Nationwide Integration of Time Resiliency for Operations (NITRO)
Information Brief
12 Sep 2023

Overall Classification Level Of This Brief: **Unclassified**

Strategic Problem Point 1

Problem: The country lacks synchronized resilient time to protect the interconnected State/Territory and U.S. critical infrastructure digital ecosystem providing public services.
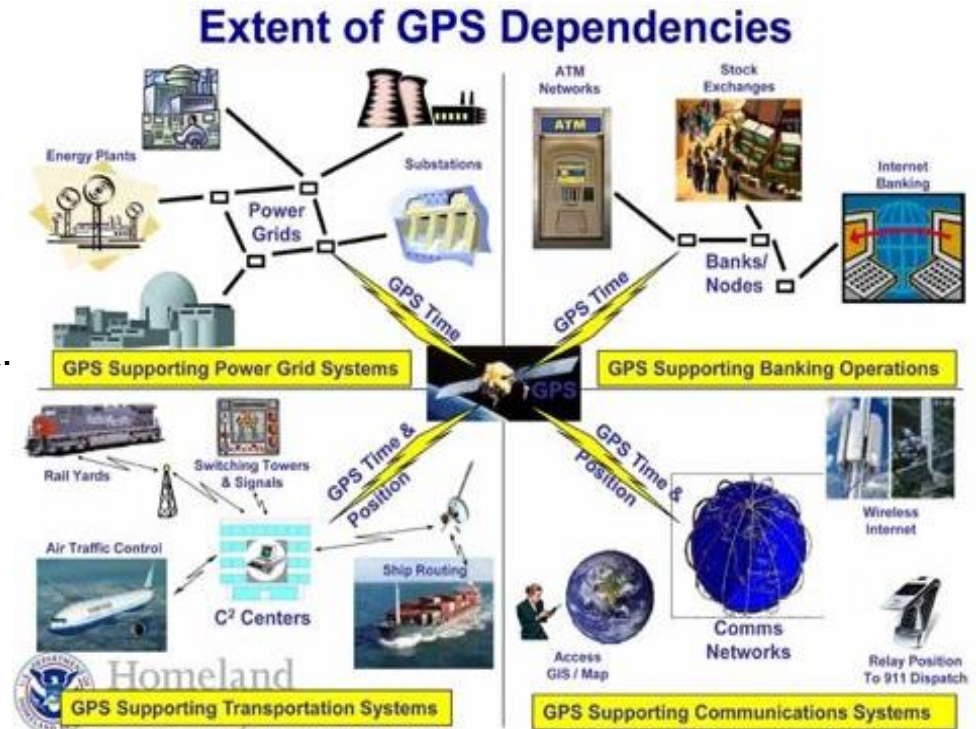
Why?

- All computers need accurate time to work.
- Over-reliance on GPS.
- Active, persisting and increasing threat.

What happens?

CNN War In Space - What would happen to America if GPS was attacked?
https://www.youtube.com/watch?v=cBZIR6RLVzQ

Extent of GPS Dependencies

"GPS still a single point of failure"
NSC Director Durkovich, Nov 2021

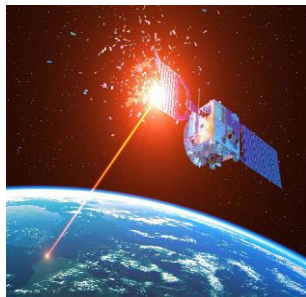## Timing disruptions & threats increasing

- Ex: Denver metropolitan area (including airport) Jan 2022, Dallas/Ft Worth Airport Nov 2022

