



governmentattic.org

"Rummaging in the government's attic"

Description of document: Department of Homeland Security (DHS) reports produced by or for the Directorate for National Protection and Programs (DNPP) on the risks of geomagnetic storms to the nation, 2012-2013

Request date: 26-April-2015

First release date: 09-June-2015
Final release date: 31-July-2015

Posted date: 19-October-2015

Note: Material released 31-July-2015 begins on PDF page 11

Source of document: U.S. Department of Homeland Security
245 Murray Lane SW
STOP-0655
Washington, D.C. 20528-0655
Fax: 202-343-4011
E-mail: foia@hq.dhs.gov
[Online FOIA Request Submission Form](#)

The governmentattic.org web site ("the site") is noncommercial and free to the public. The site and materials made available on the site, such as this file, are for reference only. The governmentattic.org web site and its principals have made every effort to make this information as complete and as accurate as possible, however, there may be mistakes and omissions, both typographical and in content. The governmentattic.org web site and its principals shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information provided on the governmentattic.org web site or in this file. The public records published on the site were obtained from government agencies using proper legal channels. Each document is identified as to the source. Any concerns about the contents of the site should be directed to the agency originating the document in question. GovernmentAttic.org is not responsible for the contents of documents published on the website.



**Homeland
Security**

June 9, 2015

SENT VIA EMAIL

Re: **2015-NPFO-00269**

This is the electronic interim response to your April 26, 2015, Freedom of Information Act (FOIA) request to the Department of Homeland Security (DHS) for a copy of each report or study produced by or for the DNPP on the risks of geomagnetic storms to the nation. This office received your request on April 27, 2015.

We are granting a portion of your request under the FOIA, Title 5 U.S.C. § 552, as amended, and DHS' implementing regulations, 6 C.F.R. Chapter I and Part 5. After carefully reviewing the responsive documents, I determined that they are appropriate for public release. They are enclosed in their entirety; no deletions or exemptions have been claimed.

Provisions of the FOIA allow us to recover part of the cost of complying with your request. If applicable, fees will be assessed in the final response.

If you need to contact us about this request, please refer to **2015-NPFO-00269**. You may contact this office at NPPD.FOIA@HQ.DHS.GOV or 703-235-2211.

Sincerely,

Sandy Ford Page
SANDY FORD PAGE
Chief, FOIA Operations

Enclosure(s): DOCUMENT(S), 9 PAGES



IP Note: GPS Risks to the Communications Sector and Critical Sector Dependencies

December 16, 2013, 1100 EDT

SCOPE

The Department of Homeland Security's Integrated Analysis Task Force/Homeland Infrastructure Threat and Risk Analysis Center (DHS/IATF/HITRAC) produces IP Notes to address issues impacting the infrastructure protection community. Every critical infrastructure sector depends on communications assets to support operations, yet sector stakeholders may not realize, or may underestimate, how such assets depend on the Global Positioning System (GPS) to function. This IP Note explains key considerations regarding the linkage between the GPS and communications assets.¹ In particular, this IP Note highlights information from previous DHS studies on the extent of GPS timing usage across sectors, and it outlines how GPS disruptions can interrupt the functionality of communications assets and, subsequently, operations across sectors.² IATF/HITRAC produced this IP Note in coordination with the DHS Office of Cybersecurity and Communications—Stakeholder Engagement and Cyber Infrastructure Resilience and the National Cybersecurity and Communications Integration Center.

KEY FINDINGS

- **IATF/HITRAC assesses the availability and increasingly widespread use of low-cost portable GPS receivers or jammers and multi-frequency jammers will create more frequent localized GPS disruptions.³**
- **IATF/HITRAC assesses that GPS-based applications may experience degradation when GPS disruptions inhibit the distribution or use of GPS timing signals for communications assets, hampering the normal functionality of communications-dependent critical infrastructure.**
- **The Communications Sector is generally resilient against most short-term disruptions due to the use of high-quality oscillators for backup timing. IATF/HITRAC assesses, however, that the Communications Sector is vulnerable to**

¹ The IP Note discusses communications assets and technology generally and does not delve into specific technologies (e.g., various Long Term Evolution (LTE) technologies and features). IATF/HITRAC recognizes that these technologies can drive timing accuracy requirements—e.g., some standards require frequency as well as precise phase and time, some require only precise phase and time, and some require only frequency synchronization. Source: DHS, National Coordinating Center for Telecommunications, (Email from private sector subject matter expert, November 1, 2013).

² The DHS Office of Infrastructure Protection produced two reports that inform this IP Note: HITRAC, National Risk Estimate: *Risks to U.S. Critical Infrastructure from GPS Disruptions*, November 29, 2012; and Infrastructure Coordination and Analysis Office, *GPS Timing Usage Report, Updated Final*, July 27, 2010.

³ Jammers prevent GPS receivers from effectively capturing and tracking the signals that GPS satellites use to direct precise positioning, navigation, and timing information toward earth.

potential long-term GPS disruptions (i.e., a few days or more) that could cause sector-wide service degradations.

BACKGROUND

GPS provides accurate, space-based positioning and navigation data in addition to timing. The extent of GPS timing usage across critical infrastructure sectors is significant: 14 of the 16 critical infrastructure sectors use the GPS timing signal, and GPS timing is essential—i.e., used for synchronization purposes—for 11 of the sectors, including the Communications Sector.^{4,5} GPS provides communications service providers with a continuous time reference to maintain the timing accuracy of internal clock components in communications assets that support network synchronization.⁶

INFRASTRUCTURE RISK

Threat Analysis:

It is difficult to assess fully the nature, intent, and source of threats to the GPS signal—particularly disruptions affecting critical infrastructure—partly because the United States does not have a nationally integrated capability to detect, identify, and locate GPS service interruptions. However, most user-reported interference events are not malicious. Government testing, equipment malfunctions, software updates, and other issues have the potential to increase the severity or duration of an event.

- In 2007, a scheduled U.S. military communication jamming exercise in San Diego—intended to block radio signals and test procedures during a communication loss—inadvertently jammed the GPS signal, as well. The effects shut down a nearby hospital’s mobile paging system used to call doctors for emergencies. In addition, two local cell phone towers shut down, and 150 others reported loss of time synchronization needed to pass calls from tower to tower.⁷
- In 2007, a national telecommunications provider experienced service disruption while implementing software updates, impacting over 100 cell sites.⁸
- In 2009, temporary broadcasting problems from a satellite control segment impacted timing for over 4,000 cell sites.⁹

Natural phenomena like geomagnetic storms can also create wide-scale degradations depending on their severity. Producing wide-scale degradation through jamming may require nation-state capabilities, but the power needed to broaden such jamming impacts would also expose the jamming source to identification and interdiction more quickly. Depending on the location of the

⁴ Presidential Policy Directive 21 (February 2013) reduces the number of critical infrastructure sectors from 18 to 16. The *GPS Timing Usage Report* assesses that 15 sectors—of the 18 at the time—use the GPS timing signal.

⁵ DHS Office of Infrastructure Protection, Infrastructure Coordination and Analysis Office, *GPS Timing Usage Report, Updated Final*, July 27, 2010.

⁶ The President’s National Security Telecommunications Advisory Committee (NSTAC), *NSTAC Report to the President on Commercial Communications Reliance on the Global Positioning System (GPS)*, February 28, 2008.

⁷ DHS, “National Risk Estimate: *Risks to U.S. Critical Infrastructure from GPS Disruptions*,” November 29, 2012, 39.

⁸ DHS, National Coordinating Center for Telecommunications, (Discussion, Arlington, VA, October 24, 2013).

⁹ Ibid.

jamming source—i.e., within the Nation’s borders as opposed to outside them—U.S. authorities could respond and limit the severity and duration of impacts.

- From 2010 through 2012, North Korea jammed GPS signals in South Korea numerous times for periods that lasted between 4 and 16 days, disrupting GPS receivers in many cell towers in addition to over one thousand aircraft and hundreds of ships.¹⁰

Many cases of GPS jamming have involved individuals using low-powered jammers purchased over the Internet, and IATF/HITRAC assesses their availability and widespread use will increase the frequency of localized GPS disruptions.

- Among the general public, motorists’ use of portable GPS jamming devices is deliberate but not necessarily malicious in nature (e.g., intended to disrupt critical infrastructure), and such use is likely to continue to increase through attempts to use jamming for privacy protection.¹¹
- Some commercial drivers use GPS jamming devices to hide their location from their employers when making unauthorized stops.¹²
- Such jamming may create unintended, localized, and short-term GPS disruptions that impact GPS-based applications in nearby critical infrastructure, as illustrated by incidents that disrupted ground-based components of the global navigation satellite system (GNSS) wide area augmentation system at Newark Liberty International Airport in New Jersey.¹³

The Federal Communications Commission (FCC) imposes legal restrictions on the use and importation of jammers, yet devices of varying sizes, frequency ranges, and output power are easily obtained illegally online through foreign manufacturers and distributors.

Vulnerability Analysis:

In general, the accuracy, availability, and reliability of GPS timing capabilities used by the infrastructure sectors have created a broad dependency on GPS timing. Communications assets using GPS for timing synchronization, location-based services, and other purposes can be vulnerable to GPS disruptions.¹⁴ Space-based GPS signals are weak, especially once they reach

¹⁰ Bob Brewin, "S. Korea Plans Navigation System to Defeat the North's GPS Jamming," *Nextgov*, January 18, 2013, <http://www.nextgov.com/defense/2013/06/s-korea-plans-navigation-system-defeat-norths-gps-jamming/65120/>, accessed September 12, 2013.

¹¹ When DHS developed the National Risk Estimate, the participating subject matter experts were in consensus that, in general, accidental sources of varying nature cause the most GPS disruptions as opposed to the public’s use of portable jammers.

¹² The National Risk Estimate: *Risks to U.S. Critical Infrastructure from GPS Disruptions*, discusses a series of incidents in 2011—127 radio-frequency interference events over a 127-day span. More recently, the FCC conducted an August 2012 investigation that resulted in a fine for a New Jersey man who admitted using a jammer to block his employer’s GPS system installed in his vehicle. See: Steve Strunsky, “N.J. man fined \$32K for illegal GPS device that disrupted Newark airport system,” August 8, 2013, www.nj.com/news/index.ssf/2013/08/man_fined_32000_for_blocking_newark_airport_tracking_system.html, accessed August 23, 2013.

¹³ Ibid.

¹⁴ Reliance on timing varies between technologies, however. For example, an oscillator could provide weeks or months of acceptable frequency synchronization while providing only 4 to 6 hours of phase and time synchronization. Source: DHS, National Coordinating Center for Telecommunications, (Email from private sector subject matter expert, November 1, 2013).

ground-based receivers. This inherent weakness makes the GPS signal susceptible to various forms of interference (e.g., accidental interference, jamming, and spoofing).¹⁵

Reliable timing accuracy underlies many communications assets. For instance, synchronization to the one-microsecond level or better is often required by various radio transmission systems, such as cellular telephony and single-frequency land mobile networks.

Jamming can cause GPS receivers to lose lock on the GPS signal and switch to a holdover mode that uses backup timing.¹⁶ Sites with backup timing sources, such as GPS-disciplined quartz and atomic (cesium or rubidium) oscillators, can mitigate the loss of GPS for a period of time depending on oscillator quality.¹⁷

- Wireless Code Division Multiple Access (CDMA)-based cell sites will begin to be affected after 24 hours of GPS outage rather than immediately.¹⁸ Calls can be maintained at a given cell site but will not necessarily be handed off to the next cell site successfully.
- In the case of wireline network infrastructure (e.g., circuit switches), they will sustain operation automatically for approximately 30 days in the event of complete loss of GPS signals. However, it is still possible for network performance to be impacted during the 30-day window.¹⁹

Overall, the appropriate backup technology depends on the specific timing needs at each site, and the sustained accuracy of the technologies increases with their expense.²⁰ Sites without any backup timing create greater vulnerability to GPS disruptions. The Communications Sector is generally resilient against most short-term disruptions given backup timing measures, whereas long-term disruptions (i.e., a few days or more) will likely cause service degradations.

Depending on the severity of a GPS disruption incident, vulnerable communications assets that experience interference may create cascading impacts for dependent sectors, as discussed below.

Consequence Analysis:

Interdependencies between the Communications Sector and other critical infrastructure sectors are substantial, as is broad user reliance on communications assets for routine operations—e.g., Federal, State, and local law enforcement investigations; emergency services dispatching; and general business functionality. When GPS disruptions inhibit the distribution or use of GPS timing, IATF/HITRAC assesses that GPS-based applications in communications assets may experience interruptions, hampering the normal functionality of such communications-dependent operations.

¹⁵ Spoofing involves the surreptitious replacement of a true satellite signal with a manipulated signal.

¹⁶ Ordinarily, GPS receivers benefit from continuous timing corrections drawn from the reliable accuracy that the GPS signal provides as a time reference. In holdover mode, the accuracy of the internal clock timing will degrade gradually; the speed of degradation depends on the quality of the internal clock. Higher quality clocks cost more and slow the degradation better than lower quality clocks. See 2008 *NSTAC Report*.

¹⁷ DHS Office of Cybersecurity and Communications, “Analysis: Communications Sector Dependencies on Global Positioning Systems,” July 25, 2013.

¹⁸ *Ibid.* The quality of the equipment’s internal clock and the requirements of the particular technology supported by the equipment will determine the ultimate holdover time possible.

¹⁹ *Ibid.*

²⁰ *Ibid.*

The magnitude and duration of a GPS disruption incident shapes the potential for cascading impacts to dependent sectors, including consequences such as loss of consumer confidence, economic loss, or even potential safety-of-life issues. Magnitude and duration also impact how easily the FCC and others might be able to locate and disable an interfering device, as disruptions of greater power or persistence are easier to identify than those of weaker power or intermittent disruptions.

Most terrestrial GPS disruptions are likely to be localized, and examples of potential consequences include a loss of efficiency for emergency services dispatching. Although dispatchers may still be able to communicate with individual first responder units during a GPS service disruption, there could be debilitating effects on radio signals or untimely delays in voice communications radio systems using simulcast technology.²¹

- Without simulcast ability, emergency services operations in an impacted area would have to fall back on less sophisticated means of communications, such as reverting to a standard single-frequency repeater, which does not require GPS to operate, but may cause an entire first responder department to share a single channel.

In addition, the positioning and navigation features of GPS available in computer-aided dispatch technologies assist some elements to more efficiently manage fleet vehicles, locate accidents, and dispatch fire, medical, and law enforcement personnel. The inability to dispatch the closest emergency vehicle to an incident poses safety-of-life issues.

- Hampered communications may prompt personnel to resort to cellular communications, but GPS timing disruptions that cause cellular towers in an area to lose their synchronization would impede the ability of those towers to hand off calls from one to another, potentially limiting the spatial extent of sustained cellular communications while an individual is moving.

Despite these risks, IATF/HITRAC recognizes that communications companies that own, operate, and supply communications infrastructure have historically factored natural disasters and accidental disruptions into network resilience architecture, business continuity plans, and disaster recovery strategies.²² Such decisions to consider the impact of disruptions in advance of actual problems can help minimize the consequences when disruptions occur.

PROTECTIVE MEASURES

To mitigate the threat of GPS service outages that can impact the Communications Sector, and other sectors through dependencies, the following protective measures should be considered:

- Use multi-system receivers that can acquire non-GPS signals from other GNSSs to expand backup options. The well-established presence of effective backups may discourage intentional jamming attacks on GPS in the first place.²³

²¹ Simulcast uses GPS for synchronization, and it allows emergency services operators to transmit broadcasts broadly and simultaneously, if needed, across multiple communications towers.

²² Communications Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan, 2010.

²³ Users must avoid a false sense of security, however, and recognize that all existing GNSSs share characteristics of high frequency and extremely low received signal that can allow various jamming devices to disrupt signal reception.

- Train technicians to distinguish between internal equipment failures (e.g., hardware or software glitches) and external problems related to GPS interruptions.²⁴
- Where and when possible, use physical and logical measures to harden GPS user equipment against jamming and spoofing.
- Test the resilience of operations when functioning without GPS for extended time periods (e.g., exercising strategies to communicate without using cellular technologies, and practicing with alternative navigation methods). Such testing can provide an accurate understanding of the viability of differing backup timing applications (e.g., quartz, rubidium, and cesium oscillators) for particular operations.

RESOURCES

- In November 2012, IATF/HITRAC released a National Risk Estimate: *Risks to U.S. Critical Infrastructure from GPS Disruptions*. The report is For Official Use Only and is available through the Homeland Security Information Network Critical Infrastructure (HSIN-CI) portal. Please contact HSINCI@hq.dhs.gov for HSIN-CI access. For more information IATF/HITRAC and its products, email risk@hq.dhs.gov.
- The Federal Government addresses GPS-related topics at www.gps.gov, which includes an unclassified National Risk Estimate factsheet and briefing.
- The National Security Telecommunications Advisory Committee's 2008 *Report to the President on Commercial Communications Reliance on the Global Positioning System* evaluates the commercial communications industry's use of and reliance on GPS. See www.dhs.gov/sites/default/files/publications/NSTAC%20GPS%20Report_0.pdf.
- The National Institute of Standards and Technology identifies alternatives to GPS networking timing protocols at www.nist.gov/pml/div688/.
- The Civil GPS Service Interface Committee is the recognized worldwide forum for civil GPS users and U.S. GPS authorities. See www.gps.gov/cgsic.
- The U.S. Coast Guard's Navigation Center of Excellence Web site hosts current GPS-related data at www.navcen.uscg.gov.
- Individuals may report GPS jamming or interference incidents to the FCC by calling 1-888-CALL-FCC or emailing jammerinfo@fcc.gov. Individuals may file reports with the USCG at www.navcen.uscg.gov/??pageName=gpsUserInput.
- The [2011 GPS World Receiver Survey](#) describes the signals that each receiver is capable of tracking so that users can easily identify multi-system and multi-frequency receivers.

~~The Homeland Infrastructure Threat and Risk Analysis Center produces Infrastructure Protection Notes, which scope the infrastructure protection community's risk environment from terrorist attacks, natural hazards, and other events being reviewed and highlight the analytic capabilities required to produce infrastructure protection related risk analytic products. The information is provided to support the activities of the Office of Infrastructure Protection and to inform the strategies and capabilities of Federal, State, local, and private sector partners. For more information, contact risk@hq.dhs.gov. For more information about the Office of Infrastructure Protection, visit www.dhs.gov/criticalinfrastructure.~~

²⁴ Even with such training, jamming devices can create harmful effects, but training can raise awareness that helps technicians to recognize when a disruption stems from a non-equipment issue.



~~(U)~~ Potential Effects of Solar Storms on U.S. Infrastructure

Release: 1700 MST: 24 January 2012

~~(U)~~ KEY FINDINGS

- ~~(U)~~ While there could be some impacts on electric power transmission and transformation, electric power systems are resilient and would likely be able to shift power distribution to backup configurations to accommodate local disruptions. If component repairs were necessary to restore normal operating configurations, they would likely require 1 day to complete except for the loss of a large power transformer which requires in excess of 6 months to replace.
- ~~(U)~~ A solar storm could affect radio communications, such as satellite communication, commercial airliners, radio, TV, cellular and high-frequency communications signals. The disruptions for these types of communications signals would likely range from a few minutes to several hours.

~~(U)~~ LEADERSHIP'S QUESTIONS

- ~~(U)~~ What is the impact of the solar storms?
 - ~~(U)~~ Solar storms are natural sources of characteristic E3 slow pulse EMP (Electromagnetic Pulse). The magnetic poles of the Sun reverse every Solar Cycle (approximately every 11 years, with 22 years for a complete solar pole-transition cycle), causing an increase in the number and intensity of solar storms during the maximum transition rates of the pole reversals. The National Oceanic and Atmospheric Administration predicts that Solar Cycle 24 (the current cycle), which started in 2008, will reach its peak in May 2013.
 - ~~(U)~~ The interaction of solar wind with Earth's magnetosphere produces electric fields on the surface of Earth that result in the creation of geomagnetically induced currents (GIC). Electromagnetic induction in Earth's surface develops a geo-electric field that can result in potential (voltage) gradients over the surface of Earth. A surface voltage gradient is a real electrical voltage that can be measured in the surface of the Earth. Over very large distances, the voltage is increased and can be detrimental to utility and transportation infrastructure. Potential gradients originate from boundary charge accumulations and ultimately drive currents that enter the power grid at ground locations of transformers and ultimately flow into utility transmission lines.
 - ~~(U)~~ The recent Hydro-Quebec Storm of 1989 had an effect on infrastructure in the United States and Canada. This geomagnetic storm caused a blackout on the Hydro-Quebec Power Authority, leaving its customers without power for 9 hours. The disturbance of the Earth's magnetic field began intensifying over the eastern U.S.-Canada border and then rapidly intensified and moved to the west across North America. The Hydro-Quebec system collapsed in 90 seconds. The most intense portion of the storm was actually centered over lower Manitoba and northern Minnesota with more than twice the magnitude of the disturbance observed over the Quebec region that caused the Quebec power grid blackout. Magnetic currents flowed from the ground into the electrical system through transformers. Although the majority of customers had power within about 9 hours after the collapse, some were without power for days. Communications were disrupted and power glitches also occurred in the northern United States.
- ~~(U)~~ What are the likely impacts from solar storms, particularly to the electric and communications systems?

- ~~(U)~~ Communications: A solar storm can affect the upper ionosphere in a way that makes it absorb radio communications signals. Satellite communication could be interrupted. Long-distance commercial airliners could lose communications signals. At the Earth's surface, radio, TV, and cellular communications signals might be disrupted. The disruptions for all types of radio communications can range from a few minutes to several hours. For communications systems, non-electrically conductive fiber-optic cables have replaced the long-distance and undersea copper cables used in the past. The potential effects of a solar storm continue to be minimized as system owners increasingly replace copper with fiber-optic cables in the 'last mile' of communications networks. Because these are non-electrically-conductive materials, electric current fluctuations do not affect their operation.
- ~~(U)~~ Electric Power: Solar wind can induce Earth surface voltage gradients, i.e., that can cause electric currents to flow in electrically conductive features, for example, electric power lines, copper communications lines, pipelines, railroad tracks, and waterways. If the electric power system experiences current overages, major transmission lines and substations may trip, producing unexpected loss of bulk power transfers along the system, potentially ending with a localized area of cascaded power system outages for the end consumer. The loss of power generation capability arises from either damage or disruptions in power plant electrical instrumentation systems, including switchyard power, control systems, combustion turbine generator packages, and control rooms. A disruption of long high-voltage electric power transmission lines and terminating substations is likely the single greatest concern related to geomagnetic solar storms. Effects typically last from a few minutes to tens-of-hours.
- ~~(U)~~ If there was a significant impact to the electric grid and/or the communications system, what would be the most significant cascading impacts?
- ~~(U)~~ Like other natural disasters, if a solar storm disrupts electric power, there could be cascading infrastructure impacts across sectors. Electric power is critical to every infrastructure sector in some way. Critical sectors that depend on electric power include Public Health and Healthcare, Communications, Information Technology, Emergency Services, and Transportation, and Water and Wastewater. As noted previously, effects typically last from a few minutes to tens-of-hours. Although the probabilities of electric power system collapse as a result of GIC are a continuing concern, the overall levels of risk are being actively reduced.

The Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) produces In Response to Your Question (IRQ) documents in response to questions received from DHS, NPPD, or IP leadership as part of the Department's efforts to carry out comprehensive assessments of the risks to critical infrastructure in the United States, and to facilitate a greater understanding of the emerging threats to and vulnerabilities of critical infrastructure in the United States. Questions or comments regarding this product should be directed to risk@hq.dhs.gov. For more information about IP, visit www.dhs.gov/criticalinfrastructure.



**Homeland
Security**

July 31, 2015

SENT VIA EMAIL

Re: 2015-NPFO-00269

This is the electronic final response to your April 26, 2015, Freedom of Information Act (FOIA) request to the Department of Homeland Security (DHS) for a copy of each report or study produced by or for the DNPP on the risks of geomagnetic storms to the nation. This office received your request on April 27, 2015.

A search of the Office of Cyber and Infrastructure Analysis for documents responsive to your request produced a total of 222 pages. Of those pages, I have determined that 204 pages of the records are releasable in their entirety and 18 pages are partially releasable pursuant to Title 5 U.S.C. § 552 (b)(6), (b)(7)E and (b)(7)(F), FOIA Exemptions 6, b7(E), and b7(F).

Enclosed are 222 pages with certain information withheld as described below.

FOIA Exemption 6 exempts from disclosure personnel or medical files and similar files the release of which would cause a clearly unwarranted invasion of personal privacy. This requires a balancing of the public's right to disclosure against the individual's right to privacy. The privacy interests of the individuals in the records you have requested outweigh any minimal public interest in disclosure of the information. Any private interest you may have in that information does not factor into the aforementioned balancing test.

Exemption 7(E) protects records compiled for law enforcement purposes, the release of which would disclose techniques and/or procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law. I determined that disclosure of the records could reasonably be expected to risk circumvention of the law. Additionally, the techniques and procedures at issue are not well known to the public.

FOIA Exemption 7(F) permits the government to withhold all information about any individual when disclosure of information about him could reasonably be expected to endanger the life or physical safety of any individual. This exemption also protects physical security at critical infrastructure sites.

You have a right to appeal the above withholding determination. Should you wish to do so, you must send your appeal and a copy of this letter, within 60 days of the date of this letter, to: Associate General Counsel (General Law), U.S. Department of Homeland Security, Washington,

D.C. 20528, following the procedures outlined in the DHS regulations at 6 C.F.R. § 5.9. Your envelope and letter should be marked "FOIA Appeal." Copies of the FOIA and DHS regulations are available at www.dhs.gov/foia.

The Office of Government Information Services (OGIS) also mediates disputes between FOIA requesters and Federal agencies as a non-exclusive alternative to litigation. If you are requesting access to your own records (which is considered a Privacy Act request), you should know that OGIS does not have the authority to handle requests made under the Privacy Act of 1974. If you wish to contact OGIS, you may email them at ogis@nara.gov or call 1-877-684-6448.

Provisions of the FOIA and Privacy Act allow us to recover part of the cost of complying with your request. In this instance, because the cost is below the \$14 minimum, there is no charge. 6 CFR § 5.11(d)(4).

If you need to contact our office again about this matter, please refer to **2015-NPFO-00269**. This office can be reached at 703-235-2211.

Sincerely,

Sandy Ford Page
SANDY FORD PAGE
Chief, FOIA Operations

Enclosure(s): Responsive Documents, 222 pages

NATIONAL RISK ESTIMATE

RISKS TO U.S. CRITICAL INFRASTRUCTURE
FROM GLOBAL POSITIONING SYSTEM DISRUPTIONS



Homeland
Security



External Reviews of this National Risk Estimate

In the upcoming decade, Global Positioning System (GPS) planners, engineers, and users will need to shift their focus to concerns over security. The subject report from the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) intelligently presages this shift. It identifies a hierarchy of security threats to GPS that range from likely to extravagant. These threats are equally applicable to the other Global Navigation Satellite Systems (GNSS) under development worldwide. The report also predicts the impact of these threats on the main application sectors of GPS (and GNSS): telecommunications, emergency services, energy, and transportation. Risk is approximated as the product of the sector-independent threat likelihood and the sector-specific consequence of the event. The HITRAC analysis has generated a very sensible picture of the overall situation. The report also describes possible futures for each sector based on varying degrees of community attention to these security challenges.

While general, the HITRAC framework does not obliterate the needed nuance and detail. For example, the report also identifies the severe risk posed by repurposing the frequency bands that neighbor GPS. The report also contains informative essays on other recent security threats such as the personal privacy devices and significant jamming events in San Diego and Half Moon Bay.

All told, the report is a significant step ahead in our understanding and a roadmap to a safer future for users of GPS.

(b)(6)

The Department of Homeland Security (DHS) has done an exemplary job in assessing the risks to the U.S. Critical Infrastructure of disruptions to the GPS. In its National Risk Estimate, DHS notes that GPS is “a largely invisible utility” with the result that dependence on GPS is “significantly underestimated” by key users throughout the Nation’s various critical infrastructure sectors. The estimate notes that the current risk is manageable, but that the widespread and growing use of GPS, coupled with threat actors possessing technologies that can disrupt GPS now and in the future, pose a long term threat that cannot be ignored.

DHS has performed a valuable service to the Nation in publishing this sobering assessment. The time is now for all users in government and the private sector to carefully evaluate their reliance on GPS and to begin taking the necessary actions to mitigate the effects of potential GPS disruptions. Such actions will serve to protect essential services as well as make GPS a less attractive target for purposeful disruption.

(b)(6)

The NRE GPS vulnerability report does a thoughtful and thorough job of analyzing current threats-- primarily those of intentional and unintentional jammers. The look at a 20-year future state correctly recognizes the critical role that spectrum management, monitoring and rapid elimination of jammers will play in mitigating GPS vulnerability. The somewhat exhaustive litany of possible future states for each of the four critical infrastructures opens the door for many of the current vulnerabilities "fixes" but fails to recognize the extent that innovation is driven by customer demand. Consumers may be willing to pay a small amount to insure availability of conveniences, but there is a limit. The fact that the government is also a customer of these critical infrastructures creates the opportunity for customer demand to drive critical infrastructure architecture such that enhanced soft failure modes are provided for critical components such as GPS. This in turn would allow the decoupling of essential services reliability from that of consumer conveniences.

(b)(6)

~~(U)~~ Table of Contents

(U) Executive Summary.....	3
(U) Chapter 1. Key Judgments	7
(U) Chapter 2. Purpose.....	11
(U) Chapter 3. Scope	11
(U) Chapter 4. Underlying Analytic Assumptions	14
(U) Chapter 5. Current Risk to Missions of Critical Infrastructure Sectors from Disruption in GPS PNT Systems.....	16
(U) 5.1 Categories of GPS PNT Disruption	16
(U) 5.2 GPS Spectrum Encroachment.....	18
(U) 5.3 GPS Disruption Scenarios.....	20
(U) 5.4 Assessment of Likelihood of GPS PNT Disruption Scenarios	22
(U) 5.5 NRE GPS Current Risk Estimate: Communications Sector	29
(U) 5.6 NRE GPS Current Risk Estimate: Emergency Services Sector	36
(U) 5.7 NRE GPS Current Risk Estimate: Energy Sector	42
(U) 5.8 NRE GPS Current Risk Estimate: Transportation Systems Sector	48
(U) Chapter 6. Sector Interdependencies.....	58
(U) Chapter 7. Estimated Evolution of GPS PNT Disruption Risks over the Next 20 Years	61
(U) 7.1 Anticipated Future GPS Technology Developments	61
(U) 7.2 Alternative Futures for the Outlook of GPS Disruption Risk to Critical Infrastructure Sectors	62
(U) Chapter 8. Current and Projected Future Mitigation Measures	80
(U) Annex A. List of Acronyms and Abbreviations.....	84
(U) Annex B. Glossary	89
(U) Annex C. NRE Risk Assessment and Monte Carlo Simulation Methodology	101
(U) Annex D. Alternative Futures Development Methodology	111
(U) Annex E. Sector Consequence Workshop Findings	113
(U) Annex F. Likelihood Workshop Findings.....	163
(U) Annex G. Sector Alternative Futures Workshop Findings	172
(U) Annex H. NRE Coordination Approach	200
(U) Annex I. Subject Matter Expert Contributors	202
(U) Annex J. Bibliography.....	207

(U) Annex K. Selected PNT and GPS Regulations, Strategies, Executive Committees, and Working Groups	214
(U) Annex L. GPS Disruption Threat Assessment [Classified]	219

~~(U)~~ Executive Summary

~~(U//FOUO)~~ U.S. critical infrastructure sectors are increasingly at risk from a growing dependency on the Global Positioning System (GPS) for space-based position, navigation, and timing (PNT). In September 2011, after a nine-month review, U.S. Government and private sector experts concluded that portions of the Nation's critical infrastructure are increasingly reliant on GPS and GPS-based services. In the short term, the risk to the nation is assessed to be manageable. However, if not addressed, this threat poses increasing risk to U.S. national, homeland, and economic security over the long term.

