# The Office of Infrastructure Protection

National Protection and Programs Directorate
Department of Homeland Security

National Risk Estimate: Risks to United States Critical Infrastructure from Global Positioning System Disruptions

Wednesday, 9 November 2011

Homeland Security

# Agenda

- National Risk Estimate (NRE)
  - Overview
  - Highlights
  - Current Status and Next Steps
- Lessons Learned

# National Risk Estimate Overview

- The Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) developed the NRE product line in 2010 to provide authoritative, coordinated, risk-informed assessments of key national security issues in the Nation's infrastructure protection community
- First NRE was on *Trends in Global Supply Chain Risk and Implications for U.S. Critical Infrastructure*
- The NRE, *Risks to U.S. Critical Infrastructure from Global Positioning System Disruptions*, analyzes short- and long-term risks to critical infrastructure sectors
- HITRAC coordinated the NRE with Department of Homeland Security (DHS) components and Federal partners in addition to gaining input from national labs and private sector consultants

# National Risk Estimate Overview (cont.)

- The NRE development process consisted of three phases: estimate, outlook, and integration
  - The estimate phase included a literature review, developing a Terms of Reference and Global Positioning System (GPS) disruption scenarios, and workshops to assess consequence and likelihood
  - In the outlook phase, HITRAC conducted alternative futures workshops for each sector
  - The integration phase concluded the drafting of the NRE chapters and demanded an interagency effort to review the NRE for soundness, consistency, and accuracy

# National Risk Estimate Overview (cont.)

- The critical infrastructure sectors highlighted in the NRE are:
  - Communications
  - Emergency Services
  - Energy
  - Transportation Systems

# Highlights

- Bottom Line: U.S. critical infrastructure sectors are increasingly at risk from a growing dependency on GPS for positioning, navigation, and timing (PNT) services; such dependencies are not always apparent
- Key Judgments:
  - GPS is increasingly integrated into sectors' operations because it is accurate, available, reliable, and provided at no cost to users
  - Awareness that GPS-supported applications are integrated in sector operations is somewhat limited, prompting the idea that GPS is a largely invisible utility
  - Interdependencies exist between critical infrastructure sectors that use GPS

# Highlights (cont.)

- The NRE identifies high-risk GPS disruption scenarios, determined by the scenarios' likelihood and associated consequences
  - The NRE considers three types of GPS disruptions: *naturally occurring*, such as space weather events; *unintentional*, such as radio frequency signals interfering with GPS signals; and *intentional*, such as purposeful jamming or spoofing
  - Jamming disruptions were judged to be more likely than spoofing incidents
  - The likelihood of disruptions was difficult to estimate accurately given limited available intelligence or information on prior disruptions
  - Economic losses and lowered consumer confidence are possible consequences to sectors from extensive GPS disruptions. Possibly safety-of-life
  - Spoofing typically judged to be of higher consequence than jamming due to the potential duration of time before users or devices would detect spoofing

# Highlights (cont.)

- Mitigating GPS Disruptions
  - Detecting, locating, and disabling sources of GPS disruption remain a challenge
  - While manual PNT techniques could be used in some sectors if GPS is disrupted, this will come at a loss in efficiency
    - Human skills for using manual techniques could erode due to lack of training and practice as GPS becomes more ubiquitous

# Highlights (cont.)

- Key uncertainties that could shape future risk of GPS disruption for critical infrastructure include:
  - The extent to which GPS-based applications are layered into sector operations
  - The vulnerability of GPS to intentional or unintentional disruptions
  - The extent to which GPS disruptions can be identified and mitigated
  - The accuracy, availability, integrity, and continuity of alternative PNT systems available to provide robustness

# Current Status and Next Steps

- Completed the coordinated NRE draft on 30 September 2011
- Provided draft for review to:
  - Assistant Secretary for Office of Infrastructure Protection
  - PNT Executive Steering Group
- Currently seeking draft concurrence and endorsement from:
  - DHS Senior Leadership
  - PNT National Executive Committee

Homeland Security

# Lessons Learned

- Mitigation Assessment
- Negating the threat of GPS disruptions
- Making GPS receivers less susceptible to jamming/spoofing


Homeland Security

For more information visit:
www.dhs.gov/criticalinfrastructure

Brandon D. Wales
HITRAC, Director
202-447-3130 | brandon.wales@dhs.gov