OAK RIDGE National Laboratory

Center for Alternate Synchronization and Timing

Augmenting GPS for National Energy Resilience

Carter Christopher, PhD
Oak Ridge National Laboratory

ORNL is managed by UT-Battelle, LLC for the US Department of Energy

U.S. DEPARTMENT OF ENERGY

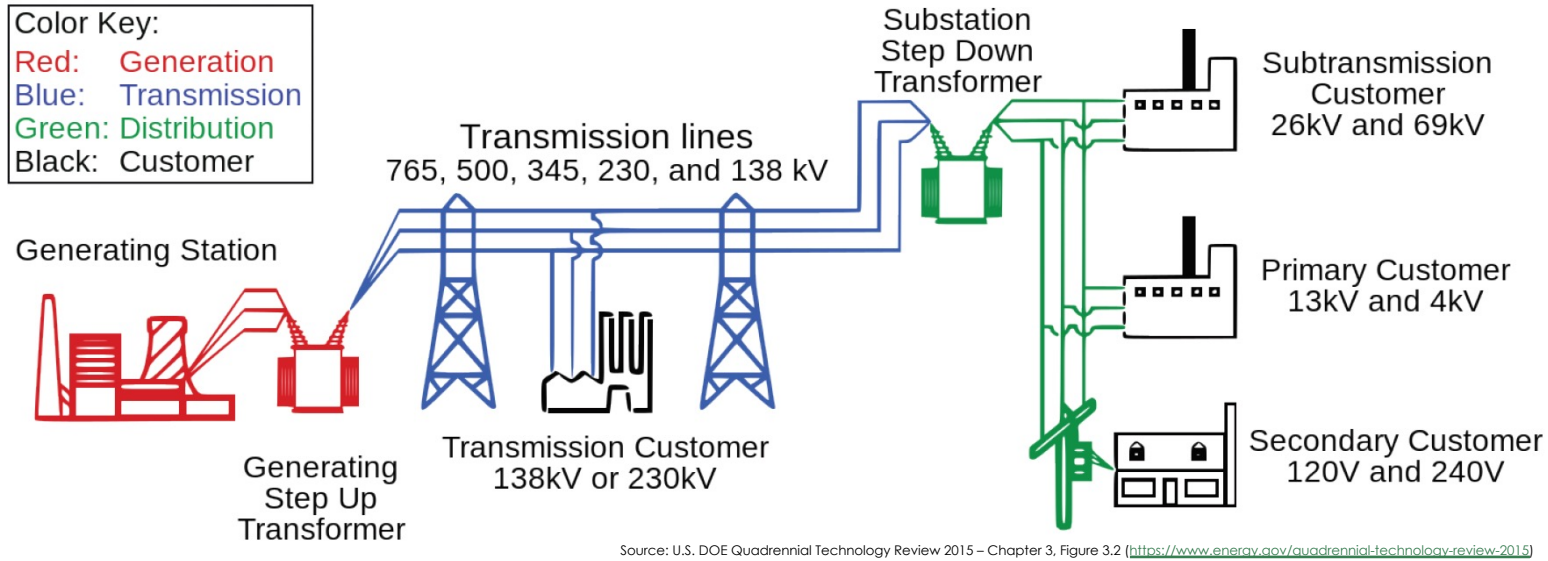
Center for Alternate Synchronization and Timing (CAST)

- Has emerged as an operational implementation of DOE's DarkNet R&D program
- DarkNet's objective: develop a system architecture and implementation approach that ensures end-to-end secure communications for the bulk power grid
- R&D areas:
  - Alternative timing
  - Wide-area situational awareness
  - Secure grid communications
  - Cyber resilience