~~(U//FOUO)~~ Awareness that GPS-supported services and applications are integrated in sector operations is somewhat limited, prompting the idea that GPS is a largely invisible utility. Therefore, dependence on GPS is likely significantly underestimated with many of the critical infrastructure sectors depending on the GPS timing function. Often, these critical dependencies do not become apparent until a GPS disruption occurs. In addition, instances of both unintentional and intentional threats against those GPS services are also increasing. Although most known GPS disruptions have been unintentional, threat actors are constantly adapting their operational tactics while technology advances, making intentional disruptions more likely in the future. For example, the market for personal protection¹ GPS jamming devices has increased markedly over the past two years. The increasing convergence of critical infrastructure dependency on GPS services with the likelihood that threat actors will exploit their awareness of that dependency presents a growing risk to the United States.

~~(U//FOUO)~~ This National Risk Estimate (NRE) examines four critical infrastructure sectors that use GPS PNT to support or fulfill core missions—Communications, Emergency Services, Energy, and Transportation Systems—and the effects that various types of GPS disruptions would have on each sector. (For the purpose of this NRE, the term *sector* refers to a logical collection of assets, systems, companies, or networks that provide a common function to the economy, government, or society.) GPS is also used by other sectors not examined by this NRE, and the U.S. Department of Defense has conducted extensive studies on the risks of GPS disruption in the military context. The NRE considers three types of GPS disruptions: naturally occurring disruptions, such as space weather events; unintentional disruptions, such as radio frequency signals interfering with GPS signals; and intentional disruptions, such as purposeful jamming or spoofing. This NRE evaluates the consequences and current risks to each of the four focal sectors from GPS disruption and considers the risk outlook over the next 20 years.

~~(U)~~ Current Risk Estimate

~~(U//FOUO)~~ The NRE identifies high-risk GPS disruption scenarios, determined by the scenarios' likelihood and associated consequences. It does not evaluate the risk of a GPS disruption compared to other threats, nor does it provide a comparative risk assessment across critical infrastructure sectors. Descriptions of all the scenarios assessed in the NRE are in Chapter 5.3.

¹ ~~(U)~~ The terms *personal protection devices* and *personal privacy devices* are often used interchangeably.

~~(U)~~ *Likelihood*

~~(U//FOUO)~~ Though less common than the unintentional GPS disruption incidents, there have been some incidents of criminals using GPS jammers, but there are no known incidents of adversaries attempting to disrupt GPS signals in the United States. Jamming disruptions were judged to be more likely than spoofing incidents since jamming takes less skill and expertise, and it can often be an unintentional consequence of other actions or devices.² The likelihood of each GPS disruption scenario was identified independent of a specific sector that might be impacted by the disruption. A classified annex to the NRE provides more details on the intentional GPS disruption threat and assesses threats to each sector using low, medium, or high designations.

~~(U)~~ *Consequence*

~~(U//FOUO)~~ In a series of sector-specific workshops, sector and GPS subject matter experts (SMEs) examined the consequences of GPS disruption scenarios. (For a listing of SME contributors, see Annex I.) Although the likelihood of disruptions was difficult to estimate accurately given limited available intelligence or information on prior disruptions, the contributions of SMEs from the four sectors provided valuable information regarding the consequences to a sector from a GPS disruption. Many sectors would suffer consequences such as economic loss and loss of consumer confidence if GPS were disrupted for several days or more. There is also the potential for safety-of-life impacts to some sectors such as the Emergency Services Sector. Spoofing scenarios were typically judged to be of higher consequence than jamming scenarios due to the potential duration of time before users or devices detect spoofing. If PNT alternatives to GPS are insufficient, these consequences could be exacerbated. SMEs identified the following GPS disruption scenarios that would have the greatest consequence for each sector:

- ~~(U//FOUO)~~ The **Communications Sector** contains components that require accurate timing and synchronization from GPS to function properly. Scenarios involving continuous, stationary, unintentional interference; multiple, low-power, continuous and intermittent, stationary and mobile jammers; or brief high-power jamming followed by continuous high-power spoofing were judged to be the highest consequence scenarios, leading to potential outages of cell phone services among other effects.
- ~~(U//FOUO)~~ The **Emergency Services Sector** is not completely dependent on GPS services, but GPS does increase the efficiency of damage mitigation and emergency response. Scenarios involving a jamming disruption from multiple, low-power, continuous and intermittent, stationary and mobile jammers or sophisticated, coordinated pinpoint spoofing attacks against multiple target receivers were judged to be the highest consequence scenarios. Reduced efficiency in Emergency Services resulting from loss of GPS could present safety of life issues.

² ~~(U)~~ Jamming prevents a receiver from tracking GPS signals while spoofing involves the surreptitious replacement of a true satellite signal with a manipulated signal.

- ~~(U//FOUO)~~ The **Energy Sector** depends on GPS for providing electrical power system reliability and grid efficiency, synchronizing services among power networks, and finding malfunctions within transmission networks. It is also used as a location/orientation tool in drilling for oil and gas. The highest consequence scenario for this sector was a sophisticated, coordinated, pinpoint spoofing attack against multiple target receivers.
- ~~(U//FOUO)~~ The **Transportation Systems Sector** uses GPS for functions such as aviation precision approaches, maritime navigation, rail maintenance and safety, mass transit vehicle tracking, pipeline safety, and shipment tracking. The highest consequence scenarios for this sector were a sophisticated, coordinated, pinpoint spoofing attack against multiple target receivers or a brief, high-power jamming event followed by continuous high-power spoofing. Consequences of GPS disruption could include losses in efficiency that cause the cost of moving people and goods to rise and delivery times to increase. A GPS disruption incident will have long-term implications for the Transportation Systems Sector as operations become more dependent on GPS. Prudent system engineering will ensure the development of appropriate architectures that do not rely overly on GPS for PNT by providing alternate non-GPS-dependent means.

~~(U)~~ *Risk*

~~(U//FOUO)~~ Although the high-consequence scenarios for the four sectors differed, the high-risk scenarios were the same. The higher relative likelihood estimates for these scenarios contributed to their higher relative risk rankings across sectors. These high-risk scenarios were:

- ~~(U//FOUO)~~ Continuous, stationary, unintentional interference.
- ~~(U//FOUO)~~ Single, low-power, continuous, stationary jammer.
- ~~(U//FOUO)~~ Multiple, low-power, continuous and intermittent, stationary and mobile jammers.

~~(U)~~ *Potential Risk Mitigation Measures*

~~(U//FOUO)~~ To mitigate a potential GPS disruption with high consequences, regulations—including technology import controls—should keep pace of advancements in GPS-enabled technology applications. Standardization and/or regulation of GPS receivers—e.g., technical characteristics and software—could mitigate future risks. Also essential is implementing a GPS backup system or PNT alternatives.

~~(U//FOUO)~~ Ensuring that receivers are capable of receiving signals from other systems in addition to GPS would allow some backup capability. The well-established presence of an effective backup would discourage a jamming attack on GPS in the first place. Furthermore, improving signal integrity monitoring, developing a suite of sensors that can detect and characterize interference, and establishing a single processing and repository site to capture information on GPS disruption incidents across the United States would allow for more accurate risk assessments in the future. Finally, the ongoing effort to harden GPS user equipment against

jamming and spoofing should be encouraged, and the Department of Homeland Security (DHS) Office of Infrastructure Protection's draft *GPS Risk Mitigation Techniques and Programs Report* provides more details on mitigation measures.

~~(U)~~ **Risk Outlook**

~~(U//FOUO)~~ Presidential Policy Directive 4, the 2010 National Space Policy, states that GPS will continue to be available as a national asset. This NRE clarifies many aspects of critical infrastructure dependence on GPS that were previously uncertain. However, this report also uncovers a number of key areas of uncertainty that make predicting future risk difficult. These key uncertainties (or "known unknowns") were similar across all four focal sectors that the NRE examines, and include the following:

- ~~(U//FOUO)~~ The extent to which GPS-based applications are layered into sector operations.
- ~~(U//FOUO)~~ The vulnerability of GPS to intentional or unintentional disruptions.
- ~~(U//FOUO)~~ The extent to which GPS disruptions can be identified and mitigated.
- ~~(U//FOUO)~~ The accuracy, availability, integrity, and continuity of alternative PNT systems available to provide robustness.

~~(U//FOUO)~~ In addition, the *National Positioning, Navigation, and Timing Architecture Implementation Plan* from the Departments of Defense and Transportation addresses capability gaps predominantly based on the limitations of GPS looking out to 2025. This *Implementation Plan*, signed in July 2010 by the Assistant Secretary of Defense for Networks and Information Integration and the Under Secretary of Transportation for Policy, was distributed to all government agencies involved with PNT to inform their planning, programming, budgeting, and execution activities.

~~(U)~~ Chapter 1. Key Judgments

~~(U//FOUO)~~ The subject matter expert (SME) workshops and additional research underpinning this National Risk Estimate (NRE) led to a series of key judgments regarding the current risk, as well as future risk outlook, of Global Positioning System (GPS) disruption to the Communications, Emergency Services, Energy, and Transportation Systems Sectors. The current risk estimate development phase considered the likelihood and consequence of a range of intentional and unintentional disruptions to GPS, including jamming, spoofing, and geomagnetic storms. The outlook development phase identified key uncertainties regarding future GPS use that can lead to various alternative futures as well as the challenges and opportunities that these futures present for government and the private sector. The key judgments below are not intended to align with actionable recommendations, which are detailed in the Department of Homeland Security (DHS) Office of Infrastructure Protection's (IP) draft *GPS Risk Mitigation Techniques and Programs Report*.

~~(U)~~ GPS Use by Critical Infrastructure Sectors

- ~~(U//FOUO)~~ U.S. critical infrastructure sectors currently rely on GPS for aspects of their core operations. The GPS signal holds significant economic appeal to all sectors because it is accurate, available, reliable, and provided at no cost to users. In addition, GPS receivers are small and inexpensive. These qualities incentivize sectors to continue developing technologies and processes that rely on the GPS signal.
- ~~(U//FOUO)~~ As GPS becomes increasingly integrated into sectors' operations, it has become an invisible utility, which users do not realize is underpinning their applications. Therefore, dependence on GPS is likely significantly underestimated with many of the critical infrastructure sectors depending on the GPS timing and location function. In these instances, it could be challenging to isolate a GPS outage as the root cause of the problem. It is therefore necessary to educate GPS users in sectors on the vulnerabilities of dependence on GPS-enabled technologies.
- ~~(U//FOUO)~~ Interdependencies exist between critical infrastructure sectors that use GPS. For example, the timing and positioning technologies of the Communications Sector support other sectors, particularly the Emergency Services and Transportation Systems Sectors, where timing and location is critical to control networks.

~~(U)~~ Likelihood of GPS Disruption

- ~~(U//FOUO)~~ There is significant uncertainty in SME judgments about the likelihood of GPS disruption scenarios. While there is some historical precedent for jamming GPS signals, there is no single repository for information regarding GPS disruption incidents.
 - ~~(U//FOUO)~~ Most known GPS disruption incidents have been unintentional. There have been some incidents of criminals using GPS jammers but no known incidents of adversaries using that technology against U.S. critical infrastructure.

- ~~(U//FOUO)~~ The technology to inflict the intentional or unintentional disruption of the GPS signal is becoming more readily available. Although illegal to import, sell, offer for sale, ship,³ or otherwise market,⁴ inexpensive mobile jammers, or personal protection devices (PPDs), are widely available for purchase on the Internet.

~~(U//FOUO)~~ Critical infrastructure is increasingly dependent on GPS, and malicious actors continue to find ways to adversely affect GPS applications.

~~(U)~~ **Consequences of GPS Disruption**

- ~~(U//FOUO)~~ The consequences of GPS disruption would generally be economic losses although there is potential for safety of life impacts in some sectors. Impacts of GPS disruption could also include ongoing loss of confidence in GPS by the user community. Moreover, due to dependencies and interdependencies between sectors, mission disruption in one sector could have adverse effects on other sectors.
- ~~(U)~~ **Communications Sector:**
 - ~~(U//FOUO)~~ The Communications Sector is significantly immune to most short-term disruptions due to the use of rubidium vapor and cesium beam oscillators for timing. Long-term disruptions (a few days or more) will cause service degradations, though.
- ~~(U)~~ **Emergency Services Sector:**
 - ~~(U//FOUO)~~ Most GPS disruption scenarios would degrade rather than prohibit sector operations. GPS spoofing scenarios are concerning to the Sector, as it uses accurate positioning and navigation data to respond efficiently to emergency incidents.
 - ~~(U//FOUO)~~ Although many jurisdictions still have conventional systems in place that do not rely on GPS, fewer legacy systems will be in use each year as reliance on GPS-based systems grows.
- ~~(U)~~ **Energy Sector:**
 - ~~(U//FOUO)~~ The electricity subsector currently has sufficient redundancies in place to withstand most GPS disruptions although spoofing attacks against multiple targets could cause significant service outages. However, as the electricity subsector becomes increasingly reliant on phasor measurement units (PMUs) as part of the smart grid evolution, vulnerability to GPS disruption could increase.

³ ~~(U)~~ 47 U.S.C. § 302a(b).

⁴ ~~(U)~~ 47 C.F.R. § 2.803(g).


▪ ~~(U)~~ **Transportation Systems Sector:**

- ~~(U//FOUO)~~ It is unlikely that a single GPS disruption incident would lead to long-term, widespread degradation or outage of services for all transportation modes.
- ~~(U//FOUO)~~ However, a GPS disruption incident will have long-term implications for the Transportation Systems Sector as operations become more dependent on GPS. Prudent system engineering will result in the development of appropriate architectures that do not rely overly on GPS for PNT by providing alternate non-GPS-dependent means.
- ~~(U//FOUO)~~ Disruption would typically result in degradation, not outages, in the aviation and maritime modes since alternative navigation methods exist.

~~(U)~~ **Mitigating GPS Disruption Risks**

- ~~(U//FOUO)~~ Detecting, locating, and disabling sources of GPS disruption remain a challenge.
 - ~~(U//FOUO)~~ Often, users will assume equipment error vice GPS disruption, which may further contribute to the duration of a disruption from spoofing or jamming.
 - ~~(U//FOUO)~~ Stationary, continuous, higher power jammers are easier to detect and mitigate against than mobile, intermittent, lower power jammers.
- ~~(U//FOUO)~~ While manual positioning, navigation, and timing (PNT) techniques could be used in some sectors if GPS is disrupted, this will come at a loss in efficiency. Human skills for using these manual techniques could erode due to lack of training and practice as GPS becomes more ubiquitous.
- ~~(U//FOUO)~~ There presently is no adequate nationwide or global backup to GPS for PNT services. There is also no integrated system for locating GPS interference sources. Unfortunately, it may take a major GPS disruption to prompt investment in these types of initiatives.
 - ~~(U//FOUO)~~ Ensuring that receivers are capable of receiving PNT information from other systems in addition to GPS would allow some backup capability.
 - ~~(U//FOUO)~~ Per National Security Presidential Directive (NSPD)-39, the Secretary of Transportation shall, in coordination with the Secretary of Homeland Security, develop, acquire, operate, and maintain backup position, navigation, and timing capabilities that can support critical transportation, homeland security, and other critical civil and commercial infrastructure applications within the United States, in the event of a disruption of the [GPS] or other space-based positioning, navigation, and timing services, consistent with Homeland Security Presidential Directive-7, Critical Infrastructure Identification, Prioritization, and Protection, dated December 17, 2003.

~~(U)~~ **GPS Outlook: 2011–2031**

- ~~(U//FOUO)~~ Presidential Policy Directive 4, the 2010 National Space Policy, states that GPS will continue to be available as a national asset.
- ~~(U//FOUO)~~ The key uncertainties that will drive the future risk posed to critical infrastructure sectors by GPS disruptions include the extent to which: GPS-based applications are knowingly and unknowingly layered into sector operations, the GPS signal is vulnerable to intentional or unintentional disruption, GPS disruption can be identified and mitigated, and alternative PNT systems are available to provide robustness.
- ~~(U//FOUO)~~ The alternative futures driven by these uncertainties could pose challenges for government and the private sector to:
 - ~~(U//FOUO)~~ Keep regulation apace of advances in GPS-enabled technology applications;
 - ~~(U//FOUO)~~ Keep GPS-enabled technology applications consistent with regulations; and
 - ~~(U//FOUO)~~ Demonstrate the need to identify, fund, and implement a GPS backup system or PNT alternatives *before* there is a major disruption of the GPS signal.
- ~~(U//FOUO)~~ The alternative futures also present opportunities for government and the private sector to mitigate GPS disruption risk proactively by:
 - ~~(U//FOUO)~~ Identifying, funding, and implementing a GPS backup system or PNT alternatives;
 - ~~(U//FOUO)~~ Developing and populating a single repository to capture information on GPS disruption incidents across the United States;
 - ~~(U//FOUO)~~ Promoting GPS program improvements like signal diversity, signal robustness, signal integrity monitoring, and user notifications of degradation;
 - ~~(U//FOUO)~~ Implementing regulations and tools to enforce technology controls on GPS interference devices and to detect, respond to, and negate interference;
 -  (b)(7)e, (b)(7)f
 - ~~(U//FOUO)~~ Conducting training and exercises to broaden awareness of GPS vulnerabilities and to prepare for continuity of operations during GPS disruption incidents.

~~(U)~~ Chapter 2. Purpose

~~(U//FOUO)~~ The DHS Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) developed the NRE series to provide authoritative, coordinated, risk-informed assessments of key security issues for the Nation's infrastructure protection community. This NRE responds to a request from the National Executive Committee for Space-Based Positioning, Navigation, and Timing (EXCOM) to complete a comprehensive risk assessment for civil uses of GPS by September 2011 that will inform executive-level decisions. The NRE focuses on analysis of the short- and long-term risks to U.S. critical infrastructure sectors that use GPS and its augmentations to support or fulfill essential missions. For the purpose of this NRE, the term *sector* refers to a logical collection of assets, systems, companies, or networks that provide a common function to the economy, government, or society

~~(U//FOUO)~~ HITRAC integrates the infrastructure analysis capabilities of the Office of Intelligence and Analysis (I&A) and IP, providing all-hazard, risk-informed analysis for Federal, State, local, tribal, territorial, private sector, and international partners. HITRAC strives to identify timely and relevant risks *before* they become critical. Early warning maximizes the number of risk management options available to partners and reduces costs. HITRAC analyzes current, evolving, and future risks through formal assessments and then works with partners to identify effective risk management strategies. The NRE is one of several HITRAC all-hazard product lines targeted at the proactive identification and management of risks.

~~(U)~~ Chapter 3. Scope

~~(U//FOUO)~~ This NRE considers disruptions to civil GPS services in the United States, the risks such disruptions pose to missions fulfilled by U.S. critical infrastructure sectors, and the resulting nationally significant impact to those missions and related government and civil dependencies on U.S. critical infrastructure.

~~(U//FOUO)~~ This NRE provides a current estimate of risks to U.S. critical infrastructure sectors that use GPS-derived PNT (GPS PNT). In addition, the NRE assesses how these risks are estimated to evolve over the next 20 years, developing an outlook based on an estimate of current and projected future risks. Excepting a brief statement on page 19, the information cut-off date for this document was July 31, 2011.

~~(U)~~ GPS provides service to military and civilian users. The civilian service is freely available to all users on a continuous, worldwide basis, and the civilian user segment includes GPS receiver equipment, which receives the signals from the GPS satellites and uses the transmitted information to calculate the user's three-dimensional position, velocity, and time. In addition, GPS service includes augmentations that aid GPS by providing accuracy, integrity, reliability, availability, or any other improvement to PNT that is not inherently part of GPS itself. Augmentation examples include federally operated systems, such as the Nationwide Differential GPS System, the Wide Area Augmentation System (WAAS), and Continuously Operating

Reference Stations (CORS), among others, as well as commercial, site-specific, and global augmentation systems.⁵

~~(U//FOUO)~~ Existing studies already assess risks to military-related PNT systems. Therefore, this NRE assesses GPS and its augmentations and their intersection with critical infrastructure sectors—an area where less comprehensive risk assessments have been conducted to date. In particular, this NRE focuses on GPS disruptions—stemming from naturally occurring events, intentional disruptions, and unintentional disruptions—that impact current and planned evolutions of U.S. critical infrastructure, including effects on our Nation’s economic security.

~~(U//FOUO)~~ The four critical infrastructure sectors highlighted in this NRE are Communications, Emergency Services, Energy, and Transportation Systems. These sectors use GPS PNT particularly to fulfill or support core missions, and they provide an appropriate cross-section of potential risks and impacts to apply broadly to the other sectors. For example, by addressing these sectors’ use of various Information Technology (IT) systems that use GPS and its augmentations, the NRE covers the critical role time and frequency play in IT functionality. Thus, the report intrinsically considers elements of the IT Sector that cut across sectors (e.g., those supporting Internet service). HITRAC coordinated the NRE with Sector-Specific Agencies (SSAs) to identify and focus on the portions of each highlighted sector that are most reliant on GPS and its augmentations.

~~(U)~~ Examples of Sector-Specific GPS Usage

~~(U)~~ The **Communications Sector** depends heavily on the timing function of GPS. Many communications components use GPS timing signals to keep their internal clocks accurate and synchronized through continuous reference to those signals. Within the Sector, GPS timing is used by wireline, wireless, satellite, cable, and broadcast networks.

~~(U)~~ The **Emergency Services Sector** relies heavily on communications that are dependent on GPS timing. This includes radios or other equipment used for dispatching first responders, as well as communications between those responders, position and navigation features from computer-aided dispatch, managing fleet vehicles, and locating accidents and stolen vehicles.

~~(U)~~ The **Energy Sector** uses GPS for monitoring—electrical power line frequency stability and malfunctions in transmission networks, for example—and for synchronizing services across networks and power grids. Subsectors also use GPS in the exploration of land and ocean resources and for location/orientation in oil and gas drilling.

~~(U)~~ The *aviation mode* of the **Transportation Systems Sector** uses GPS for various types of navigation, air traffic control, and Automatic Dependent Surveillance, a component of NextGen. The *maritime mode* uses GPS for navigation, vessel command and control, vessel and cargo container tracking and reporting, and operation salvaging. High-traffic ports use GPS for safety and situational awareness. The *surface modes* rely on GPS for shipment tracking, real-time routing, real-time traffic control and data collection, synchronizing rail inspection systems, and managing real-time train departures and arrivals.

~~(U//FOUO)~~ Some areas are beyond the scope of this document. In particular, *the NRE does not address disruptive threats from outside the United States*, but we recognize their importance and that many sectors operate outside U.S. borders. We also note that some devices made outside the United States pose a threat. So, while we do not address sectors outside the United States, we do evaluate the domestic proliferation of equipment made outside our borders. In addition, we recognize that the implications of a domestic GPS disruption could have a global reach given the increasingly globalized nature of some critical infrastructure sectors, like

⁵ ~~(U)~~ GPS.gov Web page, “Augmentation Systems,” www.gps.gov/systems/augmentations/, accessed January 2011. Note: other GPS augmentations exist and are planned that are not governed under 10 U.S.C. 2281, which defines GPS.

Transportation Systems. Similarly, a disruption of PNT services abroad could have adverse implications for domestic critical infrastructure operations.

~~(U//FOUO)~~ While the NRE does consider the role of the satellite constellation in supporting GPS services, it does not focus specifically on risks to these satellites. In lieu of discussing how disruptions impact specific Federal GPS users (e.g., scientific, weather, remote sensing), the NRE uses SME input to discuss generic government and nongovernment user missions (e.g., law enforcement operations susceptible to GPS disruption that apply beyond one particular agency). Finally, HITRAC did not conduct hardware testing for the NRE.

~~(U//FOUO)~~ Data supporting the NRE was drawn from available government, academic, and private sector reporting and analysis as well as the judgments of subject matter experts (SMEs).

~~(U//FOUO)~~ The NRE addresses the following overarching questions:

- 1) ~~(U//FOUO)~~ What risks to missions fulfilled by U.S. critical infrastructure sectors do disruptions in GPS PNT systems present?
- 2) ~~(U//FOUO)~~ How are these risks estimated to evolve over the next 20 years?
- 3) ~~(U//FOUO)~~ What are the current and projected future capabilities of critical infrastructure sectors to mitigate mission disruption risks caused by GPS PNT outages?

~~(U)~~ Chapter 4. Underlying Analytic Assumptions

~~(U//FOUO)~~ The following assumptions guided the analysis underpinning this NRE:

- ~~(U)~~ GPS PNT has three core functions: (1) positioning, (2) navigation, and (3) timing. Critical infrastructure sectors use these functions in various ways to support or fulfill their missions.
 - ~~(U)~~ Positioning is the ability to accurately and precisely determine one's location and orientation two dimensionally (or three dimensionally when required) referenced to a standard geodetic system (such as World Geodetic System 1984).⁶
 - ~~(U)~~ Navigation is the ability to determine current and desired position (relative or absolute) and apply corrections to course, orientation, and speed to attain a desired position anywhere around the world, from subsurface to surface and from surface to space.⁷
 - ~~(U)~~ Timing is the ability to acquire and maintain accurate and precise time and frequency from a time standard such as Coordinated Universal Time (UTC) anywhere in the world and within user-defined timeliness parameters.⁸ Timing includes time transfer.⁹ UTC is used for telecommunications, network synchronization, secure military communications, bank transactions, power grids, and transportation systems.¹⁰ There is a growing need in sectors for accurate Time and Frequency services to operate more efficiently and to maintain safety and security.¹¹
- ~~(U//FOUO)~~ U.S. critical infrastructure sectors will continue to rely on GPS PNT to support or fulfill their missions.
- ~~(U//FOUO)~~ A current satellite constellation provides GPS. The NRE does not address intentional risks to the satellites and operational command centers (e.g., anti-satellite missiles or physical attacks).
- ~~(U//FOUO)~~ There will continue to be natural, intentional, and unintentional threats or hazards that could disrupt GPS PNT.
- ~~(U//FOUO)~~ Effective risk management may mitigate some aspects of GPS PNT-related risks to U.S. critical infrastructure sectors.

⁶ ~~(U)~~ National Executive Committee for Space-Based PNT Web page, "What is PNT," www.pnt.gov/101/, accessed January 2011.

⁷ ~~(U)~~ Ibid.

⁸ ~~(U)~~ Time is the key element of GPS that allows determination of position. One nanosecond in error produces one foot of position error. GPS delivers 30 nanoseconds of precision.

⁹ ~~(U)~~ National Executive Committee for Space-Based PNT Web page, "What is PNT," www.pnt.gov/101/, accessed January 2011.

¹⁰ ~~(U)~~ U.S. Department of Defense, *Global Positioning System (GPS) 2008 A Report to Congress*, Washington, D.C.: October 31, 2008.

¹¹ ~~(U)~~ GPS Timing Criticality Update: Final Report.

Summary of NRE Development Approach

~~(U)~~ The findings of this NRE are informed by a comprehensive literature review and input from U.S. government and private SMEs elicited through formal analyses. Moreover, a formal analytic process supports the identification of GPS disruption risk trends within and across critical infrastructure sectors. Inherently, a level of uncertainty is associated with the assessments provided within this NRE because of uncertainties with the frequency of occurrence of various types of GPS disruptions.

~~(U//FOUO)~~ The NRE development process consisted of three phases: estimate, outlook, and integration. More detailed descriptions of the analytic methodologies used in the estimate and outlook phases can be found in Annexes C and D.

~~(U//FOUO)~~ The **estimate phase** included a comprehensive literature review, development of a Terms of Reference document, consultation with an NRE Advisory Group comprising senior government experts, and preliminary coordination with SMEs to identify scenarios leading to GPS disruptions of various magnitude and severity. HITRAC conducted data calls and workshops to elicit SME input in a structured manner on the likelihood of these scenarios and their mission disruption consequences for each highlighted critical infrastructure sector. Mission disruption consequences were considered as a function of *time* and *severity*.

- ~~(U//FOUO)~~ **Time** is the expected length of service disruption.
- ~~(U//FOUO)~~ **Severity** is the extent of the harm caused by the disruption to the service.

~~(U//FOUO)~~ The **outlook phase** involved consultation with SMEs during alternative futures development workshops to identify the key strategic uncertainties that could define future risks of GPS disruptions over the next 20 years as well as the milestones and indicators that alternative futures are unfolding. The methodology underpinning the alternative futures development was drawn from a 2008 U.S. National Intelligence Council *Disruptive Civil Technologies* report.¹²

~~(U//FOUO)~~ The **integration phase** involved an interagency effort to review the NRE for soundness, consistency, and accuracy. This phase helped identify key GPS disruption risk trends visible from research and workshop results as well as potential risk mitigation strategies that could be adopted by the public or private sectors.

¹² ~~(U)~~ U.S. National Intelligence Council, *Disruptive Civil Technologies – Conference Report*, 2008, www.dni.gov/nic/confreports_disruptive_tech.html, accessed on 24 July 2010..

~~(U)~~ Chapter 5. Current Risk to Missions of Critical Infrastructure Sectors from Disruption in GPS PNT Systems

~~(U)~~ This chapter identifies the categories of GPS PNT disruptions, presents the disruption scenarios developed for the NRE, presents the assessment of likelihood of these scenarios, and presents the highest risk scenarios and highest mission disruption consequence scenarios for each highlighted critical infrastructure sector.

~~(U)~~ 5.1 Categories of GPS PNT Disruption

~~(U)~~ GPS PNT disruptions can be caused by a variety of naturally occurring events, intentional attacks, and unintentional incidents.

