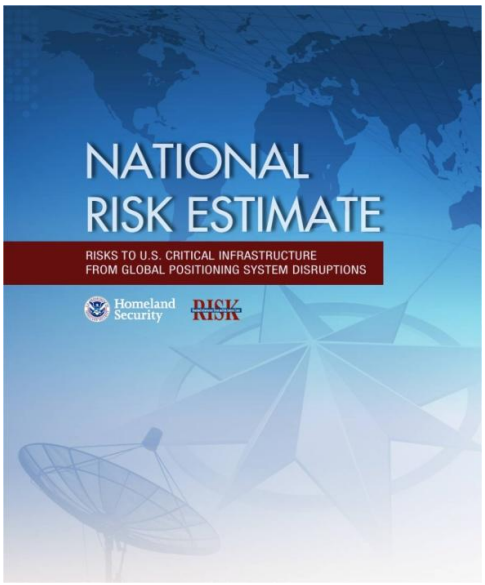
National Risk Estimate: Risks to U.S. Critical Infrastructure from Global Positioning System Disruptions

Background



In November 2010, the National Executive Committee for Space-Based Positioning, Navigation, and Timing (a Deputy Secretary-level interagency group) asked DHS to complete a comprehensive risk assessment of the civil Global Positioning System (GPS) signal. The National Protection and Programs Directorate, Office of Infrastructure Protection, Homeland Infrastructure Threat and Risk Analysis Center (NPPD/IP/HITRAC) led the effort and coordinated the development of the NRE with the interagency. The NRE is a For Official Use Only document and was released in November 2012 to certain individuals who hold the proper clearance and access approval for the information.

Overview

- The NRE is a result of extensive coordination with GPS stakeholders that included DHS components, Federal partners, the Intelligence Community, national labs, and private sector subject matter experts.
- The overall assessment is that GPS disruptions pose current and potential future risks to critical infrastructure sectors.
- The NRE examines four critical infrastructure sectors (Communications, Emergency Services, Energy, and Transportation Systems) that derive PNT information from GPS to fulfill their missions.
- The NRE concludes that U.S. critical infrastructure sectors are increasingly at risk from a growing dependency on GPS for PNT services.
- GPS is increasingly integrated into sectors' operations because it is accurate, available, and reliable at no cost to users. In addition, many critical infrastructure sectors do not realize that they rely on GPS because its application is seamless in their operations.
- The NRE considers the likelihood and consequences of certain GPS disruption scenarios—among naturally occurring, unintentional, and intentional types of disruptions—to determine which scenarios pose high risks to the four sectors.
- The NRE includes a classified annex that the DHS Office of Intelligence and Analysis produced to assess availability of GPS jammers and threat actors' capability and intent to disrupt GPS signals generally and for the four sectors.
- The NRE does not substantially address individual sources of possible interference. Rather, the NRE includes some historical case studies as summary examples.
- The NRE identifies detecting, locating, and disabling sources of GPS disruption as a challenge and finds that key uncertainties—including the extent to which GPS-based applications are layered into sector operations—will shape future risks to critical infrastructure.

Contact Information

For more information about infrastructure analysis and strategy programs, go to www.dhs.gov/infrastructure-analysis-and-strategy or send email to risk@hq.dhs.gov.