The Need for Time Agreement

The Grid Used To Be Simpler in Design & Operation

The Past

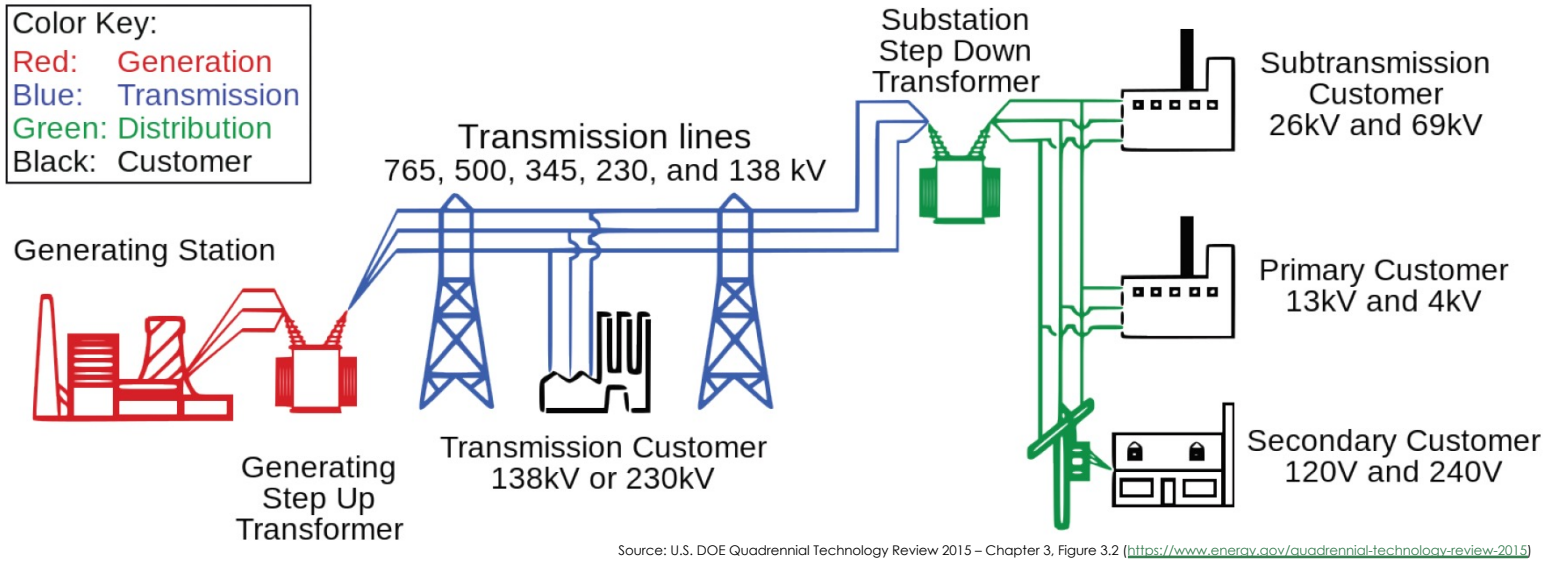


Source: U.S. DOE Quadrennial Technology Review 2015 – Chapter 3, Figure 3.2 (https://www.energy.gov/quadrennial-technology-review-2015)

The Need for Time Agreement

The Grid Used To Be Simpler in Design & Operation

The Past



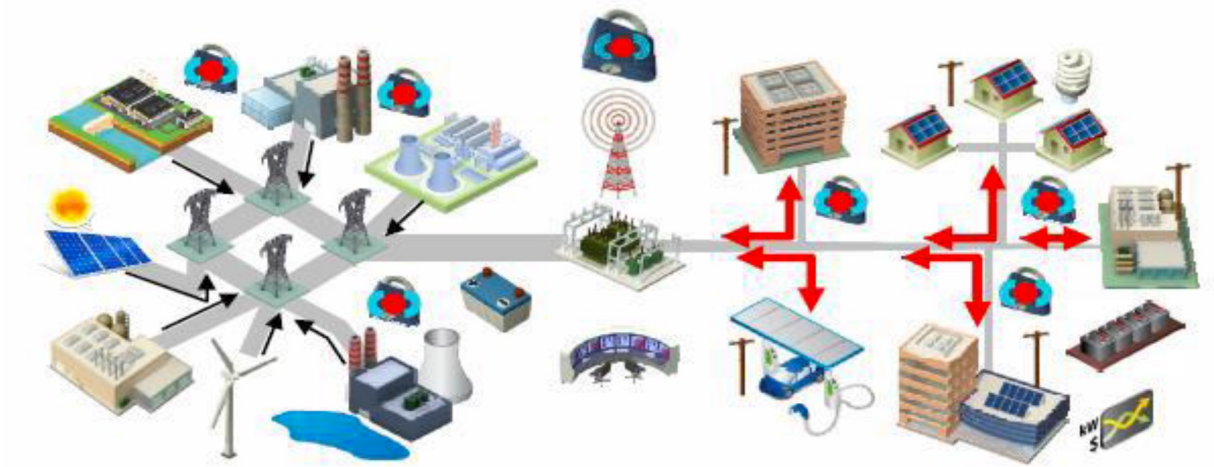
Source: U.S. DOE Quadrennial Technology Review 2015 – Chapter 3, Figure 3.2 (https://www.energy.gov/quadrennial-technology-review-2015)

- Geographic scope was limited due to segmented power networks
- Flow was uni-directional from station
- Load was over-provisioned and predicted based on past usage
- Distribution was one-to-many (hierarchical): One station, many customers

