Resilient PNT for the Civilian Sector

The research in this presentation was conducted under contract with the U.S Department of Homeland Security (DHS) Science and Technology Directorate (S&T), under task order 70RSAT19FR0000040. The opinions contained herein are those of the contractors and do not necessarily reflect those of DHS S&T.

FFRDC POWERED BY S&T™

HSSEDI POC:
Arthur Scholz
ascholz@mitre.org

Approved for public release; Distribution unlimited.
Case Number 19-0934 / DHS Reference Number 17-J-00100-05 9/16/19
Approved via email by Pamela Demory HSSEDI PMO

HSSEDI
Homeland Security Systems Engineering & Development Institute™

Introduction

- **GPS is the world's clock**
- **Civilian users require a resilient source of positioning, navigation, and timing information**

"… ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks or compromises on system resources …"

NIST SP 800-160

Approved for public release; Distribution unlimited.
Case Number 19-0934 / DHS Reference Number 17-J-00100-05 9/16/19

HSSEDI
Homeland Security Systems Engineering & Development Institute™

Resilient PNT Conformance Framework Vision

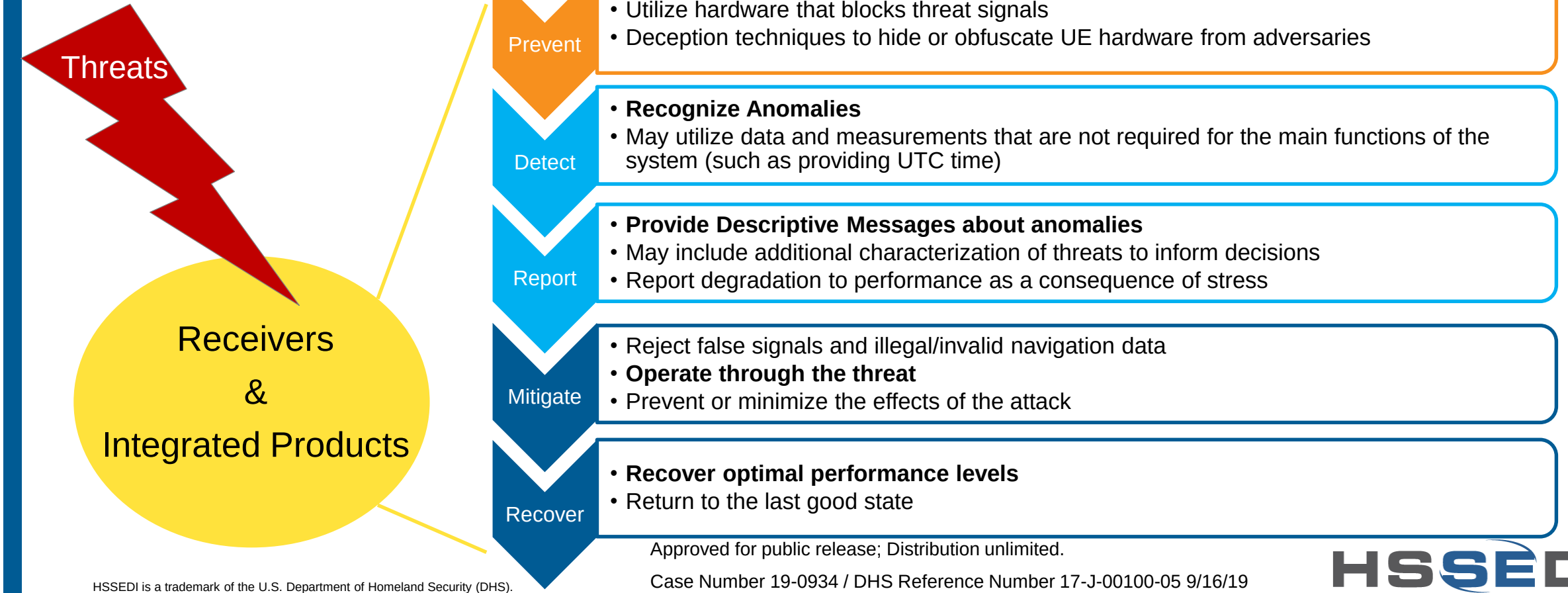
- **Operators and vendors recognize there are threats to PNT**
- **Resilient PNT products are available but it's difficult for operators to know what to purchase**
- **Conformance framework will provide a common language for describing threats and mitigations**
- **Different levels of resilience to suit industry-specific needs**
- **Levels of resilience will enable product differentiation and risk management**