~~(U)~~ **Naturally occurring events** that can disrupt PNT-supporting satellites include space weather events like geomagnetic storms, ionospheric disturbances, and other effects of solar activity. Environmental or other weather conditions on the ground can impede the monitoring and tracking capabilities of Global Navigation Satellite System (GNSS) positioning services.¹³

~~(U)~~ **Unintentional disruptions** may occur from malfunctions or accidents due to aging GPS constellation issues,¹⁴ space debris hitting satellites, errors by GPS constellation operators, defective software,¹⁵ and failures in uplink stations,¹⁶ among other causes.

~~(U)~~ Still other disruptions may result from Federal and non-Federal radio communications systems operating in close frequency or geographic proximity to a GPS receiver.¹⁷ GPS synchronizers, for example, employ GPS timing receivers and are vulnerable to radio frequency interference. This interference disturbs the timing receiver's performance and degrades its solution.¹⁸ In the Communications Sector, for example, this degraded synchronization could lead to poor quality of service and traffic handling capability as well as reduction of network key performance indicators (such as call setup success rate and drop call rate). Other types of GPS receivers used in positioning and navigation may be vulnerable to unintentional disruptions as well (e.g., portable navigation devices and wireless handsets). Given the volume of portable and mobile devices with GPS capability and the lack of industry receiver standards in some sectors, the potential for unintentional disruptions has increased. However, for some sectors, such as Transportation Systems (aviation), there are national and international standards for receivers and services, and the equipment used generally meets or exceeds those standards.

~~(U//FOUO)~~ **Intentional disruptions** typically involve the use of transmitters to intercept or interfere with GNSS signals. They may also involve an attack against the hardware involved in

¹³ (U) Salmi, Pekka, and Marko T. Torkkeli, "Inventions Utilizing Satellite Navigation Systems in the Railway Industry," *Journal of Technology Management & Innovation* 4(3)(2009): pp. 46–58..

¹⁴ (U) U.S. Department of Defense, *Global Positioning System (GPS) 2008 A Report to Congress*, Washington, D.C.: October 31, 2008.

¹⁵ (U) Comment by FCC: GPSOC software uploads to satellites may make certain models of GPS misbehave, due to the way the coding is implemented by different receiver manufacturers. Such malfunctions have happened (at a frequency of about one time/year) where one instance had a fairly large impact.

¹⁶ (U) Lilley, Robert, Gary Church, and Michael Harrison, "GPS Backup for Position, Navigation and Timing: Transition Strategy for Navigation and Surveillance," Washington, D.C.: Federal Aviation Administration, August 22, 2006.

¹⁷ (U) Association Internationale de Signalisation Maritime, "Recommendation on GNSS Vulnerability and Mitigation Measures," Saint Germain en Laye, France, December 2004.

¹⁸ (U) Khan, Faisal Ahmed and Andrew G. Dempster, "Effects on CDMA Network Performance due to Degradation of GPS based Synchronization," *Communications and Information Technologies, ISCIT 2007* (2007): pp. 517–520.

GPS signaling. The use of high-intensity radiated RF energy to disrupt equipment constitutes one form of such attack. Some interference to GPS PNT signals may come in the form of controlled experiments (e.g., electronic attack [EA] operations to test, train, and exercise in a PNT-disrupted environment). In this case, the risk of consequential disruptions to the desired GPS service within of the area of EA operations is minimized because prior warning is provided to relevant agencies and pilots in advance of the tests. Nevertheless, planned EA testing occasionally causes interference to GPS based flight operations, and impacts the efficiency and economy of some aviation operations (some operators will not plan to use efficient GPS based procedures within the confines of a planned GPS test area). Other intentional disruptions to GPS PNT signals occur when individuals attempt to interfere with GPS signals on a local level, such as with personal protection devices¹⁹ (PPDs), small, inexpensive GPS jammers used to avoid being tracked. These jammers can cause local GPS disruption. The users of such devices likely do not understand the broader potential consequences of operating the device nor intend to disrupt critical infrastructure.

~~(U//FOUO)~~ The most common types of intentional GPS signal disruption are jamming and spoofing:

- ~~(U//FOUO)~~ **Jamming** prevents a receiver from tracking GPS signals.²⁰ Attacks involving jamming signals can be air-, land-, or water-based. Relatively low-cost jamming devices are small, affordable, and easy to use.²¹ High-power jamming devices are available on the international arms market.²² Locating and mitigating the sources of GPS jamming remain a challenge.²³ This challenge is due to the absence of laws that allow quick mitigation by government authorities and insufficient legal penalties to dissuade use of jamming devices.
- ~~(U//FOUO)~~ **Spoofing** is the surreptitious replacement of a true satellite signal with a manipulated counterfeit signal. A GPS receiver is fooled into accepting counterfeit GPS signals and generates erroneous and potentially hazardous information. A spoofing attack generally involves more sophisticated equipment than a jamming attack. Unsophisticated spoofers are widely available in the form of legitimate GPS signal generators. Portable receiver-spoofers, while not commercially available, can be constructed from commercial off-the-shelf components.²⁴ These devices can produce counterfeit signals and take control of a target's tracking channels using power levels that are much lower than those used for jamming, making such an attack more difficult to detect. The use of multiple receiver-spoofers can make an attack more consequential and difficult to detect. To defend against a spoofing attack, cryptographic authentication of civil GPS signals could be combined with other receiver-autonomous techniques.

¹⁹ (U) PPDs are also commonly referred to as "personal privacy devices."

²⁰ (U) Los Alamos National Laboratory, "A Simple Demonstration that the Global Positioning System (GPS) is Vulnerable to Spoofing," *The Journal of Security Administration* 25(2002): pp. 19–28.

²¹ (U) National PNT Advisory Board Comments On Jamming the GPS – A National Security Threat, November 4, 2010, by the National PNT Advisory Board.

²² (U) Defense Science Board Task Force, *The Future of the Global Positioning System*, Washington, D.C.: U.S. Department of Defense, October 2005.

²³ (U) National PNT Advisory Board Comments On Jamming the GPS – A National Security Threat, November 4, 2010, by the National PNT Advisory Board.

²⁴ (U) Humphreys, Todd E., Brent L. Ledvina, Paul M. Kintner, Mark L. Psiaki, and Brady O'Hanlon, "Assessing the Spoofing Threat," *GPS World* (January 1, 2009).

However, current civil GPS signals are not cryptographically secured. Moreover, current and proposed GPS signal interface specifications show no plans for adding such security. In contrast, the forthcoming European Galileo satellite navigation system will include a provision for cryptographic civil signal authentication.

~~(U)~~ 5.2 GPS Spectrum Encroachment

~~(U)~~ GPS operates in several Radionavigation Satellite System (RNSS) (space-to-earth) frequency allocations, including 1575 MHz (L1), 1227 MHz (L2C), and 1176 MHz (L5), which are dedicated to GPS and similar GNSS signals. When received, GPS is an extremely low-power spread-spectrum signal that has to be pulled from beneath the radio frequency noise floor to be processed by users. In addition, its signal characteristics rely more on reception timing comparisons than on data content to deliver required precision. GPS performance requires the full spectral content of the GPS signal to enable precise tracking when GPS message bits change. As a result, the GPS signal is at risk from interference should a high-power ground-based network operate in an adjacent bandwidth. While GPS can coexist with some radio frequency systems such as low-duty cycle-pulsed radars, it cannot coexist with continuously transmitting communications systems that raise the noise floor or otherwise corrupt the quality of the incoming GPS data.

~~(U)~~ In many cases, GPS shares the spectrum in which it operates with other types of users. These non-GPS operations could either be similar to GPS or a completely different type of service, such as radars at 1215-1240 MHz, and interference from such sources is called in-band interference. In addition, GPS operations may be impacted by other users of the spectrum that are not operating in the same bands as GPS but are operating near GPS bands, and interference from these sources is called out-of-band interference. For both in-band and out-of-band interference, GPS operations may be effected based on electromagnetic interference.

~~(U)~~ Electromagnetic interference can be caused by a number of factors, including:

- ~~(U)~~ A new operation being introduced in or near a GPS band that is not compatible with GPS;
- ~~(U)~~ GPS being implemented in an RNSS band in which it is not compatible with the existing allocations;
- ~~(U)~~ A service designed to be GPS compatible changing in a way that makes it incompatible with GPS; or
- ~~(U)~~ GPS changing the way it uses the signal such that an operation that did not originally interfere with GPS then becomes an interference problem.

~~(U)~~ Over the past decade, GPS has faced threats from other systems operating in the same or adjacent radio frequency bandwidth or spectrum.²⁵ Spectrum is a finite resource, and demand for spectrum is growing. The only way to accommodate increased spectrum requirements is to reduce guard bands via very precise filtering or to repurpose spectrum from a previously

²⁵ ~~(U)~~ Lazar, Steven, et al. "GPS Spectrum: Sharing or Encroachment?" *GPS World*, September 2000.

intended service. The Federal Communications Commission (FCC) must approve any commercial use of bandwidth in the United States and typically requires users of nearby spectrum to conduct testing and demonstrate that their networks will not interfere with the GPS signal.²⁶

~~(U)~~ Two examples below illustrate cases of industry seeking to repurpose spectrum to accommodate new technologies:

- ~~(U)~~ In 2000, Ultra Wide Band (UWB) was proposed as a form of wireless communications technology that fused three technologies: wireless, radar, and positioning. Testing showed that the UWB raised the noise floor across the full L-Band spectrum and disrupted GPS services, including those used by the aviation mode. Development and deployment did not proceed.²⁷
- ~~(U)~~ In 2010, LightSquared proposed a plan to build a wireless broadband network that would operate at higher power (1525MHz to 1559MHz) next to the Aeronautical Radio Navigation Service (ARNS) band (1559MHz to 1610Mhz), which includes GPS L-1 service. Testing has shown interference to GPS services used by critical infrastructure sectors, including Communications,²⁸ Emergency Services,²⁹ and Transportation Systems.³⁰ By Public Notice dated February 15, 2012, the FCC sought comments on a National Telecommunications and Information Administration (NTIA) letter—concluding there was no practical way, at that time, to mitigate potential interference to GPS caused by LightSquared’s proposed terrestrial service—and a proposal to vacate LightSquared’s authorization to provide ancillary terrestrial service.³¹ In late February 2012, the FCC Chief, International Bureau, granted a request, in part, for an extension of time to file comments, giving LightSquared until March 30, 2012, to file comments. The FCC received comments on the February 15, 2012, Public Notice. As of June 2012, the matter remained pending and the option to vacate the waiver was still under consideration by the FCC.

~~(U)~~ Potential in-band and out-of-band interference to GPS receivers, regardless of the frequency band, is determined by the interfering signal and the design of the GPS receiver. The newer the operations packed into bands allocated to or adjacent to RNSS, the greater the potential for interference to GPS. In addition, the more creative GPS receiver designs become to take advantage of the GPS signals—e.g., using wider receiver bandwidths—the more potential there is for interference to the receivers exists. The effects of spectrum encroachment near the GPS signal could be mitigated in the long term by modifying GPS receivers or in the short term by

²⁶ (U) Thomas, Keir. “Is GPS About to be Broken?” *PC World*. Accessed March 20, 2011.

http://www.pcworld.com/businesscenter/article/221853/is_gps_about_to_be_broken.html

²⁷ (U) Luo, Ming, et al. “Testing and Research on Interference to GPS from UWB Transmitters,” 2001.

<http://waas.stanford.edu/~www/papers/gps/PDF/mingion01.pdf>

²⁸ (U) Berwin, Bob. “LightSquared cell network knocks our first responders’ GPS in tests,” NextGov.com. May 20, 2011.

http://www.nextgov.com/nextgov/ng_20110520_9569.php?oref=topstory

²⁹ (U) *Final Report of the Working Group Established by the FCC to Study Overload/Desensitization Interference on GPS Receivers and GPS-Dependent Applications from LightSquared Terrestrial Broadband Operations*. July 30, 2011. Accessed August 3, 2011.

<http://fjallfoss.fcc.gov/ecfs/document/view?id=7021690471> p.15.

³⁰ (U) Joel Szabat. Letter to Associate Administrator Karl Nebbia, National Telecommunications and Information Administration, Appendix A. July 21, 2011.

³¹ (U) “Spokesperson Statement on NTIA Letter—LightSquared and GPS.” February 14, 2012. <http://www.fcc.gov/document/spokesperson-statement-ntia-letter-lightsquared-and-gps>, accessed March 29, 2012.

additional filtering to GPS user equipment, strengthening the GPS signal, or using antennas to suppress ground-based signals.³² Modifying GPS receivers is likely to take at least 10 years, and short-term mitigations are limited and provide a lower level of service than needed, particularly for high-precision applications.³³

~~(U)~~ 5.3 GPS Disruption Scenarios

~~(U//FOUO)~~ Per the 2010 DHS Risk Lexicon,³⁴ we define “scenario” as the hypothetical situation comprising a hazard, an entity impacted by that hazard, and associated conditions, including consequences when appropriate. For the scenarios examined in this NRE, the hazard varies, and we define the “entity” and “associated conditions” as follows:

- ~~(U//FOUO)~~ The entities for each scenario are the same: four critical infrastructure sectors—Communications, Emergency Services, Energy, and Transportation Systems. We addressed each sector individually during a series of consequence workshops. In these workshops, we assessed how each sector uses GPS and would be impacted by varying GPS disruptions.
- ~~(U//FOUO)~~ Associated conditions for each scenario include the location. For our purposes, these scenarios take place in a notional metropolitan city. This notional city has an international airport less than two km from a major highway. In addition, regular private and commercial maritime traffic traverses city waterways and ports. Other conditions (e.g., the spatial extent to which a GPS disruption is experienced) are noted clearly for each scenario.

~~(U//FOUO)~~ A comprehensive set of GPS disruption scenarios was developed through a literature review and consultations with more than 30 SMEs who participated in two teleconferences during February 2011. Eight of those scenarios were selected for inclusion in the NRE and allowed for a wide variety of disruption types to be explored:

- ~~(U//FOUO)~~ **Scenario A:** A stationary interference source is causing continuous unintentional disruption. Ground receivers within a 30-km ground-to-ground (GTG) radius are affected, and airborne receivers within radio line-of-sight (radio LOS) are affected.
- ~~(U//FOUO)~~ **Scenario B:** Continuous jamming disruption from a single low-power, stationary jammer. GPS receiver tracking is affected within a 500-m GTG radius and a 20-km radio LOS radius. GPS receiver acquisition is affected within an 800-m GTG radius and a 30-km radio LOS radius.
- ~~(U//FOUO)~~ **Scenario C:** Continuous jamming disruption from a single high-power, stationary jammer (e.g., mounted on a tall building or hilltop). GPS receiver tracking is affected within a three-km GTG radius and a 230-km radio LOS radius. GPS receiver acquisition is affected within a four-km GTG radius and a 350-km radio LOS radius.

³² (U) National Space-Based Positioning, Navigation and Timing Systems Engineering Forum (NPEF). *Assessment of LightSquared Terrestrial Broadband System Effects on GPS Receivers and GPS-dependent Applications*, June 14, 2011. p. 9.

³³ (U) Ibid., pp. 9-10.

³⁴ (U) The DHS Risk Lexicon can be found at <http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf>.

- ~~(U//FOUO)~~ **Scenario D:** Jamming disruption from multiple low-power jammers on the ground. The jammers are stationary and mobile, with some continuous and others intermittently active. Pockets of intermittent tracking and acquisition disruption occur across the metropolitan area.
- ~~(U//FOUO)~~ **Scenario E:** Continent-scale natural disruption caused by a severe geomagnetic storm (G4 or higher). Tracking threshold of GPS is reduced significantly.
- ~~(U//FOUO)~~ **Scenario F:** Continuous pinpoint spoofing attack against a single target receiver. The spoofer walks off the time and position reported by the target receiver without raising alarms.
- ~~(U//FOUO)~~ **Scenario G:** Sophisticated, coordinated, continuous pinpoint spoofing attacks against multiple target receivers (one spoofer per targeted receiver). Each spoofer independently walks off the time and position reported by its target receiver without raising alarms.
- ~~(U//FOUO)~~ **Scenario H:** Continuous attack whereby a strategically placed high-power transmitter generates GPS-like spoofing signals after an initial interval (several minutes) of jamming. Receivers within a three-km GTG radius and a 230-km radio LOS radius report a confident timing and position fix, but the timing is wrong by up to hundreds of microseconds and the position fix is wrong by up to tens of kilometers.

~~(U)~~ ***Scenario Assumptions***

~~(U//FOUO)~~ The following assumptions were considered by SMEs when evaluating the disruption scenarios.

- ~~(U//FOUO)~~ The technology required to cause these disruptions is not expensive or military-grade equipment. Rather, these hazards consider primarily low-cost, commercial equipment that is accessible, either in the United States or purchased overseas.
- ~~(U//FOUO)~~ Each scenario takes place in a status quo environment. That is, any redundancies or backup capabilities exist as they are today.
- ~~(U//FOUO)~~ The power levels of the devices lead to the spatial extent described as the impacted area, and ground-to-ground disruptions will depend on varying terrain and antenna heights.

~~(U)~~ 5.4 Assessment of Likelihood of GPS PNT Disruption Scenarios

~~(U)~~ Summary of Approach

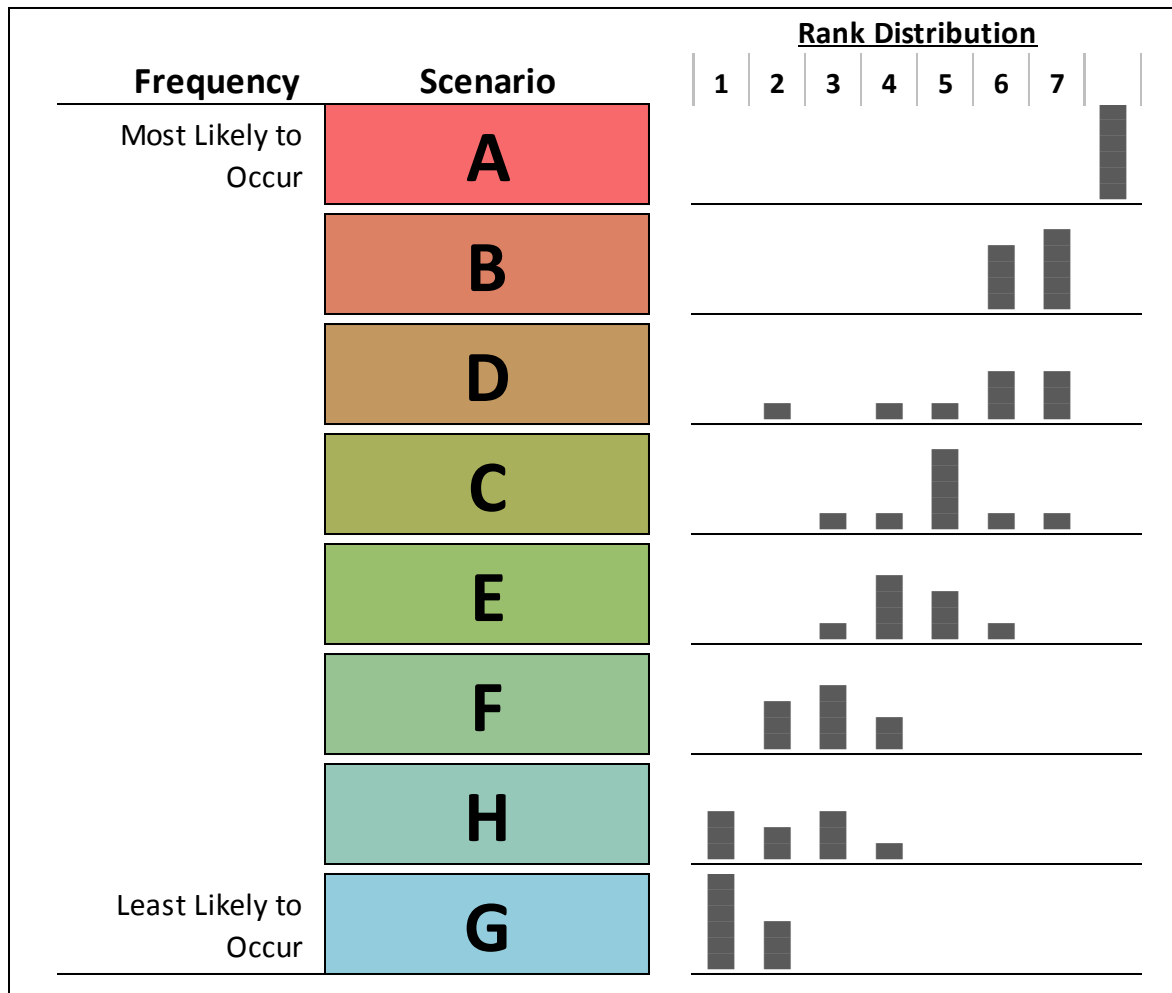
~~(U//FOUO)~~ HITRAC held a workshop on May 6, 2011, to discuss and assess the likelihood of occurrence for the eight GPS PNT disruption scenarios. SMEs first developed a rank order of scenarios based on the relative frequency of occurrence of GPS disruptions associated with each scenario. After reaching a consensus relative ranking for the scenarios, SMEs estimated the frequency of occurrence of the GPS disruptions for each scenario.

~~(U)~~ Summary of Findings

~~(U//FOUO)~~ There was an overall trend in the scenario rankings, with those scenarios that involved jamming disruptions to GPS placing higher (more frequently occurring) in the rank order than those scenarios that involved spoofing. Jamming is far easier to accomplish, and takes less skill and expertise, than spoofing, and jamming can often be an unintentional consequence of other actions or devices. In addition, there is more historical data on jamming occurrences (both intentional and unintentional) than for the other GPS disruption scenarios. SMEs noted that the absence of accurate data about incidents of GPS disruption made it challenging to estimate the likelihood of these scenarios. In many instances, users of GPS may attribute signal disruption to equipment failure and, therefore, not report to authorities what could be actual instances of jamming or spoofing.

~~(U)~~ Rank Order and Frequency

~~(U//FOUO)~~ SMEs ranked the eight scenarios in relative order of their likelihood to occur, with a score of eight being the scenario most likely to occur and one being the least likely. After the eight scenarios were ranked using a consensus based on the individual rankings (see Figure 5-1), SMEs estimated how often they believed each scenario would occur and provided numerical estimates for both minimum and maximum occurrences per year. The results of the rank order are below.



(U//FOUO) Figure 5-1: Relative likelihood of occurrence for all scenarios

(U//FOUO) **Scenario A:** *An interference source is causing unintentional disruption. Ground receivers within a 30-km GTG radius are affected, and airborne receivers within radio LOS are affected.*

(U//FOUO) All SMEs rated this scenario an eight and agreed that it is the most likely to occur. Two reasons were cited most often for this high ranking. First, there are many types of devices not intended for jamming that can, under the correct circumstances, become “accidental jammers.” These include active TV antennas with preamplifiers that can radiate harmonics and are in-band to GPS, and old or malfunctioning microwave systems. An example of an accidental jamming incident is provided in the text box below. The second cause for the high frequency of this scenario is accidental jamming from authorized or licensed users of jamming technology. For instance, there are facilities—such as doctors’ offices, hospitals, schools, courthouses, prisons—that employ types of radio-frequency disruption devices that, while not specifically aimed at GPS frequencies, can radiate harmonics that disrupt GPS signals.

~~(U//FOUO)~~ Some SMEs cautioned that this scenario's high frequency ranking is not an indication of high risk or impact to critical infrastructure. While situations such as this may occur frequently, they are generally minor and localized.

~~(U)~~ Moss Landing Jamming Incident 2001

~~(U)~~ In April 2001, the captain of the research vessel PT SUR reported that GPS in Northern California's Moss Landing Harbor was jammed.¹ The captain was told to contact the Coast Guard and the Federal Communications Commission. Both agencies made attempts to locate the source of the interference; however, by May 2001 the problem still persisted.²

~~(U)~~ Moss Landing Harbor is a medium-sized harbor in the middle of Monterey Bay, 100 kilometers from San Francisco. The Monterey Bay Aquarium Research Institute (MBARI) and Naval Postgraduate School (NPS) both maintain facilities in or near Monterey Bay. MBARI and NPS had a differential GPS station on Moss Landing, and both had been early adopters of GPS precision location data for vessels in the harbor.³ A group of MBARI and NPS faculty analyzed the jamming and determined that the Moss Landing area was being heavily jammed, and multiple reports confirmed that the jamming was not related to receivers.⁴

~~(U)~~ During the time that the GPS signal was jammed, MBARI lost its time reference and ships using the harbor were forced to rely on radar instead of GPS, which proved challenging especially during times of thick fog.⁵ Other smaller boat owners attempted to fix the problem by buying new or additional GPS receivers but found that the equipment was still jammed in the Moss Landing area.⁵

~~(U)~~ A group of MBARI and NPS faculty coordinated an attempt to identify the location of the GPS interference by driving around the bay and recording the peaks of the radio frequency interference (RFI) signal. Once peak interference areas were determined, the group asked individual boat owners to turn their power off and measured the interference again. The team found that two VHF/UHF television antennas with built-in preamplifiers were causing the majority of the interference.⁶ These antennas, which were powered even when the television onboard was not on, were emitting a signal that jammed GPS in the entire Moss Harbor area up to one mile out to sea. A third source, also a VHF/UHF antenna, was involved in the interference as well, but because the antennas were temperature sensitive it was not located until fall 2001.⁷

¹ (U) Berstis, Knute A., "Technologies of Interest to Surveyors in 2025," National Coordination Office for Space Based PNT. October 16, 2010.

² (U) Vincent, Wilber R., Richard W. Adler, Paul McGill, James R. Clynych, George Badger, Andrew A. Parker, "The Hunt for RFI," *GPS World*. January 1, 2003, http://www.gpsworld.com/gnss-system/signal-processing/the-hunt-rfi-776?page_id=2, accessed July 6, 2010.

³ (U) Ibid.

⁴ (U) Ibid.

⁵ (U) Ibid.

⁶ (U) Ibid.

⁷ (U) Berstis, Knute A., "Technologies of Interest to Surveyors in 2025," National Coordination Office for Space Based PNT. October 16, 2010.

~~(U//FOUO)~~ **Scenario B: Jamming disruption from a single low-power stationary jammer. GPS receiver tracking is affected within a 500-m GTG radius and a 20-km LOS radius. GPS receiver acquisition is affected within an 800-m GTG radius and 30-km LOS radius.**

~~(U//FOUO)~~ The consensus ranking for this scenario was seven. As with some instances within Scenario A, many SMEs ranked this scenario high because of historical cases of intentional, authorized jammers having unintended consequences. SMEs also believed this scenario would have a high rank because the kind of low-power jammer in this scenario is a relatively easy, low-

cost jammer for individuals to build or buy. However, as with Scenario A, frequency does not imply the degree of impact.

~~(U//FOUO)~~ ***Scenario D: Jamming disruption from multiple low-power jammers on the ground. The jammers are stationary and mobile, with some intermittently active. Pockets of intermittent tracking and acquisition disruption occur across the metropolitan area.***

~~(U//FOUO)~~ Although the consensus ranking for this scenario was six, a majority of SMEs were evenly split between six and seven, and the remaining SMEs gave rankings of two, four, and five. The relatively high consensus ranking is based on the increase in commercially available jammers, the ease of acquiring them (such as through the Internet), and their falling cost.

~~(U//FOUO)~~ The SME from the FAA noted that in the near term, possibly within the next 12 to 24 months, this sort of scenario could become the most frequently occurring because of the increasing number of mobile jammers and our current lack of mitigation options.³⁵ An example of this type of mobile jammer is provided in the text box below.

³⁵ While the NRE gives estimates on the duration of many of these disruptions, the SMEs noted that the duration of this scenario could be indefinite. As low-power jammers are found and/or shut off, new ones could emerge elsewhere, potentially prolonging disruptions.

~~(U)~~ Personal Protection GPS Jamming Devices

~~(U)~~ In the past two years, the market for personal protection devices (PPD) that can obscure an individual's location data by interfering with GPS and cell phone frequencies has increased markedly. PPDs are widely available on Internet auction sites and are priced as low as \$40.¹ The less expensive PPDs are known as cigarette-lighter jammers because they can be plugged into a car's cigarette lighter—an example is shown below. These jammers generally obscure only the L1 frequency and may only cause problems within a few yards of the device.² However, more expensive PPDs can block multiple GPS frequencies, and some can block cell phone signals as well. These more powerful devices can cause problems with the GPS signal for several miles.³ The use of PPDs within the United States is illegal, but possession is not a crime. PPDs are of particular concern to the law enforcement community. Criminals such as car thieves have used GPS jammers to block satellite signals that some antitheft services use to locate stolen automobiles.⁴



¹ ~~(U)~~ Murfin, Tony, "GNSS Interference: Apparently It's an Issue," *GPS World*, December 15, 2010, <http://www.gpsworld.com/professional-oem/gnss-interference-its-apparently-issue-10850>.

² ~~(U)~~ The National PNT Advisory Board Comments on Jamming the Global Positioning System – A National Security Threat: Recent Events and Potential Cures, November 4, 2010. P. 4.

³ ~~(U)~~ Ibid.

⁴ ~~(U)~~ Sorrel, Charlie. "Car Thieves Use GPS Jammers to Make Clean Getaway." *Wired*. February 24, 2010.

~~(U//FOUO)~~ **Scenario C: Jamming disruption from a single multiple-watt stationary jammer. GPS receiver tracking is affected within a three-km GTG radius and a 230-km LOS radius. GPS receiver acquisition is affected within a four-km GTG radius and a 350-km LOS radius.**

~~(U//FOUO)~~ This scenario received a consensus ranking of five, which was selected by a majority of the SMEs. No other rank received more than a single SME vote. The likelihood ranking for Scenario C was in the middle, reflecting the idea that the threat from this type of jammer—which is easily constructed and concealed—would be relatively easy to locate, lessening the probability of the scenario occurring.

~~(U//FOUO)~~ **Scenario E: Continent-scale natural disruption caused by a severe geomagnetic storm. Tracking threshold of GPS is reduced significantly.**

~~(U//FOUO)~~ The consensus ranking for this scenario was four, putting it in the bottom half of the likelihood rankings. SMEs generally agreed that the effects from a scenario like this are unpredictable, typically short lived, and would target areas locally before passing. In addition,

most degradation could occur in frequencies below those of GPS. A policy workshop from the American Meteorological Institute indicated that the effects of space weather are unpredictable because of differences in receiver standards between various user groups.³⁶

~~(U//FOUO)~~ **Scenario F: Pinpoint spoofing attack against a single target receiver. The spoofer walks off time and position reported by the target receiver without raising alarms.**

~~(U//FOUO)~~ SMEs reached a consensus score of three for this scenario. Although it was ranked near the bottom in terms of likelihood of occurrence, Scenario F was assigned the highest likelihood of the spoofing-related scenarios because it was the simplest. The spoofing scenarios, in general, received low likelihood rankings for various reasons, most notably because spoofing is a sophisticated type of attack that requires a level of skill not needed for jamming. Although schematics and instructions for constructing spoofers are available online, engineering or other technical ability would generally be needed to successfully construct and operate devices.