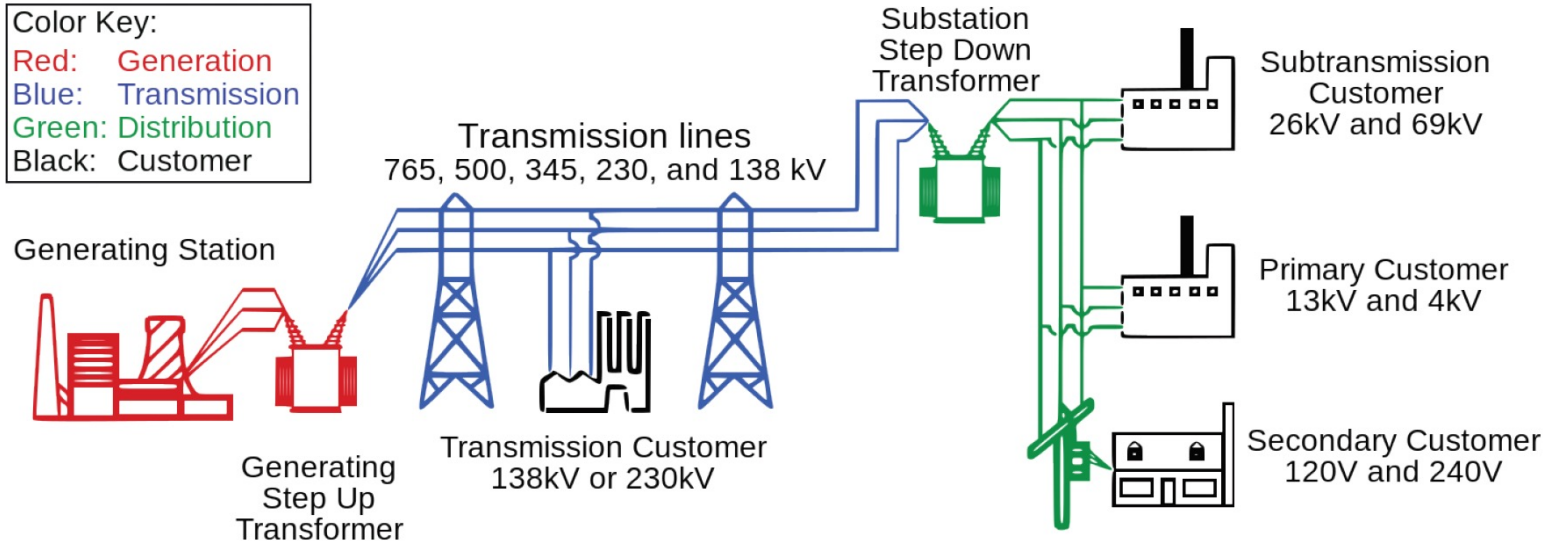
The Need for Time Agreement

The Future

The Grid is Becoming a Wide-Area Network



The Past

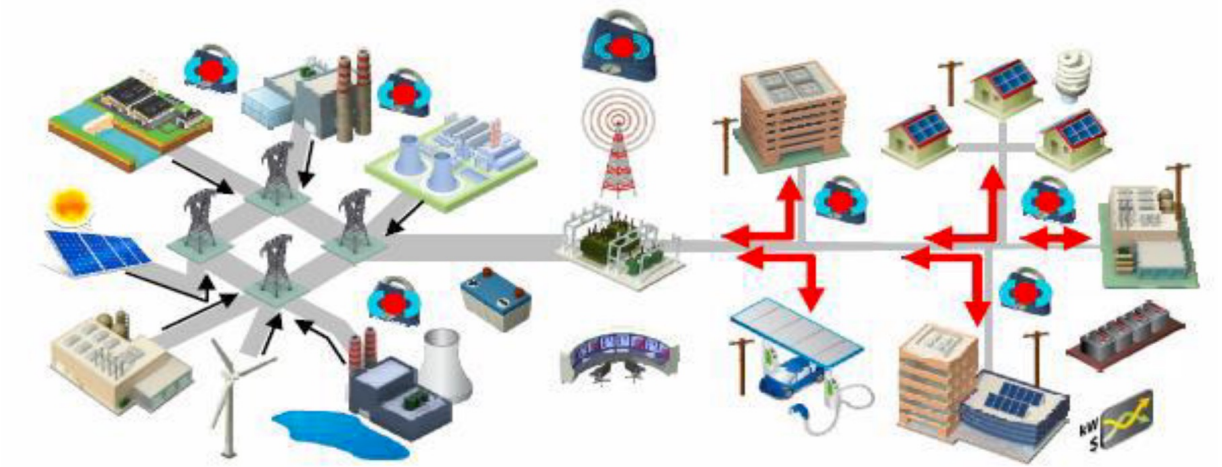


Source: U.S. DOE Quadrennial Technology Review 2015 – Chapter 3, Figure 3.2 (https://www.energy.gov/quadrennial-technology-review-2015)

The Need for Time Agreement

The Future

The Grid is Becoming a Wide-Area Network



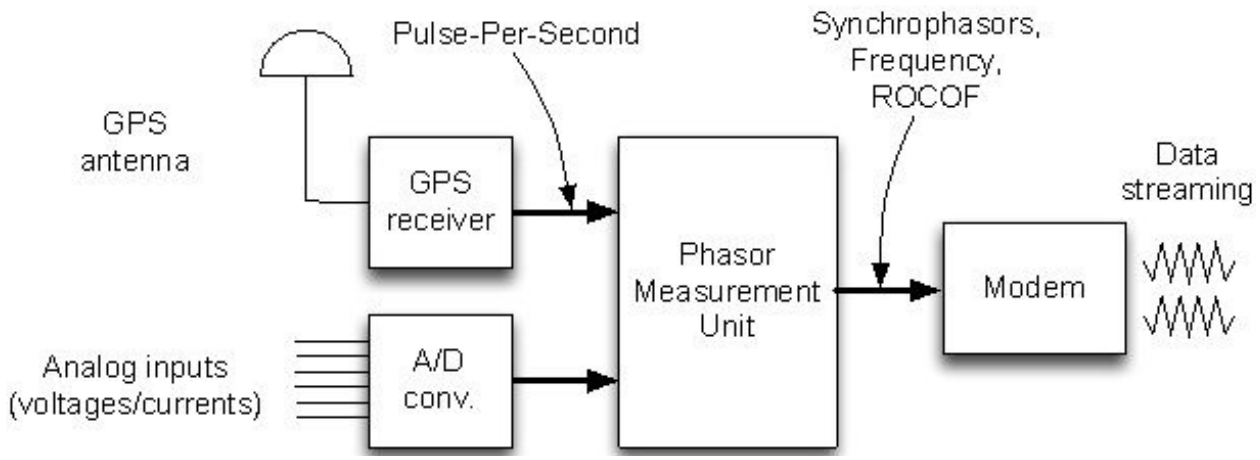
Geographic scope expanded with regional inter-connects

Flow is multi-directional

Load is based on real-time data and predictive analytics

Distribution shifts from hierarchical to peer-to-peer

A Dynamic Power Grid Requires Time-Aware Sensors



Measures 50/60 Hz waveform (voltages and currents)

