DHS SCIENCE AND TECHNOLOGY

Responsible Use of PNT for DLT in the Financial Services Sector

ATIS Time and Money Conference 2020

January 28, 2020

Ernest Wong

Technical Manager
Technology Centers Division
Science and Technology Directorate

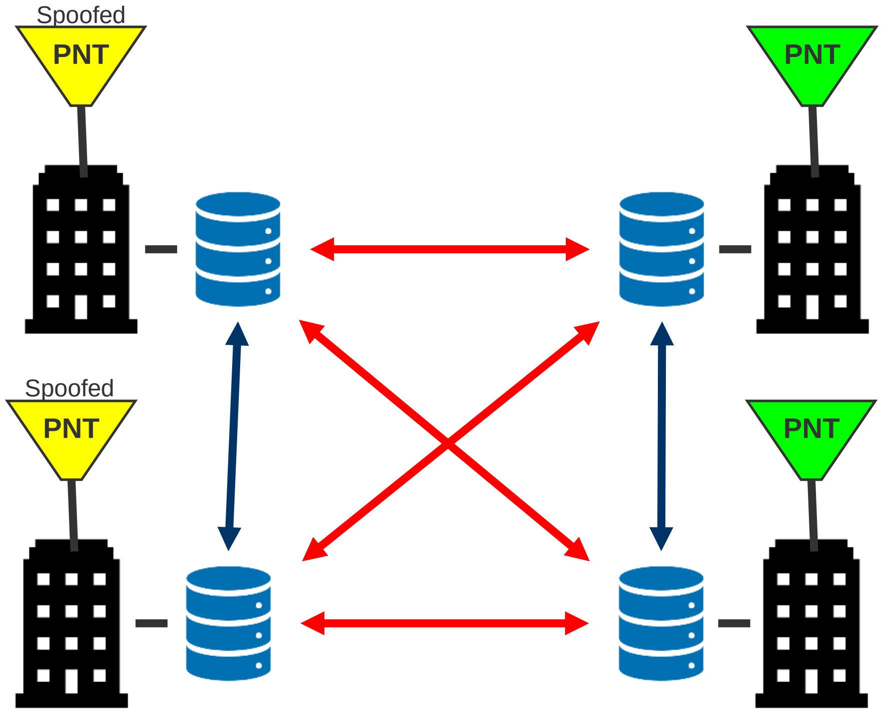
Homeland Security
Science and Technology