Approved for public release; Distribution unlimited.
Case Number 19-0934 / DHS Reference Number 17-J-00100-05 9/16/19

HSSEDI
Homeland Security Systems Engineering & Development Institute™

Resilient Framework Functions

- **Framework of Resilient Behavior: Prevent, Detect, Report, Mitigate, Recover**
- **Each of these functions can be basic to sophisticated within a system of UE.**



Approved for public release; Distribution unlimited.
Case Number 19-0934 / DHS Reference Number 17-J-00100-05 9/16/19

HSSEDI
Homeland Security Systems Engineering & Development Institute™

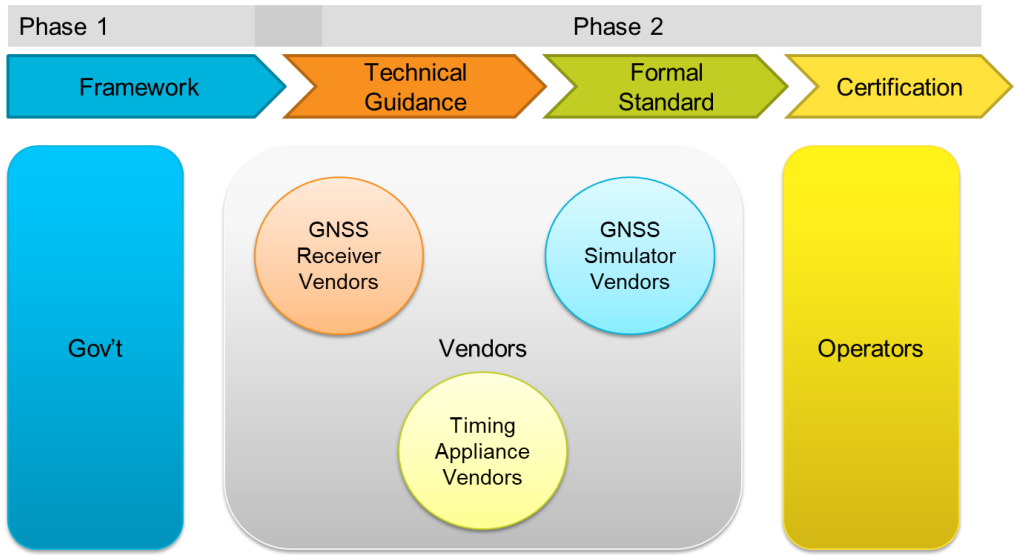
Resilient PNT Conformance Framework Working Group

Introduction:

The Resilient PNT Conformance Framework Working Group (CFWG) is established by the Department of Homeland Security to ensure resilient GNSS-derived timing sources for critical infrastructure.

Objectives:

- *Develop an integrated conformance framework for describing resilient PNT systems*
- *Create meaningful, actionable, and verifiable guidelines for ensuring resilient PNT with a focusing on GNSS dependent timing devices*
- *Transition to industry application and industry-supported body for adoption and sustainment*
- *Enable improved risk management and decision making by CI operators when acquiring PNT equipment*
- *Enable vendors to differentiate products*



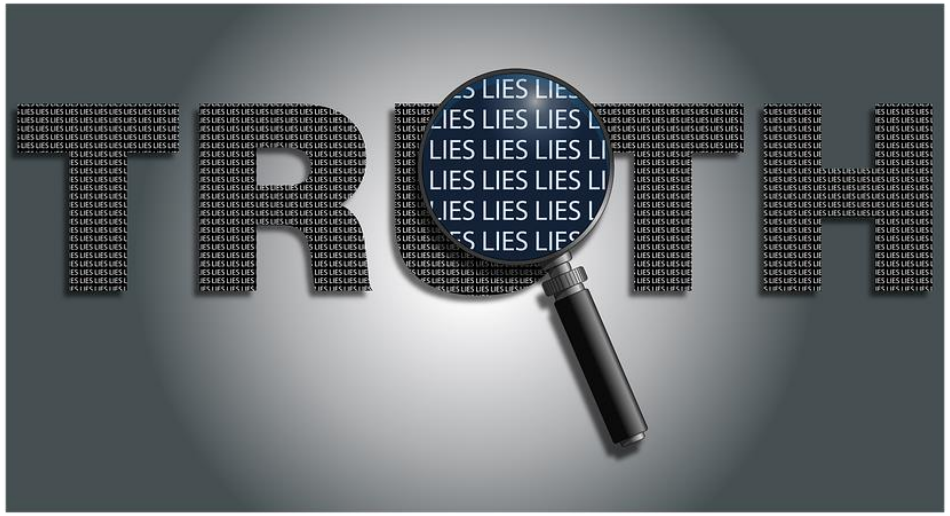
GNSS – Global Navigation Satellite System

