meters location accuracy appear to be sufficient.
- **Intelligent Transportation Systems (ITS)** – Same as telecommunications requirements above.
- **Electric Power** - Synchrophasers for real time control require multiple differently routed UTC time signals at the 1 microsecond level or better.[12] [13]
- **Financial Services** – Individual firms frequently employ sufficient fiber and clock suites to maintain internal synchronization within their own epoch to very demanding limits, sometimes within a nanosecond. However, federal regulations only require firms to maintain 100 microseconds accuracy relative to UTC.

Technologies

UTC Access – Coordinated Universal Time (UTC) for the United States is maintained by the US Naval Observatory (USNO) in Washington, DC, and the National Institute of Standards and Technology (NIST) in Boulder, CO. To use and distribute UTC, a technology must synchronize with one of these two sources. Depending on the desired level of accuracy, this can be done in a variety of ways including Two Way Satellite Time Transfer (TWSTT), fiber connection, microwave link, GPS Common View, or from a GPS receiver.

---

[10] See for example 2019 Federal Radionavigation Plan - https://www.navcen.uscg.gov/pdf/FederalRadioNavigationPlan2019.pdf

[11] ATIS Standard 0900005 GPS Vulnerability https://access.atis.org/apps/group_public/download.php/36304/ATIS-0900005.pdf

[12] M.A. Weiss, A. Silverstein, F. Tuffner, Y. Li-Baboud, "The Use and Challenges of Precise Time in Electric Power Synchrophasor Systems," *Proc. 2017 PTTI and ITM of ION*, Jan 30, 2017, available from: https://www.nist.gov/publications/use-and-challenges-precise-time-electric-power-synchrophasor-systems

[13] *Consolidated Audit Trail (CAT) Reporting Technical Specifications for Plan Participants*, available from the Consolidated Audit Trail National Market System (CAT NMS) Plan website: https://www.catnmsplan.com/

It is even possible to "physically" transfer time. Before the digital and communications revolution, entities would bring suites of atomic clocks to USNO to synchronize, and then transport those clocks to sites like Loran and Omega transmitting stations as a way of distributing UTC.

Global Navigation Satellite Systems (GNSS)/GPS – The cornerstone of the National Timing Architecture will be GPS which has a U.S. government supported 78 ns accuracy. Approval by the Federal Communications Commission (FCC) of Europe's Galileo to be used within the United States allows this second GNSS to also be included. This gives added resilience to the space-based portion of the architecture. - Note that GPS actual performance is almost always better than nominal. Accuracies of < 10 ns for timing and < 10 ft for location are typical (1 ns ≈ 1 foot).

LEO PNT – Numerous government and commercial endeavors are examining the viability and benefits of providing PNT services from satellites in low earth orbit (LEO). This could be inferred from signals of non-PNT constellations. LEO PNT systems could also be created by sharing payloads with other missions, or with purpose-built and deployed constellations. We note that at least one vendor already offers time as a subscription service from LEO satellites.

Networks / Fiber – Various levels of timing accuracy are available by networks and fiber ranging from about tens of milliseconds for NTP, to about 1 ns for dedicated bi-directional wavelengths, each pair in a single fiber. Commercial providers have technology available to provide users with localized, point, and autonomous timing to meet requirements for better than 100 ns accuracy.[14] A newly released update to IEEE 1588-2019, also known as PTP, contains a "High-Accuracy Option."[15] This is a generalization for wide area usage of the White Rabbit standard developed at CERN for sub-nanosecond synchronization accuracy of more than 1,000 nodes via connections up to 10 km of length.

Wide Area Broadcast – Demonstrations in the United States and United Kingdom have shown that eLoran technology broadcasting at 100 kHz is capable of providing better than 1 microsecond accuracy over distances up to 1,600 km from the transmitter, and better than 100ns within 55 km of a differential reference station.[16]

---

[14] M. Weiss, L. Cosart, J. Yao, J. Hanssen, "Ethernet Time Transfer through a U.S. Commercial Optical Telecommunications Network, Part 2," in *Proc. Precise Time and Time Interval Meeting*, Monterrey, 2016, available from https://tf.nist.gov/general/pdf/2813.pdf

[15] IEEE Standard 1588-2019, Standard for a Precision Clock Synchronization Protocol for Network Measurement and Control Systems https://standards.ieee.org/standard/1588-2019.html

[16] G. Offermans, S. Bartlett, C. Schue, "Providing a Resilient Timing and UTC Service Using eLoran In the United States" in *ION Journal of Navigation Vol 64, Number 3 (Fall 2017)* available from https://www.ion.org/publications/abstract.cfm?articleID=102722

Note that WWVB broadcasting at 60 kHz could conceivably be developed for this purpose also. DARPA's STOIC program also envisions a wide area time service using Very Low Frequencies (VLF).

eLoran – eLoran is a form of wide area broadcast using 100 kHz. It is at TRL 9, requiring no development, and is compatible with other Loran systems in operation around the world. This provides significant technology synergies as well as the potential for positive and beneficial engagement with other national operators.

eLoran performance as a timing signal has been demonstrated to the U.S. Department of Homeland Security as part of a Cooperative Research and Development Agreement,[17] and by research in the United Kingdom.[18] A national eLoran timing system is also among the most recent recommendations of the US National Space-based PNT Advisory Board.[19] In 2015 the US President's National Space-based PNT Executive Committee committed to establishment of an eLoran-based timing system.[20]

Local Area Broadcast – Local broadcasts can provide timing, along with positioning and navigation information. The accuracy and geographic coverages of these local systems vary with the technology, density of transmitters, and other factors. Systems have been demonstrated to have pico-second level accuracy in some instantiations.

