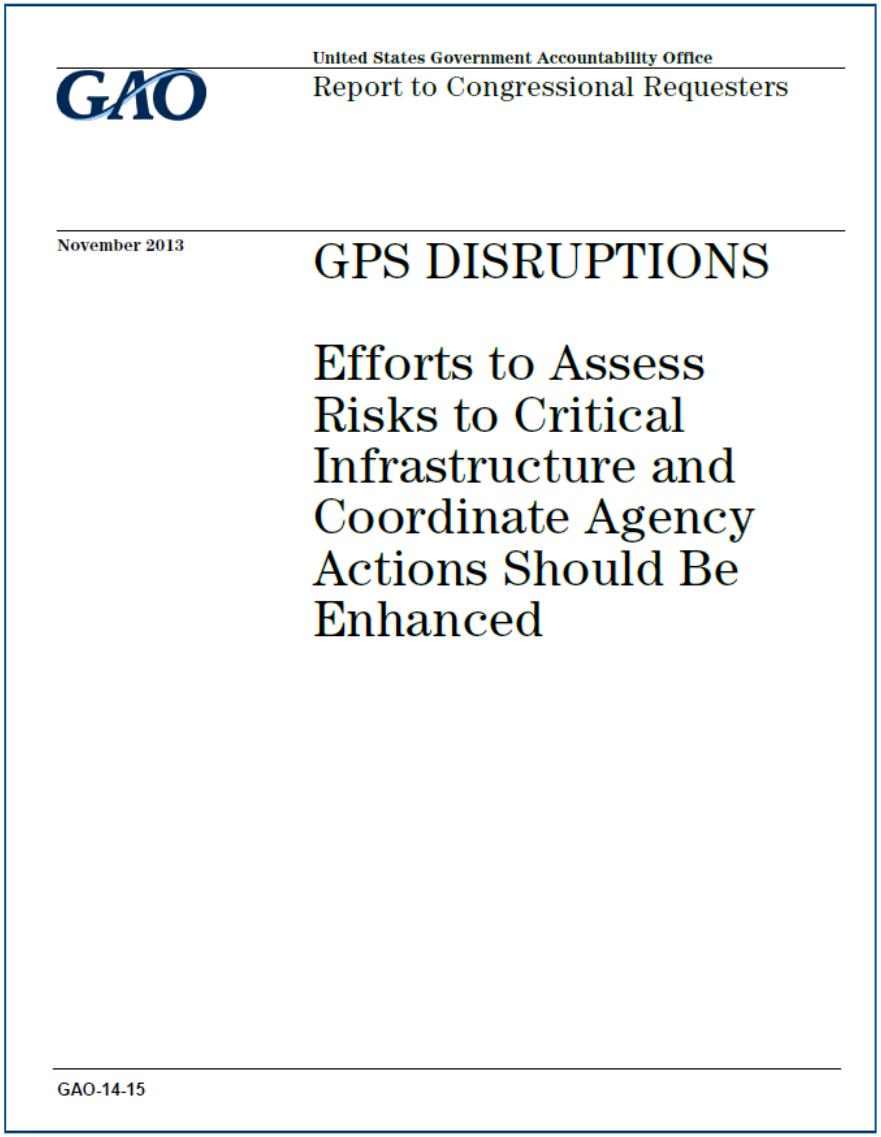


http://www.gao.gov/assets/660/658792.pdf

Overview

- Report background and objectives
- Review of DHS' GPS risk assessment
- Review of DOT and DHS mitigation efforts
- Review of sectors' mitigation strategies / DHS measurement efforts

Conclusions:

DHS risk assessment did not fully assess GPS risks

DOT /DHS initiated mitigation efforts, but made limited progress

DHS needs to measure CI sectors' mitigation efforts

- GAO recommendations

Background of GAO Report

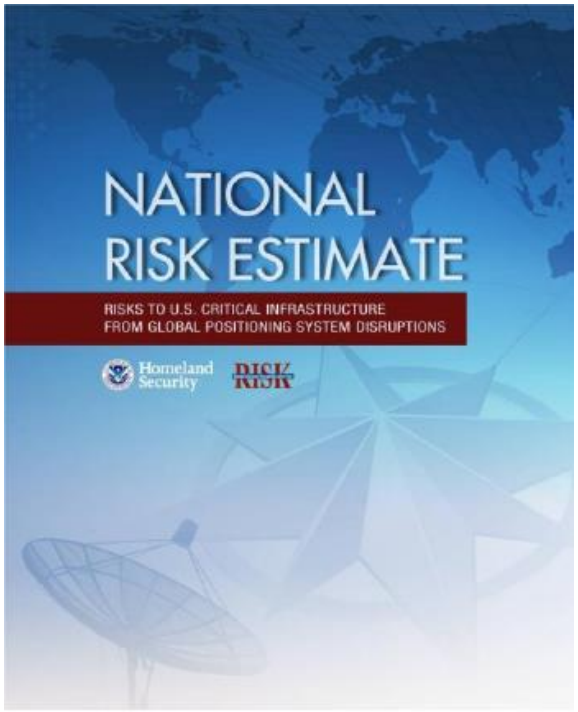
- GAO GPS assessment requested by members in both chambers
- GPS (PNT) functionality used in most of the 16 Critical Infrastructure (CI) sectors
  - Requesters specifically concerned over GPS vulnerabilities in four sectors:
    - energy, transportation, communications and financial services sectors
- GAO examined the following:
  - The extent to which DHS has assessed the risks and potential effects of GPS disruptions on CI sectors
  - The extent to which DOT and DHS have developed backup strategies to mitigate GPS disruptions
  - What strategies, if any, selected CI sectors employ to mitigate GPS disruptions and any remaining challenges
- GAO audit spanned 11/12-11/13

Background: DHS and DOT GPS Roles and Responsibilities

- Per presidential directive (NSPD-39, 2004), DHS and DOT play leading roles in supporting backup capabilities to GPS in the event of a GPS disruption:
  - DOT, in coordination with DHS, is required to develop, acquire, operate, and maintain backup capabilities that can support critical civilian and commercial infrastructure in the event of a GPS disruption.
  - DHS is assigned lead responsibility to identify, locate, and attribute interference within the U.S. that adversely affects GPS use, and develop a database for reports of GPS interference.

- NSPD-39 also established a National Executive Committee for Space-Based PNT (EXCOM) to coordinate GPS-related matters across federal agencies
  - EXCOM issued a 5-year plan for space-based PNT that recommends that DHS institute a risk management approach to assess threats, vulnerabilities, and potential consequences to interference to GPS signals and examine the best opportunities to mitigate those risks

DHS Risk Assessment



- DHS faced with a difficult task in conducting the NRE - Risk assessment was challenging:
  - Involved complex analysis, across multiple sectors, and with many unknowns and little data

DHS' GPS National Risk Estimate (NRE)

- Requested by EXCOM/NCO, NRE was issued in September 2011 (final report 2012); a separate mitigation study was issued September 2011
  - NRE was a scenario-based risk assessment for CI, using subject matter experts from inside and outside government
  - NRE considered three types of GPS disruption scenarios:
    - naturally occurring disruptions, such as space weather events
    - unintentional disruptions, such as radio frequency signals interfering with GPS signals, and
    - intentional disruptions, such as jamming or spoofing

GAO Sources for Assessing NRE

- GAO evaluated DHS's 2012 GPS' NRE against established federal risk assessment criteria for CI protection.
  - **National Security Presidential Directive 39** (NSPD-39, 2004) assigns governance roles to numerous Federal agencies
  - **National Infrastructure Protection Plan** (NIPP, 2006, 2009, 2013?)
    - Provides a risk management framework. The NIPP specifies core criteria for risk assessments. (The NIPP specifically identifies GPS as a system that supports or enables critical functions in CI sectors.)
  - **Homeland Security Presidential Directive 7** (HSPD-7)
    - DHS was directed to coordinate protection activities for each CI sector through designated Sector-Specific Agencies (SSA).
  - **Presidential Policy Directive 21** (PPD-21, 2013)
    - PPD-21 supersedes HSPD-7 and states that CI must be secure and able to withstand and rapidly recover from all hazards (focuses on physical security).
  - **Executive Order 13636** (2013) to improve CI cyber security
    - To implement 13636, DHS formed an Integrated Task Force to ensure effective integration/synchronization of PPD-21 and EO 13636

GAO: NRE Did Not Fully Follow Risk Assessment Guidance or Fully Assess GPS Risks

- GAO compared NRE risk assessment against NIPP risk assessment criteria:
  - complete, reproducible, defensible, and documented, so results can contribute to cross-sector risk comparisons that support investment, planning, and prioritization decisions
- NRE did not fully follow risk assessment guidance or fully assess GPS risks
  - Complete? - the NRE does not use its threat assessment to inform its threat-likelihood rankings, nor considers all relevant threats (e.g., spectrum encroachment) or key sectors (e.g., banking and finance)
  - Reproducible, defensible? – NRE was based on panels of Subject Matter Experts - Questionable whether the panels had sufficiently broad expertise to capture the full scope of GPS vulnerabilities within sectors
- NRE had not been widely used
  - Additionally, DHS' concurrent and separate mitigation report did not use the NRE's risk assessment results
  - However, DHS has made recent efforts to publicize NRE and increase awareness of GPS risks