~~(U//FOUO)~~ **Scenario H: Sophisticated, coordinated “navigation confusion” attack whereby a strategically placed multiple-watt transmitter generates GPS-like signals after an initial interval (several minutes) of jamming. Receivers within a three-km GTG radius and a 230-km LOS radius report a confident timing and position fix, but the timing is wrong by up to hundreds of microseconds and the position fix is wrong by up to tens of kilometers.**

~~(U//FOUO)~~ The consensus ranking for this scenario was two, although individual SME scores ranged from one to four. As with Scenario F, SMEs concurred that this scenario was one of the least likely to occur, relative to the other scenarios, because it involves a sophisticated attack requiring advanced technical skills. One SME pointed out that, although numbers for this type of scenario are low now, they are likely to increase over time as more people acquire the necessary technical skills.

~~(U//FOUO)~~ **Scenario G: Sophisticated, coordinated pinpoint spoofing attacks against multiple target receivers (one spoofer per targeted receiver). Each spoofer independently walks off the time and position without raising alarms.**

~~(U//FOUO)~~ This scenario received a consensus ranking of one, least likely to occur of all eight scenarios. As with other spoofing scenarios, SMEs agreed it was least likely to occur because of the difficulty in constructing and implementing a spoofing device, as well as the high level of complex coordination needed for the multiple spoofing devices used in this scenario.

~~(U//FOUO)~~ Just as a high frequency ranking does not always correlate to high risk, the opposite is true as well. With Scenario G and other low-ranked scenarios, some SMEs cautioned that although we may not have seen an attack of this nature before, if one were to occur and succeed, the impact could be severe. Therefore, the low ranking should not be misleading. In addition, this scenario might not be detectable for long periods of time. Often, one-off attacks (September 11, 2001, for instance) cause the most damage.

³⁶ ~~(U)~~ American Meteorological Society, *Satellite Navigation and Space Weather: Understanding the Vulnerabilities & Building Resilience*, Policy Workshop Report, March 2011, www.ametsoc.org/atmospolicy/documents/AMSSWGPSFinal.pdf.

~~(U)~~ **Limitations**

~~(U//FOUO)~~ The findings from the Likelihood Threat Workshop had one major limitation, which was found in the frequency of occurrence ranges. SMEs agreed that their estimated frequency ranges were speculation or expert opinion based on their knowledge, judgment, and experience, and hard data was often quite limited. There were various reasons for this. There is no deployed suite of sensors that can detect and characterize interference with the GPS signal. Moreover, there is currently no one single repository for reports of GPS jamming or spoofing incidents, and companies and agencies often do not share or publicize information about occurrences. Occasionally the reports are classified, another limitation on information sharing. The repository problem may be somewhat or fully mitigated when DHS's searchable PNT Incident Portal goes into use. The likelihood of GPS disruption scenarios was identified independent of a specific sector that might be impacted despite the knowledge that disruptions are dependent upon user equipment characteristics, which vary across sectors, because of the absence of information on the frequency of a *successful* attack against an individual sector. Furthermore, some threats are not targeted at any one sector but could result in collateral damage to all sectors.

(U) 5.5 NRE GPS Current Risk Estimate: Communications Sector

(U) Overview of Communications Sector Use of GPS PNT

(U) The Nation's communications infrastructure is a complex system of systems that incorporates multiple technologies and services with diverse ownership. The infrastructure includes wireline, wireless, satellite, cable, and broadcasting capabilities, and it includes the transport networks that support the Internet and other key information systems. The communications companies that own, operate, and supply the Nation's communications infrastructure have historically factored natural disasters and accidental disruptions into network resilience architecture, business continuity plans, and disaster recovery strategies.³⁷

~~(U)~~ Many communications components require accurate timing and synchronization to function properly, and service providers achieve this through timing signals derived from GPS-Disciplined Oscillators (GPSDOs)—clocks that maintain their accuracy through continuous reference to a GPS time source.³⁸ Interference with the GPS can cause a receiver to lose lock on the GPS signals, making the receiver go into holdover mode. The holdover performance is a function of the internal clock in the GPS receiver. Higher quality clocks slow the degradation but also raise the cost of the hardware.^{39 40}

~~(U//FOUO)~~ Interdependencies between Communications and other critical infrastructure sectors are significant, as is broad user reliance on communications networks for routine operations—from Federal, State, and local law enforcement investigations to general business functionality. (See Chapter 6, Sector Interdependencies, for more detailed discussion of interdependencies.)

~~(U)~~ High-Risk Scenarios

~~(U//FOUO)~~ Risk is defined as the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences. SME judgments on the consequences of GPS disruption scenarios were solicited in one workshop. The likelihood of GPS disruption scenarios, independent of the specific sector that might be impacted, was identified in another SME elicitation workshop.

~~(U//FOUO)~~ The following GPS disruption scenarios were judged to present the highest risk to the Communications Sector:

- ~~(U//FOUO)~~ Scenario A: Continuous, stationary, unintentional interference.
- ~~(U//FOUO)~~ Scenario B: Single, low-power, continuous, stationary jammer.
- ~~(U//FOUO)~~ Scenario D: Multiple, low-power, continuous and intermittent, stationary and mobile jammers.

³⁷ (U) Communications Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan, 2010.

³⁸ (U) The President's National Security Telecommunications Advisory Committee, *NSTAC Report to the President on Commercial Communications Reliance on the Global Positioning System (GPS)*, February 28, 2008.

³⁹ (U) Ibid.

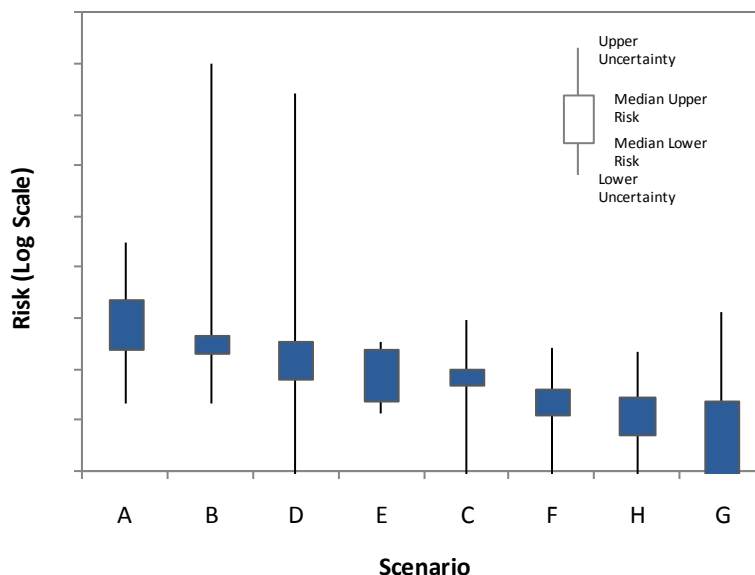
⁴⁰ (U) Kirk Montgomery, Symmetricom.

~~(U//FOUO)~~ While Scenarios A and D were among the GPS disruption scenarios judged to result in the highest consequences for the Communications Sector modes, Scenario B was among the lower ranking consequence scenarios. However, its assessed higher likelihood raised its risk ranking relative to the other GPS disruption scenarios. This was true in general for scenarios involving intentional and unintentional jamming affecting GPS signals: these scenarios were judged to be more likely because of historical precedent. Thus, their risk relative to the other scenarios was generally raised.

~~(U//FOUO)~~ The SMEs who estimated the likelihood of these scenarios noted that there is significant uncertainty in these judgments because there is limited data on historical precedent for many of the scenarios.

~~(U//FOUO)~~ The following graphic illustrates the range of uncertainty associated with the assessed risk of each scenario's GPS disruption. The vertical scale denotes the risk and is displayed on a logarithmic scale. The horizontal scale shows each of the scenarios (A through H) in rank order from highest to lowest risk. The risk is the expected loss determined by the product of the likelihood and consequence for each scenario. (Further details on the methodology used to derive the risk can be found in Annex C: NRE Risk Assessment and Monte Carlo Simulation Methodology.)

~~(U//FOUO)~~ The figure indicates that the GPS disruption scenarios A, B, and D present the highest risk to Communication Sector assets. For each scenario, the blue box represents the range of median risk scores and the vertical line indicates the uncertainty associated with the risk score. For the eight scenarios considered, the Figure 5-2 shows that the largest amount of uncertainty is associated with the assessed risk of GPS disruption scenarios B and D.



~~(U//FOUO)~~ Figure 5-2: Communications Sector Risk

~~(U//FOUO)~~ **Scenario A:** *An interference source is causing unintentional disruption. Ground receivers within a 30-km GTG radius are affected, and airborne receivers within radio LOS are affected.*

(b)(7)e, (b)(7)f

~~(U//FOUO)~~ SMEs were divided as to whether the scenario would lead to isolated degradation, widespread degradation, or isolated outage of the network.⁴² Some SMEs noted that communication outages would be unlikely, but degradation could result depending on how long the interference lasts.

~~(U//FOUO)~~ ***Scenario B: Jamming disruption from a single low-power stationary jammer. GPS receiver tracking is affected within a 500-m GTG radius and a 20-km LOS radius. GPS receiver acquisition is affected within an 800-m GTG radius and 30-km LOS radius.***

~~(U//FOUO)~~ Most SMEs judged that the effects of this scenario would last for less than seven days. While the majority of SMEs judged the scenario would result in isolated degradation, some SMEs judged it would result in isolated outage. SMEs noted that the weaker signals from the jammer could complicate locating the device and could likely extend the duration of the jamming. Those investigating disruptions might first suspect faulty equipment rather than jamming, or they might look for hardware or software glitches across the network as an explanation before considering disruptions to GPS.

~~(U//FOUO)~~ ***Scenario D: Jamming disruption from multiple low-power jammers on the ground. The jammers are stationary and mobile, with some intermittently active. Pockets of intermittent tracking and acquisition disruption occur across the metropolitan area.***

~~(U//FOUO)~~ SMEs generally agreed that the effects of this scenario would last for less than 30 days, although they were divided on whether the effects would involve isolated degradation, widespread degradation, or isolated outage. SMEs noted that it could take authorities up to a month (and possibly longer) to resolve a scenario involving multiple, mobile, low-powered jammers. Some SMEs noted that the extent to which the jammers themselves were widespread would affect how widespread the impacts of the scenario would be. Participants noted that mobile, low-power devices present a scenario that could easily take a long time to resolve—possibly a month or longer. Participants discussed different possibilities for what would constitute degradation versus an outage, but they agreed that how widespread the jammers are situated would determine the breadth of the impact. Degradation of service might mean impairing signal handoff within pockets of the cellular communication system for short periods of time, and this dynamism could cause sufficient uncertainty among investigators or the network operators, who could suspect system-related issues before looking for GPS anomalies.

(b)(7)e, (b)(7)f

⁴² ~~(U)~~ Poor network performance or outages mean that cell phones would not function not only for E911, but also in general use as time drifts off.

~~(U//FOUO)~~ One SME suggested that jamming long enough near a central office could isolate a Signaling System #7 (SS7) node,⁴³ which could disable a sizable part of a the metropolitan cellular communications network, but participants disagreed on how plausible such a scenario would be, as it could require multiple systems, which comprise key backbone infrastructure with sophisticated architecture, to fail.

~~(U//FOUO)~~ The text box below summarizes the effects of intentional multiple but short-term GPS jammers operated by North Korea and targeted into South Korea in 2010 and 2011.

⁴³~~(U)~~ SS7 is a telecommunications protocol that links telecoms, cellular, and long distance networks and connects disparate telecommunications providers into one common signaling network. "Cisco SS7 Fundamentals," www.cisco.com/univercd/cc/td/doc/product/tel_pswt/vco_prod/ss7_fund/ss7fun01.pdf , accessed July 15, 2011.

~~(U)~~ **North Korean Malicious Jamming Events 2010 and 2011**

~~(U)~~ The majority of all reported instances of GPS interference in the United States have been the result of training events or unintentional interference. However, reports from South Korea indicate that North Korea has engaged in deliberate GPS jamming in at least two instances in 2010 and 2011. Even though there are other sources of timing, this text box describes the events as they took place in 2010 and 2011.

~~(U)~~ The first jamming event took place between August 23 and 25, 2010.¹ The South Korea Communications Commission reported that during this time, signals from North Korea interfered with both military and civilian GPS receivers on land and at sea.² The jammers were switched on for 10 minutes at a time over the 3-day period, and South Korean Defense Minister Kim Tae-young stated that the jammers were effective up to 100 km.³ The U.S. Forces Korea spokesman at the time, Colonel Jonathan Withington, declined to discuss the effects of the jamming event on U.S. military personnel and equipment in the region.⁴ A Japanese technical consultant speculated that the event may have been an operational test or an attempt to simply prove that North Korea possessed GPS jamming capabilities.⁵

~~(U)~~ A second jamming event took place in March 2011 during a joint South Korea-U.S. command post and field training exercise.⁶ The jammers, believed to be of Russian origin and mounted on vehicles, were successful at disabling GPS tracking devices used by the South Korean military, by government officials, by intelligence personnel, and by some civilian telephone networks.⁷ The South Korean government also confirmed that an artillery unit's distance measuring devices were impacted.⁸ Once again, the jamming was intermittent, and officials speculated that the event might be a test of new equipment. The effects of the jamming were concentrated in Seoul, the port city of Incheon, and Paju, near the Military Demarcation Line (MDL).⁹ The signals are believed to have come from two North Korean military bases situated near the MDL.¹⁰

¹ (U) The National PNT Advisory Board. "Comments on – Jamming the Global Positioning System – A National Security Threat: Recent Events and Potential Cures." November 4, 2010. p. 5.

² (U) "North Korea Appears Capable of Jamming Receivers." Telemantics. 2010. <http://www.defence.pk/forums/military-forum/76068-north-korea-appears-capable-jamming-gps-receivers.html> Accessed July 7, 2011.

³ (U) The National PNT Advisory Board. "Comments on – Jamming the Global Positioning System – A National Security Threat: Recent Events and Potential Cures." November 4, 2010. p. 5.

⁴ (U) "North Korea Appears Capable of Jamming Receivers." Telemantics. 2010. <http://www.defence.pk/forums/military-forum/76068-north-korea-appears-capable-jamming-gps-receivers.html> Accessed July 7, 2011.

⁵ (U) "North Korea Appears Capable of Jamming Receivers." Telemantics. 2010. <http://www.defence.pk/forums/military-forum/76068-north-korea-appears-capable-jamming-gps-receivers.html> Accessed July 7, 2011.

⁶ (U) Sung-Ki, Jung. "S. Korea Blames North for GPS, Phone Jamming." *Defense News*. March 6, 2011. <http://www.defensenews.com/story.php?i=5883068&c=ASI&s=LAN> Accessed July 7, 2011.

⁷ (U) Ibid.

⁸ (U) Ibid.

⁹ (U) Ibid.

¹⁰ (U) Ibid.

~~(U)~~ **High-Consequence Scenarios**

~~(U//FOUO)~~ The GPS disruption scenarios judged to be of highest potential consequence (severity and duration) were similar to those judged to be of highest potential risk. As noted previously, the limited divergence results from the inclusion of likelihood estimates in the determination of risk. Independent of considerations of likelihood, the following GPS disruption scenarios were judged to be of highest potential consequence for the Communications Sector:

- ~~(U//FOUO)~~ Scenario A: Continuous, stationary, unintentional interference.

- ~~(U//FOUO)~~ Scenario D: Multiple, low-power, continuous and intermittent, stationary and mobile jammers.
- ~~(U//FOUO)~~ Scenario H: Brief high-power jamming followed by continuous high-power spoofing.
- ~~(U//FOUO)~~ Scenario E: Severe geomagnetic storm.
- ~~(U//FOUO)~~ Scenario G: Continuous multiple spoofers.

~~(U//FOUO)~~ This section discusses the highest ranking consequence scenarios, with the exception of Scenarios A and D, which were discussed in the current risk estimate section above. More detailed descriptions of the consequences resulting from the lower ranking scenarios can be found in Annex E.

~~(U//FOUO)~~ **Scenario H: Sophisticated, coordinated “navigation confusion” attack whereby a strategically placed multiple-watt transmitter generates GPS-like signals after an initial interval (several minutes) of jamming. Receivers within a three-km GTG radius and a 230-km LOS radius report a confident timing and position fix, but the timing is wrong by up to hundreds of microseconds and the position fix is wrong by up to tens of kilometers.**

~~(U//FOUO)~~ Most SMEs judged that the effects of this scenario would last for less than seven days but they were divided as to whether the scenario would result in isolated degradation, widespread degradation, or isolated outage. Most SMEs agreed that the effects would generally be isolated, though, because of the small area affected.

(b)(7)e, (b)(7)f

(b)(7)e, (b)(7)f

~~(U//FOUO)~~ **Scenario E: Continent-scale natural disruption caused by a severe geomagnetic storm. Tracking threshold of GPS is reduced significantly.**

~~(U//FOUO)~~ Most SMEs agreed that this scenario would result in widespread degradation in the Communications Sector and that the effects of the scenario would last for less than seven days. SMEs noted that the severity of the scenario depends on solar wind density: if solar wind is slow or less dense, there are fewer impacts; if solar wind is dense, effects could last for two to three days. Disruption to GPS would be intermittent since the impacts come in waves, which could last several hours at a time. Not only would this degrade end-user communications, but it could also affect the operations of the telecom carrier and its ability to respond to emergencies that arise.

~~(U//FOUO)~~ SMEs noted that when moving, the rate at which the GPS signal would fade depends on the direction of travel: for a given speed of travel, east/west fading is more rapid than north/south fading. GPS receivers would go into acquisition/reacquisition phase for the duration

(b)(7)e, (b)(7)f

of the storm, but they would likely reacquire the GPS signal approximately two hours after sundown in most instances.

~~(U//FOUO)~~ ***Scenario G: Sophisticated, coordinated pinpoint spoofing attacks against multiple target receivers (one spoofer per targeted receiver). Each spoofer independently walks off the time and position without raising alarms.***

~~(U//FOUO)~~ SMEs generally agreed that this scenario would result in isolated degradation to the Communications Sector but disagreed on the estimated duration of this degradation. SMEs noted that it would be difficult to locate and eliminate the spoofers, but the extent of disruption would likely stimulate intense effort to find the sources. However, a sophisticated, coordinated spoofing attack would likely trigger anomalies that would be noticed within the network, and, if such anomalies were indeed noticed, network rerouting would mitigate the attack quickly.

(U) 5.6 NRE GPS Current Risk Estimate: Emergency Services Sector

(U) Overview of Emergency Services Sector Use of GPS PNT

~~(U)~~ The Emergency Services Sector's communications network architecture is often reliant upon GPS UTC or 1 pulse-per-second (PPS) Timing. If a first responder's radio network architecture pivots around GPS Timing, there is no readily available backup if the GPS component is compromised. While dispatchers may still be able to communicate with individual first responder units, there could be debilitating effects on radio signals or untimely delays in communications voice radio systems using simulcast technology. Without simulcast ability, the Sector would have to fall back on less sophisticated means of communications, such as reverting to a standard single frequency repeater, which does not require GPS to operate. An entire department would have to share a single channel, which would likely cause chaos. In addition, the positioning and navigation features of GPS available in computer-aided dispatch (CAD) technologies assist some elements of this sector in managing fleet vehicles, locating accidents and stolen vehicles, and dispatching fire, medical, and law enforcement personnel.⁴⁵ While this Sector has not reached the point of total dependency on GPS services, the use of GPS improves the ability of the sector to perform damage mitigation and assist in timely rescue response.⁴⁶

~~(U)~~ High-Risk Scenarios

~~(U//FOUO)~~ Risk is defined as the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences. SME judgments on the consequences of GPS disruption scenarios to the Emergency Services Sector were solicited in one workshop (see Annex I for a listing of the SMEs). The likelihood of GPS disruption scenarios, independent of the specific sector that might be impacted, was identified in another SME elicitation workshop.

~~(U//FOUO)~~ The following GPS disruption scenarios were judged to present the highest risk to the Emergency Services Sector:

- ~~(U//FOUO)~~ Scenario A: Continuous, stationary, unintentional interference.
- ~~(U//FOUO)~~ Scenario D: Multiple, low-power, continuous and intermittent, stationary and mobile jammers.
- ~~(U//FOUO)~~ Scenario B: Single, low-power, continuous, stationary jammer.

~~(U//FOUO)~~ While these GPS disruption scenarios do not always result in the highest consequences for the Emergency Services Sector, their assessed higher likelihood raised their risk rankings relative to the other GPS disruption scenarios. The SMEs who estimated the likelihood of these scenarios noted that there is significant uncertainty in these judgments as there is limited data on historical precedent for many of the scenarios. However, as there is

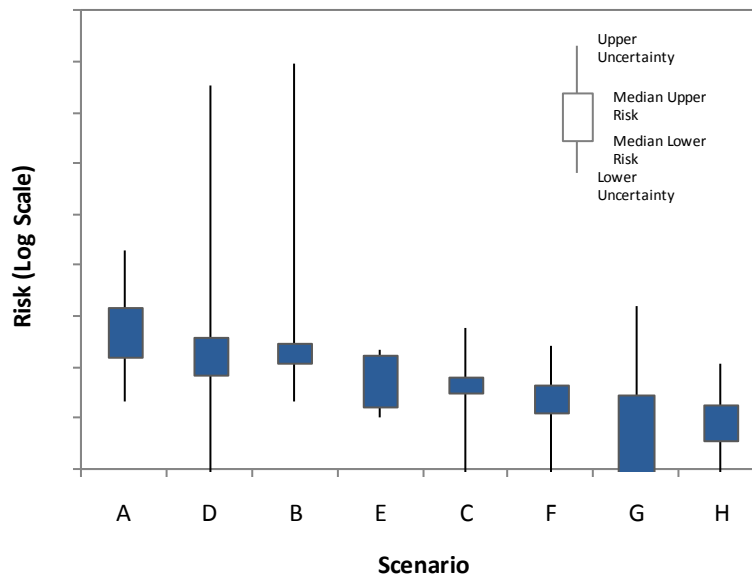
⁴⁵ (U) National Security Space Office, National Positioning, Navigation, and Timing Architecture Study Final Report, September 2008.

⁴⁶ (U) Jules G. McNeff, The Global Positioning System, March 2002.

historical precedent for scenarios involving intentional and unintentional jamming affecting GPS signals, these scenarios were judged to be more likely, thereby raising their relative risk.

(U//FOUO) The following graphic illustrates the range of uncertainty associated with the assessed risk of each scenario's GPS disruption. The vertical scale denotes the risk and is displayed on a logarithmic scale. The horizontal scale shows each of the scenarios (A through H) in rank order from highest to lowest risk. The risk is the expected loss determined by the product of the likelihood and consequence for each scenario. (Further details on the methodology used to derive the risk can be found in Annex C: NRE Risk Assessment and Monte Carlo Simulation Methodology.)

(U//FOUO) The figure indicates that the GPS disruption scenarios A, D, and B present the highest risk to Emergency Services Sector assets. For each scenario, the blue box represents the range of median risk scores and the vertical line indicates the uncertainty associated with the risk score. For the eight scenarios considered, Figure 5-3 shows that the largest amount of uncertainty is associated with the assessed risk of GPS disruption scenarios D and B.



(U//FOUO) Figure 5-3: Emergency Services Sector Risk

(U//FOUO) **Scenario A: An interference source is causing unintentional disruption. Ground receivers within a 30-km GTG radius are affected, and airborne receivers within radio LOS are affected.**

(U//FOUO) Scenario A had the highest risk score for all the scenarios. The SMEs judged this scenario would result in either isolated or widespread degradation, and most SMEs agreed the degradation would last for less than seven days. SMEs noted that the stationary nature of the interference would likely make it easy to locate within a short timeframe. In addition, because this scenario would affect ground and airborne systems, both the FCC and Federal Aviation Administration (FAA) would be involved in finding and mitigating the cause of the interference, likely increasing the amount of resources devoted to the issue.

~~(U//FOUO)~~ During the degradation, fire and rescue, police, and 911 call centers could have to find manual workarounds, which would minimize disruption somewhat but increase inefficiencies. This would result in increased response time from first responders. Airborne emergency services would be impacted as well because they might require visual landmarks or maps to respond to incidents.

~~(U//FOUO)~~ ***Scenario D: Jamming disruption from multiple low-power jammers on the ground. The jammers are stationary and mobile, with some intermittently active. Pockets of intermittent tracking and acquisition disruption occur across the metropolitan area.***

~~(U//FOUO)~~ SMEs were divided about the severity and timing of the effects from this scenario. A plurality of SMEs agreed the scenario would result in widespread degradation for greater than 30 days across the Sector; however, an equal number of SMEs judged the effect would be isolated degradation, although timing varied from less than 1 day to more than 30 days. A single SME judged the scenario would lead to widespread outages lasting less than 30 days. Because some of the jammers are mobile, there would be intermittent pockets of disruptions that could be very difficult to track, hampering mitigation efforts.

~~(U//FOUO)~~ As with other scenarios, this situation would cause disruptions for police, fire, and emergency medical services (EMS), and force them to revert to older systems as a workaround (assuming they still had the capability). Several SMEs noted that one of the greatest consequences from this scenario could be an erosion of the public's trust in GPS reliability and capabilities.

~~(U//FOUO)~~ ***Scenario B: Jamming disruption from a single low-power stationary jammer. GPS receiver tracking is affected within a 500-m GTG radius and a 20-km LOS radius. GPS receiver acquisition is affected within an 800-m GTG radius and 30-km LOS radius.***

~~(U//FOUO)~~ SMEs mostly agreed this scenario would result in isolated degradation for less than seven days. SMEs generally believed the jammer could be detected and located in a short timeframe owing to its stationary nature and the limited area in which it could be located, which would quickly create a known "dead zone." However, because of the small scope of the jamming, it could take some time before the issue was noticed and a response triggered.

~~(U//FOUO)~~ One SME mentioned that this kind of degradation likely would affect the operations of the Emergency Services Sector, requiring the use of workarounds in order to maintain the Sector's services, and another mentioned that this sort of incident might only lead to an issue with a component of the Sector (because of the size of the affected area), rather than the Sector itself. The text box below describes an unintentional jamming event similar to Scenario B that took place in San Diego, CA in 2007.

~~(U)~~ **2007 San Diego GPS Jamming Event**

~~(U)~~ PNT and GPS experts agree that one of the greatest threats to critical infrastructure is developing a hidden critical dependency on GPS systems. This occurs when cell phone network operators, airline pilots, and emergency responders think they either have a backup for GPS or are not dependent on GPS but then find critical functions inoperable when a GPS outage occurs. Perhaps the best example of this comes from San Diego, where in 2007 a scheduled military communication jamming exercise inadvertently jammed the GPS signal as well.

~~(U)~~ In January 2007, two U.S. Navy ships began a scheduled communication jamming exercise in San Diego Harbor.¹ The exercise was meant to block radio signals and test procedures for communication loss. After two hours, operators onboard realized that their GPS system would not initialize and discontinued the jamming exercise.² Within that two-hour window, the loss of GPS signal had ripple effects across the Communications, Emergency Services, and Transportation Systems sectors.

~~(U)~~ Within 30 minutes of the launch of the jamming exercise, various GPS agencies began to receive reports of disruptions.³ The San Diego Bob Wilson Naval Medical Center, located approximately five miles from the site of the jammer, reported that the event shut down the hospital's mobile paging system used to call doctors in the event of emergencies.⁴ At the San Diego International Airport, about seven miles away from the jamming site, general aviation GPS-enabled navigation equipment experienced outages, but commercial airlines did not report any disruption.⁵ Two local cell phone towers shut down, and 150 others reported loss of time synchronization needed to pass calls from tower to tower.⁶ U.S. Coast Guard ships in the harbor area operated on restricted status due to interference in the harbor's traffic management system, and the San Diego Differential GPS (DGPS) site was unavailable for 32 minutes.⁷

~~(U)~~ Once the Naval technicians involved in the exercise turned off the jammer, conditions returned to normal. However, because the jamming exercise was not intended to impact the GPS band, the technicians did not report the incident to any of the relevant authorities.⁹ The signal was stationary, unintentional, and self-corrected. In short, outside of a scheduled GPS outage, the event was a best-case scenario. However, it took NAVCEN and other agencies over 72 hours to determine the source of GPS interference responsible for the unexpected disruptions.¹⁰

¹ (U) Carrol, James and Kirk Montgomery. "Global Positioning System Timing Criticality Assessment – Preliminary Performance Results." *40th Annual Precise Time and Time Interval (PTTI) Meeting*. December 1, 2008. p. 487

² (U) Hambling, David. "GPS Chaos: How a \$30 Box Can Jam Your Life." *The New Scientist*. March 6, 2011.

³ (U) Carroll, James and Kirk Montgomery. "Global Positioning System Timing Criticality Assessment – Preliminary Performance Results." *40th Annual Precise Time and Time Interval (PTTI) Meeting*. December 1, 2008. p. 487

⁴ (U) Hambling, David. "GPS Chaos: How a \$30 Box Can Jam Your Life." *The New Scientist*. March 6, 2011.

⁵ (U) Carrol, James and Kirk Montgomery. "Global Positioning System Timing Criticality Assessment – Preliminary Performance Results." *40th Annual Precise Time and Time Interval (PTTI) Meeting*. December 1, 2008. p. 487

⁶ (U) Bellows, Charlie. "GPS Operations Center." <http://www.navcen.uscg.gov/pdf/cgsicMeetings/47/%5B09%5D%2017%20GPSOC%2047%20A.pdf> Accessed July 6, 2011.

⁷ (U) Ibid.

⁸ (U) Hambling, David. "GPS Chaos: How a \$30 Box Can Jam Your Life." *The New Scientist*. March 6, 2011.

⁹ (U) Carroll, James and Kirk Montgomery. "Global Positioning System Timing Criticality Assessment – Preliminary Performance Results." *40th Annual Precise Time and Time Interval (PTTI) Meeting*. December 1, 2008. p. 487

¹⁰ (U) Jewell, Don. "GPS Insights-April 2007." *GPS World*. April 2007. Accessed July 6, 2011. <http://www.gpsworld.com/defense/gps-insights-april-2007-8428>

~~(U)~~ **High-Consequence Scenarios**

~~(U//FOUO)~~ The GPS disruption scenarios judged to be of highest potential consequence (severity and duration) differed from those judged to be of highest potential risk. Scenario D was the only exception as it is both a high-risk and a high-consequence scenario for the Emergency Services Sector. As noted previously, this divergence results from the inclusion of likelihood estimates in the determination of risk. Independent of considerations of likelihood, the following GPS disruption scenarios were judged to be of highest potential consequence for the Emergency Services Sector.

