DHS SCIENCE AND TECHNOLOGY

Resiliency in Design, Implementation and Operations for Critical Infrastructure

September 26, 2017

Keith Conner
Program Manager / Senior Engineer
Office for Interoperability and Compatibility
Science and Technology Directorate

Homeland Security
Science and Technology

Critical Infrastructure relies on GPS as a "Hidden Utility"

Power Grid Systems

Banking Operations

Transportation Centers

Communications Systems

Resiliency requires adapting to changing [threat] conditions

From Presidential Policy Directive 21 (PPD-21):

The term *"resilience"* means the ability to prepare for and adapt to changing conditions, and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.

Security requires recognizing changing threat conditions

From Presidential Policy Directive 21 (PPD-21):

The terms *"secure"* and *"security"* refer to reducing the risk to critical infrastructure by physical means or defense cyber measures to intrusions, attacks, or the effects of natural or manmade disasters.

From Executive Order 13800 (EO 13800):

"…known, but unmitigated vulnerabilities are among the highest cybersecurity risks."

Twenty years ago, PNT via GPS came from a receiver

20th Century Perspective	End-User Result
GPS is like the Internet: wonderful technology, nice people	Trust the source
GPS satellites are scarce, so receivers must be promiscuous	More is better
GPS receivers are radios	Be mindful of interference sources

Today, PNT via GPS comes from a "computer"

21st Century Perspective	Adapting End-User Mindset
GPS is like the Internet: wonderful technology, threats abound	Trust but verify
Threats to GPS abound, so receivers must be robust and discriminating	Be wary of "too good"
GPS receivers are networked computers with an additional RF input	Does IT know this device is connected?

Resiliency includes design, implementation and operations

- "AR3" – Resiliency objectives (from DoD):
  - Avoidance: reduce likelihood and consequence
  - Robustness: resist degradation
  - Reconstitution: replenish lost or diminished capability
  - Recovery: re-establish full operational capability
- AR3 (mitigation) applies to individual components, a system, and system of systems

Resiliency requires an active COI addressing changing threats

- Information sharing
- Cooperative R&D
- Testing & evaluation

- Jamming
- Spoofing
- Cyber attacks

- Requirements
- Best practices
- Standards
- Implementation

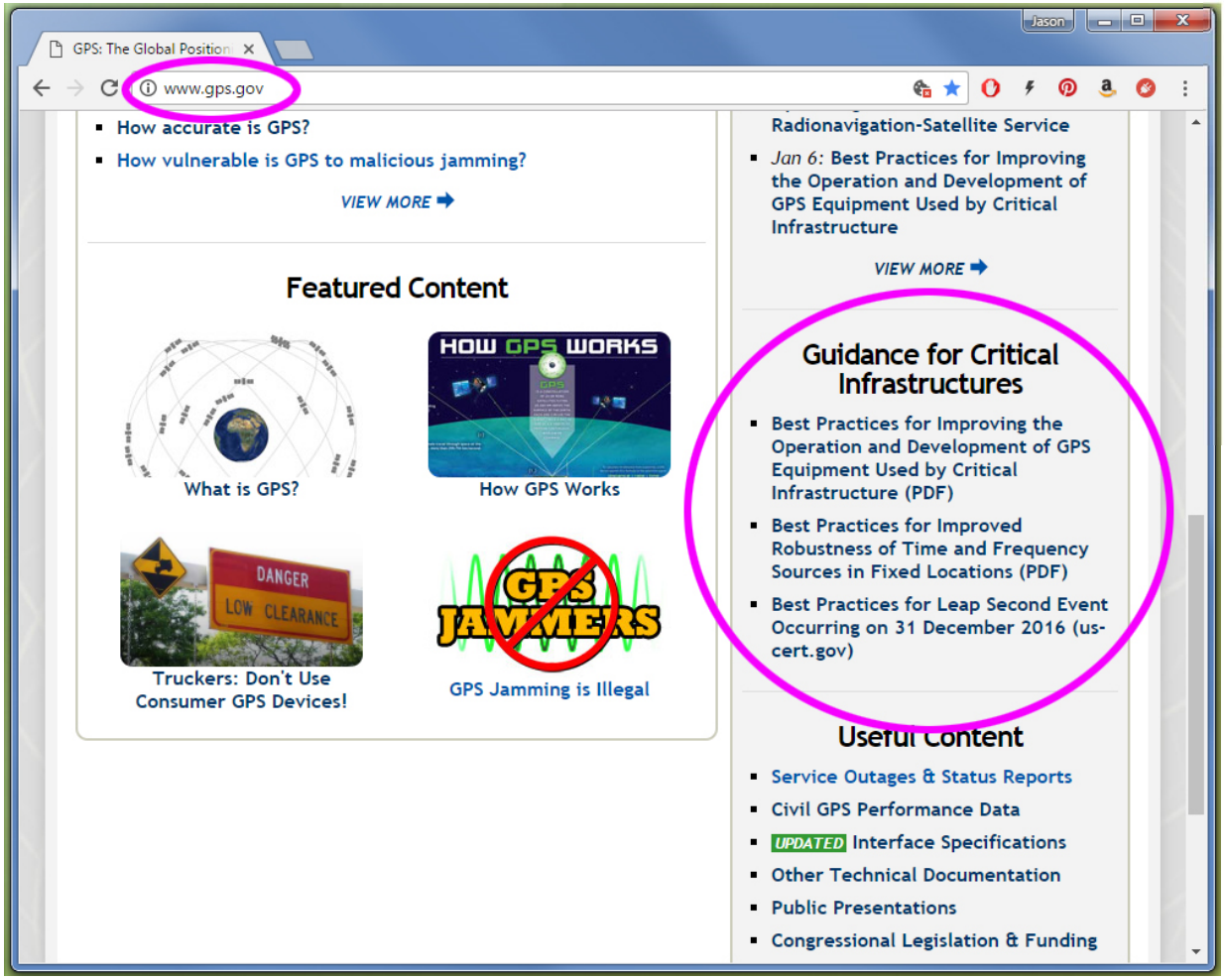
S&T is actively engaging the COI regarding security and resiliency