Distributed Clocks – The federal government maintains various federal clock suites for its own purposes that appear to be able to independently maintain a 1 microsecond level of accuracy relative to UTC indefinitely.

- The Department of Defense, in addition to maintaining UTC at the US Naval Observatory, Washington, DC, has a backup capability at Schriever AFB. Synchronization is maintained via two way satellite time transfer (TWSTT). DoD also maintains a Defense Regional Clock Program.
- The Department of Commerce also maintains UTC at NIST Boulder, CO, with a backup at Ft Collins, CO. Synchronization is maintained by GPS Common-View Time Transfer. NIST Gaithersburg, MD also maintains a clock suite using GPS Common View for synchronization. NIST is exploring synchronizing these sites with fiber networks, potentially at the 1 nanosecond level.
- The Department of Energy maintains suites of clocks at Oakridge, Sandia, and Lawrence Livermore.

---

[17] ibid

[18] See for example C. Curry "Delivering a National Time Scale Using eLoran" 7 June 2014 https://rntfnd.org/wp-content/uploads/Delivering-a-National-Timescale-Using-eLoran-Ver1-0.pdf

[19]https://www.gps.gov/governance/advisory/recommendations/2018-09-topic-papers.pdf

[20] Letter 8 Dec 2015 from PNT Executive Committee Co-chairs DoD Dep Sec Work and DoT Dep Sec Mendez to several members of Congress. See: https://rntfnd.org/wp-content/uploads/DSD-and-Dep-DOT-reply-to-Mr.-Garamendi.pdf

Network Access Points NAPs – NAPs are physical locations, usually in major cities, where Interexchange carriers, Independent Local Exchange Carriers, Competitive Local Exchange Carriers, National Carriers, Local Fiber Carriers, etc. “interconnect” with each other’s services. All participating operators contribute to the cost. The national network is made up of hundreds of these NAPs.

The fiber component of the National Timing Architecture will have these interconnect “touch points” at its heart. All monitoring probes, testing, configurations, and connections for further, more localized distribution will occur at these locations.

Network Control & Performance Assurance – Coherent networks require management and control systems to ensure their operation and performance. These involve geographically distributed sensors, testing, performance and fault reporting. Such a control system requires its own redundancy and resilience. GPS, Loran-C and-similar systems have ensured that full network monitoring and control is available at two or more geographical locations remote from each other.

Cybersecurity – While not a technology in and of itself, authentication, access controls, system and user cybersecurity must be considered throughout. The ability of users to trust the timing they receive is paramount. If, as has been seen around the world with positioning, timing is not trustworthy, it may not be used. Worse, it could provide potentially hazardously misleading information.

Policy Considerations

Federal Leadership - ***The first duty of government is to afford protection to its citizens.***[21]

Timing’s criticality and essentiality to such a broad spectrum of the public and critical infrastructure means that government has a responsibility to ensure such an architecture is established, and quickly.[22]

The essentiality of time to a nation’s economy and security has been recognized since at least 1714. The British “Longitude Act” of that year might have been better titled “The Time Keeping Act.” It led to development of Harrison’s chronometer and untold immediate benefits to the Royal Navy and merchant fleets. In the United States, USNO has been dropping a time ball since 1845 to mark mean solar noon. Since then, the U.S. government has been communicating time across increasingly large sections of the nation at increasing levels of accuracy.

---

[21] Cong. Globe, 39th Congress 2nd Sess. 101 (1867) (remarks of Rep. Farnsworth debating Reconstruction Act of 1867) See also Preamble to the Constitution: “…in Order to form a more perfect Union, establish Justice, insure domestic Tranquility, provide for the common defence, promote the general Welfare, and secure the Blessings of Liberty to ourselves and our Posterity…”

[22] As noted earlier, the responsibility to establish at least part of the timing architecture is required by the National Timing Resilience and Security Act of 2018.

The federal role is also essential as the government's imprimatur is required for a time signal to be credible, nationally interchangeable and as useful as possible. Any sufficiently stable time source is adequate for "relative time" to synchronize interconnected sources and other applications that require events to be coordinated only with each other, but not the world at large. Macro, national enterprise synchronization and interoperability, though, is only possible with a widely communicated time signal endorsed by the sovereign.

As discussed earlier, while the National Timing Architecture must provide multiple diverse pathways for delivery of authoritative time, responsibility for providing these sources will vary. Direct federal involvement (leadership, funding, etc.) must ensure all citizens have reasonable access to more than one path to UTC to prevent time being a single point of failure. Other aspects of the architecture such as augmentations that increase accuracy, hold-over time in the event no external sources are available, and supplemental space-based signals may be the responsibility of users.

The federal government's role in establishment and communication of national time is a critically important one. Yet it need not be onerous. Experience with similar efforts such as FirstNet and the FAA's ADS-B system has shown that often the least cost and quickest path to system implementation is a partnership between the government and the commercial sector.

Further reducing the burden on government is a recent technology demonstration done by the Department of Transportation. It showed that sufficient systems exist today to complete a robust National Timing Architecture.

Costs - ***There are risks and costs to action. But they are far less than the long-range risks of comfortable inaction.*** *– Attributed to President John F. Kennedy*

No discussion of a proposed federal investment would be complete without at least a general consideration of costs to both the federal government and users. These costs will be relatively modest, yet absolutely necessary.