Approved for public release; Distribution unlimited.
Case Number 19-0934 / DHS Reference Number 17-J-00100-05 9/16/19

HSSEDI
Homeland Security Systems Engineering & Development Institute™

Types of Threats

- **Availability**
  - Interference which degrades or denies reception of GNSS signals
- **Integrity**
  - Interference which introduces erroneous data and measurements
- **Incidental**
  - Unintentional interference with a receiver's operation
- **Targeted**
  - Intentional interference with a receiver’s operation



Threat Class Descriptions

RF Attacks

Cyber Attacks

- **Interference or jamming**
  - RF waveforms that disrupt receiver processing
  - Effect: Deny or degrade the receiver's ability to process desired signals
- **Measurement spoofing**
  - False GNSS RF waveforms intended to gain access to receiver processing
  - Effect: Deny, degrade, deceive (e.g. incorrect PVT solution to data processing)
- **Data spoofing**
  - Incorrect data messages to disrupt the processing of signals and PVT calculation
  - Effect: Deny, degrade, deceive
- **Timing Equipment and Network attacks**
  - Embedded System Attacks via external interfaces
  - Supply chain vulnerabilities, Malware, Tamper

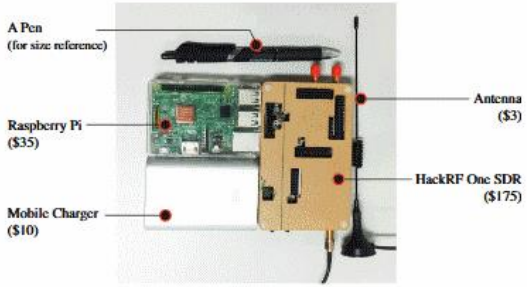
Attacks can involve a combination of jamming, spoofing, and cyber

PVT – Position, Velocity, Time

Approved for public release; Distribution unlimited.
Case Number 19-0934 / DHS Reference Number 17-J-00100-05 9/16/19

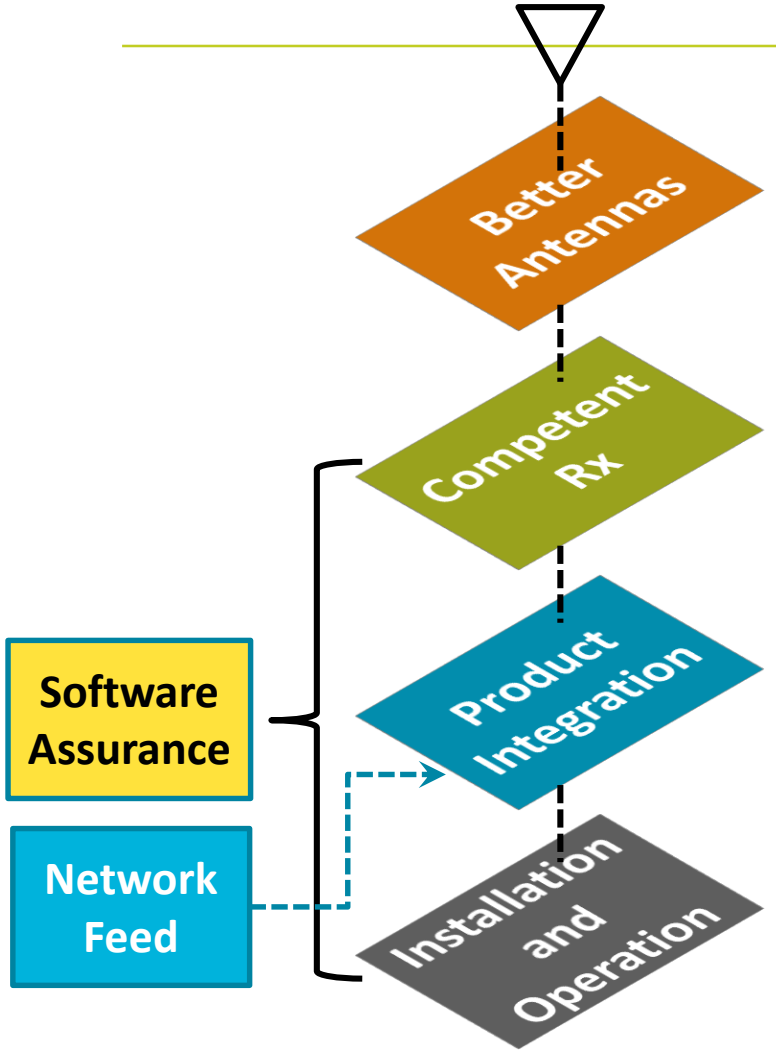
HSSEDI
Homeland Security Systems Engineering & Development Institute™