- ~~(U//FOUO)~~ Scenario D: Multiple, low-power, continuous and intermittent, stationary and mobile jammers.
- ~~(U//FOUO)~~ Scenario G: Continuous multiple spoofers.
- ~~(U//FOUO)~~ Scenario E: Severe geomagnetic storm.
- ~~(U//FOUO)~~ Scenario F: Continuous single spoofer.

~~(U//FOUO)~~ As the consequences of Scenario D were already discussed above, the consequences of Scenarios G, E, and F are described below. Descriptions of the lower consequence scenarios can be found in the Emergency Services Sector Workshop Findings Report in Annex E.

~~(U//FOUO)~~ ***Scenario G: Sophisticated, coordinated pinpoint spoofing attacks against multiple target receivers (one spoofer per targeted receiver). Each spoofer independently walks off the time and position without raising alarms.***

~~(U//FOUO)~~ Most SMEs agreed that this scenario would result in widespread degradation for more than 30 days; with many SMEs believing consequences could last much longer than that. After the lengthy time required to discover the cause of the disruption, the presence of multiple spoofers means that it could take a significant period of additional time to locate those spoofers and affected devices.

~~(U//FOUO)~~ SMEs discussed effects on the Emergency Services Sector, depending on various ways this scenario could occur. The Sector is often divided into municipalities, so whether these multiple spoofing attacks target multiple receivers in a single jurisdiction or receivers across multiple jurisdictions would determine the scope of the impact to emergency services. Smaller attacks across a wider area could erode public confidence in the Sector.

~~(U//FOUO)~~ ***Scenario E: Continent-scale natural disruption caused by a severe geomagnetic storm. Tracking threshold of GPS is reduced significantly.***

~~(U//FOUO)~~ All SMEs agreed that this scenario would cause widespread degradation; however, they were split on whether the effects would last less than seven days or less than one day, with most leaning toward less than one day.

~~(U//FOUO)~~ A severe geomagnetic event would degrade the command and control, location-based service, and airborne activities of the Emergency Services Sector. However, with this type of disruption, and with the effects and source known, there may be advance notice of

degradation, allowing emergency services to plan and mitigate with possible countermeasures accordingly, as well as alert and educate the public. In addition, any degradation effects could be equipment specific; for example, according to one SME, this scenario could cause less disruption in assisted GPS (A-GPS) systems, e.g., cell phone GPS receivers assisted by cell phone towers, which use data from non-satellite sources, such as networks, to allow GPS devices to obtain GPS satellite measurements to determine their positions more quickly using much weaker GPS signals than conventional GPS receivers can obtain.

~~(U//FOUO)~~ ***Scenario F: Pinpoint spoofing attack against a single target receiver. The spoofer walks off time and position reported by the target receiver without raising alarms.***

~~(U//FOUO)~~ All SMEs judged that isolated degradation would result from this scenario; however, estimated durations varied, with most SMEs believing the degradation would last more than 30 days, but the remaining SMEs split between various durations, all of which were of less than 30 days. SMEs generally agreed that the duration would be greater than 30 days because pinpointed spoofing that attacks a single, possibly isolated, target could take a good deal of time to detect and/or diagnose and could necessitate a lengthy physical search for the spoofer.

~~(U//FOUO)~~ Although this scenario involves a single target, SMEs agreed upon various ways disruptions to the Emergency Services Sector could result. A spoofer could take control of a target receiver but apply zero error functions to it for a time, leaving the Sector unaware the receiver had been compromised. At a later date, perhaps during a crisis or some other vulnerability, the spoofer could spoof the system, affecting public safety in various ways. For instance, instead of shifting the location, the spoofer could slowly drag the time off, disrupting the communications capability. If the Emergency Services Sector is using a synchronous station and that station's timing is off, the station would essentially be taken off the air, degrading communications.

(U) 5.7 NRE GPS Current Risk Estimate: Energy Sector

(U) Overview of Energy Sector Use of GPS PNT

(U) The Energy Sector depends on GPS for providing electrical power system reliability and grid efficiency, synchronizing services among power networks, and finding malfunctions within transmission networks. The GPS timing signal can be used to assist in maintaining services across electricity grids.⁴⁷ GPS is a key component of Wide Area Monitoring Systems, phase monitoring units, and disturbance monitoring equipment.⁴⁸

~~(U//FOUO)~~ For example, Wide Area Monitoring Systems may ultimately perform some of the grid controls now done by the power grid operators and require the tight synchronization that GPS and high-quality atomic clocks can provide.⁴⁹ The Energy Sector (especially the electricity subsector) uses phasor measurement units (PMUs), also known as synchrophasors, to measure AC power phase and amplitude. Synchrophasor data is sent to central control centers, which allow grid operators to monitor and control systems in real time and support updates, system changes, and troubleshooting.⁵⁰ PMUs rely on a GPS time signal for extremely accurate time-stamping of the power system information. A GPS satellite receiver provides a precise timing pulse, which is correlated with sampled voltage and current inputs. The exact microsecond when the phasor measurement is taken is permanently attached to it. Collecting and collating these measurements provides powerful techniques for monitoring and modeling power networks.⁵¹

~~(U)~~ GPS supports the exploration of land and ocean resources and is used as a location/orientation tool in drilling for oil and gas.⁵² For example, oil and gas exploration increasingly uses networks of seismic monitors that are synchronized with GPS. The rail, sea, and land transportation systems that distribute coal, natural gas, oil, and biofuels to electric power plants and other energy users also depend on GPS for location awareness and just-in-time deliveries.

~~(U)~~ High-Risk Scenarios

~~(U//FOUO)~~ Risk is defined as the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences. SME judgments on the consequences of GPS disruption scenarios to the Energy Sector were solicited in one workshop. The likelihood of GPS disruption scenarios, independent of the specific sector that might be impacted, was identified in another SME elicitation workshop.

~~(U//FOUO)~~ The following GPS disruption scenarios were judged to present the highest risk to the Energy Sector:

- ~~(U//FOUO)~~ Scenario A: Continuous, stationary, unintentional interference.

⁴⁷ (U) Jules G. McNeff, The Global Positioning System, March 2002.

⁴⁸ (U) GPS Timing Criticality Assessment – Preliminary Performance Results.

⁴⁹ (U) Ibid.

⁵⁰ (U) Synchrophasor System Benefits Fact Sheet, North American SynchroPhasor Initiative (NASPI).

⁵¹ (U) ABB Review, A New Approach to Power Network Modeling, 2001.

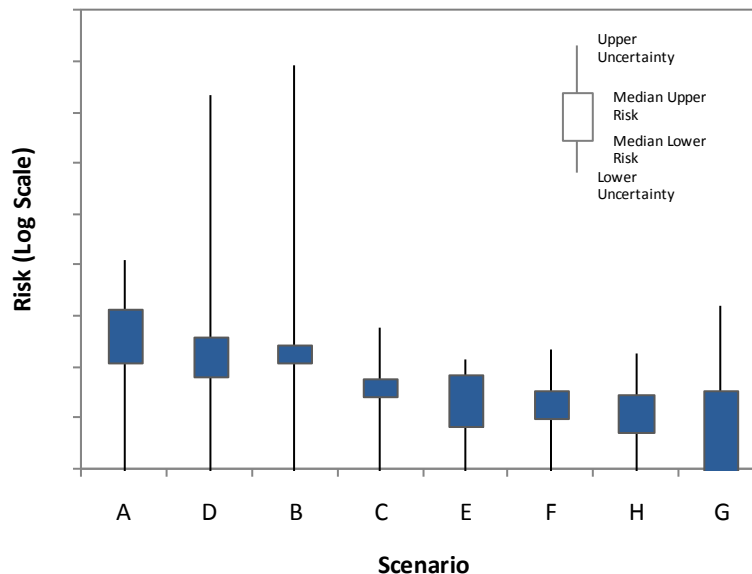
⁵² (U) National Security Space Office, National Positioning, Navigation, and Timing Architecture Study Final Report, September 2008.

- ~~(U//FOUO)~~ Scenario D: Multiple, low-power, continuous and intermittent, stationary and mobile jammers.
- ~~(U//FOUO)~~ Scenario B: Single, low-power, continuous, stationary jammer.

~~(U//FOUO)~~ While these GPS disruption scenarios do not always result in the highest consequences for the Energy Sector, their assessed higher likelihood raised their risk rankings relative to the other GPS disruption scenarios. The SMEs who estimated the likelihood of these scenarios noted that there is significant uncertainty in these judgments as there is limited data on historical precedent for many of the scenarios. However, since there is documented historical precedent for scenarios involving intentional and unintentional jamming affecting GPS signals, these scenarios were judged to be more likely, thereby raising their relative risk.

~~(U//FOUO)~~ The following graphic illustrates the range of uncertainty associated with the assessed risk of each scenario's GPS disruption. The vertical scale denotes the risk and is displayed on a logarithmic scale. The horizontal scale shows each of the scenarios (A through H) in rank order from highest to lowest risk. The risk is the expected loss determined by the product of the likelihood and consequence for each scenario. (Further details on the methodology used to derive the risk can be found in Annex C: NRE Risk Assessment and Monte Carlo Simulation Methodology.)

~~(U//FOUO)~~ The figure indicates that the GPS disruption scenarios A, D, and B present the highest risk to Energy Sector assets. For each scenario, the blue box represents the range of median risk scores and the vertical line indicates the uncertainty associated with the risk score. For the eight scenarios considered, Figure 5-4 shows that the largest amount of uncertainty is associated with the assessed risk of GPS disruption scenarios D and B.



~~(U//FOUO)~~ Figure 5-4: Energy Sector Risk

~~(U//FOUO)~~ *Scenario A: An interference source is causing unintentional disruption. Ground receivers within a 30-km GTG radius are affected, and airborne receivers within radio LOS are affected.*

~~(U//FOUO)~~ Most SMEs agreed that this scenario would result in isolated or no degradation and that the degradation would last for less than seven days. SMEs noted that it could take up to seven days (and perhaps longer) for authorities to detect, locate, and disable the jammer, although continuous interference sources are easier to identify. SMEs noted that within the Energy Sector, this scenario could affect a single substation, assuming there is no backup to a terrestrial clock. The device that loses clock synchronizing will provide erroneous measurement, such as frequency and phase angle, resulting in erroneous power flow calculations. This could cause overheating to some elements of the grid in the affected area, such as overloaded lines or overloaded transformers. If the device is used for adaptive protection, in the case of a fault, coordination of the protection system could be disrupted and backup protection might operate to isolate the fault before the local protection device operates. SMEs agreed that outages are not likely to occur because of the redundancy in the power grid system and similar redundancy in other Energy subsectors. The text box below describes how the events of 9/11 contributed to the use of GPS technology in the U.S. Power Grid system.

(U) Power Grid Post-9/11

(U) The availability, reliability, accuracy, and low cost of GPS services have led to innovative uses by the industry, including in the electric utility subsector, where GPS was used after September 11, 2001 to restore electricity services. The attacks on New York City destroyed two substations in lower Manhattan, forcing a large electric company to transfer load to other local substations.¹ The company was able to transfer load without any significant disruptions but needed to bring a new substation online before summer 2002, when the cooling season would require additional energy resources.

(U) The electric company quickly began work on a new substation, but the company also needed a way to bring the station onto the power grid. This process had previously been accomplished by measuring phase displacement² between two stations using copper phone wires.³ The phase displacement between the new and old stations had to be carefully monitored to ensure that the flow did not trip the network circuit breakers and cause power outages. However, the traditional process for measuring phase displacement between two stations, through copper phone wires, was no longer an option. Telecom companies had replaced the financial district's copper phone wires with fiber optic cables capable of processing data at the speed of light but incapable of measuring an electrical current's phase displacement.⁴

(U) The electric company partnered with a research and development corporation to develop an alternative technology for measuring phase displacement, and they found that by using the internal processor of the GPS clock, phase displacement could be accurately time stamped to one microsecond.⁵ One firm built an interface to help the electric company's engineers control the load transfer to the new substation based on the independent GPS timing reference.⁶ On April 27, 2002, with GPS monitoring phase displacement and providing updates every second, the load transfer took place without causing any disruptions in the Manhattan power supply.⁷ In addition, the entire process took four hours as opposed to the 72 hours previously required when copper wires were used.⁸

(U) The electric company has continued to use the GPS timing function for load transfers,⁹ and across the country electric power companies are integrating the GPS timing function to monitor line frequency and stability, maintain synchronization and syntonization (frequency) services between providers, and accurately locate and isolate faults in the network.¹⁰

¹ (U) Stergiou, Paul and David Kalokitis. "Keeping the Lights On: GPS and Power Grid Intermesh," *GPS World*. November 1, 2003. p.1

² (U) Defined by Stergiou and Kalokitis as "the difference between the phases of the 60Hz sinusoidal waves at both stations."

³ (U) Stergiou, Paul and David Kalokitis. "Keeping the Lights On: GPS and Power Grid Intermesh," *GPS World*. November 1, 2003. p.2

⁴ (U) Ibid.

⁵ (U) Ibid., p.3

⁶ (U) Ibid.

⁷ (U) Ibid., p.4

⁸ (U) Ibid.

⁹ (U) Ibid.

¹⁰ (U) Carroll, James and Kirk Montgomery. "Global Positioning System Timing Criticality Assessment – Preliminary Performance Results." *40th Annual Precise Time and Time Interval (PTTI) Meeting*. December 1, 2008. p. 493.

~~(U//FOUO)~~ **Scenario D: Jamming disruption from multiple low-power jammers on the ground. The jammers are stationary and mobile, with some intermittently active. Pockets of intermittent tracking and acquisition disruption occur across the metropolitan area.**

~~(U//FOUO)~~ SMEs were divided as to whether the effects of this scenario would persist for less than or more than 30 days. The presence of multiple, intermittent jammers would be difficult to identify, locate, and disable, thus enabling effects to persist for up to or more than 30 days. Most SMEs judged the scenario would result in isolated degradation of services in the Energy Sector, although some SMEs thought the degradation would be widespread and could result in isolated outages. SMEs judged that electrical services would be degraded because when operators cannot

depend on the better operability provided by GPS, they adopt safer operating conditions, which means less efficiency. If the intermittent jamming was longer than 15 seconds, time synchronization might be lost, affecting the state parameters calculation used for load flow and system stability and line carrying margin. In that case, the time-stamped data would be ignored by operators and they would consider the state estimation algorithm in order to detect faults and undesirable states that require remedial action to be taken.⁵³

~~(U//FOUO)~~ **Scenario B: Jamming disruption from a single low-power stationary jammer. GPS receiver tracking is affected within a 500-m GTG radius and a 20-km LOS radius. GPS receiver acquisition is affected within an 800-m GTG radius and 30-km LOS radius.**

~~(U//FOUO)~~ Most SMEs judged that this scenario would result in isolated degradation lasting less than 30 days. SMEs noted that the duration of the scenario effects would depend on the length of time it takes to detect, locate, and disable the jammer. It is more difficult to detect and locate low-power stationary jammers than high-power stationary jammers. However, SMEs indicated that the range of the low-power jammer is so short that it would probably cause limited degradation to the Energy Sector because of the redundancy in the systems. The text box describes the dependency on GPS by the Electricity Subsector.

~~(U)~~ Electricity Subsector Considerations

~~(U//FOUO)~~ Overall, the electricity subsector of the Energy Sector uses GPS to assist in operations. The electricity subsector's use of GPS timing through PMUs is still not prevalent throughout the power grid. Industry has been hesitant to install PMUs especially for the operational control of the grid, since it is just in the testing phase for using PMUs for real-time control of the grid. As of 2009, approximately 200 PMUs were installed throughout the North American power grid but this number is expected to increase in coming years with the Department of Energy providing stimulus funding for 800 additional PMUs.

~~(U)~~ High-Consequence Scenarios

~~(U//FOUO)~~ The GPS disruption scenarios judged to be of highest potential consequence (severity and duration) differed from those judged to be of highest potential risk. Scenario D was the only exception as it is both a high-risk and a high-consequence scenario for the Energy Sector. As noted previously, this divergence results from the inclusion of likelihood estimates in the determination of risk. Independent of considerations of likelihood, the following GPS disruption scenarios were judged to be of highest potential consequence for the Energy Sector:

- ~~(U//FOUO)~~ Scenario G: Continuous multiple spoofers.
- ~~(U//FOUO)~~ Scenario D: Multiple, low-power, continuous and intermittent, stationary and mobile jammers.

~~(U//FOUO)~~ As the consequences of Scenario D were already discussed above, the consequences of Scenario G are described below. Descriptions of the consequences of scenarios with lower ranking consequences can be found in Annex E.

⁵³ ~~(U)~~ NASA Ames Research Center, "State Estimation," <http://www.nasa.gov/centers/ames/research/technology-onepaggers/state-estimation.html>, 29 March 2008, accessed 22 September 2011.

~~(U//FOUO)~~ *Scenario G: Sophisticated, coordinated pinpoint spoofing attacks against multiple target receivers (one spoofer per targeted receiver). Each spoofer independently walks off the time and position without raising alarms.*

~~(U//FOUO)~~ Most SMEs judged that this scenario would result in widespread outage of a duration ranging from less than seven days to more than 30 days. This scenario could cause significant damage to the power grid due to the degradation of numerical data. Certain generators could erroneously detect an oscillating signal and attempt to dampen that oscillation. In this case, generators would automatically try to dampen an oscillation that did not exist, leading to a potential outage. SMEs noted that this scenario could cause a major and widespread outage. It would take a long time to locate the spoofers because they do not need to radiate power to track the victim antennas (because they are stationary).

(U) 5.8 NRE GPS Current Risk Estimate: Transportation Systems Sector

(U) Overview of Transportation Systems Sector Use of GPS PNT

(U) GPS functions support all modes of transportation: aviation, maritime, mass transit, highway, freight rail, and pipeline, as well as the intermodal connections between the modes.

~~(U)~~ The *aviation mode* uses GPS PNT for oceanic navigation, en route navigation, terminal navigation, non-precision approaches, precision approaches, Automatic Dependent Surveillance (ADS), air traffic control, airport surface operations, and timing. GPS supports flight position, navigation, and management; broadcast surveillance; and fuel monitoring and efficiency optimization.⁵⁴ GPS and other navigation systems support Area Navigation (RNAV), allowing for flying “point to point” where permitted or on published RNAV routes.⁵⁵ Backup systems for GPS typically are available, although these systems can reduce the capacity and efficiency of the transportation system.

~~(U//FOUO)~~ In addition, the Wide Area Augmentation System (WAAS) and the ground-based augmentation system (GBAS) rely on GPS. Either WAAS or GBAS are needed to support precision approach based on GPS. They correct GPS to improve accuracy and monitor GPS to detect and remove any faults (to provide integrity assurance). Both of these functions are conducted in real time. With WAAS or GBAS, the GPS data is corrected so that it can be used to position the aircraft to the required precision (especially vertical precision) for certain classes of landings under poor visibility conditions. With WAAS, the GPS data can be used for en route navigation, terminal-area navigation, and precision approaches including LPV (localizer performance with vertical guidance). With GBAS, the GPS data will be used for PVT (position, velocity, and time) in and around the airport and for CAT I landings. In the future, GBAS is expected to support all categories of landings. The evolving airspace system, including the Next Generation Air Transportation System (NextGen), will use GPS for PNT functions.⁵⁶

~~(U//FOUO)~~ For the *maritime mode*, GPS supports maritime navigation, vessel command and control, vessel tracking and reporting, and salvage operations.⁵⁷ A number of maritime applications, including the Global Maritime Distress Safety System, the Ship Security Alert System, Emergency Position Indicating Radio Beacons, among others, rely on electronic PNT input provided by GPS.⁵⁸ In high traffic ports, GPS is an important safety and situational tool and alternate methods reduce efficiency.⁵⁹ It is also used to track cargo containers in maritime shipping.⁶⁰

~~(U//FOUO)~~ GPS supports both primary surface transportation modes—*highways (passenger vehicles and trucks supporting freight movement) and rail*—in shipment tracking, real-time routing, just-in-time inventory optimization, vehicle operations and maintenance scheduling, and

⁵⁴ (U) National Security Space Office, National Positioning, Navigation, and Timing Architecture Study Final Report, September 2008.

⁵⁵ (U) Ibid.

⁵⁶ (U//FOUO) Ward, K., FAA, e-mail message to Moore, R., HITRAC, February 1, 2011.

⁵⁷ (U) National Security Space Office, National Positioning, Navigation, and Timing Architecture Study Final Report, September 2008.

⁵⁸ (U//FOUO) U.S. Department of Transportation, Maritime Administration, “Response to Positioning, Navigation, and Timing Data Call,” 2009.

⁵⁹ (U) Ibid.

⁶⁰ (U) German Federal Bureau of Maritime Casualty Investigation, Grounding of the LT CORTESIA on 2 January 2008 on the Varne Bank in the English Channel, 1 April 2009.

vehicle systems monitoring.⁶¹ For highways, GPS supports real time traffic control, vehicle tracking and dispatching for transit and commercial fleets, traffic data collection, work zone site management, transit signal priority systems, among other applications.⁶² For example, GPS can provide data on position, speed, and distance traveled to support supply chain management, routing, security, and dispatch services in the trucking industry.⁶³ Moreover, Vehicular Communications Services use GPS information to ensure road safety and efficient traffic patterns.⁶⁴ For rail, GPS is used for vehicle tracking and in digital communications to determine train locations and prevent train collisions, control speed, and maintain rail integrity.⁶⁵ GPS also supports track defect location, surveying, and bridge monitoring.⁶⁶ In particular, the rail industry uses GPS to synch rail inspection systems and keep track of real-time train departures and arrivals.⁶⁷ On the other hand, Positive Train Control, which is planned for implementation by 2015, will not be GPS dependent.

~~(U//FOUO)~~ For *pipelines*, the supervisory control and data acquisition (SCADA) system that controls how products flow is automatically timed by GPS. The U.S. Department of Transportation (DOT) continues to liaise with industry to determine the extent to which operations of pipelines should be GPS dependent.

(U) High-Risk Scenarios

~~(U//FOUO)~~ Risk is defined as the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences. SME judgments on the consequences of GPS disruption scenarios were solicited in two separate workshops: one on the aviation mode and one on the other transportation modes. The likelihood of GPS disruption scenarios, independent of the specific sector that might be impacted, was identified in another SME elicitation workshop. A similar pattern of high-risk scenarios occurred for both the aviation mode and the other transportation modes.

~~(U//FOUO)~~ The following GPS disruption scenarios were judged by the SMEs to present the highest risk to the Transportation Systems Sector:

- ~~(U//FOUO)~~ Scenario A: Continuous, stationary, unintentional interference.
- ~~(U//FOUO)~~ Scenario D: Multiple, low-power, continuous and intermittent, stationary and mobile jammers.
- ~~(U//FOUO)~~ Scenario B: Single, low-power, continuous, stationary jammer.

⁶¹ (U) Los Alamos National Laboratory, A Simple Demonstration that the Global Positioning System (GPS) is Vulnerable to Spoofing, 2002.

⁶² ~~(U//FOUO)~~ U.S. Department of Transportation, Federal Highway Administration, "Response to Positioning, Navigation, and Timing Data Call," 2009.

⁶³ (U) Salmi, Pekka, and Marko T. Torkkeli, "Inventions Utilizing Satellite Navigation Systems in the Railway Industry," Journal of Technology Management & Innovation 4(3)(2009).

⁶⁴ (U) Papadimitratos and Javanovic, GNSS-based Positioning: Attacks and Countermeasures, MILCOM 2008.

⁶⁵ (U) National Security Space Office, National Positioning, Navigation, and Timing Architecture Study Final Report, September 2008.

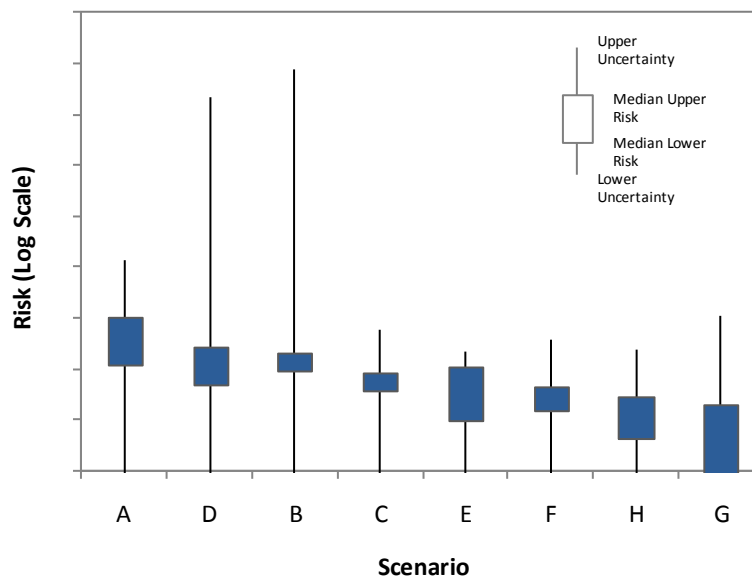
⁶⁶ ~~(U//FOUO)~~ U.S. Department of Transportation, Federal Railroad Administration, "Response to Positioning, Navigation, and Timing Data Call," 2009.

⁶⁷ (U) Salmi, Pekka, and Marko T. Torkkeli, "Inventions Utilizing Satellite Navigation Systems in the Railway Industry," Journal of Technology Management & Innovation 4(3)(2009).

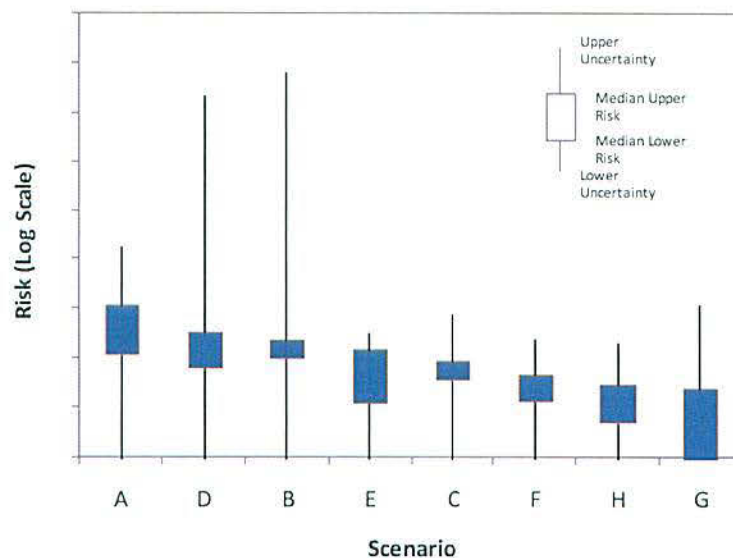
(U//FOUO) While these GPS disruption scenarios do not always result in the highest consequences for the Transportation Systems Sector modes, their assessed higher likelihood raised their risk rankings relative to the other GPS disruption scenarios. The SMEs who estimated the likelihood of these scenarios noted that there is significant uncertainty in these judgments as there is limited data on historical precedent for many of the scenarios. However, because there is historical precedent for scenarios involving intentional and unintentional jamming affecting GPS signals, these scenarios were judged to be more likely, thereby raising their relative risk.

(U//FOUO) The following two graphics illustrate the range of uncertainty associated with the assessed risk of each scenario's GPS disruption. The vertical scale denotes the risk and is displayed on a logarithmic scale. The horizontal scale shows each of the scenarios (A through H) in rank order from highest to lowest risk. The risk is the expected loss determined by the product of the likelihood and consequence for each scenario. (Further details on the methodology used to derive the risk can be found in Annex C: NRE Risk Assessment and Monte Carlo Simulation Methodology.)

(U//FOUO) Both graphics indicate that the GPS disruption scenarios A, D, and B present the highest risk to Transportation Systems Sector assets. For each scenario, the blue box represents the range of median risk scores and the vertical line indicates the uncertainty associated with the risk score. For the eight scenarios considered, Figures 5-5 and 5-6 show that the largest amount of uncertainty is associated with the assessed risk of GPS disruption scenarios D and B.



(U//FOUO) Figure 5-5: Aviation Subsector Risk



(U//FOUO) Figure 5-6: Maritime and Surface Subsector Risk

(U//FOUO) *Scenario A: An interference source is causing unintentional disruption. Ground receivers within a 30-km GTG radius are affected, and airborne receivers within radio LOS are affected.*

(U//FOUO) The majority of SMEs judged that this scenario would result in an isolated degradation in the aviation mode for less than seven days. When GPS interference is detected, air traffic controllers would act swiftly to change flight approaches and utilize legacy ground-based navigation aids, but capacity, efficiency, and surveillance could be impacted. Some SMEs noted that a degradation of GPS at a high-traffic airport would have broader impacts than would a similar degradation at a low-traffic airport.

(U//FOUO) Most SMEs judged the effects of this scenario would be isolated degradation of services of the other transportation modes also lasting for less than seven days. SMEs emphasized that this scenario would only have an isolated impact because the Transportation Systems Sector is diverse with multiple conveyance options. However, one SME noted that all modes are not alike—while rail could pick up some elements of highway transit or vice versa, the services provided by the maritime shipping industry in moving large quantities of goods into ports could not be readily replicated by other modes. Mariners would have to revert to manual methods of navigation, degrading the efficiency of services provided. For surface transport, remote traffic control systems and right-of-way controls at rail-highway interfaces could be disrupted.

(b)(7)e, (b)(7)f

(b)(7)e, (b)(7)f

Given that the interference

(b)(7)e, (b)(7)f

source is stationary and continuous, it should be relatively easy to locate within seven days. Disabling the interference source could involve coordination with a number of government agencies, including the FAA, FCC, and Federal Bureau of Investigation (FBI). The text box below describes the outcome of an intentional jamming exercise in the United Kingdom for maritime operations that are highly dependent on GPS technology.

(U) Pole Star Jamming Exercise

(U) Maritime operations have become heavily dependent on GPS-provided position, navigation, and timing information. The General Lighthouse Authorities of the United Kingdom and Ireland (GLA) have conducted multiple GPS jamming exercises to determine the effects of GPS loss on maritime navigation.