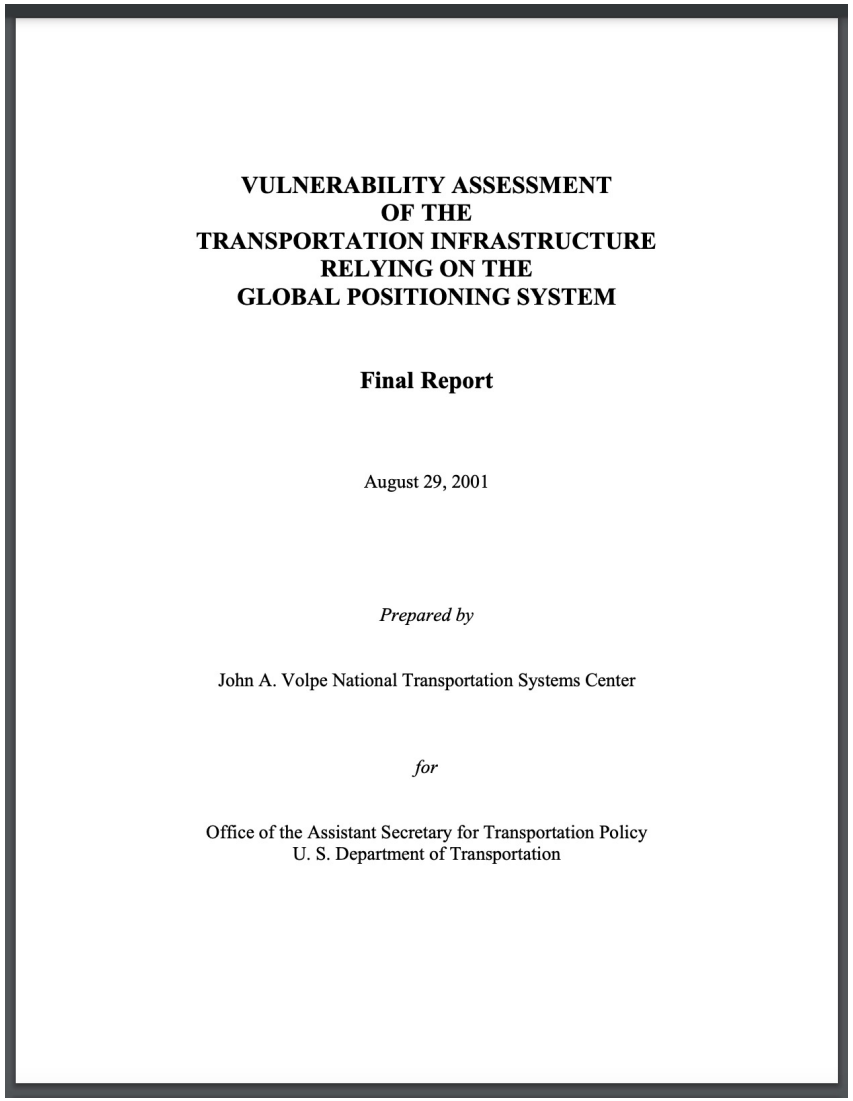
60-120 samples/second

- Situational awareness is achieved through sensors placed throughout the grid
- These sensors, called Phasor Measurement Units or PMUs, are **time-synchronized**
  - Standards call for 1000ns uncertainty from UTC
- Measurements streamed throughout system, providing significant improvements in grid monitoring and situational awareness

Traditional Source of Synchronization: GPS

Concerns about Vulnerabilities of GPS

- The ubiquitous power grid application currently depends on civilian GPS technology
- The power grid is critical infrastructure and must be able to withstand sophisticated, and potentially state-sponsored, multi-actor attacks



VULNERABILITY ASSESSMENT
OF THE
TRANSPORTATION INFRASTRUCTURE
RELYING ON THE
GLOBAL POSITIONING SYSTEM

Final Report

August 29, 2001

Prepared by

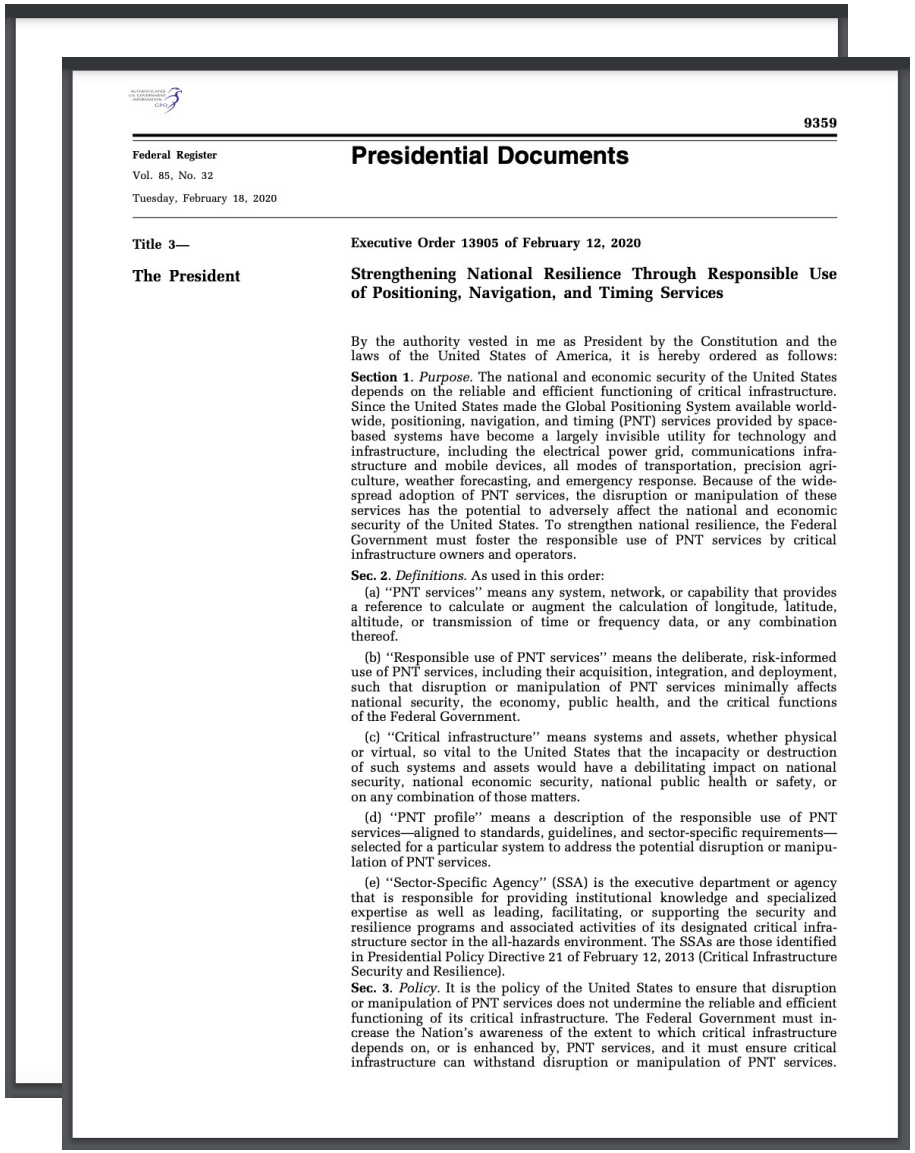
John A. Volpe National Transportation Systems Center

for

Office of the Assistant Secretary for Transportation Policy
U. S. Department of Transportation