Threat Classification

	Denial	Deception
Incidental		hannover airport
Targeted		

HSSEDI
Homeland Security Systems Engineering & Development Institute™

GPS Timing Defense-in-Depth Strategy



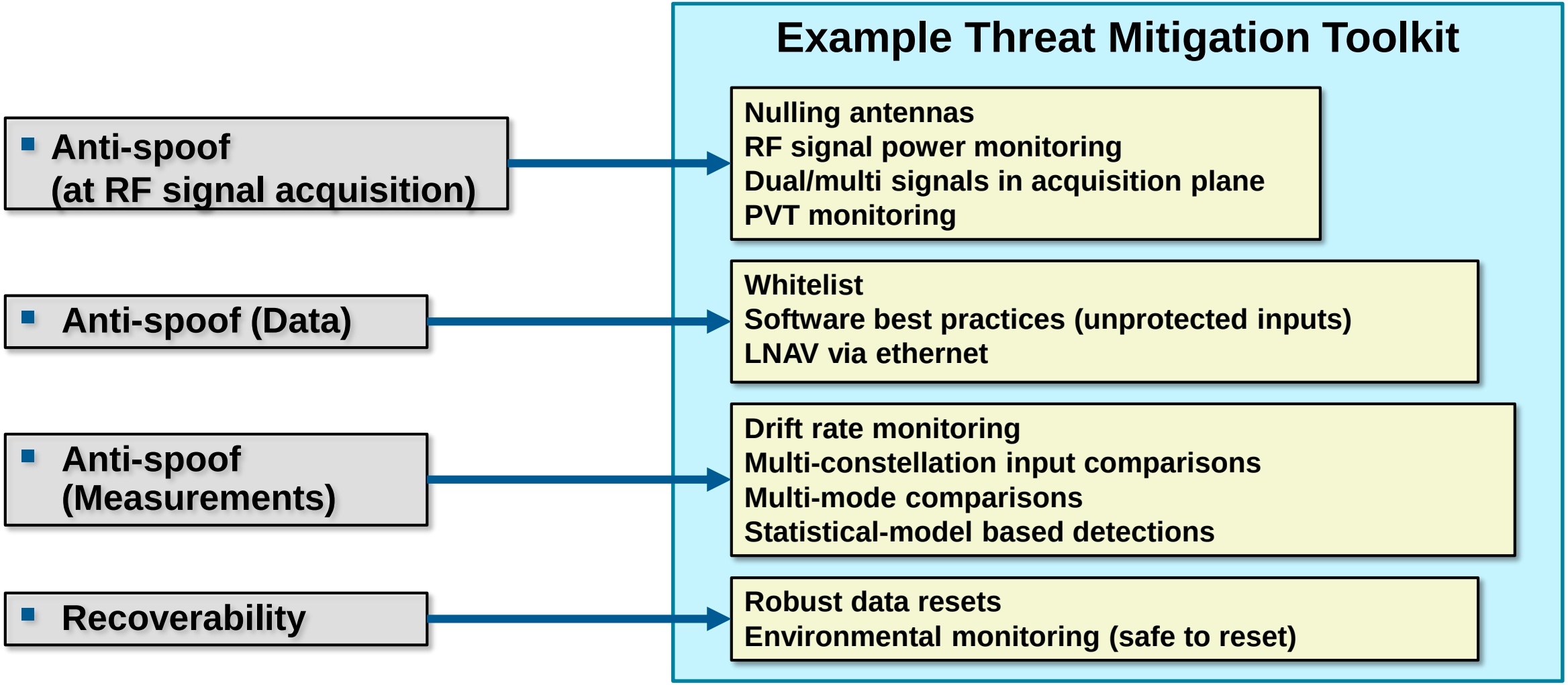
- Anti-Jam (AJ) Antennas
- Anti-Measurement Spoofing (AS)
- Anti-Data Spoofing
- Improved Oscillators/Holdover
- Data Message (Cyber) Security
- Timescale (fusion of sources)
- Assess GPS Dependencies
- Configuration

Detection and mitigation techniques apply to all system layers, design, development, and user practices.

