DHS SCIENCE AND TECHNOLOGY

Resilient PNT Conformance Framework

Civil GPS Service Interface Committee

Homeland Security
Science and Technology

September 22, 2020

Ernest Wong

Technical Manager
Technology Centers Division
Science and Technology Directorate

PNT Risks in Civil Critical Infrastructure

- **PNT in Critical Infrastructure**: Accurate position, navigation and timing (PNT) information is important for many critical infrastructure sectors. GPS is primary source of PNT for many.

- **Problem**: PNT disruptions are becoming recognized as a risk to critical infrastructure.
  - Awareness campaign over past few years.
  - Growing trend of high-profile disruptions across the world as reported on by industry trade publications.

- **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.

Resilient PNT Conformance Framework

Vision: Develop common language for defining resilient PNT equipment

- Has multiple levels of resilience to account for different user needs & risk tolerance

Definition of Resilience: The ability to "withstand and recover rapidly from disruptions" (PPD-21)

Enables:

- Product differentiation for vendors
- Improved risk management and decision making by CI operators when acquiring new PNT equipment

Approach:

- Developed in collaboration with industry and federal interagency partners
- Outcome-based and PNT source agnostic to encourage industry innovation

Core Functions with embedded detection functionality.

Acknowledgements: Industry Collaborators

Ernest Wong	U.S. Department of Homeland Security	Dr. Sai Kalyanaraman	Collins Aerospace	Monty Johnson	OPNT
Benjamin Salazar	U.S. Department of Homeland Security	Helmut Imlau	Deutsche Telekom	John Fischer	Orolia
Dr. Arthur Scholz	MITRE	Andrew F. Bach	Financial services technology consultant	David Sohn	Orolia
Dr. Patricia Larkoski	MITRE	Victor Yodaiken	FSMLabs Inc.	Jeff Dagle	Pacific Northwest National Laboratory
Dr. William Young	MITRE	Dr. Steve Guendert	IBM Corporation	Lori Ross O'Neil	Pacific Northwest National Laboratory
Dr. Bradley Moran	MITRE	Leigh Whitcomb	Imagine Communications	Dan Rippon	Schweitzer Engineering Laboratories
Brian Callahan	MITRE	Lee Cosart	Microchip	Francisco Girela Lopez	Seven Solutions
Lannie Herlihy	Federal Aviation Administration	Rich Foster	Microchip	Marc Weiss	Spirent Consultant
Dr. Paul E. Black	National Institute of Standards and Technology	Greg Wolff	Microchip	Dr. Michael O'Connor	Satelles
Ya-Shian Li-Baboud	National Institute of Standards and Technology	Magnus Danielson	Net Insight AB	Christina Riley	Satelles
David Howard	U.S. Department of Energy	Dr. Deepak Maragal	New York Power Authority	Mitch Narins	Strategic Synergies, LLC.
Dr. Hadi Wassaf	U.S. Department of Transportation Volpe Center	Dr. Cristina Seibert	NextNav	Haroon Muhammad	Trimble
		Dr. Stefania Römisch	Northrop Grumman Mission Systems	Jeffery Sanders	UHU Technologies
		Charles Swain	Johns Hopkins University – Applied Physics Lab	Dr. Steven W. Lewis	

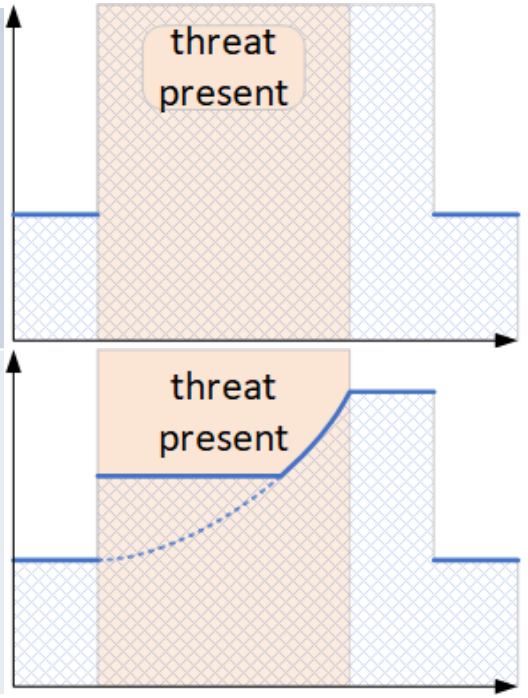
And many others (80+ participants)