(U) In April 2008, the Northern Lighthouse Board vessel *NLV Pole Star* was directed to take a course through an area of GPS interference off the eastern coast of the United Kingdom. GLA and its partners used a low-to medium-power jammer transmitting a pseudo-random noise code on the L1 band of the GPS bandwidth at the 25-meter above ground level.¹ The *Pole Star* steered a course through the jamming area several times, exiting the area each time to reestablish contact with satellites. In addition to the *Pole Star's* GPS-enabled navigation equipment, GLA also installed two marine-grade differential receivers and a dual-frequency surveying receiver.²

(U) The crew of the *Pole Star* was able to quickly identify and shut off all alarms linked to GPS functions onboard the ship once the vessel passed into the jamming zone. The process of identifying and shutting down the alarms took 10 minutes, likely expedited because the crew of the *Pole Star* had been fully briefed and were prepared for system failure.³ Systems that failed included the differential GPS receivers, the dynamic positioning system, the automatic identification system transponder, the gyro calibration system, and digital selective calling.⁴ In addition, the crew became frustrated when the Electronic Chart Display and Information System (ECDIS) maintained a static position, so they shut the ECDIS off completely.⁵

(U) All receivers aboard the *Pole Star* lost GPS lock and either reported erroneous positioning in the case of the differential receivers or did not report any positioning data at all in the case of the survey-grade receiver.⁶ In addition, the receivers reported inflated speeds of up to 5000 knots. The greatest position and speed errors were recorded just as the ship passed into and out of the jamming area.⁷ As the GLA report indicates, should such loss of integrity in positioning and speed data occur during a maneuver, at night when the bridge of a ship is generally manned by one officer or in the future as ships shift to e-Navigation, the result could be catastrophic, particularly if the crew is not easily able to transition to non-GPS modes of attaining positioning data.⁸

¹ (U) The Royal Academy of Engineering, *Global Navigation Space Systems Reliance and Vulnerabilities* (March 30, 2011): p. 40.

² (U) Ibid., p. 42.

³ (U) Ibid., p. 41.

⁴ (U) Ibid.

⁵ (U) Ibid.

⁶ (U) The Royal Academy of Engineering, *Global Navigation Space Systems Reliance and Vulnerabilities* (March 30, 2011): p. 42-43.

⁷ (U) The National PNT Advisory Board. "Comments on – Jamming the Global Positioning System – A National Security Threat: Recent Events and Potential Cures." November 4, 2010. p.6.

⁸ (U) The Royal Academy of Engineering, *Global Navigation Space Systems Reliance and Vulnerabilities* (March 30, 2011): p. 41.

~~(U//FOUO)~~ *Scenario D: Jamming disruption from multiple low-power jammers on the ground. The jammers are stationary and mobile, with some intermittently active. Pockets of intermittent tracking and acquisition disruption occur across the metropolitan area.*

~~(U//FOUO)~~ For the aviation mode, most SMEs agreed that the effects of this scenario would last for more than 30 days and that these effects would be isolated degradation—generally a nuisance to aviation operations. Mitigation exists with legacy ground-based navigation aids, although capacity at affected airports could be reduced. One SME noted that there would need to be at least three WAAS reference stations out to have a widespread effect on WAAS services provided at locales other than those directly affected by jamming. This scenario also ranked as one of the higher consequence scenarios for aviation.⁶⁹

~~(U//FOUO)~~ For the rest of the Transportation Systems Sector, SMEs were divided as to whether the effects would last more or less than 30 days and on the severity of the outage. Most SMEs judged that the effects would be isolated degradation, while others judged isolated outage or widespread degradation. Affected maritime operations would shift to manual methods of navigation, reducing efficiency. Intermodal connection points, such as where maritime and rail meet, could also be adversely affected.

~~(U//FOUO)~~ For all transportation modes, SMEs attributed the duration of the scenario to the time it would take to identify, locate, and disable jammers that are dispersed and operating intermittently. One SME mentioned that there also could be psychological impacts from the scenario—GPS users in the Transportation Systems Sector might lose confidence in the reliability of GPS, and it is uncertain when they would regain it. For example, the loss of confidence in GPS has a greater consequence for air transportation in that flight dispatchers and pilots might plan flights without using GPS, impacting capacity and efficiency. This is particularly true with intermittent interruptions. This use of non-RNAV routing increases time in the air and fuel costs and reduces airport capacity. The textbox below describes an experience at Newark Liberty International Airport that is an example of Scenario D.

⁶⁹ ~~(U//FOUO)~~ The SME from the FAA estimated for Scenario D the highest frequency of occurrence on the scale – 10/day in CONUS, indicating that the proliferation of mobile jammers makes this the scenario that will occur most frequently. Because the median frequency of occurrence was selected for each scenario, this scenario's ranking is much lower than the FAA's estimate. Hence, the risk score is also lower.

~~(U)~~ The Newark International Airport Experience

~~(U//FOUO)~~ GPS reception on the ground at Newark Liberty International Airport (EWR) by differential GPS ground reference receivers is affected by multiple, mobile, low-power jammers (typically one jammer at any given time). There are daily events that constitute radio frequency interference (RFI) above FAA expectations as established in the interference mask for GPS. PPDs in vehicles on adjacent roadways are the source of the jamming. During a 127-day period in 2011, there were 127 events of RFI at EWR attributable to PPDs.¹ In another study, as many as five events per day were observed and could have been from PPDs.² Aviation receivers suffer unintended, collateral damage; the targeted GPS receivers are located in the same vehicles as the jammers. Isolation, detection, and confirmation of the interference sources by responsible authorities have been measured in months. Despite some enforcement and public education efforts,³ interference continues.

~~(U//FOUO)~~ The interference mask used in the design of the ground station was established by the FAA based on the policy and legal framework for spectrum protection afforded to GPS L1 by the USG for ARNS signals in the past. This expected level is codified in aviation ground and airborne equipment minimum operating standards.

~~(U//FOUO)~~ The differential GPS ground station at EWR is FAA approved and meets or exceeds the interference requirements. However, the airport authority, controllers, and operators are not satisfied with the performance and have rejected it until its interference robustness is increased significantly beyond the government standard. Note that each event could be longer than the duration of the jamming, since the cause for the anomaly would have to be understood to continue or resume operation in order to meet the high level of integrity expected of GBAS. The facility cannot be used for aviation operations while the ground manufacturer updates the design and site installation criteria (including geographical separation criteria for the ground receivers and antennas) and completes the FAA approval process again.

~~(U//FOUO)~~ While confirming the source of interference, multiple interference events at EWR were correlated with interference at a nearby National Geodetic Survey Continuously Operating Reference Station (CORS) site.⁴ Observations were consistent with a jammer located in a vehicle transiting the New Jersey Turnpike. The CORS station is significantly further from the roadway and correspondingly suffered less degradation.

~~(U//FOUO)~~ In an effort to identify if Newark was an isolated L1 interference environment, the FAA examined WAAS reference station data. The reference station sites are located in the United States (20 CONUS, 7 Alaska, 1 Hawaii, 1 Puerto Rico), Mexico (5), and Canada (4). Based on a 90-day observation period in 2010, 8 sites in the CONUS and 1 in Puerto Rico were identified as "problematic." These sites had a suspected interference event on at least 15 of the 90 days. The analysis was repeated for another 90 days with similar results. Note that the events cannot be positively attributed to PPDs.⁵

~~(U//FOUO)~~ At one of these "problem sites," however, interference from February through May 2011 was positively identified as originating from a PPD in a moving vehicle. Unfortunately, despite termination of broadcasts from that device, another mobile source has initiated transmissions at this location and has eluded efforts to isolate it.⁶

~~(U//FOUO)~~ The WAAS system did not suffer any significant operational performance degradations during this period due to PPDs, although there were five cases of brief, localized LPV service disruptions due to RFI according to the corresponding WAAS Performance Analysis Reports (1 July 2010 – 31 March 2011).^{7,8,9} LPV service is the most demanding approach service provided by WAAS.

~~(U//FOUO)~~ There is anecdotal evidence from pilot forums that low-level flight above certain stretches of roadways (such as along I-95 and I-35 near certain convenience stops) typically results in loss of GPS satellite tracking in small aircraft. PPDs are a suspected cause of the disruptions.

~~(U//FOUO)~~ The aviation experience seems to indicate a higher prevalence of PPDs in the United States, as well as a larger jamming radius for common cigarette lighter styles than previously assumed. It also highlights the effect of victim/jammer proximity and orientation on disruptions.

¹ (U) Zeta Associates, *PPD Detections near EWR*, TM 110708, dated 8 July 2011.

² (U) Zeta Associates, *EWR RFI Investigation – Characteristics of RFI between March 25 - April 19*, dated 9 June 2010.

³ (U) FCC Enforcement Bureau Steps Up Education and Enforcement Efforts Against Cellphone and GPS Jamming: Targeted Education and Outreach Coupled with Strict Enforcement. Action on February 9, 2011 by Public Notice (DA 11-249; DA 11-250).

⁴ (U) Zeta Associates, *Ongoing EWR RFI Investigation - Two G-II Receivers and Rotating Antenna*, TM100402, dated 2 April 2010.

⁵ (U) Federal Aviation Administration AJW-19, *GPS L1 RFI Quick Look Report Using Wide Area Reference Station (WRS) Data*, LAAS-229-001414-A, unpublished draft dated 10 November 2010.

⁶ (U) Zeta Associates - FAA correspondence, 2011.

⁷ (U) Federal Aviation Administration, NSTB/WAAS T&E Team, *Wide Area Augmentation System Performance Analysis Report, Report #34, Reporting Period to 1 July – 30 September 2010*, October 2010.

⁸ (U) Federal Aviation Administration, NSTB/WAAS T&E Team, *Wide Area Augmentation System Performance Analysis Report, Report #35, Reporting Period to 1 October – 31 December 2010*, January 2011.

⁹ (U) Federal Aviation Administration, NSTB/WAAS T&E Team, *Wide Area Augmentation System Performance Analysis Report, Report #36, Reporting Period to 1 January – 31 March 2011*, April 2011.

~~(U//FOUO)~~ **Scenario B: Jamming disruption from a single low-power stationary jammer. GPS receiver tracking is affected within a 500-m GTG radius and a 20-km LOS radius. GPS receiver acquisition is affected within an 800-m GTG radius and 30-km LOS radius.**

~~(U//FOUO)~~ Most SMEs agreed that this scenario would result in isolated degradation in the aviation mode and that this degradation would last for less than seven days. Service would be degraded, but legacy systems would provide sufficient services to preclude an outage. Aircraft would still be able to land but airport capacity would be reduced.

~~(U//FOUO)~~ For other transportation modes, SMEs also generally agreed that this scenario would result in isolated degradation lasting less than seven days. The effects would be isolated given the short range of the jammer.

~~(U//FOUO)~~ SMEs noted that it is easier for authorities to locate stationary jammers than moving ones, but that this jammer might be somewhat more challenging to locate than jammers in other scenarios because it is a lower power jammer.

~~(U)~~ **High-Consequence Scenarios**

~~(U//FOUO)~~ The GPS disruption scenarios judged to be of highest potential consequence (severity and duration) generally differed from those judged to be of highest potential risk. As noted previously, this divergence results from the inclusion of likelihood estimates in the determination of risk. Independent of considerations of likelihood, the following GPS disruption scenarios were judged to be of highest potential consequence for the Transportation Systems Sector. One exception for the aviation mode was Scenario D (multiple, low-power, continuous and intermittent, stationary and mobile jammers), which ranked high for both risk and consequence.

~~(U)~~ **Aviation Mode**

- ~~(U//FOUO)~~ Scenario G: Continuous multiple spoofers
- ~~(U//FOUO)~~ Scenario D: Multiple, low-power, continuous and intermittent, stationary and mobile jammers
- ~~(U//FOUO)~~ Scenario F: Continuous single spoofer
- ~~(U//FOUO)~~ Scenario H: Brief high-power jamming followed by continuous high-power spoofing

~~(U)~~ **Maritime and Surface Modes**

- ~~(U//FOUO)~~ Scenario G: Continuous multiple spoofers
- ~~(U//FOUO)~~ Scenario H: Brief high-power jamming followed by continuous high-power spoofing

~~(U)~~ **Aviation**

~~(U//FOUO)~~ The section that follows discusses the highest ranking consequence scenarios for the aviation mode of transportation, with the exception of Scenario D, which was discussed in the current risk estimate section above. More detailed descriptions of the consequences resulting from the lower ranking scenarios can be found in Annex E.

~~(U//FOUO)~~ **Scenario G: Sophisticated, coordinated pinpoint spoofing attacks against multiple target receivers (one spoofer per targeted receiver). Each spoofer independently walks off the time and position without raising alarms.**

~~(U//FOUO)~~ SMEs generally agreed that this scenario would result in widespread degradation to the aviation mode with effects lasting for more than 30 days. If spoofing was suspected or detected, aviation would no longer use GPS, WAAS, or GBAS. The scenario could particularly affect the general aviation industry, which relies more heavily on GPS and WAAS. Degradation would be widespread, but there likely would not be a mission outage because alternative systems like VHF omnidirectional range (VOR) are currently available. However, airspace performance and efficiency would be adversely affected.

~~(U//FOUO)~~ **Scenario F: Pinpoint spoofing attack against a single target receiver. The spoofer walks off time and position reported by the target receiver without raising alarms.**

~~(U//FOUO)~~ Most SMEs agreed that the effects of this scenario would be isolated degradation of services lasting for more than 30 days. SMEs noted that the aviation subsector might not realize a spoofing incident had occurred until an airplane crashed, for example, and then public confidence would be lost. Effects would be isolated, because the FAA would switch to an alternate navigation system—VOR—if spoofing was detected. SMEs agreed that a sophisticated hostile actor would perpetrate this scenario. It would be challenging to locate the spoofing source and terminate its operation. However, such an attack is generally only effective against one aircraft at a time.

~~(U//FOUO)~~ **Scenario H: Sophisticated, coordinated “navigation confusion” attack whereby a strategically placed multiple-watt transmitter generates GPS-like signals after an initial interval (several minutes) of jamming. Receivers within a three-km GTG radius and a 230-km LOS radius report a confident timing and position fix, but the timing is wrong by up to hundreds of microseconds and the position fix is wrong by up to tens of kilometers.**

~~(U//FOUO)~~ Most SMEs agreed that the effects of this scenario would be widespread degradation but there was some disagreement on the duration of the effects, with estimates ranging from less than 1 day to more than 30 days. SMEs agreed that there would be malicious intent behind implementation of this scenario and that it would require some sophistication to execute. In general, spoofing is much more complex than jamming, although there are multiple levels of mitigation for aircraft. Pilots would start using conventional navigation until the spoofing was shut down. One SME noted that it could take more than 30 days to locate the spoofing device unless military-grade equipment was used because the jamming portion is too brief for the FAA to find it. However, once GPS was declared unreliable, alternative navigation and surveillance systems would be used at the expense of airport capacity and system efficiency.

~~(U)~~ **Maritime and Surface**

~~(U//FOUO)~~ The following section discusses the highest ranking consequence scenarios for the maritime and surface modes of transportation. More detailed descriptions of the consequences resulting from the lower ranking scenarios can be found in Annex E.

~~(U//FOUO)~~ **Scenario G: Sophisticated, coordinated pinpoint spoofing attacks against multiple target receivers (one spoofer per targeted receiver). Each spoofer independently walks off the time and position without raising alarms.**

~~(U//FOUO)~~ SMEs disagreed as to whether the effects would last more or less than 30 days, because it would be difficult to locate and disable all spoofers. In addition, the adversary could activate the spoofers at different times over the course of an extended period of time. There also could be a longer-term loss of confidence in the GPS signal by users. SMEs were divided on the severity of the consequences of the scenario—from isolated degradation to widespread outage. One SME noted that, if an adversary was in possession of sophisticated spoofers, they would use them for maximum effect. Other SMEs emphasized that it would not be likely that a spoofing attack could disable the entire Transportation Systems Sector, but rather that cascading effects on the efficiency of the transportation system could extend beyond a metropolitan area. Some SMEs judged the effects could be widespread, because the spoofers are located throughout the country. SMEs noted that it is challenging to convey messages about suspected GPS disruptions throughout the Transportation Systems Sector; there are mechanisms in place to inform aviators and mariners but not the trucking industry, for example.

~~(U//FOUO)~~ **Scenario H: Sophisticated, coordinated “navigation confusion” attack whereby a strategically placed multiple-watt transmitter generates GPS-like signals after an initial interval (several minutes) of jamming. Receivers within a three-km GTG radius and a 230 – km LOS radius report a confident timing and position fix, but the timing is wrong by up to hundreds of microseconds and the position fix is wrong by up to tens of kilometers.**

~~(U//FOUO)~~ Most SMEs agreed that the effects of this scenario would be isolated outage and that the effects would last either less than 30 days or less than seven days. SMEs indicated that short jamming intervals followed by spoofing would be difficult to detect and disable. SMEs noted that the scenario has the potential to result in the outage of one subsector (such as maritime) but not the entire Transportation Systems Sector. SMEs noted the potential for catastrophe if a ship carrying hazardous cargo navigated off course but emphasized that a ship’s licensed pilot should be well trained in alternative methods of navigation to avert an accident. Location spoofing would be far more difficult to detect on the open ocean than near port. Erroneous timing could cause disruptions of SCADA nodes with loss of function until reset by human intervention. Public confidence in the reliability of the GPS signal also could be adversely affected.

~~(U)~~ Chapter 6. Sector Interdependencies

~~(U)~~ The four critical infrastructure sectors examined in this NRE share many dependencies and interdependencies with each other, as well as with the other critical infrastructure sectors not examined in the NRE. Because of dependencies between sectors, a GPS disruption that directly affects one sector may result in cascading and expanding effects to other sectors that rely on the affected sector, leading to collateral damage. Detailed information regarding the effects of GPS disruption on specific sectors can be found in the sector-specific current risk estimate sections of Chapter 5 (sections 5.5 through 5.8). This chapter focuses on the interdependencies among the four sectors to highlight the potential amplification of consequences of GPS disruptions.

~~(U//FOUO)~~ The Communications Sector has an important role because all other sectors depend on it to provide the means for information exchange.⁷⁰ In particular, the Emergency Services Sector depends on it to direct resources, coordinate response, alert the public, and receive emergency 911 calls.⁷¹ A GPS disruption affecting only this sector would affect those sectors, with the magnitude of impact depending on those sectors' backups. The Communications Sector heavily depends on the Energy Sector, which, through the electric grid, provides the electricity needed to power all communications nodes, systems equipment, and management and operations systems, for example.⁷²

~~(U//FOUO)~~ The Emergency Services Sector also has a unique interdependent relationship with all other sectors as it is the primary protector for all other sectors, which depend on the Emergency Services Sector for assistance with disaster planning, prevention, and mitigation, as well as response to day-to-day incidents and catastrophic situations.⁷³ However, GPS disruptions that only affect the Emergency Services Sector would likely have few, if any, direct effects on the other sectors.

~~(U//FOUO)~~ The Emergency Services Sector depends on the Energy and Transportation System Sectors⁷⁴ but is most heavily dependent on the Communications Sector. For example, the Enhanced 911 (E911) system is designed to provide location information for any cellular call placed to a 911 call center. Generally, the area code associated with a telephone number will be used to route the call to a local Public Safety Answering Point (PSAP); however, because cell phone users may not be located in the jurisdiction where their area code routes an emergency call, the E911 system location data allows the PSAP to route the call to the correct emergency services provider. Cellular companies provide the GPS timing and location information that makes the E911 system operable. Should GPS services not be available, E911 location services would be compromised.

⁷⁰ (U) Federal Communications Commission: Public Safety and Homeland Security Bureau Web page, "Tech Topic 19: Communications Interdependencies," <http://transition.fcc.gov/pshs/techtopics/techtopics19.html>, accessed August 22, 2011.

⁷¹ (U) U.S. Department of Homeland Security Web page, "Communications Sector: Critical Infrastructure and Key Resources," www.dhs.gov/files/programs/gc_1189102978131.shtm, accessed August 22, 2011.

⁷² (U) Federal Communications Commission: Public Safety and Homeland Security Bureau Web page, "Tech Topic 19: Communications Interdependencies," <http://transition.fcc.gov/pshs/techtopics/techtopics19.html>, accessed August 22, 2011.

⁷³ (U) U.S. Department of Homeland Security Web page, "Emergency Services Sector: Critical Infrastructure and Key Resources," www.dhs.gov/files/programs/gc_1189094187811.shtm, accessed August 22, 2011.

⁷⁴ (U) Office of Infrastructure Protection, *Emergency Services Sector-Specific Plan An Annex to the National Infrastructure Protection Plan*, Washington, DC: U.S. Department of Homeland Security, 2010, www.dhs.gov/xlibrary/assets/nipp-ssp-emergency-services.pdf, accessed August 22, 2011.

~~(U//FOUO)~~ The Energy Sector is another sector in which all other critical infrastructure sectors rely on it to some extent because it supplies energy to all sectors.⁷⁵ For instance, although many infrastructure systems have backup generators, those generators require refueling to continue operating. The Sector depends on the Communications and Transportation Systems Sectors.⁷⁶ For example, the Energy Sector relies on the Transportation Systems Sector for shipping crude oil and petroleum products into and throughout the country.⁷⁷ The Energy Sector's dependence on the Communications Sector is illustrated by its use of telecommunications providers for timing information needed to synchronize its servers.

~~(U//FOUO)~~ The Transportation Systems Sector is, as mentioned above, directly interdependent with the Energy Sector.⁷⁸ A sector that is indirectly dependent on the surface subsector of the Transportation Systems Sector is Communications, which often places its networking equipment along transportation routes (such as rail lines, highway tunnels, and bridges).⁷⁹ The maritime subsector shares interdependencies with other sectors as well. For example, if the Communications Sector were impacted by a GPS disruption, ports and other waterfronts would become less efficient, and safety could be indirectly affected. Because the Transportation Systems Sector consists of several subsectors—aviation, highway, maritime, mass transit, pipeline systems, and rail—it also has to deal with interdependencies among these modes.⁸⁰

⁷⁵ (U) U.S. Department of Homeland Security Web page, "Energy Sector: Critical Infrastructure and Key Resources," www.dhs.gov/files/programs/gc_1189013411585.shtm, accessed August 22, 2011.

⁷⁶ (U) Office of Infrastructure Protection, *Energy Sector-Specific Plan An Annex to the National Infrastructure Protection Plan*, Washington, DC: U.S. Department of Homeland Security, 2010, www.dhs.gov/xlibrary/assets/nipp-ssp-energy-2010.pdf, accessed August 22, 2011.

⁷⁷ (U) Office of Infrastructure Protection, *National Infrastructure Protection Plan Energy Sector*, Washington, DC: U.S. Department of Homeland Security, http://www.dhs.gov/xlibrary/assets/nipp_snapshot_energy.pdf, accessed August 22, 2011.

⁷⁸ (U) Office of Infrastructure Protection, *Transportation Systems Critical Infrastructure and Key Resources Sector-Specific Plan as Input to the National Infrastructure Protection Plan*, Washington, DC: U.S. Department of Homeland Security, May 2007, www.dhs.gov/xlibrary/assets/nipp-ssp-transportation.pdf, accessed 22 August 2011.

⁷⁹ (U) Ibid.

⁸⁰ (U) Office of Infrastructure Protection, *National Infrastructure Protection Plan Transportation Systems Sector*, Washington, DC: U.S. Department of Homeland Security, www.dhs.gov/xlibrary/assets/nipp_snapshot_transportation.pdf, accessed August 22, 2011.

~~(U)~~ The Banking and Finance Sector

~~(U//FOUO)~~ The Banking and Finance Sector is an example of a critical infrastructure sector that does not have direct critical dependencies on GPS but is dependent on other sectors that increasingly utilize GPS-enabled applications to fulfill their missions.

~~(U//FOUO)~~ While the Banking and Finance Sector does use GPS as a mechanism for coordinating Network Time Protocol (NTP) servers, it is not critical to the Sector's operation, and the disruption of GPS, even for a prolonged period of time, could be accommodated by the Sector. Although GPS provides a reference time signal to multiple time source applications used by the Sector, these time sources are designed to operate in the absence of a GPS signal. The accuracy of the time source could drift over a period of time if GPS is disrupted, but the NTP servers are designed to automatically select the best available time source from multiple alternative time sources available on the network.

~~(U//FOUO)~~ The Sector requires the ability to accurately determine the exact sequence of a set of events or transactions that take place over a period of time, but knowing the exact time is not critical. For some highly specialized systems, including high frequency trading systems, there is a need to coordinate time source in a way that enables precise determination of transaction sequences and elapsed time intervals between various transactions. This time sequencing takes place on collocated systems, which can provide a unified time reference. As a result, the effects of network delays and latency are highly controlled and not vulnerable to GPS interference.

~~(U//FOUO)~~ The Banking and Finance Sector is dependent on other sectors, particularly the Communications and Energy Sectors,¹ both of which increasingly use GPS-enabled applications.² A degradation of the services of these sectors caused by disruption of GPS could have adverse effects on the Banking and Finance Sector:

- ~~(U//FOUO)~~ The Banking and Finance Sector depends on the Energy Sector because loss of electric power over an extended period could hinder the efficient flow of electronic financial transactions, as well as result in the possible closure of bank branches and automatic teller machines (ATMs). However, critical Banking and Finance Sector processing facilities generally are protected from the loss of electrical grid power by a combination of uninterruptible power supplies and power generation capabilities that are tested under full load at regular intervals.³
- ~~(U//FOUO)~~ The Banking and Finance Sector depends on the Communications Sector to transmit transactions and for the operations of financial markets. A degradation of the telecommunications network could disrupt the ability of the Banking and Finance Sector to process transactions.

~~(U//FOUO)~~ The Banking and Finance Sector is working with other sectors and appropriate Government agencies to address these interdependencies and improve information sharing regarding interdependencies and potential protective measures.⁴

¹ ~~(U)~~ Office of Infrastructure Protection, National Infrastructure Protection Plan: Banking and Finance Sector, Washington, DC: U.S. Department of Homeland Security, www.dhs.gov/xlibrary/assets/nipp_snapshot_banking.pdf, accessed August 22, 2011.

² ~~(U//FOUO)~~ See Chapter 5 of this document: U.S. Department of Homeland Security, Homeland Infrastructure Threat and Risk Analysis Center, *National Risk Estimate: Risks to U.S. Critical Infrastructure from Global Positioning System Disruptions*, 2011.

³ ~~(U)~~ From an email from D. Edelman to R. Moore, September 27, 2011

⁴ ~~(U)~~ Office of Infrastructure Protection, *Banking and Finance Sector: Critical Infrastructure and Key Resources Sector-Specific Plan as Input to the National Infrastructure Protection Plan*, Washington, DC: U.S. Department of Homeland Security, May 2007, www.dhs.gov/xlibrary/assets/nipp-ssp-banking.pdf, accessed August 22, 2011.

~~(U)~~ Chapter 7. Estimated Evolution of GPS PNT Disruption Risks over the Next 20 Years

~~(U)~~ 7.1 Anticipated Future GPS Technology Developments

~~(U//FOUO)~~ As a national asset, GPS is expected to be available for the foreseeable future. The U.S. Air Force, as the GPS program manager, has plans to upgrade the system incrementally through 2020 with four programmed “block upgrades.” Most of these upgrades relate to the system’s military capabilities, but some are key improvements that will affect the civil sector.

- ~~(U//FOUO)~~ In 2017, military users will have access to a new signal—the Military-code, or M code—which will be more secure, have more power and will be more robust to jamming and spoofing than the present Precision encrypted or P(Y) code.
- ~~(U//FOUO)~~ Also in 2017, the Modernized GPS Control Segment will explicitly monitor the quality and integrity of the civil signal. Currently, only the Military P(Y)-code signal is explicitly monitored.
- ~~(U//FOUO)~~ In 2020, civil users will have access to multiple signals—L1 C/A, L1C, L2C, and L5. This signal diversity provides an inherent robustness to unintentional interference, but this is not necessarily true for intentional interference. The L5 signal is the safety of life signal, which is in a spectrum protected by international agreement.

~~(U//FOUO)~~ Notwithstanding the expected availability of an improving GPS system, the civil sector—both government and commercial—will face challenges to fully exploit these capabilities and to mitigate jamming and spoofing threats.

- ~~(U//FOUO)~~ The DOD, through the GPS Directorate, has requirements for civil signal monitoring and data distribution, but the details are still being finalized. The DOD’s GPS Directorate is working with DOT and FAA on this issue.
- ~~(U//FOUO)~~ Entities in our critical civilian infrastructure appear not to be fully aware of the potential for loss of GPS and of the options they might employ to mitigate that loss, such as chip-scale atomic clocks, multiple frequencies, anti-jam antennas, inertial navigation sensors, and intelligent receiver processing.
- ~~(U//FOUO)~~ Two possible threat mitigation initiatives would require U.S. policy and funding actions in addition to civilian sector involvement. One is the establishment of a “J911” system modeled on the E911 system, but this system is only a concept at this time.⁸¹ Under such a system, all cell phones would serve as passive detectors that would use crowd-sourcing to locate GPS jammers. The second initiative would be the establishment of a land-based backup system to GPS. A system called eLoran, based on Loran-C, was in development and included a signal authentication (anti-spoofing) feature, but that development was suspended with the termination of the Loran-C

⁸¹ ~~(U)~~ Scott, Logan, 911 *The Case for Fast Jammer Detection and Location Using Crowdsourcing Approaches*, paper presented at ION-GNSS-2011, September 20-23, 2011.

program. The FAA continues to investigate alternative PNT sources for the future as ground-based navigation aids are reduced.

~~(U//FOUO)~~ The dependence of the civil sector on GPS will face risks unless more proactive steps are taken to mitigate those risks.

~~(U)~~ **7.2 Alternative Futures for the Outlook of GPS Disruption Risk to Critical Infrastructure Sectors**

~~(U//FOUO)~~ This section presents alternative futures for how the risk of GPS disruption to critical infrastructure sectors might evolve over the next 20 years and discusses the implications for the public and private sectors in each alternative future. These alternative futures are not intended to predict the future, but to illustrate how each sector would be impacted if a specific future were a reality. This section also presents potential milestones that could serve as indicators for the development of these alternative futures as well as strategic surprises that could significantly alter their trajectories. These findings are drawn from a series of sector-specific workshops with SMEs held in May and June 2011. A full description of the methodology used to develop the alternative futures can be found in Annex D. Complete sector-specific alternative futures workshop reports can be found in Annex G.

~~(U//FOUO)~~ For additional information on capability gaps predominantly based on the limitations of GPS looking out to 2025, see the *National Positioning, Navigation, and Timing Architecture Implementation Plan*, a 2010 report from the Departments of Defense and Transportation.

~~(U)~~ **Communications Sector Alternative Futures**

~~(U//FOUO)~~ **Sector Growth/Dependency on GPS and GPS PNT** served as the two uncertainties facing the Sector that defined the four alternative futures (see Figure 7-1).