Because of the shortcomings we found in the NRE, we do not believe that DHS has instituted an adequate risk management approach to address the risks associated with GPS interference

DOT AND DHS MITIGATION EFFORTS

Mitigation Efforts Initiated …

- Agencies developed plans and strategies:
  - Issued The National PNT Architecture report in 2008
  - Released The National PNT Architecture Implementation Plan in 2010
  - DHS developed plans and strategies for GPS interference detection and mitigation (IDM)
- DHS conducted studies:
  - 2009 federal agency survey to understand their GPS capabilities, requirements, and backup systems.
  - 2011 mitigation study (concurrent with the NRE).
- Ongoing alternative PNT studies (non-space based):
  - DOT, via the FAA - is conducting feasibility studies on three potential systems that can be used as GPS backup for NextGen
  - The Coast Guard - researching possibilities for non-space based nationwide timing backup
  - NIST - researching the use of fiber networks as an alternative, non-space-based source of precise time
  - DHS in July 2013, commissioned a study to assess potential sector-specific and cross-sector threat mitigation technologies

… But Limited Progress Has Been Made:
Agencies' efforts hampered by a lack of effective collaboration

- **Criteria:** Defining roles, responsibilities and agreed upon outcomes ensures that agencies have clearly articulated and agreed on which entity will do what and what is expected of each party.
- **DOT and DHS have not clearly defined their respective roles, responsibilities, and authorities or what outcomes would satisfy the presidential directive**.
  - DOT officials told us that they handle backup capabilities for aviation, but they depend on DHS and industry to provide backup capabilities for the other CI sectors
  - DHS officials told us that NSPD-39 places lead responsibility with DOT, not DHS
  - DOT and DHS have not established clear, agreed-upon outcomes that clarify what would satisfy the NSPD-39 backup-capabilities requirement, and neither agency has been consistently monitoring its progress. Establishing clear outcomes for efforts that require collaboration ensures that agencies have agreed on how they will satisfy mutual responsibilities and what specifically they are working toward

GAO

Agencies' Positive Steps Toward Collaboration

- The agencies were in the process of finalizing a written agreement on interagency procedures for information sharing among agency PNT operations centers when GPS disruptions occur

- In the first half of 2013, EXCOM established an Interagency IDM/Alternative PNT task force to address the needed resiliency of CI relying on GPS
  - However, agencies still had different understandings, as of July 2013 - DOT's understanding was that the task force would mostly monitor sector activities, while DHS highlighted a broader scope of activity for the task force, including elevating awareness of critical sectors' dependencies on GPS

SECTORS EMPLOY MITIGATION STRATEGIES, …
BUT DHS HAS NOT MEASURED THEIR EFFECTIVENESS

Sectors Vary in Reliance on GPS and Employ Different Mitigation Strategies

- GPS reliance and mitigation strategies:
  - Reliance is currently low, but growing or sectors have alternatives
    - Bulk Power System subsector of the Energy Sector; Transportation subsectors - Rail; Aviation)
- 3 of 4 sectors have initiated further efforts to study GPS vulnerability and potential mitigations
- Sectors may be reluctant to bear significant costs for mitigation - GPS disruptions are often perceived as low risk since the number of reported incidents is low
  - (However user awareness is low regarding disruptions and reporting procedures)

GAO

DHS Has Not Measured the Effectiveness of the Sectors' Efforts to Mitigate GPS Disruptions

- While sectors have taken steps to prepare for GPS disruptions, DHS had not measured the effectiveness of sectors' mitigation efforts to ensure sector resiliency against GPS disruptions
  - Furthermore, no plan or timeline had been developed or approved for identifying and assessing measures of effectiveness
- DHS officials indicated:
  - It is not necessary to measure effectiveness of individual programs and that the absence of resilience measures for an individual program (such as IDM) does not mean that DHS is not measuring overall resilience at the sector level
  - Measurement may be cost prohibitive
  - DHS is focusing on increasing awareness of GPS embeddedness and potential disruptions within three sectors—the communications, information technology, and transportation systems sectors

Measuring Program Effectiveness is Important

- **Criteria:**
  - The NIPP requires DHS to work with SSAs and CI partners to measure the effectiveness of CI protection programs by establishing performance metrics that enable DHS to objectively assess improvements, track progress, establish accountability, document actual performance, provide feedback mechanisms, and inform decision-making
  - Furthermore: PPD-21 emphasizes efforts to strengthen and maintain resilient CI and requires DHS to use a metrics and analysis process to measure the nation's ability to manage and reduce risks to CI.
  - Additionally, focusing on measuring outcomes—and not just on testing the GPS devices—in critical sectors is important

As a result of not having measurements, or a plan to assess the impact of GPS disruptions on CI sectors, DHS cannot provide assurance that the CI sectors would be able to maintain operations in the event of a GPS disruption without significant economic loss, or loss of life.