Framework Levels 1-2

- Near-term resilience towards most impactful legacy issues.
- Also results in raising difficulty in vulnerability exploitation chains.

Increasing levels align with increasing resilience and expected time-to-market.

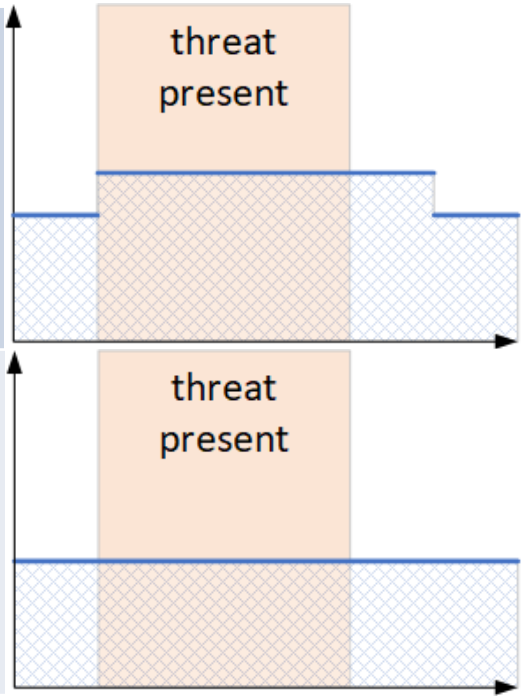
	Minimum Requirements (Cumulative)
Level 1	**Ensures recoverability after removal of the threat.** 1. Must verify that stored data from external inputs adheres to values and formats of established standards. 2. Must support full system recovery by manual means, making all memory clearable or resettable, enabling return to a proper working state, and returning the system to the defined performance after removal of the threat. 3. Must include the ability to securely reload or update firmware.
Level 2	**Provides a solution (possibly with unbounded degradation) during threat.** **Includes capabilities enumerated in Level 1 plus:** 4. Must identify compromised PNT sources and prevent them from contributing to erroneous PNT solutions. 5. Must support automatic recovery of individual PNT sources and system.



Framework Levels 3-4

- Push towards NextGen PNT in mid to long-term.
- May require substantial architectural updates.

	Minimum Requirements (Cumulative)
Level 3	**Provides a solution (with bounded degradation) during threat.** **Includes capabilities enumerated in Levels 1 and 2 plus:** 6. Must ensure that corrupted data from one PNT source cannot corrupt data from another PNT source. 7. Must cross-verify between PNT solutions from all PNT sources.
Level 4	**Provides a solution without degradation during threat.** **Includes capabilities enumerated in Levels 1, 2 and 3 plus:** 8. Must have diversity of PNT source technology to mitigate common mode threats.



Potential Transition Pathways

Document Public Release:
- Targeting Dec2020

Conformance Framework

Industry

- **Standards Development Organizations**
  - Use framework as common guidance for developing voluntary standards across sector SDOs.
- **PNT Equipment Manufacturers**
  - Begin developing to framework concepts and articulate products based on framework levels.
- **Critical Infrastructure End-Users**
  - Incorporate framework behaviors into acquisition requirements.

Federal

- **GSA Schedule**
- **PNT EO Federal Acquisition Requirements**

Homeland Security

Science and Technology

DIVERSE PERSPECTIVES + SHARED GOALS = POWERFUL SOLUTIONS