Concerns about Vulnerabilities of GPS

- The ubiquitous power grid application currently depends on civilian GPS technology
- The power grid is critical infrastructure and must be able to withstand sophisticated, and potentially state-sponsored, multi-actor attacks



9359

Federal Register
Vol. 85, No. 32
Tuesday, February 18, 2020

Presidential Documents

Title 3—
The President

Executive Order 13905 of February 12, 2020

Strengthening National Resilience Through Responsible Use of Positioning, Navigation, and Timing Services

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. *Purpose*. The national and economic security of the United States depends on the reliable and efficient functioning of critical infrastructure. Since the United States made the Global Positioning System available worldwide, positioning, navigation, and timing (PNT) services provided by space-based systems have become a largely invisible utility for technology and infrastructure, including the electrical power grid, communications infrastructure and mobile devices, all modes of transportation, precision agriculture, weather forecasting, and emergency response. Because of the widespread adoption of PNT services, the disruption or manipulation of these services has the potential to adversely affect the national and economic security of the United States. To strengthen national resilience, the Federal Government must foster the responsible use of PNT services by critical infrastructure owners and operators.

Sec. 2. *Definitions*. As used in this order:

(a) ''PNT services'' means any system, network, or capability that provides a reference to calculate or augment the calculation of longitude, latitude, altitude, or transmission of time or frequency data, or any combination thereof.

(b) ''Responsible use of PNT services'' means the deliberate, risk-informed use of PNT services, including their acquisition, integration, and deployment, such that disruption or manipulation of PNT services minimally affects national security, the economy, public health, and the critical functions of the Federal Government.

(c) ''Critical infrastructure'' means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on national security, national economic security, national public health or safety, or on any combination of those matters.

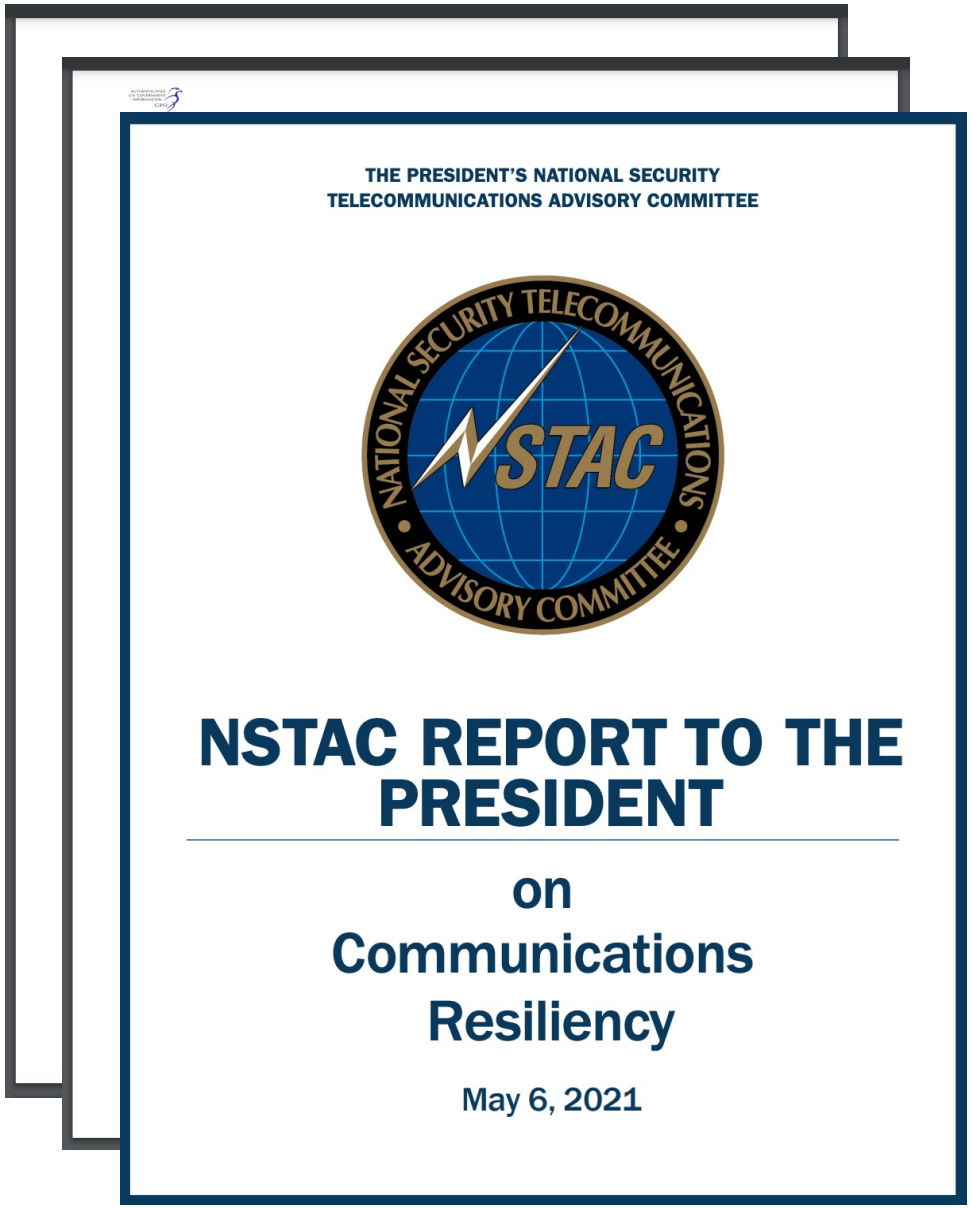
(d) ''PNT profile'' means a description of the responsible use of PNT services—aligned to standards, guidelines, and sector-specific requirements—selected for a particular system to address the potential disruption or manipulation of PNT services.