Relatively Modest – By leveraging public-private-partnerships, service-agreements, and the like, government can encourage and establish the infrastructure described herein at a cost measured in tens of millions of dollars per year. This is relatively modest when compared to annual expenditures on GPS which exceed $1B.

The cost of end-user equipment will undoubtedly decline as more and more users access the fiber-based and wireless signals. As was the case with GPS and most other technologies, early user equipment will likely be larger and more expensive than in later receiver models. An early pallet-sized GPS receiver, complete with two operator chairs, was budgeted for hundreds of thousands of dollars. Miniaturization, technological advances, and mass production have enabled production of the cheapest GPS for several dollars each.

User costs will also be offset by the need to recapitalize equipment and improvements in utility.

After implementation of the National Timing Architecture there will be little incentive for production of GPS/GNSS-only timing receivers. Just as manufacturers have incorporated other GNSS systems alongside GPS in almost all new receiver models, so too will they almost certainly include over time the ability to use the architecture's terrestrial systems. Thus, the additional cost for new builds and recapitalized equipment will be only marginally greater than it would have been otherwise in these cases.

More resilient and reliable time will also provide many users increased functionality by virtually eliminating disruptions and providing a higher guaranteed accuracy. As one example of increased utility, this could allow reduced error margins in multiplexing wireless signals, enabling greater use of existing spectrum allocations.

Absolutely Necessary – Often lost in calculating the cost of doing something are the costs of doing nothing. When GPS fails, transportation-related systems immediately suffer. They become less efficient/ more costly, can carry less capacity, and are more accident prone. Land-mobile radio systems and digital broadcasts degrade or fail. In prolonged outages, two-thirds of U.S. wireless networks are projected to fail after about 24 hours. Then, as backup clocks de-synchronize, more network and other failures will ensue, including the loss of consumer financial services and impacts to utilities. One Air Force-sponsored academic paper projected civil unrest within 72 hours.

Quantitative analyses of the impact of GPS outages have always struggled. Most openly admit their inability to gauge the overall impact to the national economy and limit themselves to specific applications or sectors. Notable studies have estimated prolonged disruption of GPS signals costing the US economy across a wide range of $1B[23] to $82B[24]per day.

It is perhaps not possible to capture GPS' true economic value and the impact of its potential loss or prolonged outage. Dollar numbers may not have sufficient meaning in this context. As one writer replied when asked about the value of GPS – "What's the value of oxygen?"[25]

PNT services, especially timing services, are an existential necessity for life in the United States as we know it. Not ensuring they will always be available poses unthinkable risks and costs.

---

[23] https://www.nist.gov/document/economic-benefits-global-positioning-system-gps-final-report
[24] https://mkt-bcg-com-public-images.s3.amazonaws.com/public-pdfs/legacy-documents/file109372.pdf
[25] "Pinpoint – How GPS is Changing our World and our Minds" – Greg Milner, Norton, 2016

Adoption

Wide adoption and use of the National Timing Architecture's terrestrial systems is key to its success. Merely making them available will not increase national and economic security a whit.

Fortunately, America's experience with implementation and adoption of GPS and other GNSS provides some lessons in this regard. And the government has a variety of tools available to encourage this process

The GPS Experience – While there were a number of technical and historical factors in the unparalleled wide adoption of GPS, the following were key:

- **No cost access** – GPS is free to access for anyone who can afford a receiver.[26] Access to the basic terrestrial services in the National Timing Architecture should be without charge also. This does not preclude the government, one of its partners, or another entity from providing fee-based services. But, in the interest of national and economic security, the service levels outlined herein must be without charge, to encourage wide use.
- **Broad availability** – GPS is available to anyone with a view of the sky. This means that it is not location dependent. Something developed for use with GPS in New York also works in California and Alaska. The architecture's terrestrial systems must be available to all users in the United States, regardless of location. The entire nation and its coastal waters will have an accuracy of $\leq$500 ns, with densely populated areas having $\leq$100 ns relative to UTC. However, after implementation of Phase III, any 70-mile wide area can be upgraded to $\leq$100 ns with the installation of a (<$75,000) differential reference station. This is relatively inexpensive when compared to the $400,000+ cost of a Differential GPS site.
- **Open source** – This has been a dual edged sword for GPS and other GNSS. While it allows for easy (and wide) adoption, use, and integration of signals into myriad applications, it has also made the system much easier to jam and spoof. America's terrestrial systems must walk a fine line between encouraging wide and wise use and doing as much as possible to prevent interference. There are many methods for doing this, including having parallel services (perhaps an open system for free public use and a closed, more secure one for government and fee-based use). Encryption, authentication and other security measures will be important aspects of development and operation.
- **Government agencies leading the way** – The initial goal of GPS was for the Air Force to "…put five bombs in the same hole."[27] Early in its implementation, though, many

[26] Early versions of the internet failed, in the opinion of many because administrators sought a small fee to cover overhead costs.
[27] Dr. Bradford Parkinson, Chief Architect of GPS, speaking at Smithsonian Air and Space seminar March 21, 2013

military leaders saw no need for the system and actively opposed it. In fact, at the end of the first Gulf War there was no plan to install GPS in military aircraft. Congress had to insist on it. Adoption and use of GPS by the government was key to its broader adoption across society. This led to a virtuous cycle of improved performance and usability with decreasing costs. The current administration's Executive Order on responsible use of PNT[28] already mandates federal leadership by mandating future federal contracts include a requirement for use of resilient PNT equipment and systems.