- Smaller impact disruptions common

- Threats: Cyber-attack, solar activity, criminal/malicious, accidental

Dallas Nov 22
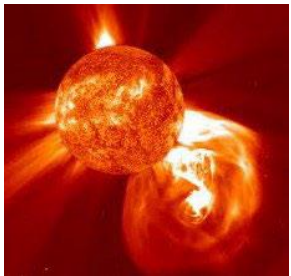
Solar Max July 2025

Jammers $15-$1,500

Tactical Need

Resilient, Alternate, Complementary Timing

National Guard, First Responders GPS-denied or manipulated operations
- Land mobile radio communications
- Operational command & coordination
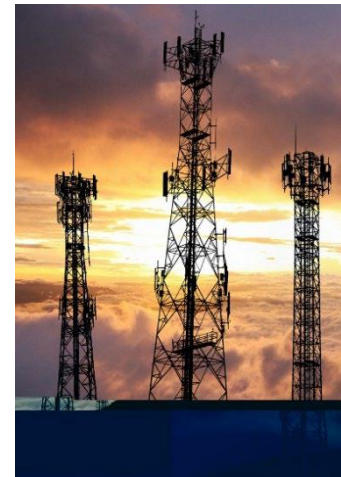- Homeland Security systems

States/Territories critical infrastructure systems
- Energy (electricity, gas, jet fuel), water/waste water, communications, transportation, financial/billing, etc.

Broadband Equity Access & Deployment (BEAD)
- Base stations synchronization, applications, user equipment
- Implementation without resilient time increases national risk

Two Strategic Problems*
One Solution

NITRO (Nationwide Integration of Time Resiliency for Operations)

- State/Federal Partnership

- National Guard in coordination with Homeland Security Advisors/Emergency Managers

- 31 States/Territories currently engaged

- Prototype fielded & serving
  - 7 states (VA, MD, CA, WV, WA, IL, LA)
  - 250+ orgs
  - 30M+ people

- Supported by Adjutants General Association of the U.S.

○ 100nm

★ FEMA Region HQ

NOTIONAL US DEPLOYMENT

* Strategic Problems:
1. Critical Infrastructure over-relies on GPS timing (Slide 2)
2. Timing disruptions & threats increasing (Slide 3)
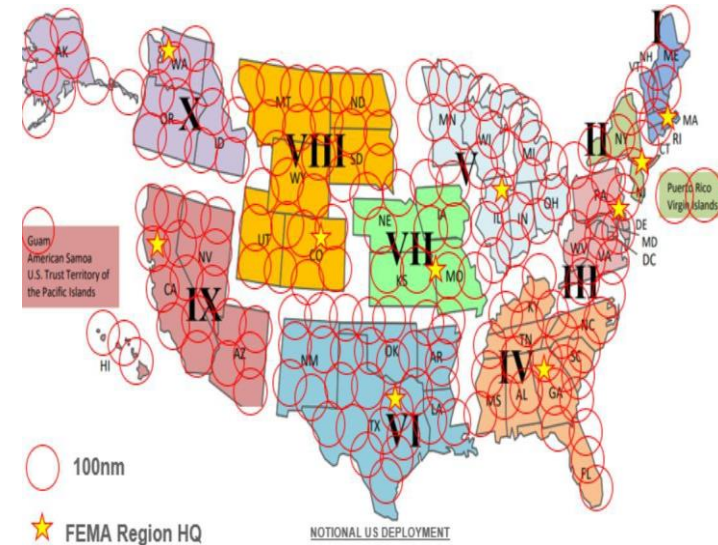
Implementation

National Guard – All Adjutants General

Governance:
- NITRO Board: Maj Gen Neely (IL) + WV, VA, WA, MD, CA, LA Adjutants General
    - States/Territories Homeland Security Advisors/ Emergency Managers
- Staff & Execution: National Guard Bureau, Dr. Laura Callahan