~~(U//FOUO)~~ **Sector Growth/Dependency on GPS** includes:

- ~~(U//FOUO)~~ Sector growth includes:
 - ~~(U//FOUO)~~ The pace and extent of growth of communications services for which GPS is an enabler.
 - ~~(U//FOUO)~~ The pace and extent of continued expansion of services requiring high capacity, synchronized transmission of wireless data (pictures, video, mobile users).
 - ~~(U//FOUO)~~ Industry willingness to adopt communications/navigation requirements that place burdens on communications services (transmit precise time, aiding information).
 - ~~(U//FOUO)~~ Communications demands for tighter timing synchronization.
- ~~(U//FOUO)~~ Sector growth implies dependency on GPS and includes:

- ~~(U//FOUO)~~ The degree to which the Sector depends on GPS, such as acceptance and prevalence of GPS-enabled components and systems in the Sector.
- ~~(U//FOUO)~~ The availability of alternatives, such as nationwide systems (e.g., a land-based backup), Sector-embedded systems (e.g., chip-scale atomic clocks, anti-jam antennas, and inertial navigation systems), and alternative signals of opportunity or better autonomous communications network timing sources.
- ~~(U//FOUO)~~ The ability to function with interference/loss.
- ~~(U//FOUO)~~ The ability of the Sector to recognize interference/loss of GPS and thereby enable rapid localization of interference sources.

~~(U//FOUO)~~ GPS PNT includes:

- ~~(U//FOUO)~~ The likelihood of a successful attack on GPS signal availability.
- ~~(U//FOUO)~~ The likelihood of a successful disruption of GPS signal availability and its impact on the Communications Sector (e.g., GPS attack, significant geomagnetic storm).
- ~~(U//FOUO)~~ PNT robustness realized through continued U.S. GPS program improvements, such as signal diversity and civil signal integrity monitoring, availability of accurate geospatial information, and enhancement of the National PNT architecture, including the provision of user notifications for any degradation.
- ~~(U//FOUO)~~ Interference threat mitigation capability, such as the ability to enforce technology controls and detect, respond to, and negate interference; practical defenses against spoofing and jamming; the ability of government to sustain the RNSS radio frequency environment used by GPS; and the ability of GPS manufacturers to design receivers that are less susceptible to spectrum interference.

		GPS PNT	
		Robust GPS system/resource	Vulnerable GPS system/resource
Sector Growth / Dependency on GPS	High growth, increasing GPS dependence	Low Maintenance Sports Car	High Maintenance Hot Rod
	High growth, decreasing GPS dependence	Reliable Minivan	Multi-fuel Jalopy

~~(U)~~ Figure 7-1: Communications Sector Alternative Future Matrix

~~(U//FOUO)~~ The **Reliable Minivan** and **High Maintenance Hot Rod** futures present unique challenges and are highlighted below.⁸² Annex G provides more detailed descriptions of all four alternative futures.

~~(U//FOUO)~~ **Reliable Minivan**

~~(U//FOUO)~~ The Reliable Minivan future will be marked by high growth in the sector, but with low dependence on GPS, along with a robust GPS system. In this future, time, attention, and money have been spent to ensure GPS robustness; however, because complete robustness cannot be ensured, there have been some moves toward other PNT services, possibly to a worldwide non-GPS standard.⁸³ PRS (Public Regulated Service), Galileo's service for military and police, is successful and may become the industry standard, allowing the Sector freedom from GPS dependence. Galileo has from the same vulnerability to jamming as GPS, however. Alternatively, the costs associated with IEEE 1588, a protocol for time transfer over wireline networks, may be reduced significantly, driving the market to that option. The widespread use of IEEE 1588 in this future, assuming that it is developed and deployed, will provide significant alternate timing capability to networks. That improvement will also make networks less vulnerable to jamming and spoofing. However, PTP does not provide timing to the precision available via GPS nor does it mitigate jamming and spoofing of non-timing applications of GPS. The use of IEEE 1588 will also lead to the loss of the ability to locate in some applications and the loss of some bandwidth and throughput because asynchronous networks will result in less accurate timing than synchronous ones. With the loss of GPS location services, positioning is disabled or extremely hampered, and E911 services are affected. There may also be some interoperability issues in this future as some communications products or subsectors continue to rely on GPS while others do not.

~~(U//FOUO)~~ In this future, the Sector is challenged to identify, afford, and implement alternative PNT systems. There could be the opportunity to partner with other GNSS systems for the provision of civil services. Technologies also could be developed that employ multiple available GPS frequencies.

~~(U//FOUO)~~ Workshop participants identified the following **milestones and variables**, which can be monitored by government and industry and could serve as indicators of the potential direction of identified uncertainties over the next 20 years:

- ~~(U//FOUO)~~ Rollout of a communications infrastructure that does not depend on GPS indicates the industry is moving toward a lessening dependence on GPS PNT.
- ~~(U//FOUO)~~ International treaties/agreements on GNSS that promote interchangeability indicate a lessening dependence on GPS as well as acknowledgment of the need for worldwide interoperability.

⁸² Each of the alternative future scenarios is given a short name that is consistent with the description of that particular future scenario and distinguishes that future from the other future scenarios.

⁸³ U.S. PNT policy actually targets non-reliance on foreign PNT systems.

- ~~(U//FOUO)~~ IEEE 1588 is implemented as an industry standard and cost-effective alternative, indicating that its ubiquity and drop in price have made it a viable alternative for timing.
- ~~(U//FOUO)~~ Multisystem receivers are used in the Communications Sector, indicating the industry has moved away from total GPS dependence by integrating the use of other systems.
- ~~(U//FOUO)~~ Galileo is successful and becomes the industry standard for PNT services, indicating a lessened or eliminated dependence on GPS but no substantive guard against jamming.
- ~~(U//FOUO)~~ Policy to promote GPS disruption monitoring, reporting, and mitigation is successful, indicating that policymakers understand the importance of maintaining a robust GPS system.
- ~~(U//FOUO)~~ IEEE 1588 technology fails to augment or replace GPS; there is a low uptake of the system. This would indicate that attempts to lessen dependence on GPS PNT were tried but failed.
- ~~(U//FOUO)~~ GPS continues to be an integral part of evolving communications infrastructure, indicating that the Sector has remained highly dependent on GPS.
- ~~(U//FOUO)~~ Failure of a policy to promote GPS disruption monitoring, reporting, and mitigation would likely indicate that GPS robustness has not been a priority.

~~(U//FOUO)~~ **High Maintenance Hot Rod**

~~(U//FOUO)~~ The High Maintenance Hot Rod future encompasses high growth and an increasing dependence on GPS but a vulnerable GPS system and resources. In this future, the Sector decisionmakers did not proactively implement policy, take technology changes into account, or pay attention to data indicating interference would continue, and also paid insufficient attention to a mitigation strategy. Instead, they were forced into a reactive posture in response to the proliferation of PPDs, issues with unintentional interference, spectrum conflicts and pressure, and possibly a coordinated attack on a metropolitan area, or some other significant, compelling event. Because this future leaves the Communications Sector open to a full range of periodic GPS outages, it has learned to live with nuisance-level impacts but is still open to a dire scenario. Networks serving large numbers of customers are affected more quickly than base/macro stations, and persistent flywheeling quickly causes problems for major service providers.

~~(U//FOUO)~~ A core challenge for government and industry in this future is explaining to the public how the situation was reached and that the system was left unprotected. The Sector would be challenged to overcome severe stresses on the GPS system and potential simultaneous loss of electric power and communications. Opportunities in this future include increasing the effectiveness of clocks in order to increase flywheel time as well as developing improved disciplining and learning algorithms for backup oscillators. There would also be an opportunity for policymakers to implement U.S. policy to detect and mitigate GPS interferences.

~~(U//FOUO)~~ Workshop participants identified the following **milestones and variables**, which can be monitored by government and industry and could serve as indicators of the potential direction of identified uncertainties over the next 20 years:

- ~~(U//FOUO)~~ National policy is ignored and GPS is as vulnerable as ever.
- ~~(U//FOUO)~~ Rollout of a communications infrastructure that is based upon GPS, along with predictions of higher throughput premised on that alone, indicates an increasing dependence on GPS in a growing sector.
- ~~(U//FOUO)~~ Lack of government analysis of alternatives to GPS as a PNT system would be a sign of increasing unilateral dependence on GPS.
- ~~(U//FOUO)~~ Failure to recognize PNT architecture as the basis for future government investment in PNT systems.
- ~~(U//FOUO)~~ Increased introduction of jammers and spoofers would indicate that the absence of a robust GPS signal has encouraged those interested in interfering with the system.
- ~~(U//FOUO)~~ Continued increase in interference events for privacy, criminal, and unintentional reasons would indicate that GPS has remained vulnerable.
- ~~(U//FOUO)~~ Demonstrable indication from the U.S. Government that GPS is a vulnerable system (along the lines of a cyber response) would indicate that policymakers understand the weaknesses of the system and are willing to address them.

~~(U//FOUO)~~ Workshop participants identified the following **strategic surprises**, which are low-probability, high-consequence events that could bring chaos to the sector and GPS:

- ~~(U//FOUO)~~ A sophisticated terrorist attack using GPS jamming and spoofing. Attackers would black out services in an area prior to an attack, impairing first responder capabilities.
- ~~(U//FOUO)~~ Systemic problem with GPS ground stations from the delivery of new software that is not backed up.
- ~~(U//FOUO)~~ Exploitation of a natural disaster by adversaries by impairing GPS services.
- ~~(U//FOUO)~~ Hiding a spoofing/jamming attack behind a space weather event, thereby exacerbating the damages caused by the event while concealing the existence of an intentional spoofing/jamming attack.
- ~~(U//FOUO)~~ Physical attack on operational command centers.
- ~~(U//FOUO)~~ Insider threat from satellite upload.
- ~~(U//FOUO)~~ A significant solar flare damages the satellite and smart grid systems, leaving temporal and long-term effects.

- ~~(U//FOUO)~~ A high-altitude, non-nuclear EMP.
- ~~(U//FOUO)~~ Half of the GPS constellation is wiped out by old age.
- ~~(U//FOUO)~~ A technological breakthrough makes GPS obsolete.
- ~~(U//FOUO)~~ Chip-scale atomic clock technology becomes ubiquitous.
- ~~(U//FOUO)~~ Private cellular providers roll out a fiber network that provides positioning, relative timing, and other GPS related services.

~~(U)~~ **Emergency Services Sector Alternative Futures**

~~(U//FOUO)~~ **Complexity of Growth** and **GPS PNT Disruption Likelihood** served as the two uncertainties facing the sector that defined four alternative futures (see Figure 7-2).

~~(U//FOUO)~~ **Complexity of growth** includes:

- ~~(U//FOUO)~~ Pace and extent of growth of emergency services for which GPS is an enabler, especially in the emergency services subsectors of law enforcement, fire and emergency services, emergency management, emergency medical services, and public works.
- ~~(U//FOUO)~~ Alternative and/or intermittent emergency services that require automated network control.
- ~~(U//FOUO)~~ Shift of communications technology to Internet Protocol-based technology (which would still result in GPS dependencies).
- ~~(U//FOUO)~~ Complexity of growth implies dependency on GPS, which includes:
 - ~~(U//FOUO)~~ Degree to which the Sector depends on GPS, such as acceptance and permeation of GPS-enabled components and systems in the sector and increasing reliance on GPS for safe operation of future vehicles.
 - ~~(U//FOUO)~~ Availability of alternatives, such as nationwide systems (e.g., a land-based backup) and/or sector-embedded systems, such as chip-scale atomic clocks, anti-jam antennas, and inertial navigation systems.
 - ~~(U//FOUO)~~ Ability to function with interference/loss, including ability of the Sector to recognize interference/loss of GPS, using a built-in detector in the automatic gain control of each GPS receiver, preparedness of the Sector for GPS outages, inadequate training or loss of Sector fallback operating skills given the loss of GPS.

~~(U//FOUO)~~ **GPS PNT Disruption Likelihood** includes:

- ~~(U//FOUO)~~ The likelihood of a successful intentional attack on GPS signal availability.
- ~~(U//FOUO)~~ PNT robustness realized through continued U.S. GPS program improvements, such as signal diversity and civil signal integrity monitoring; availability of accurate geospatial information; and enhancement of the National PNT architecture, including the provision of rapid user notifications for any degradation.
- ~~(U//FOUO)~~ Interference threat mitigation capability, such as the ability to enforce technology controls and rapidly detect, respond to, and negate interference.

		GPS PNT Disruption Likelihood	
		Mild/Moderate	Severe/Catastrophic
Complexity of Growth / Dependency on GPS	Robust	As Good As It Gets	It Wasn't Pretty But We Did It
	Vulnerable	Should Have Known Better	Knife to a Gun Fight

~~(U)~~ Figure 7-2: Emergency Services Sector Alternative Future Matrix

~~(U//FOUO)~~ The *Should Have Known Better* and *It Wasn't Pretty But We Did It* futures present unique challenges and are highlighted below. Annex G provides more detailed descriptions of all four alternative futures.

~~(U//FOUO)~~ **Should Have Known Better**

~~(U//FOUO)~~ In this future, the Sector is highly reliant on GPS to fulfill its mission and is faced with a mild or moderate GPS disruption—it is a test the Sector fails. Both GPS-enabled systems and backup manual skills failed. The Sector has become so reliant on GPS that backup manual navigation skills have not been adequately taught and maintained. Some systems that users did not know were tied to GPS also fail. The Sector does not demonstrate redundancy or the imagination to identify and implement alternative solutions. As a result, human life is at risk. Human resources are stretched thin, and budget resources drive dependence on inexpensive technology solutions that are not sufficiently robust. This future represents a teachable moment whereby the Sector can identify lessons learned and invest in mitigations to prevent more severe consequences in the future.

~~(U//FOUO)~~ A key challenge for the Sector in this scenario is avoiding a false sense of security that changes are not necessary since the Sector survived a GPS disruption. It would be important for the Sector to promote public awareness of the vulnerability of GPS-enabled systems to disruption and to promote awareness at the policy level of the need for long-range planning and funding for GPS backups. This future presents an opportunity for the Sector to provide training and organize exercises to prepare for potential future outages. These exercises could enable the Sector to develop a better understanding of the relationships between first responders in emergency situations as well as their reliance on GPS-enabled systems. There is also the opportunity in this future for industry to capitalize on an emerging marketplace and develop alternative PNT systems and capabilities.

~~(U//FOUO)~~ Workshop participants identified the following **milestones and variables**, which can be monitored by government and industry and could serve as indicators of the potential direction of identified uncertainties over the next 20 years:

- ~~(U//FOUO)~~ The widespread use of GPS-enabled devices by the Sector indicates the Sector is becoming increasingly dependent on GPS services. In addition, the inclusion of

GPS systems as built-ins for first responder vehicles and equipment could indicate increased reliance on GPS.

- ~~(U//FOUO)~~ Lack of focus on training and exercise of manual navigation techniques would make the Sector increasingly reliant on GPS services.
- ~~(U//FOUO)~~ Limited resources and lack of resolve to prioritize GPS backups suggest the United States is on the path toward this future.

~~(U//FOUO)~~ It Wasn't Pretty But We Did It

~~(U//FOUO)~~ In this future, the Sector is not entirely dependent on GPS to fulfill its mission when it is faced with a severe or catastrophic GPS disruption. The Sector had identified and preserved the fundamental human skills and knowledge needed to serve as a backup to GPS and was able to implement them during the GPS disruption. While the Sector is stressed and less efficient, it is able to accomplish its mission and minimize loss of life. In order to reach this future, the Sector had planned and trained for additional system capabilities other than GPS to provide robustness through alternative PNT sources.

~~(U//FOUO)~~ A core challenge for the Sector in this future is developing warning and notification systems to alert Sector users that GPS is down and that backup capabilities need to be employed. The Sector also will be challenged to find cost-effective ways to build appropriate levels of robustness, including ensuring a robust training and exercise regimen to maintain adequate GPS backup capabilities. This future presents the opportunity for the Sector to conduct civil preparedness drills focusing on GPS dependencies as well as to promote awareness of the vulnerability of GPS-enabled systems among users in the Sector. This future would also present an opportunity for government and industry to promote the development and implementation of innovative GPS backup systems and disruption mitigation measures.

~~(U//FOUO)~~ Workshop participants identified the following **milestones and variables**, which can be monitored by government and industry and could serve as indicators of the potential direction of identified uncertainties over the next 20 years:

- ~~(U//FOUO)~~ The dual use of military technology to improve the robustness of commercial GPS technology could foster a more resilient sector.
- ~~(U//FOUO)~~ The proactive identification and implementation of key capabilities to overcome or circumvent disruptions would enable the Sector to adapt to the disruption of GPS.
- ~~(U//FOUO)~~ The inclusion of GPS disruption in emergency response exercises would indicate the Sector is aware of the vulnerability and is taking steps to ensure adequate backup or mitigation measures are in place.
- ~~(U//FOUO)~~ The preponderance of portable jamming devices and information on jamming and spoofing techniques make it more likely that an intentional or unintentional GPS disruption incident could occur.

- ~~(U//FOUO)~~ Increased pressure to accommodate more GNSS systems in RNSS spectrum leaves less spectrum than originally envisioned for individual GNSS systems and could make them more vulnerable to disruption.

~~(U//FOUO)~~ Workshop participants identified the following **strategic surprises**, which are low-probability, high-consequence events that could bring chaos to the sector and GPS:

- ~~(U//FOUO)~~ A localized or widespread natural disaster coupled with intentional disruption of GPS services could impair the ability of the Sector to fulfill its mission.
- ~~(U//FOUO)~~ A massive solar event that takes out the electric power grid could disrupt the Sector's ability to communicate and employ GPS services.
- ~~(U//FOUO)~~ The Sector adapts a system wherein dependency on GPS services is not widely known.
- ~~(U//FOUO)~~ An intentional software virus disables GPS software.
- ~~(U//FOUO)~~ An alternative PNT system is developed by another country and widely adopted throughout the world. The United States becomes dependent on that system.
- ~~(U//FOUO)~~ The malicious, simultaneous manipulation of international PNT systems would cause havoc for the Sector.

~~(U)~~ **Energy Sector Alternative Futures**

~~(U//FOUO)~~ **Complexity Growth/Dependency on GPS** and **GPS Attack** served as the two uncertainties facing the Sector that defined the four alternative futures (see Figure 7-3).

~~(U//FOUO)~~ **Complexity Growth/Dependency on GPS** includes:

- ~~(U//FOUO)~~ The pace and extent of the growth of energy sources for which GPS is an enabler, such as smart grid.
- ~~(U//FOUO)~~ Alternative and/or intermittent energy sources that require enhanced automated network control.
- ~~(U//FOUO)~~ Exploration, extraction, and transportation approaches that require PNT.
- ~~(U//FOUO)~~ Dependency on GPS also includes:
 - ~~(U//FOUO)~~ The degree to which the Sector depends on GPS, such as acceptance and permeation of GPS-enabled components and systems in the Sector.
 - ~~(U//FOUO)~~ Availability of alternatives, such as nationwide systems (e.g., a land-based backup) and/or Sector-embedded systems, such as chip-scale atomic clocks, anti-jam antennas, inertial navigation systems, and jamming detection on GPS receivers and software tools.
 - ~~(U//FOUO)~~ The ability to function with interference/loss, including ability of the Sector to recognize the interference/loss of GPS.

~~(U//FOUO)~~ **GPS Attack** includes:

- ~~(U//FOUO)~~ The likelihood of a successful attack on GPS signals availability.
- ~~(U//FOUO)~~ PNT robustness realized through continued U.S. GPS program improvements, such as signal diversity and civil signal integrity monitoring, availability of accurate geospatial information, and enhancement of the National PNT architecture, including the provision of user notifications for any degradation.
- ~~(U//FOUO)~~ Interference threat mitigation capability, such as the ability to enforce technology controls and detect, respond to, and negate interference.

		GPS Attack	
		Limited Impact	Extensive Impact
Complexity Growth / Dependency on GPS	Integrated Dependence	Lights On, Pipes Full	I Might Survive
	Unilateral Dependence	I Will Survive	Lights Off, Pipes Clogged

(U) Figure 7-3: Energy Sector Alternative Future Matrix

(U//FOUO) The *I Will Survive* and *I Might Survive* futures present unique challenges and are highlighted below. Annex G provides more detailed descriptions of all four alternative futures.

(U//FOUO) I Will Survive

(U//FOUO) In the I Will Survive future, technology evolution will allow for unilateral dependence on GPS because new technologies mitigate against the effects of attacks on GPS. However, because of unilateral dependence, the Sector has anticipated and accepts a level of inefficiency and risk in the system, including isolated, sporadic outages and intermittent energy shortages. Inefficiencies may be exacerbated by the need for islanding, in which parts of the system are not operating in sync with the rest of the system and phase regulation is no longer being controlled. Critical areas such as hospitals; public utilities such as drinking water systems, firefighting hydrants, wastewater treatment plants; and first responders might require their own energy backup systems to mitigate effects from outages. In addition, the anticipated need for more energy emergency backup capabilities will drive up expenses associated with purchasing and maintaining the redundant systems.

(U//FOUO) Challenges presented by this future include convincing Sector owners and operators to invest in local GPS backups for their facilities. The availability of an extremely reliable GPS system leads to no incentive to advance alternative systems. The future does offer the opportunity for technology shifts that could change the way the Sector does business, e.g., large capacity or long-term storage. GPS receiver manufacturers could be encouraged to make multi-system/multi-frequency receivers. Government regulations could require systems to be tested to demonstrate that operations can continue without GPS.

(U//FOUO) Workshop participants identified the following **milestones and variables**, which can be monitored by government and industry and could serve as indicators of the potential direction of identified uncertainties over the next 20 years:

- (U//FOUO) The industry accepting more dependency on GPS without mitigations is an indicator the Sector is moving toward unilateral dependence.

- ~~(U//FOUO)~~ The North American Electric Reliability Corporation (NERC) designating GPS as a Critical Cyber Asset (CIP-002) shows that the industry recognizes GPS needs to be protected like other cyber assets owing to the unilateral dependence upon it.
- ~~(U//FOUO)~~ Acceptance of nuisance outages by the Sector and public forecast the limited impact of GPS attacks in this future.
- ~~(U//FOUO)~~ Erosion of commitment to protect the GPS portion of L Band satellite services increases potential for GPS disruptions.
- ~~(U//FOUO)~~ Emergence of threats like cigarette lighter privacy jammers and other easily available jammers as well as hackers is an indicator that the Sector could be prone to GPS disruptions.
- ~~(U//FOUO)~~ The shift in use of the PMUs from simple monitoring to a control function would indicate the Sector is increasingly reliant on GPS.

~~(U//FOUO)~~ I Might Survive

~~(U//FOUO)~~ The I Might Survive future encompasses integrated dependence on GPS but nevertheless experiences extensive impact from GPS attacks. In this future, the Sector attempted to provide backups for GPS but was ultimately unprepared for various reasons, including that an effective backup capacity was not achieved, alternative PNT systems did not work out, the technology or Sector went in an unexpected direction, or the Sector misjudged the requirements for energy capacity or the sophistication of an attack. GPS attacks have the potential to last a long time and affect a large geographic area. This future may necessitate falling back on earlier methods in which GPS is not a critical function. Because onsite backup systems are not in place, there is a premium on awareness, responsiveness, and alternative plans in the face of attacks.

~~(U//FOUO)~~ In this future, the Sector would be challenged to demonstrate the independence of backup systems to ensure there is no single point of failure and to ensure that the backup could last for a long period of time or indefinitely. The Sector would also need to develop contingency plans for a “graceful” recovery from a GPS disruption. This future presents an opportunity for the Sector to develop continuity of operations plans and exercises to demonstrate its ability to operate without GPS. There is also an opportunity for sharing of best practices for backups and mitigations within the Energy Sector and across other sectors.

~~(U//FOUO)~~ Workshop participants identified the following **milestones and variables**, which can be monitored by government and industry and could serve as indicators of the potential direction of identified uncertainties over the next 20 years:

- ~~(U//FOUO)~~ Investments in GPS backup systems, assuming that alternative sources of PNT become available.
- ~~(U//FOUO)~~ Other sectors (IT, Communications) have impetus to innovate by means other than GPS, especially in precision time transfer.
- ~~(U//FOUO)~~ The use of non-GNSS systems instead of GPS for PMUs by other countries.

- ~~(U//FOUO)~~ Increased deployments of PMUs over a wider area.
- ~~(U//FOUO)~~ Other countries (particularly Canada) continue to embrace and quickly deploy PMU technology.
- ~~(U//FOUO)~~ Emergence of new businesses/research and development results that recognize threats to GPS and offer expertise to the Energy Sector to enhance systems' robustness.
- ~~(U//FOUO)~~ International agreements regarding the need to protect GPS in the civilian arena from the production and employment of GPS interference devices, such as privacy jammers.
- ~~(U//FOUO)~~ Effective use of U.S. power lines as a means of data transfer.

~~(U//FOUO)~~ Workshop participants identified the following *strategic surprises*, which are low-probability, high-consequence events that could bring chaos to the sector and GPS:

- ~~(U//FOUO)~~ Mounting an attack on Energy and GPS in the near term, most likely through a hacker.
- ~~(U//FOUO)~~ A large geomagnetic storm takes out capacity, which could affect both GPS and the Sector.
- ~~(U//FOUO)~~ A September 11, 2001-type attack on a major metropolitan area, such as a vehicle-borne improvised explosive device (IED) in concert with a preemptive GPS jamming attack to exacerbate consequences by introducing confusion to first responders operations.
- ~~(U//FOUO)~~ A kinetic attack against substations and then jamming or spoofing, possibly at the same time a major, widespread weather event is occurring.
- ~~(U//FOUO)~~ Alternating attacks between the east and west coasts to exceed spare requirements or move spares in one direction and attack in the other.

~~(U)~~ **Transportation Systems Sector Alternative Futures**

~~(U//FOUO)~~ **Dependency on GPS** and **Debilitating GPS Attack** served as the two uncertainties facing the Sector that defined four alternative futures (see Figure 7-4).

~~(U//FOUO)~~ **Dependency on GPS** includes:

- ~~(U//FOUO)~~ The degree to which the Sector depends on GPS, such as acceptance and permeation of GPS-enabled components and systems in the Sector.
- ~~(U//FOUO)~~ The availability of alternatives, such as nationwide systems (e.g., a land-based backup) and/or Sector-embedded systems, such as chip-scale atomic clocks, anti-jam antennas, and inertial navigation systems.
- ~~(U//FOUO)~~ The ability to function with interference/loss, including ability of the Sector to recognize interference/loss of GPS (e.g., with built-in interference detectors in the GPS receivers).

~~(U//FOUO)~~ **Debilitating GPS Attack** includes:

- ~~(U//FOUO)~~ The likelihood of a successful attack that interferes with GPS signal availability.
- ~~(U//FOUO)~~ PNT robustness realized through continued U.S. GPS program improvements, such as signal diversity and civil signal integrity monitoring; availability of accurate geospatial information; and enhancement of the national PNT architecture, including provision of user notifications for any degradation.
- ~~(U//FOUO)~~ Interference threat mitigation capability, such as the ability to enforce technology controls and detect, respond to, and negate interference.

		Debilitating GPS Attack	
		Effective Response	Ineffective Response
Dependency on GPS	Shared Dependency	Blue Sky and Sunshine	Muddle Through
	Unilateral Dependency	High Anxiety	GPS 9/11

~~(U)~~ **Figure 7-4: Transportation Systems Sector Alternative Future Matrix**

~~(U//FOUO)~~ The **High Anxiety** and **Muddle Through** futures present unique challenges and are highlighted below. Annex G provides more detailed descriptions of all four alternative futures.

~~(U//FOUO)~~ **High Anxiety**

~~(U//FOUO)~~ In the High Anxiety future, the Transportation Systems Sector is dependent on GPS without backup systems, but the government and industry are able to effectively detect, respond to, and mitigate against a debilitating attack on the GPS system. Disruption of GPS leads to economic losses as well as potential safety and security impacts. Aircraft are forced to use alternative navigation systems, and timing disturbances could affect rail and pipelines. The effective response capabilities of government and industry to an attack on the GPS system ensure that the Sector can operate through the attack but at lower efficiency levels. There is a high demand on human operators to take effective actions to back up GPS services.

~~(U//FOUO)~~ A key challenge for the Sector in this future is identifying an acceptable threshold for economic losses and determining an adequate response. There would also need to be training in each transportation mode for the use of non-GPS systems. An additional challenge would be convincing policymakers that there is a real threat posed by this future and that there needs to be political will to promote investments in backup systems. This future presents opportunities for promoting research and development of backup systems and discussion on the development of GPS alternatives. There is also an opportunity to educate government and industry about the danger to transportation modes of using GPS as a sole source for PNT services.

~~(U//FOUO)~~ Workshop participants identified the following **milestones and variables**, which can be monitored by government and industry and could serve as indicators of the potential direction of identified uncertainties over the next 20 years:

- ~~(U//FOUO)~~ A drastic increase in the number of devices sold with GPS-enabled applications, such as smart phones, is an indicator of increased dependence on GPS.
- ~~(U//FOUO)~~ An increase in the international investment in GPS alternatives, including ground-based systems, indicates a recognition that sole reliance on GPS is inadequate.
- ~~(U//FOUO)~~ More regulation requiring use of GPS, such as for mileage taxes or inland river navigation, signals an increased dependence on GPS.
- ~~(U//FOUO)~~ Moves away from backup or redundant systems to save money are another indicator of sole dependence on GPS.
- ~~(U//FOUO)~~ Increased privacy concerns among the public about the location-tracking capabilities of GPS-enabled devices could indicate GPS is ubiquitous.

~~(U//FOUO)~~ **Muddle Through**

~~(U//FOUO)~~ The Muddle Through future is marked by low dependence on GPS due to available backup systems, but government and industry are not able to effectively detect, respond to, and mitigate against a debilitating attack on the GPS system. Investments in backup systems over the

previous 20 years ensure PNT functions are still available but at reduced efficiency, leading to some economic losses. However, this future reflects a lack of system robustness and poor planning in building capacity to detect, respond to, and mitigate against GPS disruptions. The government is perceived to be incompetent. A core question for policymakers in this future is how much they are willing to spend on GPS backups to maintain a sufficient level of operation.

~~(U//FOUO)~~ This future presents the challenge of convincing policymakers to maintain multiple systems to ensure that national GPS operations continue and that there is continuity of operations for each transportation mode. The Sector would need to determine the length of time the public would be willing to accept a lower quality backup system. The Sector would also need to cope with the limited skills of those who are forced to use alternative PNT systems, including manual navigation techniques. This future offers opportunities for investment in R&D for alternative PNT systems. The Sector could explore ways to operate without GPS and practice operations with those alternatives. In addition, the sharing of information across modes would allow for coordination of requirements and development of solutions that benefit a broad user base throughout the Sector.

