DHS SCIENCE AND TECHNOLOGY

# Incorporating Resilience into IDM

United Nations International Committee on GNSS – 9th Interference Detection and Mitigation Workshop

**August 24, 2021**

**Ernest Wong**

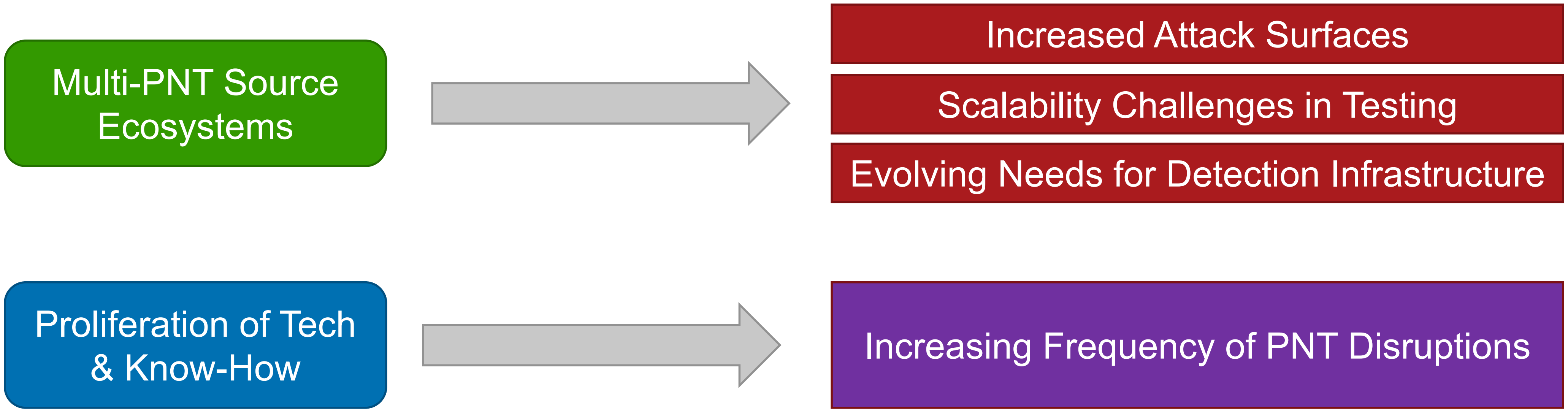
Technical Manager
Technology Centers Division
Science and Technology Directorate

Homeland Security
Science and Technology

# Agenda

- New Trends, New Challenges, and the New Paradigm
- New and Updated Policies:
  - PNT Executive Order
  - Space Policy Directive 7
- System Resilience
- Operational Resilience

# New Trends, New Challenges



Trends

Challenges

Multi-PNT Source Ecosystems

- Increased Attack Surfaces
- Scalability Challenges in Testing
- Evolving Needs for Detection Infrastructure

Proliferation of Tech & Know-How

- Increasing Frequency of PNT Disruptions

**Emerging Paradigm**: Operations will need to expect interference and an increasingly complex threat environment

# Responding to the Emerging Paradigm

- Goals:
  - Ability to withstand, operate through, and recover from disruption events
  - Proactive threat agnostic model to evolving multi-PNT ecosystem

- Requires:
  - Resilient system architectures
  - Operational resilience
  - Growing importance of on-device IDM capabilities to enable resilient response

# New Policy: PNT Executive Order

- Executive Order 13905: “Strengthening National Resilience Through Responsible Use of Positioning, Navigation, and Timing Services”

> **Sec. 3**. *Policy.* It is the policy of the United States to ensure that disruption or manipulation of PNT services does not undermine the reliable and efficient functioning of its critical infrastructure. The Federal Government must increase the Nation's awareness of the extent to which critical infrastructure depends on, or is enhanced by, PNT services, and it must ensure critical infrastructure can withstand disruption or manipulation of PNT services. To this end, the Federal Government shall engage the public and private sectors to identify and promote the responsible use of PNT services.

- PPD-21 definition of resilience: “the ability to… withstand and recover rapidly from disruptions.”

- Policy reinforces need for both system resilience and operational resilience to PNT disruptions and interference