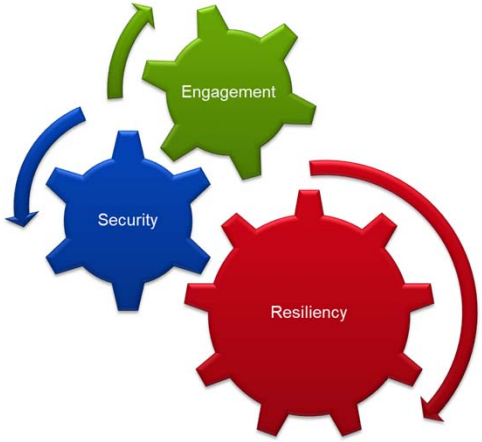
- Information sharing
- Cooperative R&D
- Testing & evaluation

- Jamming
- Spoofing
- Cyber attacks

- Requirements
- Best practices
- Standards
- Implementation

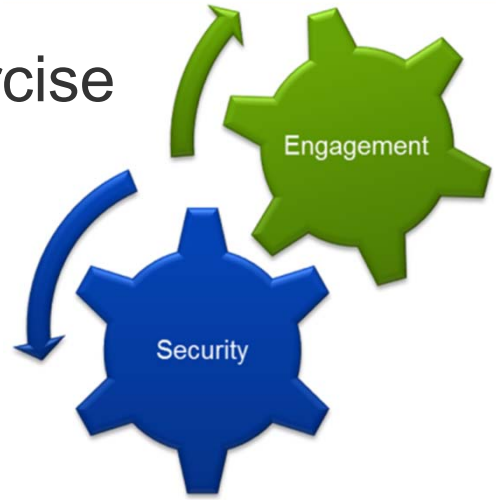
S&T is working with the COI to improve security and resiliency





S&T is hosting multiple "live threat" events for the COI

- First Responder Electronic Jamming Exercise (JamX) 2016 and 2017
  - Focused on end-users / scenarios
  - Publish a series of knowledge products for federal and public safety organizations



- GPS Equipment Testing for Critical Infrastructure (GET-CI) 2017
  - Allow PNT "developers" to experience multiple jamming and spoofing scenarios
  - Evolve event to test emerging threats and solutions

S&T is championing R&D to assess and counter threats

- PNT Broad Agency Announcement – Assured Timing for Critical Infrastructure (HSHQDC-15-R-B0008)
- Awards across three technical topic areas:
  - Development of Assured Timing Technologies
  - System-level Testing and Analysis to Understand Impacts
  - Development of Timing Manipulation Detection Capabilities

S&T and NIST are working towards a Compliance Program

- Collaborate with multiple industry groups
- Use requirements collected by DHS NPPD/IP
- Leverage existing standards and specifications
- Include best practices and testing procedures
- Address both hardware and software device components
- Incorporate oversight by sector stakeholders
- Support both a Supplier's Declaration of Conformity (SDOC) and third-party certification

Homeland Security

Science and Technology