Presentation Outline

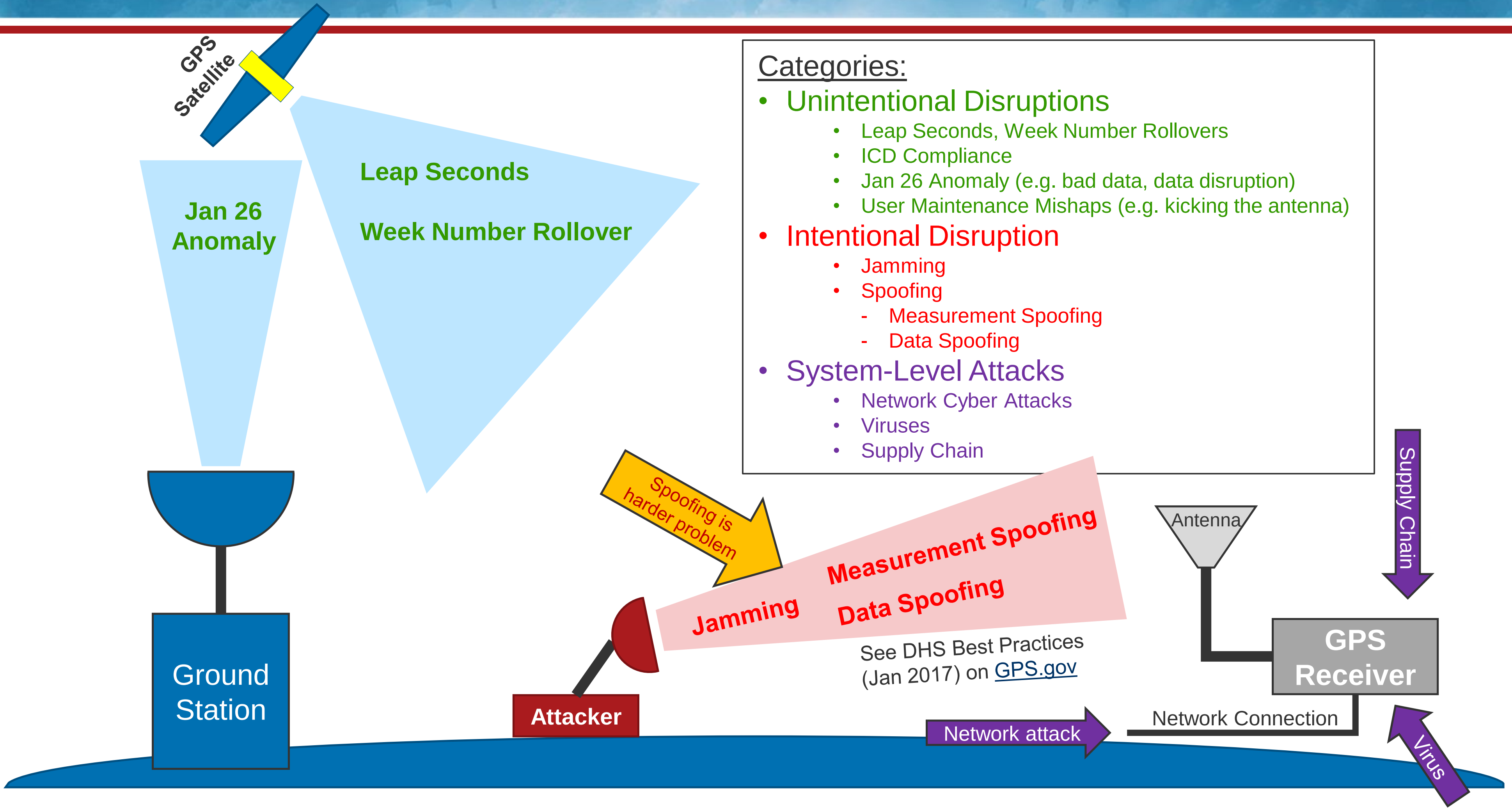
- Introduction Sections
  - Precision Timing in DLT: What could go wrong? (or right?)
  - Overview of Threats to GPS Timing
  - Role of DHS
- Protecting the Financial Services Sector against PNT Spoofing
  - Risk Assessment Spectrum
  - PNT Receivers and Attack Surfaces
  - Resilient PNT Conformance Framework
  - Mitigations: The Flip
  - Other Mitigations
  - Other Things Coming “Soon” from DHS

Precision Timing in DLT:
What Could Go Wrong?

- Potential Applications
  - Trading
  - Market Data
  - Clearance and Settlements
  - Timing Compliance
- Building the Case
  - A trade is a trade, regardless of underlying technology.
    - All (DLT) transactions will need to be time stamped (assumption).
  - Firms have to trace to sovereign time / UTC.
    - This generally means a GPS receiver.
  - GPS time can be spoofed.
  - What happens when the time stamps are wrong?
    - When would the discrepancy be noticed?
    - Would DLT help identify the discrepancy? (maybe not)
    - Would it hurt or help?



GPS/PNT Threat Classes



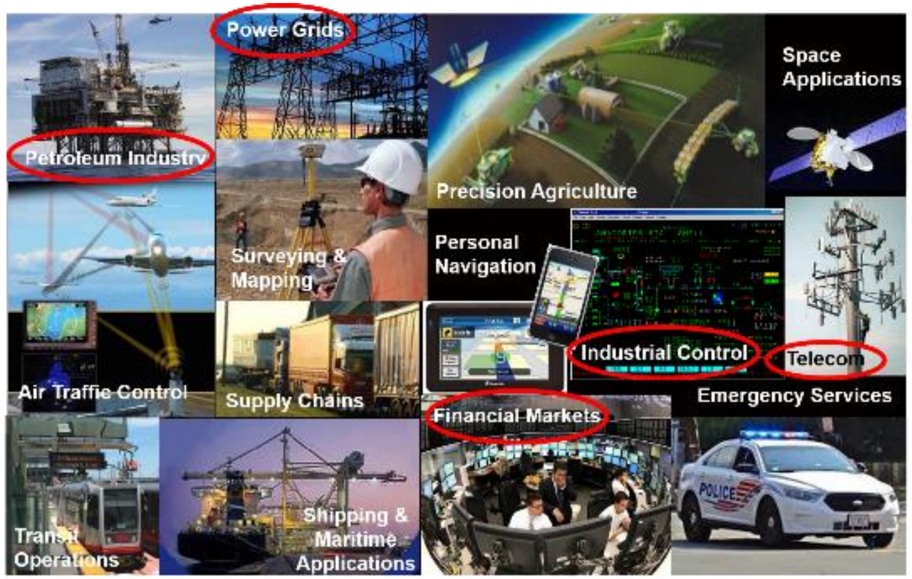
Categories:

- Unintentional Disruptions
  - Leap Seconds, Week Number Rollovers
  - ICD Compliance
  - Jan 26 Anomaly (e.g. bad data, data disruption)
  - User Maintenance Mishaps (e.g. kicking the antenna)
- Intentional Disruption
  - Jamming
  - Spoofing
    - Measurement Spoofing
    - Data Spoofing
- System-Level Attacks
  - Network Cyber Attacks
  - Viruses
  - Supply Chain

See DHS Best Practices (Jan 2017) on GPS.gov

DHS Role in Timing for Critical Infrastructure

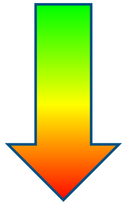
- **PNT in Critical Infrastructure**: Accurate position, navigation and timing (PNT) information is necessary for the functioning of many critical infrastructure sectors.
  - Precision timing is particularly important.
  - Primary source of distributed & accurate timing is currently through GPS.
- **Problem**: GPS susceptible to disruption (both intentional and unintentional)
  - Jamming (Newark I-95, North Korea, criminal activity)
  - Spoofing (Possible examples from recent open source media)
    - **Spoofing also becoming easier w/ low-cost SDRs & open source code**
- **DHS Role:**
  - Improve the resilience of critical infrastructure against PNT threats and disruptions via:
    - Engaging with industry for information sharing and risk management.
    - Developing technology and mitigations.



Protecting the Financial Services Sector Against PNT Spoofing

Risk Assessment Spectrum

- **Large-scale, high-speed, high-value operations with multiple Cesium atomic Clocks**
  - Operation: Trusting the atomic clock and keeping it on holdover during the weekday.
    - Significantly reduces risk due to the smaller attack window.
  - Remaining Risk: Attack Surface ≠ Attack Window. Attack surface open to data & measurement spoofing.



- **Traditional operations with low-cost GPS receiver**
  - Operation: Time is provided from a basic GPS receiver constantly listening through the RF port.
  - Risk: Susceptible to both measurement spoofing and data spoofing.
  - Options: There are mitigations you can employ that won’t cost as much as a Cs atomic clock.

PNT Receivers and Attack Surfaces

- PNT receivers should be treated like computers rather than radios.
  - The PNT antenna is like an open port.
  - There is data processing inside the receiver.
- When mitigating for PNT resilience, need to assess both the threat and the attack surface.

- **Caution when mitigating**: Adding more PNT sources does not automatically provide resilience.
  - More PNT sources = more attack surfaces.
  - When incorporating other PNT sources, they should also be examined from this perspective and hardened.

Resilient PNT Conformance Framework

Vision: Develop common language for defining resilient PNT equipment

- Accomplished through defining multiple levels of resilience.

- **Working Group:**
  - Industry working group consisting of most major system integrators (timing).
  - Looking for additional CI end-user representation and input.

Resilience Levels (Preview)

- **Level 1**: Robust Recovery
- **Level 4**: Operate through Threats

Levels apply to:

- GNSS Chipsets
- Integrated Receivers
- System of Systems

Key Concepts:

- Defense-in-Depth
- Resilience Levels
- Core Functions

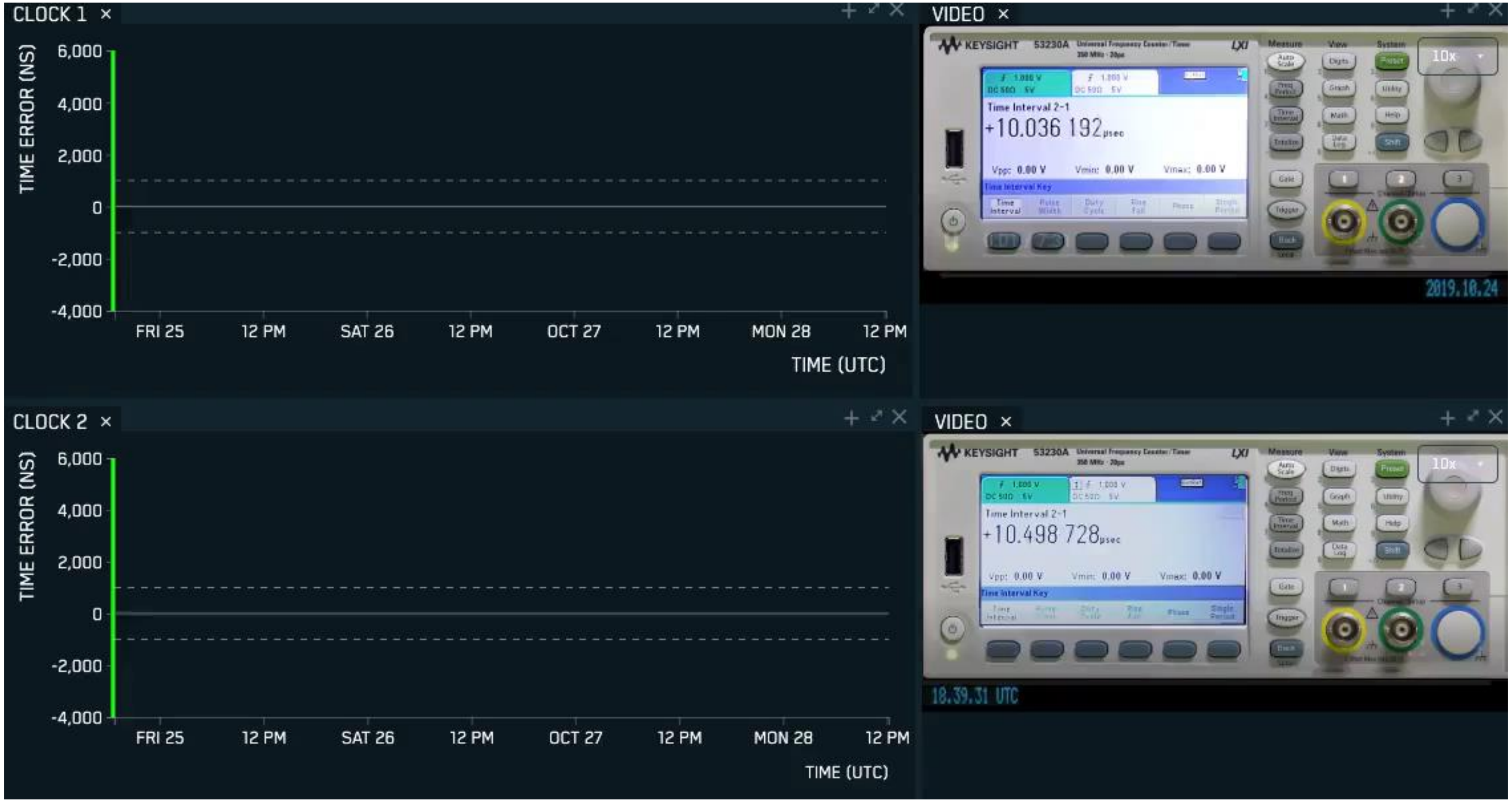
Will enable:

- Product differentiation for vendors
- Improved risk management and decision making by CI operators when acquiring new PNT equipment (or updating existing deployments).

- **Initial Focus**: GNSS-based timing equipment

Mitigations: The Flip

(Courtesy of HSSEDI)