Federal Interagency Coordination (emerging)
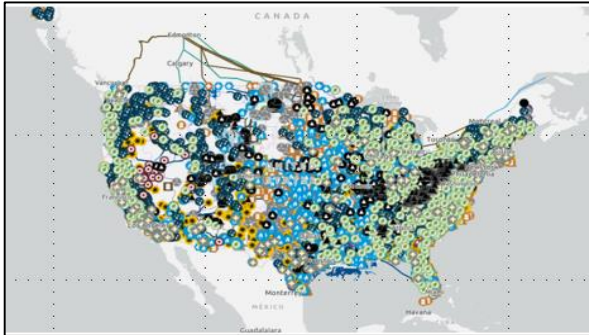- NITRO Advisory Group: NGB*, DHS*, DOC, DOT,* DOE*, National Cyber Director's Office, National Security Council*
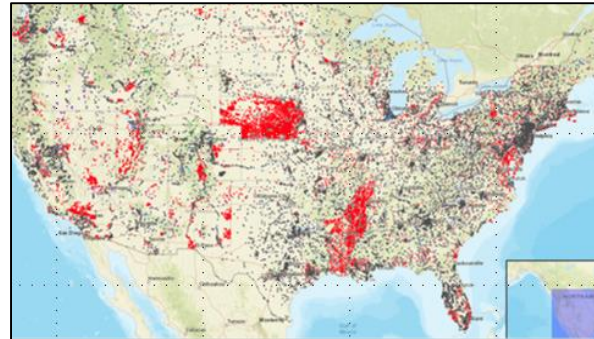
* Confirmed

100nm
⭐ FEMA Region HQ   NATIONAL US DEPLOYMENT

Critical Infrastructure Examples

U.S. Energy

U.S. Water Locations

U.S. Dams

U.S. Manufacturing Facilities

- **Public information available to all, including adversaries**
- **Resilient PNT operations requires a different way of thinking**
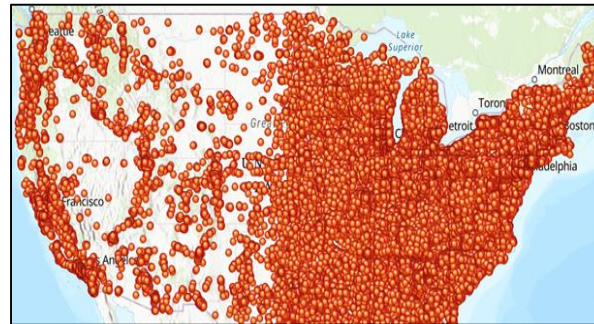
- SLTT infrastructures are interconnected with U.S. critical infrastructure to provide public services. Examples:
  - Transportation uses 64 Communications frequencies
  - Equipment across all sectors require electricity
  - Hydroelectric dams generate power
  - Billing and financial systems are embedded throughout at various levels
- Accurate time is required by and flows throughout this interconnected intrastate and interstate operational environment.
- Domestic emergencies caused by lack of accurate time are not bound by sectors or "system ownership" because the indiscriminate impact traverses across the interconnected operational ecosystem.

NITRO Capability

- Operational prototype which provides resilient time to SLTT and U.S. critical infrastructure to prevent disruptions to public services people depend upon.

- Survivable and mitigates GPS/GNSS jamming, spoofing, and cyber-related vulnerabilities.

- Addresses 11 domestic timing infrastructure operational gaps.

- Receives data from multiple space and terrestrial PNT services and does not require changes to end-user equipment.

- Creates a fully meshed nationwide "sensor grid" and common operating picture of the underlying timing infrastructure. Current roles:
    - Operations center personnel (IOC, EOC, JOC, etc.)
    - Cyber defenders
    - IT/System administrators

- Allows National Guard and civil authorities to work behind the scenes to resolve the situation – essentially making any disruption "invisible" to the general population.