(e) ''Sector-Specific Agency'' (SSA) is the executive department or agency that is responsible for providing institutional knowledge and specialized expertise as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the all-hazards environment. The SSAs are those identified in Presidential Policy Directive 21 of February 12, 2013 (Critical Infrastructure Security and Resilience).

Sec. 3. *Policy*. It is the policy of the United States to ensure that disruption or manipulation of PNT services does not undermine the reliable and efficient functioning of its critical infrastructure. The Federal Government must increase the Nation's awareness of the extent to which critical infrastructure depends on, or is enhanced by, PNT services, and it must ensure critical infrastructure can withstand disruption or manipulation of PNT services.

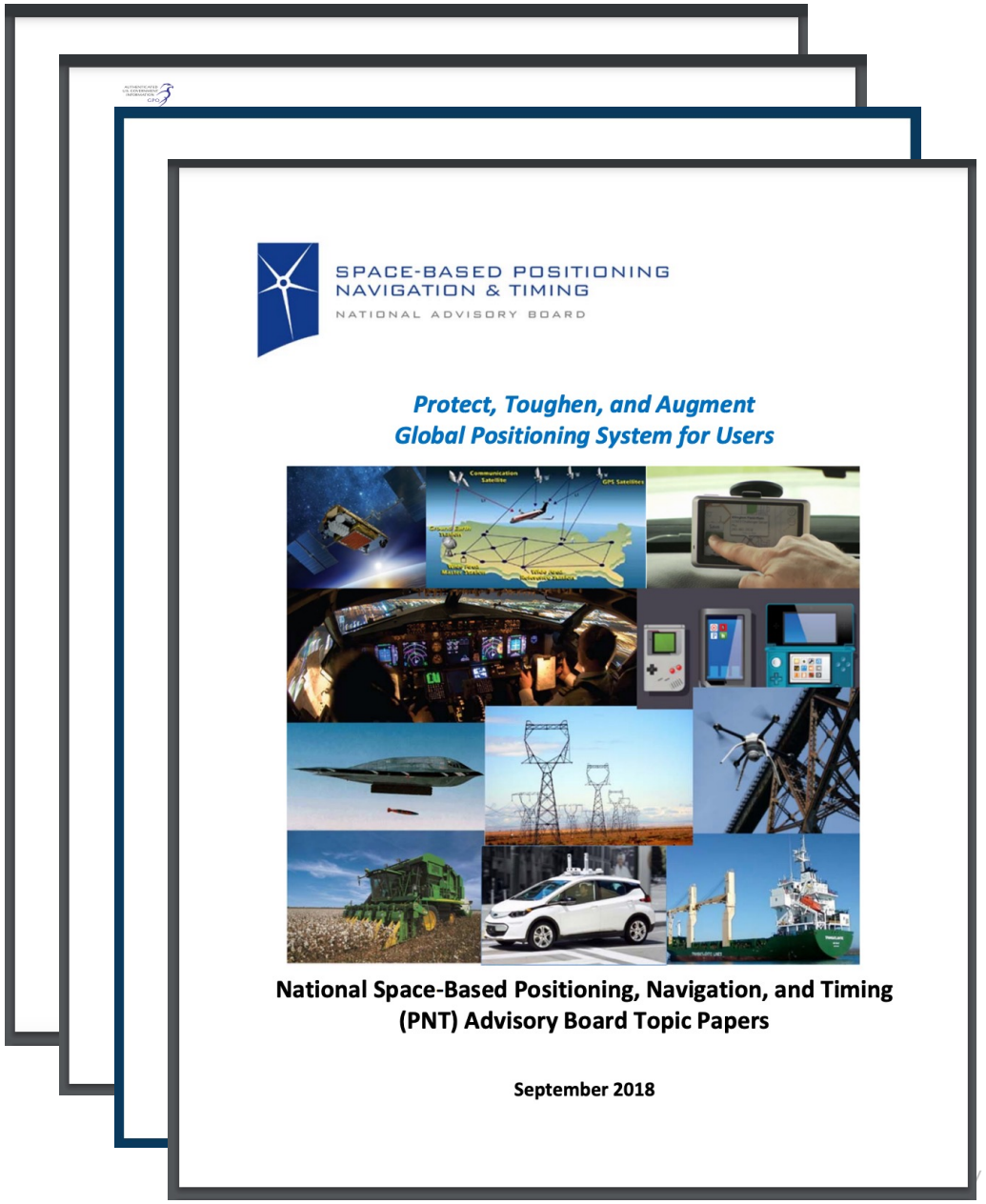
Concerns about Vulnerabilities of GPS

- The ubiquitous power grid application currently depends on civilian GPS technology
- The power grid is critical infrastructure and must be able to withstand sophisticated, and potentially state-sponsored, multi-actor attacks



Concerns about Vulnerabilities of GPS

- The ubiquitous power grid application currently depends on civilian GPS technology
- The power grid is critical infrastructure and must be able to withstand sophisticated, and potentially state-sponsored, multi-actor attacks