# Updated Policy: Space Policy Directive 7

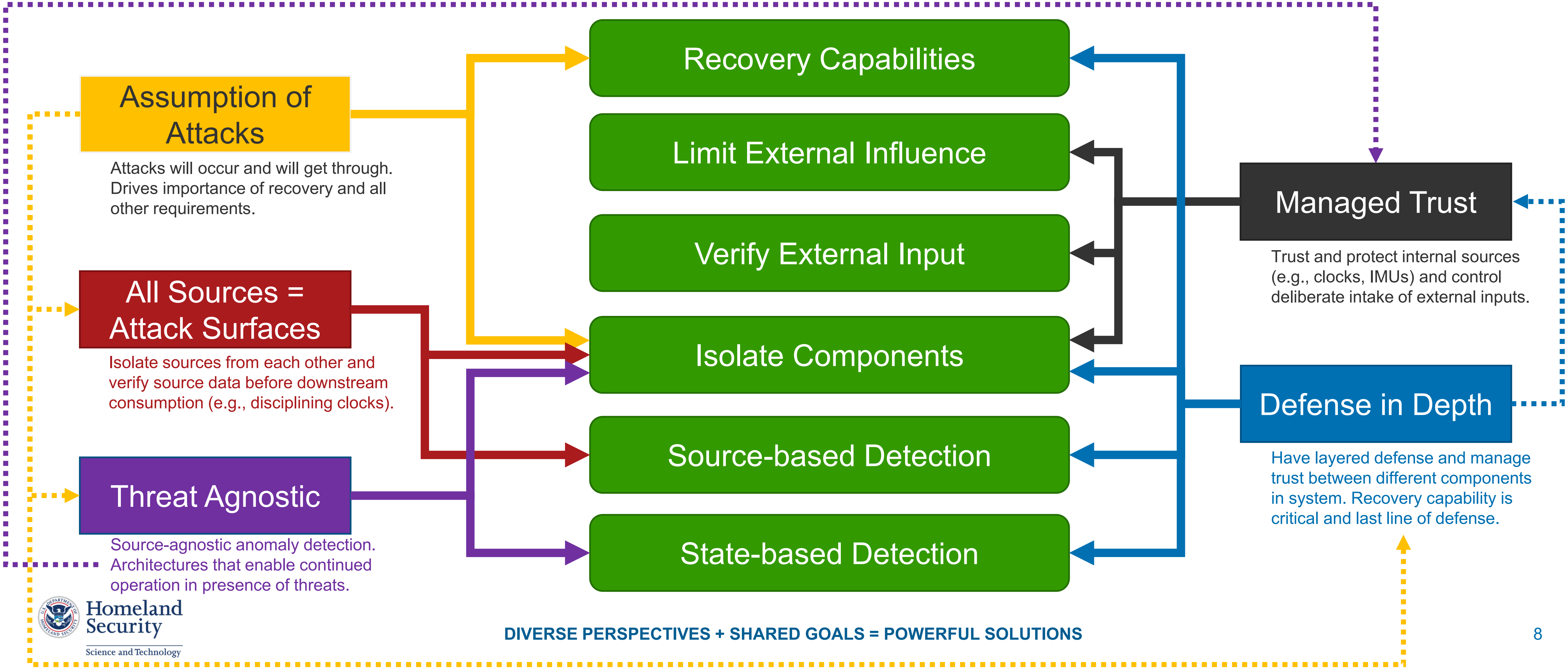
- SPD-7 reinforces the trend of multi-PNT ecosystems, the importance of resilience in IDM, and the need for cybersecurity:
  - "The United States is also encouraging the development of alternative approaches to PNT services and security that can incorporate new technologies and services as they are developed, such as quantum sensing, relative navigation and private or publicly owned and operated alternative PNT services."
  - "(e) Improve the cybersecurity of GPS, its augmentations, and United States Government owned GPS-enabled devices, and foster private sector adoption of cyber-secure GPS enabled systems"
  - "(g) Invest in domestic capabilities and support international activities to detect, mitigate, and increase resilience to harmful disruption or manipulation of GPS, and identify and implement, as appropriate, alternative sources of PNT for critical infrastructure, key resources, and mission-essential functions"

# Resilient PNT System Architectures

- DHS's Holistic Cybersecurity-based Approach to Resilient PNT Architectures
  - Focuses on addressing the emerging paradigm
  - Aligns with themes from PNT EO and SPD-7

- Assumptions and Requirements:
  - Systems will be attacked
  - Every PNT source is an attack surface
  - Proactive and agnostic approach to threats
  - Cybersecurity approach of not assuming trust
  - Defense in Depth

# Holistic Approach to Resilient Architectures



Assumption of Attacks

Attacks will occur and will get through. Drives importance of recovery and all other requirements.

All Sources = Attack Surfaces

Isolate sources from each other and verify source data before downstream consumption (e.g., disciplining clocks).

Threat Agnostic

Source-agnostic anomaly detection. Architectures that enable continued operation in presence of threats.

Recovery Capabilities

Limit External Influence

Verify External Input

Isolate Components

Source-based Detection

State-based Detection

Managed Trust

Trust and protect internal sources (e.g., clocks, IMUs) and control deliberate intake of external inputs.

Defense in Depth

Have layered defense and manage trust between different components in system. Recovery capability is critical and last line of defense.

# Operational Resilience

- Driven by PNT EO

- Operator capabilities for resilience:
  - Able to detect interference
  - Have response plans to PNT interference (and exercised them)
  - Understand PNT vulnerabilities and dependencies within their systems
  - Design downstream operational system-of-systems to minimize PNT dependences

- NIST Foundational PNT Profile:
  - Applying the Cybersecurity Framework for the Responsible Use of PNT Services
  - Full Document + Supplemental Quick Guide
    - https://csrc.nist.gov/publications/detail/nistir/8323/final

# Key Takeaways

- **Emerging Paradigm**: Multi-PNT Ecosystems & Increasing Frequency of Interference
  - Traditional approach of detecting and locating interference will not be sufficient
  - Need to be resilient and able to live with and operate through disruptions

- **Two Aspects to Achieving Resilience**:
  - System Resilience (Hardware Aspect)
    - PNT systems designed with resilient system architectures
    - PNT systems incorporate cybersecurity principles for holistic approach to threats
  - Operational Resilience (End-User Aspect)
    - Operators plan for and know how to respond to PNT disruptions
    - Operators understand and minimize PNT dependencies in downstream systems
    - Operators able to withstand, operate through, and recover from PNT disruptions

Homeland Security

Science and Technology

DIVERSE PERSPECTIVES + SHARED GOALS = POWERFUL SOLUTIONS