Every agency at every level of government has ample reasons to adopt terrestrial services from the National Timing Architecture. Dispatch, asset coordination, land mobile radios, networks – all are degraded or disabled in GPS-denied environments. Imagine the National Guard responding to a disaster without the ability to navigate easily or use their handheld radios. Government agencies and forces will need to use these terrestrial systems, if for no other reason than to ensure continuity of government.

The GNSS Experience

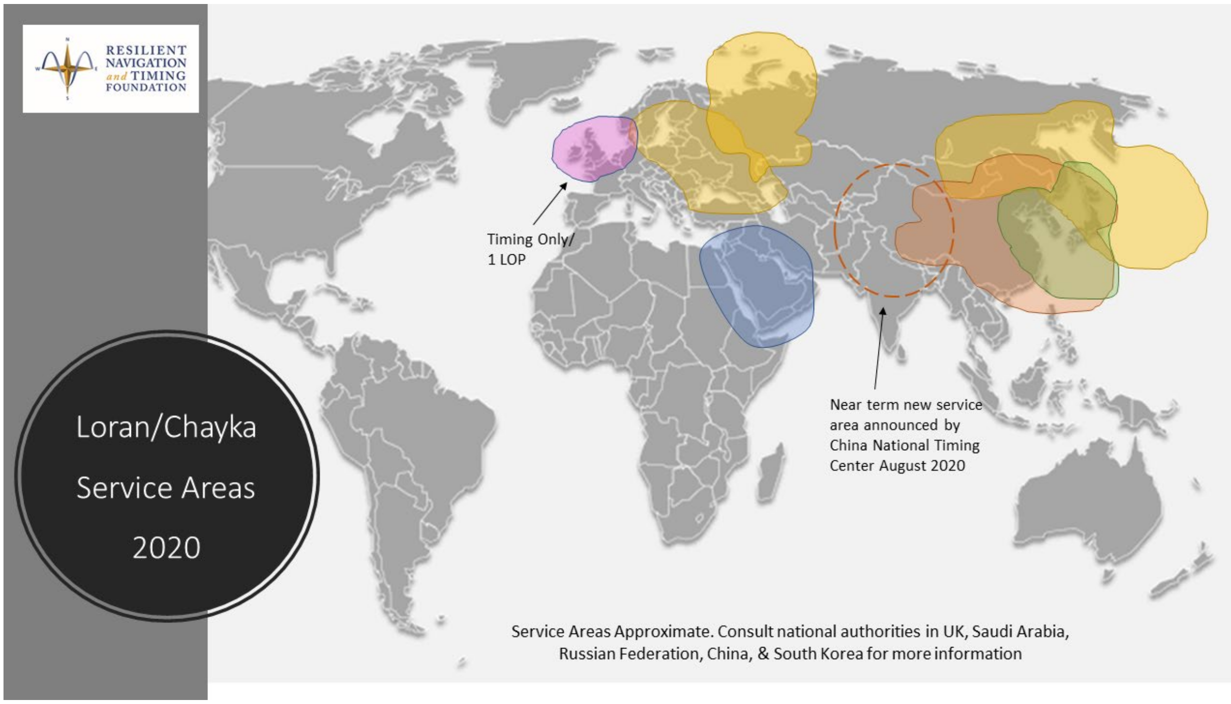
GPS was the world's first satellite navigation system available to consumers. As Russian and European systems became available, receiver manufacturers began incorporating the capability to use them on most of their products. This is happening again with inclusion of signals from the recently completed Chinese Bei Dou system. For years most receivers in the United States, for example, have included the ability to access Russia's GLONASS satnav system, despite federal prohibitions on its use. Many manufacturers ensure this feature is disabled while the equipment is within the U.S. but include it nonetheless. This is because:

- The additional cost is minimal due to decades of technological advancement,
- Building receivers to be as capable as possible is a competitive advantage, or at least prevents a competitive disadvantage,
- Making different receivers for different markets is not cost effective, and
- Users don't want their equipment restricted by geography and expect it to operate at maximum efficiency everywhere.

We can expect that as receiver technology develops and improves in the critical areas of size, weight, power and cost, more and more receivers will include the ability to use the terrestrial components of the National Timing Architecture as part of their timing and navigation solutions.

Incorporation of eLoran will be especially incentivized as compatible signals are already available across a significant portion of the globe (see graphic).

[28] Executive Order on Strengthening National Resilience through Responsible Use of Positioning, Navigation, and Timing Services – Issued February 12, 2020



Government Encouragement & Requirements

Officials truly concerned about the impact of timing resilience on the nation's security and economy have multiple tools at their disposal to encourage adoption of better systems and practices.

The February 2020 Presidential Executive Order on Responsible Use of PNT[29] outlined the administration's plan to use educational efforts and government contracting requirements to stimulate increased PNT resilience across critical infrastructure and industries.

Should these efforts not sufficiently protect the nation, greater incentives and requirements should be considered and implemented. In the past these have included things like tax credits for installing new equipment and performance-based regulations.

Putting Together the Pieces

Put simply, we find time transfer by eLoran and fiber are mature technologies easily capable of spanning the nation. When combined with GNSS, users will have three independent pathways for authoritative Coordinated Universal Time.

---

[29] Ibid

Maintaining and reinforcing America’s network and IT infrastructure is more important now than ever.