Concerns about Vulnerabilities of GPS

- The ubiquitous power grid application currently depends on civilian GPS technology
- The power grid is critical infrastructure and must be able to withstand sophisticated, and potentially state-sponsored, multi-actor attacks

atis

1200 G Street, NW
Suite 500
Washington, DC 20005

P: +1 202-628-6380
W: www.atis.org

May 7, 2021

The Honorable Adam Smith
Chair
Committee on Armed Services
United States House of Representatives
Washington, D.C. 20515

The Honorable Eddie Bernice Johnson
Chair
Committee on Science, Space and Technology
United States House of Representatives
Washington, D.C. 20515

The Honorable Mike Rogers
Ranking Member
Committee on Armed Services
United States House of Representatives
Washington, D.C. 20515

The Honorable Frank Lucas
Ranking Member
Committee on Science, Space and Technology
United States House of Representatives
Washington, D.C. 20515

The Honorable Peter DeFazio
Chair
Committee on Transportation and Infrastructure
United States House of Representatives
Washington, D.C. 20515

The Honorable Bennie Thompson
Chairman
Committee on Homeland Security
United States House of Representatives
Washington, D.C. 20515

The Honorable Sam Graves
Ranking Member
Committee on Transportation and Infrastructure
United States House of Representatives
Washington, D.C. 20515

The Honorable John Katko
Ranking Member
Committee on Homeland Security
United States House of Representatives
Washington, D.C. 20515

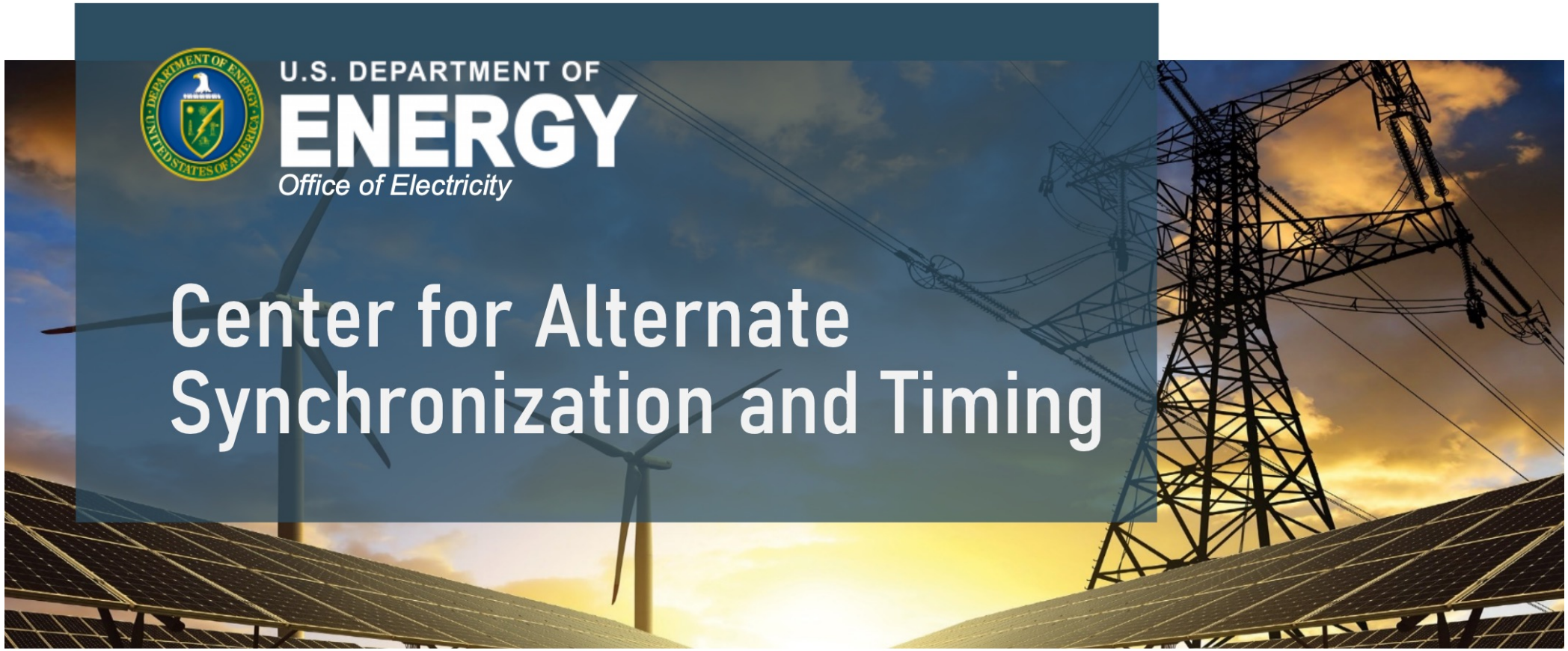
Re: Urgent Need for Alternative Positioning, Navigation, and Timing Systems Funding

Dear Members of Congress:

The Alliance for Telecommunications Industry Solutions (ATIS), on behalf of its SYNC Committee (SYNC), is writing to explain the urgent need for funding the deployment and adoption of Alternative Positioning, Navigation, and Timing (PNT) Systems in U.S. critical infrastructure, including the U.S. telecom industry.