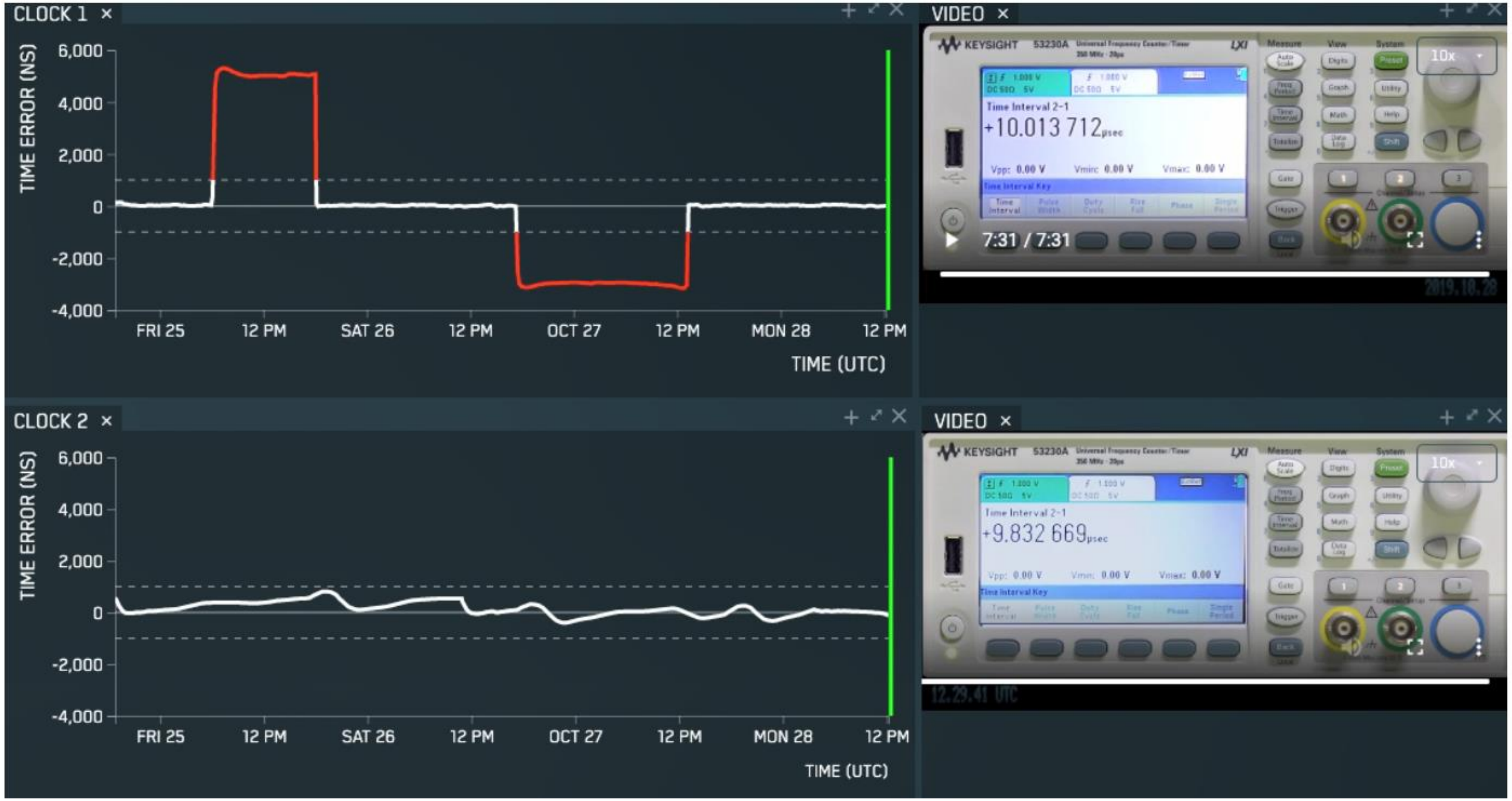
Time Interval 2-1
+10.036 192 psec
Vpp: 0.00 V Vmin: 0.00 V Vmax: 0.00 V

Time Interval 2-1
+10.498 728 psec
Vpp: 0.00 V Vmin: 0.00 V Vmax: 0.00 V

Credit: Homeland Security Systems Engineering and Development Institute (HSSEDI) FFRDC

Mitigations: The Flip

(Courtesy of HSSEDI)