Approved for public release; Distribution unlimited.
Case Number 19-0934 / DHS Reference Number 17-J-00100-05 9/16/19

HSSEDI
Homeland Security Systems Engineering & Development Institute™

Toolkit for Mitigation of Timing Threats



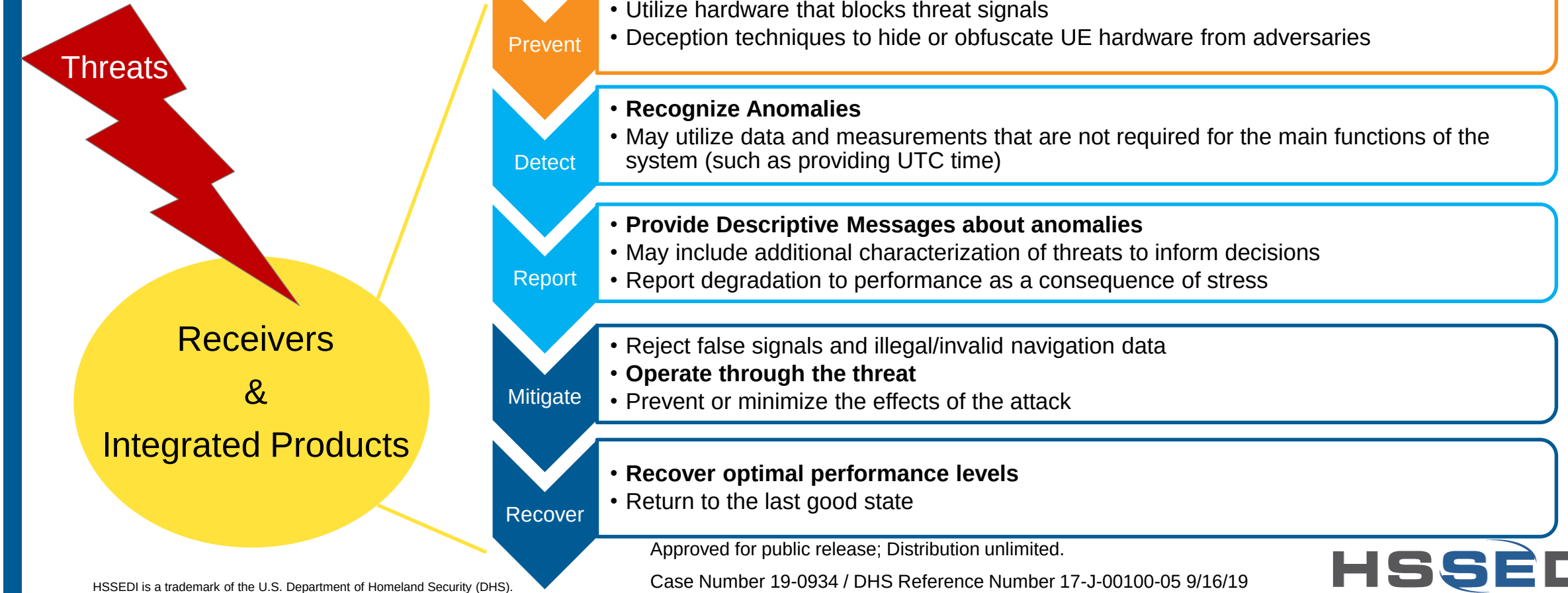
LNAV – IS-GPS-200 Legacy Navigation Message

Approved for public release; Distribution unlimited.
Case Number 19-0934 / DHS Reference Number 17-J-00100-05 9/16/19

HSSEDI
Homeland Security Systems Engineering & Development Institute™

Resilient Framework Functions

- **Framework of Resilient Behavior: Prevent, Detect, Report, Mitigate, Recover**
- **Each of these functions can be basic to sophisticated within a system of UE.**



Approved for public release; Distribution unlimited.
Case Number 19-0934 / DHS Reference Number 17-J-00100-05 9/16/19

HSSEDI
Homeland Security Systems Engineering & Development Institute™

Conclusion

- The *Resilient PNT Conformance Framework* will provide a threat/response classification system
- Included mitigation toolkit and resilient behavior functions will provide guidance for effective responses to threats

Goal: provide uninterrupted, reliable time to users, even in the presence of advanced threats.

References:
https://www.gps.gov/multimedia/presentations/2017/12/CIPRNA/skey.pdf
https://www.navcen.uscg.gov/pdf/gps/Best%20Practices%20for%20Improving%20the%20Operation%20and%20Development%20of%20GPS%20Equipment.pdf