ATIS is a leading developer of standards and other technical deliverables for Information and Communications Technology (ICT) and Services companies. ATIS develops standards on a broad range of important issues, including 5G and the Internet of Things (IoT). Industry subject matter experts work collaboratively in ATIS' open industry committees, such as SYNC. ATIS SYNC develops and

Center for Alternate Synchronization and Timing (CAST)

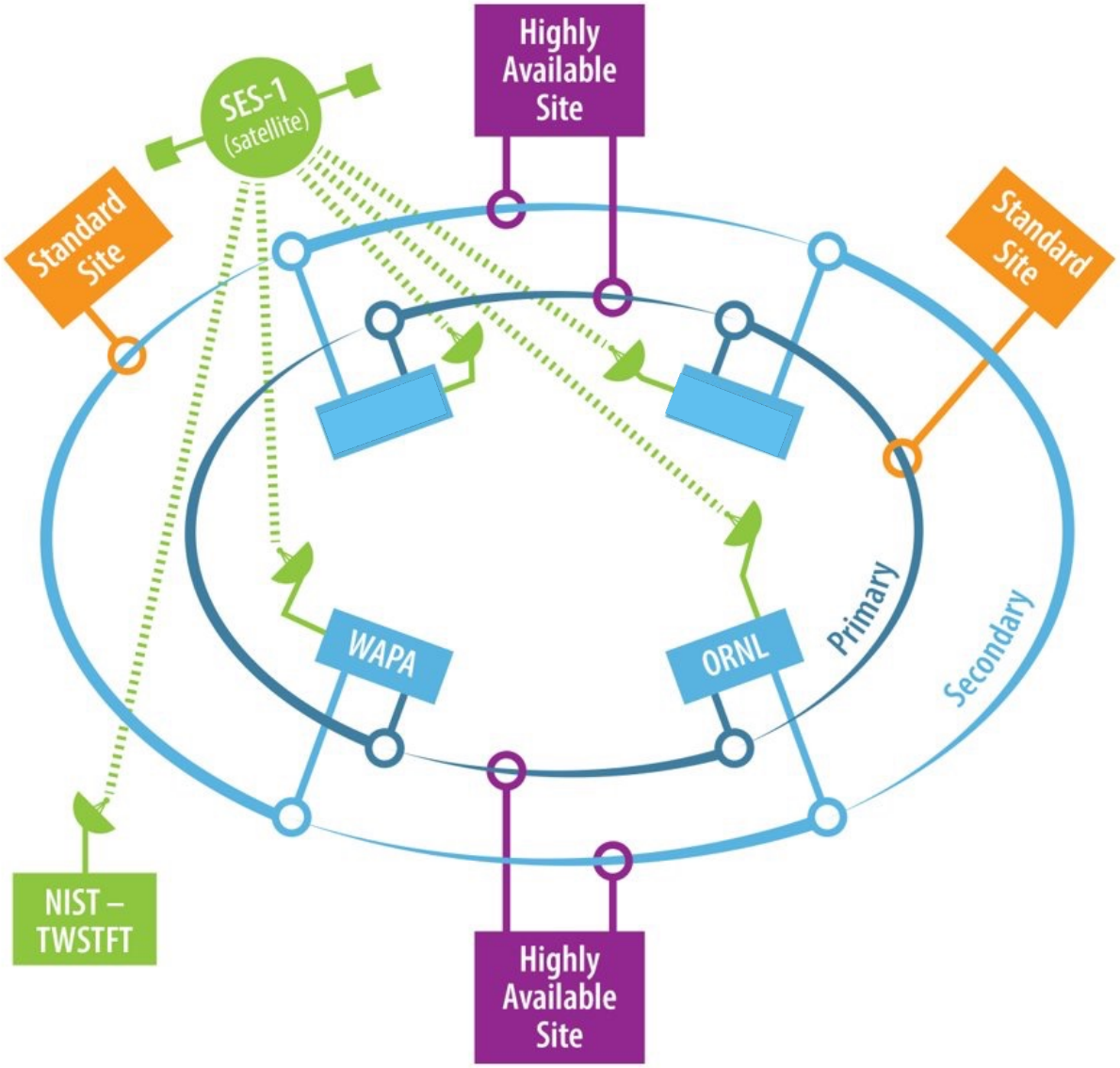


DELIVERING TERRESTRIAL SYNCHRONIZED TIMING

FOR THE NATION'S ENERGY SECTOR AND CRITICAL INFRASTRUCTURE

CAST Design

- Redundant & Resilient
  - SATCOM backed up by terrestrial
  - Best Master Clock across multiple Master Nodes
- Secure
  - Jamming (terrestrial redundancy)
  - Spoofing (terrestrial, quantum, MACsec)
  - Cyber (quantum, MACsec)
  - Physical (ORNL campus, badged access)
- Scalable
  - Hierarchical design
- Precise & Traceable
  - IEEE standards-based
  - TWSTFT with NIST



CAST Architecture

- Network of synchronized Grand Master Clock Nodes
  - ORNL and the Federal Power Marketing Administrations (PMAs)
  - Geographic and hardware redundancy
- GMC Nodes connected through redundant SATCOM and terrestrial links
- System clocks with verified agreement with UTC through SATCOM
- GMC Nodes securely propagate time to downstream infrastructure
  - Sensors, OT, IT
- Power grid operators can integrate with the CAST Network

The Potential of CAST

- Augments the power grid's utilization of GPS with a resilient time synchronization source
- Insulates the power grid's synchronized timing requirements from bad-actors intent on disrupting GPS
- Improves grid resilience through better anomaly detection from a nation-wide time synchronization network

CAST Timeline and Next Steps

- FY22
  - ORNL and WAPA CAST GMCs online with time synchronization and propagation
  - TWSTFT for PTP validated
- FY23
  - Architecture and BoM validated for early-adopter commercial additions to CAST network
- FY24
  - CAST fully operational with nation-wide terrestrial time synchronization

Summary

- US power grid is moving toward a wide-area network; requires precise, secure, and resilient time synchronization
- GPS is an amazing capability for domestic and global PNT needs, but inherent limitations lead to grid vulnerabilities
- A network of terrestrial GMCs, synchronized across a redundant set of network links, provide a robust source of timing for US critical infrastructure
- DOE's CAST is designed to deliver secure, resilient, and cost-efficient time synchronization-as-a-service to the nation's power grid operators