Principle: Trust your clock

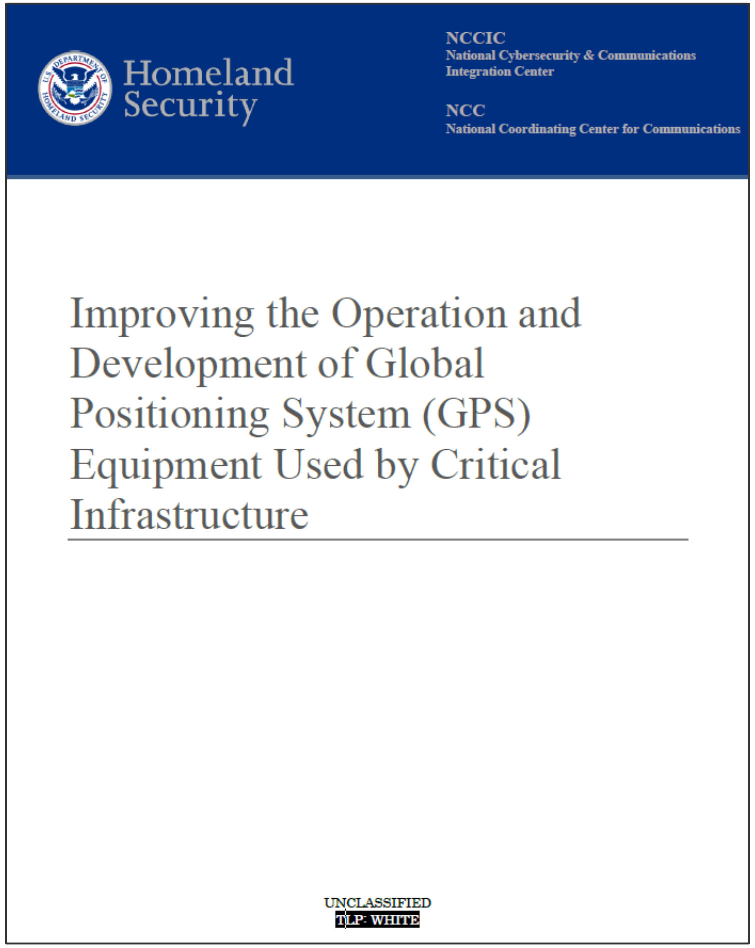
- Likely do not need the precision GPS provides (40ns).
- Therefore keep clock in holdover and perform intermittent disciplining as needed.
- Significantly reduces attack window.

Attacker can't spoof or jam a receiver if it isn't listening.

Credit: Homeland Security Systems Engineering and Development Institute (HSSEDI) FFRDC

Other User Mitigations & Considerations

- Horizon Nulling Antennas
- DHS Best Practices
  - User Deployment strategies
    - E.g. obscure view of antenna, decoys, placement
  - On GPS.gov (lower right-hand corner):
    - “Best Practices for Improving the Operation and Development of GPS Equipment Used by Critical Infrastructure - Jan 2017”
- “Resilient PNT Equipment”
  - Spoofing detection capabilities
    - Resilient PNT Conformance framework can help with this comparison.
  - Robust recovery capabilities
    - Ability to “return to a known good state” (DHS Best Practices, Jan 2017)
    - Essential since there’s no such thing as perfect security.
    - This is foundational capability for defense-in-depth approach.



Homeland Security

NCCIC
National Cybersecurity & Communications Integration Center

NCC
National Coordinating Center for Communications

Improving the Operation and Development of Global Positioning System (GPS) Equipment Used by Critical Infrastructure

UNCLASSIFIED
TLP: WHITE

Other Things Coming “Soon” from DHS

- **Epsilon Algorithms**
  - What: Spoofing detection algorithms focused on consistency checks using PVT data.
  - Who (Intended Use):
    - System Integrators: For integration into their products.
    - DIY End-user: Algorithms can utilize outputs from an existing GPS receiver.
  - When: By end of calendar year 2020

- **Spoofing Detection Toolkit**
  - What: API with a suite of spoofing detection algorithms for the full RF-processing chain.
  - Who (Intended Use):
    - System Integrators: For integration into their products. Algorithms for the full RF-processing chain requires sufficient data (either revised chipsets or a SDR)
    - DIY End-user : With DIY documentation, will be able to take the API and algorithms for use on an SDR and processor (e.g. SoC).
  - When: Targeting end of calendar year 2020

Other Things Coming “Soon” from DHS (con’t)

- **Best Practices for Financial Services Sector**
  - What: DHS best practices document tailored for financial services sector
    - Will likely include risk and mitigation information & recommendations on how to apply the Conformance Framework.
    - Will include suggestions for different scale operations and take into consideration tradeoffs of economic costs vs. risks.
  - For Who: Financial Sector End-users
  - When: TBD (likely Calendar Year 2021)

- **2020 GPS Equipment Testing for Critical Infrastructure (GET-CI 2020)**
  - What: Live-sky GPS spoofing event for industry to test and evaluate their equipment
  - For Who: Equipment manufacturers, critical infrastructure end-users
  - When: Expecting 2nd half of 2020
  - How to apply: RFI for participation will be posted on SAM.gov

Questions?

Engage With Us!