Cyber security needs are increasing. Demands on telecommunications service providers are increasing. Space is more and more crowded. GNSS intentional or unintentional interference is increasing.

The COVID pandemic has greatly increased our reliance on networks and distributed work. The number of people who must work remotely, often in locations outside of major metropolitan network nodes has grown significantly. A failure or even temporary outage in any part of our far-flung networks will have much greater impact that it would have had even a year ago.

Adding to domestic concerns, we must also maintain the nation’s competitiveness and standing in the world. Europe, China, and others have and are establishing foundational timing systems, sometimes as part of coherent architectures, to provide innovators and engineers needed infrastructure for current and yet-to-be-developed systems.

While the technologies we propose are mature, and the structure fairly uncomplicated, bringing a National Timing Architecture into reality will have its difficulties. Network design, implementation, contract and project management, ongoing operation – all will be challenges. The experiences of projects like FirstNet and ADS-B, though, will be good guides.

Most important and fundamental will be fostering and maintaining the political understanding and imperative for action outlined in the National Timing Resilience and Security Act of 2018.

The task is a relatively straight forward one.

We can ill afford to do less.

II. Proposed Architecture

Structure & Implementation

Recognizing the differences in readiness levels of various solutions, and the differences in cost and ease of implementation, this proposal takes a phased approach to implementing the National Timing Architecture.

Implementing by increments also provides opportunities for user feedback before the entire system is built out. If solutions are not adopted or prove difficult, the architecture and the systems it includes can be modified or changed completely without incurring major costs.

This proposal also:

- Recognizes the higher demand for timing services and concurrently higher return on investment in geographic centers of population and infrastructure,
- Conforms to the National PNT Architecture final report,
- Uses the layered principled outlined in the US Department of Defense PNT Strategy.[30]

Technologies

GNSS, eLoran, and fiber-based timing were selected as the primary sources for the National Timing Architecture because they:

- Provide maximum diversity of sources and least common failure modes,
- Are mature and ready to deploy,
- Have the potential for further development to increase accuracy, resilience, and cyber security, and
- Are already supported, to varying degrees, by existing infrastructure
    - GNSS is clearly fully deployed and in use
    - eLoran primary transmitter sites are already owned by the US government
    - Fiber networks and government distributed clock suites are extant and continue to grow.

And while a comparative cost analysis is not part of this paper, prima facia, the terrestrial systems listed above are of modest cost relative to GNSS and other terrestrial systems.

The selection of eLoran over other mature broadcast technologies is also based upon extensive research in the U.S. and U.K. showing its effectiveness (see previous references). Also, alternative analyses performed by the U.S. government show it as the only technology that combines wide area coverage with sufficient accuracy.[31]

---

[30] https://rntfnd.org/wp-content/uploads/DoD-PNT-Strategy.pdf
[31] See for example "GPS Dependencies in the Transportation Sector" August 2016, U.S. Department of Transportation, Volpe Center, pg 45

Network Control & Performance

Operational performance integrity will be key to acceptance and use of the National Timing Architecture. Critical users will demand “always on” performance, the ability to view the operational stability in real time, an automated failover capability, centralized reporting, and management in the event of a fault. Just as the Air Force commits to and publishes a performance standard for the broadcast of GPS signals, so too the government must commit to a performance standard for the terrestrial portions of the National Timing Architecture.

Notional Phases

The following notional implementation phases are suggested to progressively support critical infrastructure, technology development and maximize the practical use for citizens.

Phase I National Timing Architecture							
	Global Layer		***Continental Layer***		***Local Layer***		
	GNSS 78ns	LEO PNT	**eLoran ≤1 µs 6 sites**	**N. Clock Ntwk ≤100 ns**	**Df eLoran ≤100 ns**	**NAP ≤100 ns**	User Clocks
Fixed Users w/ntwk access							
Everywhere (50 states, EEZ)							
Major Metro					Selected	Selected	
Fixed Users w/ No ntwk access							
Everywhere (50 states, EEZ)							
Major metro					Selected		
Mobile Users							
Everywhere (50 states, EEZ)			*				
Major Metro			*		*Selected		
Govt sponsored/PPP, No/low barrier to entry				Available, commercial, fee based			

Phase I Notes:

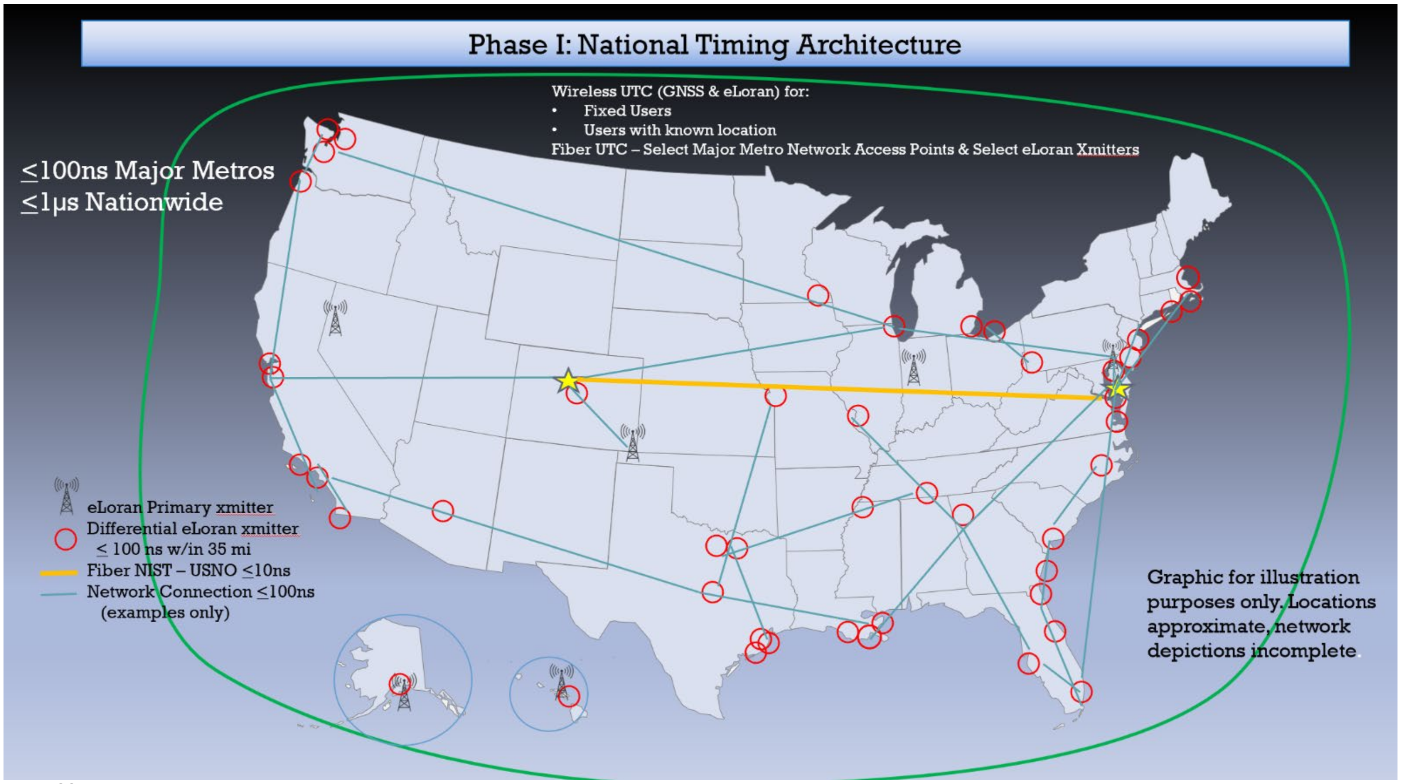
National Clock Network (N. Clock Ntwk) - Fiber: Connect

- NIST Boulder with USNO to establish ≤10 ns sync.
- Selected (TBD) major metros, eLoran differential transmitters, and eLoran primary transmitters ≤100 ns sync

eLoran: Establish 6 primary transmitter sites (4 in CONUS, 1 each in AK & HI)

Differential (Df) eLoran: Establish differential sites in selected (TBD) metro areas

*If GNSS location information is available to a mobile receiver, eLoran time info will be usable and, if properly integrated, can make receivers much less susceptible to GNSS disruption.



32

---

32 Graphics adapted with permission from UrsaNav presentations

Phase II National Timing Architecture							
	Global Layer		***Continental Layer***		***Local Layer***		
	GNSS 78ns	LEO PNT	**eLoran $\leq$500 ns 12 sites**	**N. Clock Ntwk $\leq$100 ns**	**Df eLoran $\leq$100 ns 75 sites**	**NAP $\leq$100 ns**	User Clocks
Fixed Users w/ntwk access							
Everywhere (50 states, EEZ)							
Major Metro							
Fixed Users w/ No ntwk access							
Everywhere (50 states, EEZ)							
Major metro							
Mobile Users							
Everywhere (50 states, EEZ)			*				
Major Metro			*		*	*	
Govt sponsored/PPP, No/low barrier to entry				Available, commercial, fee based			

Phase II Notes:

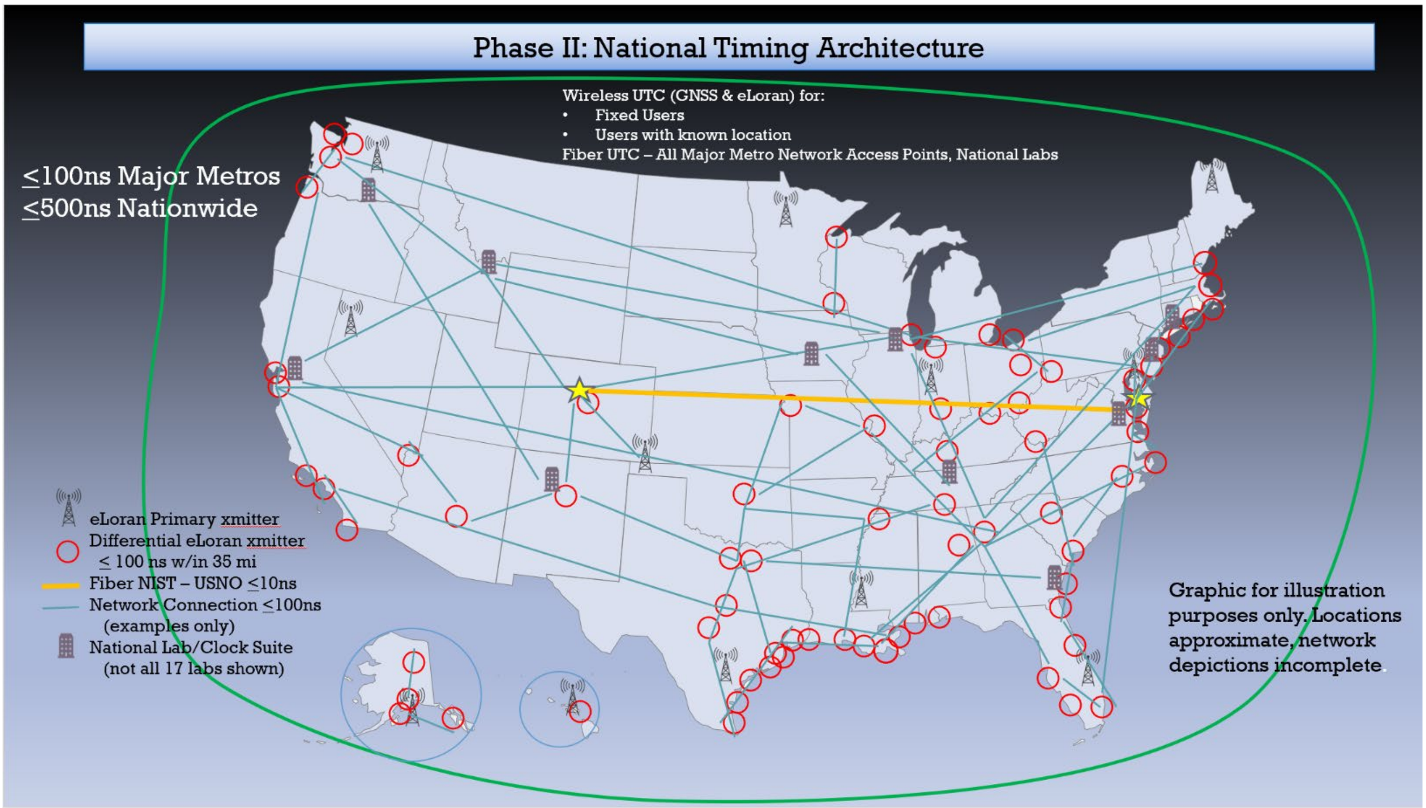
N. Clock Ntwk - National Clock Network (Fiber) Connect:

- National Laboratories & other federally endorsed clock suites. Maintain accuracy at the 100ns level or better (to be determined) relative to UTC.
- Connect to Network Access Points and differential eLoran sites in major metro areas at $\leq$100 ns level relative to UTC for possible further distribution by govt/ commercial services.

eLoran: Establish 6 additional primary transmitter sites in CONUS (system total of 10 in CONUS, 1 ea AK & HI) for $\leq$500 ns relative UTC (exception are remote areas of AK $\leq$1 µs)

Differential (Df) eLoran: Establish total of 75 differential sites to serve the 50 largest metro areas, 50 busiest airports, 50 busiest seaports in CONUS, 3 locations in AK and 1 in HI.

*If GNSS location information is available to a mobile receiver, eLoran time broadcast info will be usable. If properly integrated, eLoran signals can make receivers much less susceptible to GNSS disruption.



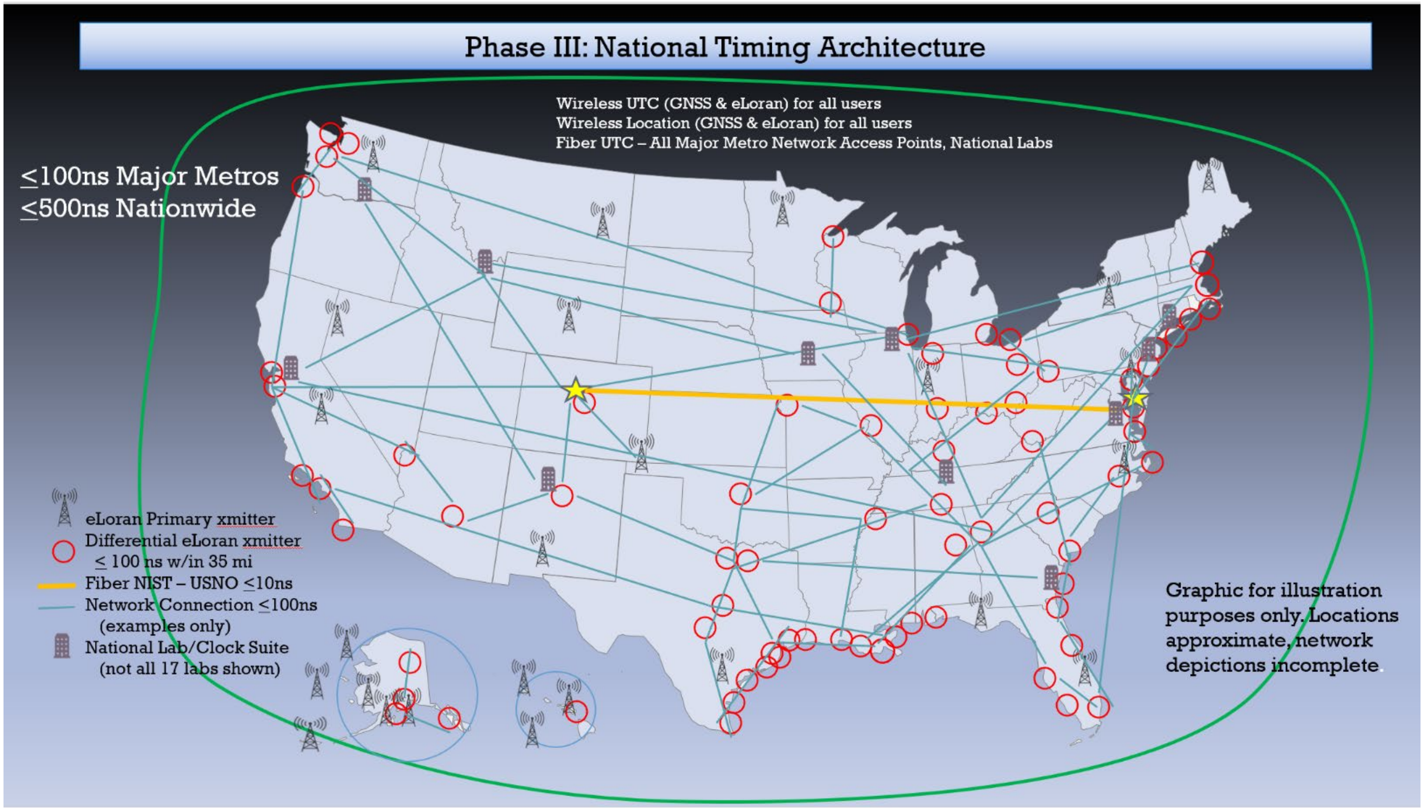
Phase III National Timing Architecture							
	Global Layer		***Continental Layer***		***Local Layer***		
	GNSS 78ns	LEO PNT	**eLoran ≤500 ns ≈25 sites**	**N. Clock Ntwk ≤100ns**	**Df eLoran ≤100 ns 75 sites**	**NAP ≤100 ns**	User Clocks
Fixed Users w/ntwk access							
Everywhere (50 states, EEZ)							
Major Metro							
Fixed Users w/ No ntwk access							
Everywhere (50 states, EEZ)							
Major metro							
Mobile Users							
Everywhere (50 states, EEZ)							
Major Metro							
Govt sponsored/PPP, No/low barrier to entry				Available, commercial, fee based			