NITRO System Overview
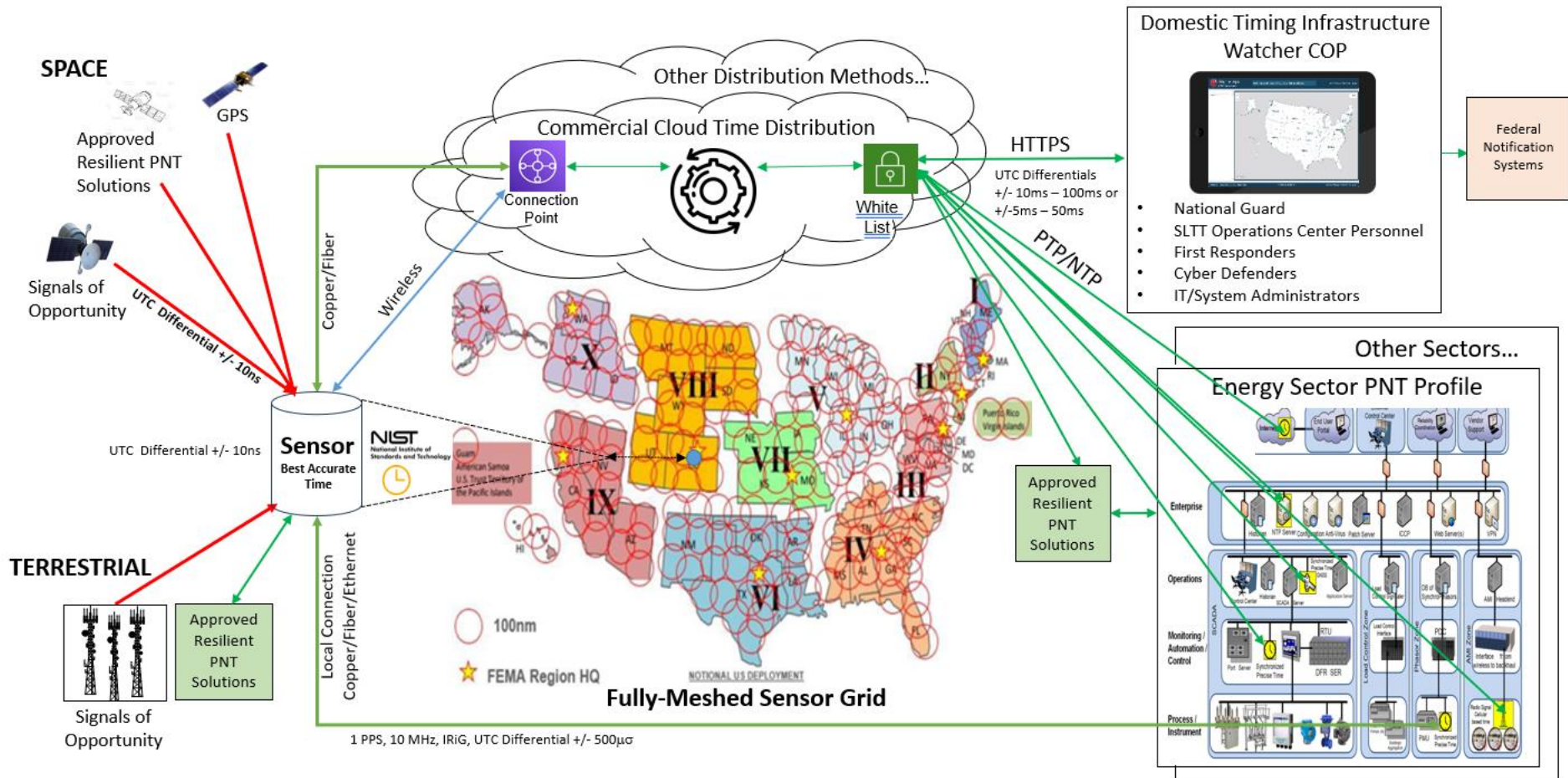
Policy Alignment

- National Timing Resilience & Security Act of 2018
- E.O. 13905, Responsible use of PNT
- SPD-7 Space-based PNT Policy
- OMB Memo 23-18, 27 June 2023, Cybersecurity Priorities
  - "Leverage Federal grants and Other Incentives to Build in Security"
- National Cyber Security Strategy Implementation Plan, July 2023
  - 3.4.1 Leverage Federal grants to improve infrastructure cybersecurity
  - Pillar Four: Invest in A Resilient Future

Questions

National Guard Lead:	**Subject Matter Lead:**
Maj Gen Rich Neely	Dr. Laura Callahan
The Adjutant General for Illinois	Special Advisor to the Vice Chief,
Commander, Illinois National Guard	National Guard Bureau
richard.r.neely.mil@army.mil	*llcalla@cybercom.mil*