WEBSITE
scitech.dhs.gov

PERISCOPE
periscope.tv/dhsscitech/

TWITTER
@dhsscitech

YOUTUBE
youtube.com/dhsscitech

FACEBOOK
@dhsscitech

FLICKR
flickr.com/photos/dhsscitech/

U.S. DEPARTMENT OF HOMELAND SECURITY

Homeland Security

Science and Technology

DIVERSE PERSPECTIVES + SHARED GOALS = POWERFUL SOLUTIONS

Backup Slides

Conformance Framework Approach

Phases:

- Phase 1: Guidance documentation (targeting Spring 2020)
- Phase 2: Standards development (starting by 2021)

Reference Architecture:

- Reference Architecture documentation (FY20)
- Reference Implementation Demo (FY21)

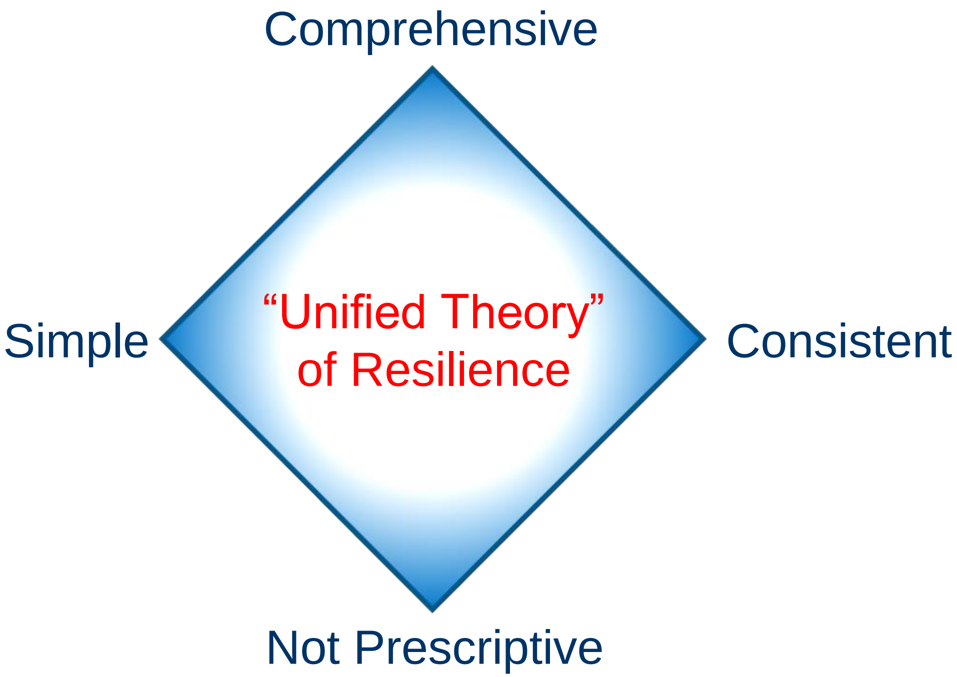
Industry Participation:

- Most major system integrators are part of working group (WG)
  - DOT and FAA also part of WG (to ensure extensibility to P/N)
- Looking for more end-user participation and input

Conformance Framework: Guiding Principles

- **Guiding Principles:**
    - Must be comprehensive
    - Must be simple
    - Must be consistent
    - Must NOT be prescriptive

- **Challenge**: Iterative process to distill framework into something that fits this “quadruple constraint.”



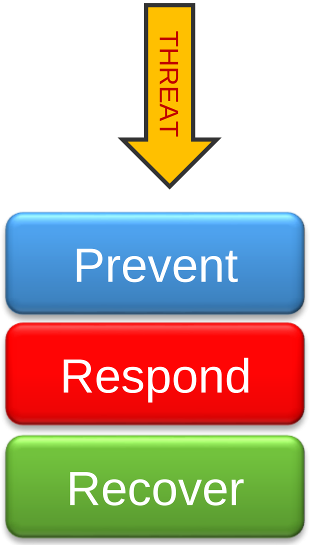
Conformance Framework: Key Concepts

Key Concepts:

- Defense-in-Depth *(2 dimensions)*
- Resilience Levels
- Core Functions

Core Functions

Blends NIST Cybersecurity Framework & PPD-21 National Preparedness System for Resilience



Resilience Levels (Preview)

- **Level 1**: Robust Recovery

Have working definitions, but needs some refinement to better satisfy the four guiding priorities.

- **Level 4**: Operate through Threats