Measuring Effectiveness of Mitigation Efforts: Key GPS Concerns

- **Low awareness** - Sector awareness of the extent to which GPS is embedded in their systems is frequently unknown / understated. For example:
  - 2007 San Diego short term incident should not have impaired mobile communications, but did
  - UK maritime test sounded numerous alarms and raised concerns of hazardous conditions to mariners
- **Sustainability** of sectors' current level of operations
  - Legacy systems may be less efficient causing economic losses
  - Users may no longer have the skills or staff to adequately use legacy backup systems

Measuring Effectiveness of Mitigation Efforts: Key GPS Concerns

- **Increasing dependency**
  - Energy, Transportation subsectors' use of GPS (PMUs, NextGen, Positive Train Control)
- **Likelihood of Disruption could be growing**
  - Jamming:
    - ~500,000 hits for "GPS Jammer"
    - Jammers are likely to become smaller, more powerful, and less expensive, increasing the likelihood of disruptions
  - Spoofing:
    - Growing number of papers and industry presentations available on the Internet that discuss or show the ability to spoof GPS receivers in multiple sectors
  - Potential for unintended interference from new communication services
    - Difficulty in estimating these disruptions in advance and isolating them.

Conclusions

- GPS is a key and increasingly important component in economic growth, safety, and national CI sectors.
- DHS conducted a GPS risk assessment (NRE) which faced several difficult challenges.
  - While DHS attempted to overcome these challenges, the NRE lacks some of the key characteristics of risk assessments. As such, the NRE is limited in its usefulness to inform mitigation planning, priorities, and resource allocation.
- Although the President directed DOT, in coordination with DHS in 2004, to develop backup capabilities to mitigate GPS disruptions, the agencies have made limited progress amid continued uncertainty.
  - Both agencies cited resource constraints—such as budget and staffing—as a reason why they have not made additional progress.
  - Furthermore, DOT and DHS have not defined their respective roles, responsibilities, and authorities or what agreed-upon outcome would satisfy the presidential directive. As a result, DOT and DHS cannot ensure that they will satisfy mutual responsibilities.

Conclusions

- CI sectors have employed various mitigation strategies, however sector risks may be underestimated, growing, and interdependent. Therefore it is unclear whether sectors' efforts are sufficient.

- DHS has not measured the effectiveness of sector mitigation efforts to GPS disruptions. As a result, DHS cannot ensure that CI sectors could sustain essential operations during GPS disruptions.
  - Furthermore, the lack of agreed-upon metrics to measure the actual effectiveness of sector mitigation efforts hinders DHS's ability to objectively assess improvements, track progress, establish accountability, provide feedback mechanisms, or inform decision makers about the appropriateness of—or need for additional—mitigation activities.

GAO RECOMMENDATIONS

Recommendations to DHS

- Increase the reliability and usefulness of GPS risk assessment by developing a plan and timeframe to collect relevant threat, vulnerability and consequence data for CI sectors.
- As part of current CI protection planning with Federal agencies and sector partners, develop and issue a plan and metrics to measure the effectiveness of GPS risk mitigation efforts on CI resiliency.

Recommendations to DHS and DOT

- To improve collaboration and address uncertainties in fulfilling the NSPD-39 backup-capabilities requirement, establish a formal, written agreement that details how the agencies plan to address their shared responsibility:
  - Clarify and define DOT's and DHS's respective roles, responsibilities, and authorities
  - Establish clear, agreed-upon outcomes and how the agencies will monitor and report on progress
  - Detail the agencies plans for addressing issues, such as:
    - the roles of SSAs and industry,
    - whether an update to the NSPD-39 is needed

GAO on the Web

Web site: http://www.gao.gov/

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@gao.gov
(202) 512-4400, U.S. Government Accountability Office
441 G Street, NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov
(202) 512-4800, U.S. Government Accountability Office
441 G Street, NW, Room 7149, Washington, DC 20548

Copyright