Phase III Notes:

National Clock Network: Link in-development and future optical clocks for scientific and research. Frequency accuracies pushing the boundaries of science and human imagination.

eLoran: Establish ≈13 additional primary transmitter sites (total of ≈16 CONUS, 6 in AK, 3 in HI)

GPS/GNSS-Independent Positioning, Navigation, and Timing – Accessing terrestrial wireless time for mobile users requires their locations be known. Sufficient primary eLoran transmitters are deployed in Phase III to provide that information without regard to signals from space. This also enables positioning and navigation based solely on eLoran, in the event that signals from space become unavailable. Continuous synchronization with UTC by fiber or other means to one or more points in the primary eLoran transmitter network and the ability of the network to self-synchronize enables it to operate indefinitely providing PNT in the event of a prolonged GPS/GNSS outage.



Phase III: National Timing Architecture
Wireless UTC (GNSS & eLoran) for all users
Wireless Location (GNSS & eLoran) for all users
Fiber UTC – All Major Metro Network Access Points, National Labs
≤100ns Major Metros
≤500ns Nationwide
eLoran Primary xmitter
Differential eLoran xmitter ≤ 100 ns w/in 35 mi
Fiber NIST – USNO ≤10ns
Network Connection ≤100ns (examples only)
National Lab/Clock Suite (not all 17 labs shown)
Graphic for illustration purposes only. Locations approximate, network depictions incomplete.

About the Authors

Marc Weiss, PhD

Dr. Weiss worked at the NIST Time and Frequency Division from 1979 through 2013. He has since been a consultant on precision timing systems for NIST and for various companies. He received several awards during his tenure at NIST. He led the NIST program to support the GPS program office in developing their clocks and timing systems. In 1992, Dr. Weiss founded and has continued to lead the Workshop on Synchronization and Timing Systems (WSTS), now the premier conference on timing and synchronization in industry. In April, 2019, Dr. Weiss was awarded the Marcel Ecabert Lifetime Achievement Award "For his key contributions to remote clock comparisons, to time scale algorithm development and to accurate synchronization for science and industry."

Patrick Diamond, PhD

Dr. Diamond has 40+ years in development and design of network technologies. His tenure in the network technology, design and implementation marketplace has been, specifically in the commercial marketplace. He has and is a participant in Standards body development organizations, IEEE, IETF, ITU. He has helped develop numerous Wide Area Network technologies such as SONET/SDH, TCP/IP, IEEE 1588, IEEE 802.1AS, 3GPP and numerous others specifically dedicated to precision timing in networks and end user systems. He developed and managed organizations that created highly complex System on a Chip technologies in semiconductors for these end implementations. He now serves and a member of the US National Space-Based Positioning, Navigation and Timing Advisory Board.

Dana A. Goward, SES (ret), CAPT (ret)

Mr. Dana A. Goward is President of the Resilient Navigation and Timing Foundation, a scientific and educational charity dedicated to protecting GPS/GNSS signals and users.

He is a lifelong practical navigator orienteering ashore, serving as a ship's navigator at sea, and in the air as a career Coast Guard helicopter pilot.

He retired in 2013 from the Senior Executive Service as the maritime navigation authority for the United States and now serves as a member of the US National Space-Based Positioning, Navigation, and Timing Advisory Board. He is also a senior advisor to Space Command's Purposeful Interference Response Team, is an emeritus Chairman of the Board for the Association for Rescue at Sea, and is the proprietor at Maritime Governance, LLC.