~~(U//FOUO)~~ Workshop participants identified the following **milestones and variables**, which can be monitored by government and industry and could serve as indicators of the potential direction of identified uncertainties over the next 20 years:

- ~~(U//FOUO)~~ The occurrence of interference events could indicate an increased likelihood of a successful debilitating attack on GPS as well as highlight ineffective response capabilities.
- ~~(U//FOUO)~~ The investigation by individual government agencies of GPS alternatives could indicate a trend toward developing backup systems (shared dependency).
- ~~(U//FOUO)~~ The emergence of U.S. policy requiring GPS backups as a function of government that agencies must implement would also promote a shift toward shared dependency.
- ~~(U//FOUO)~~ Public pressure for a GPS backup system could affect the pace of R&D efforts to enhance response capabilities.
- ~~(U//FOUO)~~ An increase in the international investment in GPS alternatives, including ground-based systems or low-earth orbiting satellites, could signal a growing trend toward a future with available GPS backups.
- ~~(U//FOUO)~~ The continual iterations of GPS robustness plans without actual plan implementation could lead to a future where government and industry are not able to effectively respond to an attack on GPS.

~~(U//FOUO)~~ Workshop participants identified the following **strategic surprises**, which are low-probability, high-consequence events that could bring chaos to the sector and GPS:

- ~~(U//FOUO)~~ Solar weather takes out a significant portion of satellites, leading to a depleted constellation that would take years to replace.

- ~~(U//FOUO)~~ The confluence of a natural disaster and GPS disruption affecting emergency response, communications systems, etc.
- ~~(U//FOUO)~~ Government issues a license for a ground-based transmitter frequency close to the GPS L Band, leading to disruptions in GPS.
- ~~(U//FOUO)~~ Aging constellations that are well beyond their useful life, leading to a potential cascading GPS failure.
- ~~(U//FOUO)~~ A major hazardous materials (HAZMAT) incident in the transportation system caused by GPS disruption.
- ~~(U//FOUO)~~ A spoofing incident targeting offshore drilling platforms.
- (U//FOUO) Systemic GPS failure from new software supporting the GPS system.
- ~~(U//FOUO)~~ Lack of confidence in GPS because of repeated disruptions leads to missed economic benefits in areas such as intelligent highways.
- ~~(U//FOUO)~~ A public backlash against GPS because of privacy concerns.
- ~~(U//FOUO)~~ A transfer to a foreign PNT system due to a major loss of confidence in GPS.
- ~~(U//FOUO)~~ A nation-state or terrorist group publicizing an attack on the GPS system.

~~(U)~~ Chapter 8. Current and Projected Future Mitigation Measures

~~(U//FOUO)~~ During a series of NRE sector-specific workshops, the SMEs discussed various mitigation strategies. One series of workshops addressed Alternative Futures looking out 20 years and a second series of workshops focused on the consequences of GPS disruptions.

~~(U//FOUO)~~ The NRE sector-specific alternative futures workshops presented the following opportunities for government and the private sector to mitigate disruption risk proactively by:

- ~~(U//FOUO)~~ Identifying, funding, and implementing a GPS backup system or PNT alternatives;
- ~~(U//FOUO)~~ Developing and populating a single repository to capture information on GPS disruption incidents across the United States;
- ~~(U//FOUO)~~ Promoting GPS program improvements like signal diversity, signal robustness, signal integrity monitoring, and user notifications of degradation;
- ~~(U//FOUO)~~ Implementing regulations and tools to enforce technology controls on GPS interference devices and to detect, respond to, and negate interference;
- ~~(U//FOUO)~~ Implementing regulations and training for law enforcement to locate and eliminate sources of interference and jamming; and
- ~~(U//FOUO)~~ Conducting training and exercises to broaden awareness of GPS vulnerabilities and to prepare for continuity of operations during GPS disruption incidents.

~~(U//FOUO)~~ During the series of NRE sector-specific consequence workshops, SMEs also discussed various mitigation strategies to deal with the consequences of various types of GPS disruptions. Some mitigation strategies can be applied across multiple sectors and others are targeted uniquely at specific sectors. In addition, some mitigations discussed aim to lessen the impact of GPS disruptions while others eliminate the disruptions.

~~(U//FOUO)~~ For example, methods for using inertial sensors combined with signals of opportunity stabilized with rubidium oscillators offer possible means for filling the gap that might develop in the event of degradation of GPS availability.⁸⁴

~~(U)~~ Communications Sector

~~(U//FOUO)~~ SMEs identified mitigation measures in use throughout the Communications Sector to minimize the effects of disruption of GPS services. Built-in timing backups (e.g., rubidium vapor or cesium beam oscillators) can continue timing functionality for the Sector in the event of

⁸⁴ (U) Matthews, Michael. B., Peter. F. MacDoran, and Kenn L. Gold, "SCP Enabled Navigation Using Signals of Opportunity in GPS Obstructed Environments," *Navigation* 58(2)(2011): pp. 91–110.

a GPS disruption or degradation, but these are not uniformly deployed across telecommunications or data networks. Rubidium vapor or cesium beam oscillators could provide reliable timing for about a month without GPS while ovenized crystal oscillators will last for about two days. After that, timing error will drift beyond acceptable bounds.

~~(U)~~ **Emergency Services Sector**

~~(U//FOUO)~~ There are various mitigation methods used within the Emergency Services Sector that could potentially lessen or eliminate the effects of the disruptions encountered in the scenarios. On a general level, if a jurisdiction within the Sector has maintained its conventional legacy systems (various nonspecific systems predating the use of GPS in the Sector) or, if not the old equipment, at least the frequencies on which the legacy systems run, then this offers an option. However, while it may be possible today for jurisdictions to maintain their legacy systems, at least in the Federal sector, many users have been required to release their legacy frequencies for reassignment, narrow-banding, or sale to the private sector. In these cases, either the legacy frequencies are not longer available or the legacy equipment is no longer compatible with frequencies that have been compressed into narrow-band segments. Most users will not be able to maintain two separate systems and infrastructure forever.

~~(U//FOUO)~~ Workshop participants concluded that the Sector has the advantage of being trained for emergencies, such as those in the scenarios—many, if not most, emergency agencies are trained on how to operate manually, should the need arise. The Emergency Services Sector also relies heavily on dispatchers, who can, during GPS-based disruptions and outages, serve as a hub of sorts, collecting and relaying information manually.

~~(U//FOUO)~~ Should a GPS disruption lead to communications failures, several specific mitigations were also discussed. If the GPS timing reference were lost, simulcast capabilities would be lost as well. Multiple timing systems that currently exist could offer a backup, but the *GPS Risk Mitigation Techniques and Programs Report* addresses this in depth. In addition, simplex or half duplex systems on conventional repeaters could offer an additional avenue for communication (should a jurisdiction choose to provide this backup capability). If location-based GPS services are lost, the easiest mitigation is the use of manual fixes. The Sector could, if necessary, revert to using paper maps, if the maps and adequate training are available, or even getting directions from another person to locate addresses.

~~(U)~~ **Energy Sector**

~~(U//FOUO)~~ There are various mitigation methods used within the Energy Sector that could potentially lessen or eliminate the effects of the disruptions encountered in the scenarios. The Energy Sector has several advantages when dealing with disruptions. Baseline operations for the Sector include occasional degradation of services, so the Sector has experience and procedures for mitigation of the cause. In addition, there is a great deal of redundancy in the power grid and other energy subsectors, which would also minimize the effects that would result from the scenarios described. The sources of continuous or higher powered GPS disruption can be more readily located than the sources of intermittent or lower powered GPS disruption. Locating and disabling these sources requires timely coordination across multiple government agencies.

~~(U)~~ *Transportation Systems Sector*

- ~~(U//FOUO)~~ The diversity of transportation options available across the Transportation Systems Sector makes the Sector inherently resilient to disruptions in a single mode. However, an outage in one mode could result in reduced efficiency system-wide. In particular, it would be challenging for other modes to take on the transport of large cargo that is normally transported around the world on container ships.
- ~~(U//FOUO)~~ Aviation in the National Airspace System (NAS) has a number of backup systems to GPS in place (VOR, distance measuring equipment [DME], instrument landing systems [ILS]) that are based on terrestrial navigation aids that were used before satellite navigation became available. If GPS interference is detected, air traffic controllers will begin to migrate aircraft to ground-based navigation, if available. Monitoring within the avionics of both the received GPS signal and the current receiver performance may provide multiple opportunities for the detection of spoofing. Pilots would start using alternate means of navigation until the spoofing is shut down. If aircraft are currently equipped with these ground based navigational aids, no additional cost to the users would be incurred. If users are not equipped to use these alternate means of navigation, however, required avionics modifications may involve significant costs.
- ~~(U//FOUO)~~ However, aviation in the NAS is becoming increasingly dependent on GPS services, with planned phase-out of many land-based navigation aids over the next several years. In particular, general aviation is very dependent on GPS for daily operations in airspace not supported by other land navigation aids. The terrestrial navigation aids that were used before satellite navigation became available could fade quickly as FAA's planned Next Generation Air Transportation System (NextGen) is implemented. The FAA is transforming air traffic control from a ground-based system of radars to a GPS and GPS-augmented satellite-based system through NextGen. NextGen is critically important because, as FAA has stated publicly, "[t]he current system will not be able to handle traffic that is expected to increase to one billion passengers by 2015 and double current levels by 2025."⁸⁵
- ~~(U//FOUO)~~ In the event of a GPS outage, mariners can use alternative methods of navigation, including radar, celestial, and visual navigation; visual ranges; lights; and buoys. In addition, in high-traffic ports many types of commercial vessels are required to bring aboard a pilot to guide the ships in the port, adding another layer of protection. AIS systems on ships, which get some of their position and timing data from GPS, can function without GPS—albeit with diminished situational awareness—because they rely on other navigation systems as well. In addition, some, but not all, maritime users have equipment that has integrity monitoring (such as Differential Global Positioning System [DGPS]) and will alert them to GPS disruptions. These methods may be less efficient than GPS-based navigation methods. Mariners may also be able to use GLONASS (and eventually Galileo) PNT signals as an alternative to the GPS signal; however, while these systems would provide an alternative in the event of a problem with GPS itself, a disruption arising from space weather would affect all space-based systems equally.

⁸⁵ ~~(U)~~ FAA Web page, "Fact Sheet – Next Generation Air Transportation System 2006 Progress Report," www.faa.gov/news/fact_sheets/news_story.cfm?newsId=8336, accessed 21 September 2011.

~~(U//FOUO)~~ Other transportation modes have no such procedures for dealing with GPS disruptions. For rail, Positive Train Control, which is to be implemented by 2015, will not be entirely GPS dependent but will instead utilize radio dispatch.

~~(U)~~ **Annex A. List of Acronyms and Abbreviations**

A-GPS	Assisted GPS
ADS	Automatic Dependent Surveillance
ARNS	Aeronautical Radio Navigation Service
ATM	Automatic Teller Machine
CAD	Computer-Aided Dispatch
CATV	Cable Television
CBP	U.S. Customs and Border Patrol
CCZ	U.S. Coastal Confluence Zone
CDMA	Code Division Multiple Access
CIKR	Critical Infrastructure and Key Resources
CONUS	Continental United States
CORS	Continuously Operating Reference Stations
DGPS	Differential Global Positioning System
DHS	U.S. Department of Homeland Security
DME	Distance Measuring Equipment
DOD	U.S. Department of Defense
DOT	U.S. Department of Transportation
E911	Enhanced 911
EA	Electronic Attack
ECDIS	Electronic Chart Display and Information System
eLoran	Enhanced Long-Range Navigation
EMP	Electromagnetic Pulse

EMS	Emergency Medical Services
ESG	Executive Steering Group of the National Executive Committee for Space-Based Positioning, Navigation, and Timing
ESS	Emergency Services Sector
EWR	Newark Liberty International Airport
EXCOM	The National Executive Committee for Space-Based Positioning, Navigation, and Timing
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FRP	Federal Radionavigation Plan
GBAS	Ground-Based Augmentation System
GETS	Government Emergency Telecommunications System
GLA	General Lighthouse Authorities of the United Kingdom and Ireland
GLONASS	Russian Federation's Global Navigation Satellite System
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GPSDO	Global Positioning System Disciplined Oscillator
GPS PNT	Global Positioning System Positioning Navigation and Timing
GPS UTC	Global Positioning System Coordinated Universal Time
GTG	Ground-to-Ground
HAZMAT	Hazardous Materials
HITRAC	Homeland Infrastructure Threat and Risk Analysis Center
HSPD	Homeland Security Presidential Directive

I&A	Office of Intelligence and Analysis (DHS)
IED	Improvised Explosive Device
ILS	Instrument Landing System
IP	Internet Protocol
IP	Office of Infrastructure Protection
IT	Information Technology
J911	Jamming 911
LF	Low Frequency
Loran	Long-Range Navigation
LOS	Line of Sight
LPV	Localizer Performance with Vertical guidance
M-Code	Military Code
MBARI	Monterrey Bay Aquarium Research Institute
MDZ	Military Demarcation Line
MF	Medium Frequency
NAS	National Airspace System
NAVCEN	U.S. Coast Guard Navigation Center
NCO	The National Coordination Office
NERC	North American Electric Reliability Corporation
NextGen	Next Generation Air Transportation System
NIPP	National Infrastructure Protection Plan
NLE	National Level Exercise
NORS	National Outage Reporting System

NPPD	National Protection and Programs Directorate
NPS	Naval Post Graduate School
NRE	National Risk Estimate
NSHS	National Strategy for Homeland Security
NTP	Network Time Protocol
PBX	Private Branch Exchange
PMU	Phasor Measurement Unit
PNT	Position, Navigation and Timing
PNT IDM	Position, Navigation and Timing Interference Detection and Mitigation Plan
PPD	Personal Privacy Device/Personal Protection Devices
PPD	Presidential Policy Directive
PPS	Pulse Per Second
PRS	Public Regulated Service
PSAP	Public Safety Answering Point
PSTN	Public Switched Telephone Network
PVT	Position, Velocity and Timing
P(y)	Precision Encrypted Code
R&D	Research and Development
RF	Radio Frequency
RFI	Radio Frequency Interference
RMA	Office of Risk Management and Analysis
RNAV	Area Navigation
RNSS	Radionavigation Satellite Service

SCADA	Supervisory Control and Data Acquisition
SME	Subject Matter Experts
SPS GPS	Standard Positioning Service Global Positioning Service
SS7	Signaling System #7
SSAs	Sector Specific Agencies
SSP	Sector-Specific Plan
TOR	Terms of Reference
TSS	Transportations Systems Sector
U.K.	The United Kingdom
USG	U.S. Government
UTC	Coordinated Universal Time
UWB	Ultra-Wide Band
VHF	Very High Frequency
VLf	Very Low Frequency
VOR	VHF Omnidirectional Range
WAAS	Wide Area Augmentation System
WPS	Wireless Priority Service

~~(U)~~ Annex B. Glossary

Accuracy: the degree of conformance between the estimated or measured position and/or velocity of a platform at a given time and its true position or velocity. PNT system accuracy is usually presented as a statistical measure of system error and is specified as:

- **Predictable:** the accuracy of a GPS system's position solution with respect to the charted solution. Both the position solution and the chart must be based upon the same geodetic datum.
- **Repeatable:** the accuracy with which a user can return to a position whose coordinates have been measured at a previous time with the same navigation system.
- **Relative:** the accuracy with which a user can measure position relative to that of another user of the same navigation system at the same time. (*2010 Federal Radio Navigation Plan*)

Alternative Future: plausible alternative views about how the future may develop. (*U.S. National Intelligence Council, Disruptive Civil Technologies, 2008*)

Augmentation: space- and/or ground-based systems that provide users of space-based positioning, navigation, and timing signals with additional information that enables users to obtain enhanced performance when compared to the un-augmented space-based signals alone. These improvements include better accuracy, availability, integrity, and reliability, with independent integrity monitoring and alerting capabilities for critical applications. (*NSDP-39 Fact Sheet*)

Banking and Finance Sector: a service-based industry providing a wide variety of financial services in the United States and throughout the world. Financial institutions are organized and regulated based on the services the institutions provide. Therefore, the sector profile is best described by defining the services offered. These services include:

- **Deposit and Payment Systems and Products:** depository institutions of all types (banks, thrifts, and credit unions) are the primary providers of wholesale and retail payments services, such as wire transfers, checking accounts, and credit and debit cards. These institutions are the primary point of contact with the sector for many individual customers. In addition, these institutions may be Federal or State-chartered banks or credit unions; however, in most instances, the Federal financial regulators have at least some authority over these institutions.
- **Credit and Liquidity Products:** financial institutions such as depository institutions, finance and lending firms, securities firms, and government-sponsored enterprises (GSE) meet customers' long- and short-term liquidity and credit needs. Some of these entities provide credit directly to the end customer, while others do so indirectly by providing wholesale liquidity to those financial services firms that provide these services on a retail

basis. The law provides for consumer protections against fraud involving these products, as well as certain other consumer protections, many of which are tied directly to the specific type of credit and liquidity product.

- **Investment Products:** these products provide opportunities for both short- or long-term investments and include debt securities (such as bonds and bond mutual funds), equities (such as stocks or stock mutual funds), and derivatives (such as options and futures). Securities firms, depository institutions, pension funds, and GSEs all offer financial products that are used for investing needs. These investment products are issued and traded in various organized markets, from physical trading floors to electronic markets. The Treasury, the Securities and Exchange Commission (SEC), the Commodity Futures Trading Commission (CFTC), banking regulators, and insurance regulators all provide financial regulation for certain investment products.
- **Risk-Transfer Products:** insurance companies and futures firms offer financial products that allow customers to transfer various types of financial risks. Customers may transfer risk such as the risk of a financial loss due to theft or the destruction of physical or electronic property resulting from a fire, cyber attack, or other loss event, or the loss of income due to a death or disability in a family. Marketplace efficiency often requires that market participants engage in both financial investments as well as in financial risk transfers that enable risk hedging. Financial derivatives, including futures and security derivatives, can provide both of these functions for market participants. (*Banking and Finance Sector Specific Plan, 2007, <http://www.dhs.gov/xlibrary/assets/nipp-ssp-banking.pdf>*)

Communications Sector: a collection of assets and private and public sector entities that have equities in the provisioning, use, protection, or regulation of communications networks and services. The Communications Sector is made up of five industry sectors:

- **Wireline:** consists primarily of the public switched telephone network (PSTN) but also includes enterprise networks. The PSTN is a domestic communications network accessed by telephones, key telephone systems, private branch exchange (PBX) trunks, and data arrangements. Despite the industry's transition to packet-based networks, the traditional PSTN remains the backbone of the communications infrastructure. Includes landline telephone, the Internet, and submarine cable infrastructure.
- **Wireless:** refers to telecommunication in which electromagnetic waves (rather than some form of wire) carry the signal over part of or the entire communication path. Consists of cellular telephone, paging, personal communication services, high-frequency radio, unlicensed wireless, and other commercial and private radio services.
- **Satellite:** a space vehicle launched into orbit to relay audio, data, or video signals as part of a telecommunications network. Signals are transmitted to the satellite from earth station antennas, amplified, and sent back to earth for reception by other earth station antennas. Satellites are capable of linking two points, one point with many others, or multiple locations with other multiple locations. Uses a combination of terrestrial and space components to deliver various communications, Internet data, and video services.

- **Cable:** a wireline network offering television, Internet, and voice services that interconnect with the PSTN through end offices. Primary cable television (CATV) network components include headends and fiber optic and/or hybrid fiber cables. Since the CATV network was designed primarily for downstream transmission of television signals, most of the existing network is being refitted to support two-way data transmissions.
- **Broadcasting:** a signal transmitted to all user terminals in a service area. Refers to content carried over air waves, using these waves to distribute radio or television programs that are available for reception by the public. Much of the broadcasting infrastructure overlaps with the other subsectors of the Communications Sector, especially satellites that are widely used for transmission. (*Communications Sector-Specific Plan, 2007*)

Compatible: the ability of U.S. and foreign space-based positioning, navigation, and timing services to be used separately or together without interfering with each individual service or signal, and without adversely affecting navigation warfare. (*NSDP-39 Fact Sheet*)

Consequence: the effect of an event, incident, or occurrence. (*DHS Lexicon, 2010*)

Coordinated Universal Time (UTC): an atomic time scale and the basis for civil time. UTC is occasionally adjusted by one-second increments to ensure that the difference between the uniform time scale, defined by atomic clocks, does not differ from the Earth's rotation by more than 0.9 s. (*2010 Federal Radio Navigation Plan*)

Critical Infrastructure: systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters, across any Federal, State, regional, territorial, or local jurisdiction. (*DHS Lexicon, 2010*)

Dependency: the one-directional reliance of an asset, system, network, or collection thereof, within or across sectors, on input, interaction, or other requirement from other sources in order to function properly. (*National Infrastructure Protection Plan, 2009*)

Emergency Services Sector: a system of preparedness, response, and recovery elements that forms the Nation's first line of defense for preventing and mitigating the risk from physical and cyber attacks and manmade and natural disasters. The ESS is a primary "protector" for other critical infrastructure and key resources (CIKR) sectors. The sector consists of:

- **Law Enforcement:** maintaining law and order and protecting the public from harm. Law enforcement activities may include investigation, prevention, response, court security, and detention, as well as other associated capabilities and duties.
- **Fire and Emergency Services:** prevention and minimizing loss of life and property during incidents resulting from fire, medical emergencies, and other all-hazards events.

- **Emergency Management:** leading efforts to mitigate, prepare for, respond to, and recover from all types of multijurisdictional incidents.
- **Emergency Medical Services:** providing emergency medical assessment and treatment at the scene of an incident, during an infectious disease outbreak, or during transport and delivery of injured or ill personnel to a treatment facility as part of an organized EMS system.
- **Public Works:** providing essential emergency functions, such as assessing damage to buildings, roads, and bridges; clearing, removing, and disposing of debris; restoring utility services; and managing emergency traffic. (*Emergency Services Sector Specific Plan, 2010, <http://www.dhs.gov/xlibrary/assets/nipp-ssp-emergency-services.pdf>*)

Energy Sector: a collection of assets that are geographically dispersed and connected by systems and networks to deliver products and services in three interrelated subsectors:

- **Electricity:** comprises more than 5,300 power plants with approximately 1,075 gigawatts of installed generating capacity. The electricity infrastructure is highly automated and controlled by utilities and regional grid operators using sophisticated energy management systems.
- **Petroleum:** includes the exploration, production, storage, transport, and refinement of crude oil. The crude oil is refined into petroleum products that are then stored and distributed to key economic sectors.
- **Natural Gas:** includes production, transport, storage, and distribution to customers through the use of over 550 operable gas processing plants and over 300,000 miles of interstate and intrastate pipeline for transmission. (*National Infrastructure Protection Plan, Energy Sector Snapshot, 2009, http://www.dhs.gov/xlibrary/assets/nipp_snapshot_energy.pdf*)

Enhanced 911 (E911): the requirement that most 9-1-1 systems automatically report the telephone number and location of 9-1-1 calls made from wireline phones. The FCC also requires wireless telephone carriers to provide 9-1-1 and E9-1-1 capability, where a Public Safety Answering Point (PSAP) requests it. (*FCC, <http://transition.fcc.gov/pshs/services/911-services/Welcome.html>*)

Executive Steering Group (ESG): the executive steering group of the National Executive Committee for Space-Based Positioning, Navigation, and Timing (EXCOM). The ESG provides a mechanism for elevating interagency issues to a senior level between National Executive Committee meetings. The ESG seeks to resolve issues that do not rise to the level of the Deputy Secretaries on the National Executive Committee. The ESG sets the agenda for the National Executive Committee meetings and makes recommendations on those issues that are presented to the Deputy Secretaries. (*<http://www.pnt.gov/groups>*)

Factor: the relative direction of an uncertainty that will shape alternative future scenarios. (*NRE Scenario Workshop Guidance, 2011*)

Federally Mandated Missions: the compilation of core strategic objectives or functions that critical infrastructure sectors fulfill, as identified in key homeland security guidance documents, including the Homeland Security Act, National Strategy for Homeland Security, Homeland Security Presidential Directive 7, Homeland Security Presidential Directive 20, and the National Infrastructure Protection Plan. Federally Mandated Missions include ensuring national security, public health, and an orderly economy; maintaining order; and providing essential public services. *(2011 National Risk Estimate Terms of Reference)*

Frequency: the number of events or outcomes per defined unit of time. *(American National Standard Vocabulary for Risk Management)*

Global Navigation Satellite System (GNSS): refers collectively to the worldwide positioning, navigation, and timing (PNT) determination capability available from one or more satellite constellations, such as the United States' Global Positioning System (GPS) and the Russian Federation's Global Navigation Satellite System (GLONASS), the European Union (GALILEO) and China (Compass). Each GNSS system employs a constellation of satellites operating in conjunction with a network of ground stations. *(2010 Federal Radio Navigation Plan)*

Global Positioning System (GPS): provides service to military and civilian users. GPS PNT has three core functions: (1) positioning, (2) navigation, and (3) timing. Critical infrastructure sectors use these functions in various ways to support their missions. The civilian service is freely available to all users on a continuous, worldwide basis, and the civilian user segment includes GPS receiver equipment, which receives the signals from the GPS satellites and uses the transmitted information to calculate the user's three-dimensional position, velocity and time. In addition, GPS service includes some augmentations "that aid GPS by providing accuracy, integrity, availability, or any other improvement to [PNT] that is not inherently part of GPS itself." Augmentation examples include Federally-operated systems, such as the Nationwide Differential GPS System, the Wide Area Augmentation System, and Continuously Operating Reference Stations, as well as commercial, site-specific, and global augmentation systems. *(www.gps.gov)*

Homeland Security: a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur. *(DHS Lexicon, 2010)*

IEEE 1588: a protocol enabling precise synchronization of clocks in measurement and control systems implemented with technologies such as network communication, local computing, and distributed objects. The protocol is applicable to systems communicating by local area networks supporting multicast messaging including but not limited to Ethernet. The protocol enables heterogeneous systems that include clocks of various inherent precision, resolution, and stability to synchronize. The protocol supports system-wide synchronization accuracy in the sub-microsecond range with minimal network and local clock computing resources. *(http://www.nist.gov/el/isd/ieee/intro1588.cfm)*

Infrastructure: the framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of

the United States, the smooth functioning of government at all levels, and society as a whole. Consistent with the definition in the Homeland Security Act, infrastructure includes physical, cyber, and/or human elements. (*National Infrastructure Protection Plan, 2009*)

Intentional disruption: involves the use of radios to intercept or interfere with GNSS signals. Can result from attacks by adversaries on any equipment or part involved with GNSS signaling: ground stations, satellites, receivers, and communication occurring between nodes; attempts by individuals to jam GPS signals on a very local level, such as with personal protection devices; and training exercises where the risk of consequential disruptions to the desired GPS service outside of the area operations are mitigated. (adapted from *Papadimitratos and Javanovic, GNSS-based Positioning: Attacks and Countermeasures, MILCOM 2008; NRE Intro Text*)

Interdependency: a mutually reliant relationship between entities (objects, individuals, or groups). (*DHS Lexicon, 2010*)

Interference: any electromagnetic disturbance that interrupts, obstructs, or otherwise degrades or limits the performance of user equipment. (*2010 Federal Radio Navigation Plan*)

Interoperable: the ability of civil U.S. and foreign space-based positioning, navigation, and timing services to be used together to provide better capabilities at the user level than would be achieved by relying solely on one service or signal. (*NSDP-39 Fact Sheet*)

Jamming: preventing a receiver from tracking GPS signals. (*Los Alamos National Laboratory, A Simple Demonstration that the Global Positioning System (GPS) is Vulnerable to Spoofing, 2002*)

Key Resources: publicly or privately controlled resources essential to the minimal operations of the economy and government (*DHS Lexicon, 2010*)

Likelihood: the estimate of an incident or event's occurrence. (*DHS Lexicon, 2010*)

Likely: a greater than even chance of occurrence. (*Office of the Director of National Intelligence, Explanation of Estimative Language, 2007*)

Loran: contraction of long-range navigation, used to describe an electronic navigation system using a chain of transmitting stations that allows mariners or aviators to determine their position. (*USCG Loran-C Users Handbook* <http://www.navcen.uscg.gov/pdf/loran/handbook/APP-C.pdf>)

- **eLoran:** envisioned as an independent, complementary, multi-modal back up to GPS, eLoran was a PNT service for use by many modes of transport and other applications. It was the latest in the longstanding and proven series of low-frequency Loran systems, one that took full advantage of 21st century technology. eLoran was expected to meet the accuracy, availability, integrity, and continuity performance requirements for aviation non-precision instrument approaches, maritime harbor entrance and approach maneuvers, land-mobile vehicle navigation, and location-based services, and was a precise source of time and frequency for applications such as telecommunications. (*International LORAN*

Association Enhanced Loran Definition Document, 2007

<http://www.loran.org/ILAArchive/eLoran%20Definition%20Document/eLoran%20Definition%20Document-1.0.pdf>)

- **Loran-C:** discontinued federally provided radionavigation system for the U.S. Coastal Confluence Zone (CCZ). The CCZ is defined as the area seaward of a harbor entrance to 50 nautical miles offshore or the edge of the Continental Shelf 100 fathom curve, whichever is greater. (*USCG Loran-C Users Handbook*
<http://www.navcen.uscg.gov/pdf/loran/handbook/CHAPTER1.pdf>)

Milestones: indicators that an alternative future scenario is unfolding. (*NRE Scenario Workshop Guidance, 2011*)

Mitigation: ongoing and sustained action to reduce the probability or lessen the impact of an adverse incident. (*DHS Lexicon, 2010*)

National Security: a comprehensive program of integrated policies and procedures for the Departments, agencies, and functions of the United States Government aimed at protecting the territory, population, infrastructure, institutions, values, and global interests of the Nation. (*DHS Lexicon, 2010*)

National Coordination Office (NCO): the secretariat of the National Executive Committee for Space-Based PNT. The National Coordination Office is responsible for organizing meetings, tracking projects and tasks, coordinating interagency documents, etc. It is also responsible for developing the annual Five-Year National Plan for Space-Based PNT and assessing its implementation by the member agencies. (<http://www.pnt.gov/office/>)

National Executive Committee for Space Based Positioning, Navigation and Timing (EXCOM): a U.S. Government organization established by Presidential directive to advise and coordinate federal departments and agencies on matters concerning the Global Positioning System (GPS) and related systems. (www.pnt.gov/)

Naturally Occurring Disruptions: events that can disrupt PNT-supporting satellites, including space weather like geomagnetic storms, ionospheric vulnerabilities, and other effects of solar activity. Environmental or other weather conditions on the ground can also impede the monitoring and tracking capabilities of Global Navigation Satellite Systems' positioning services. (*Salmi and Torkeli, Inventions Utilizing Satellite Navigation Systems in the Railway Industry, Journal of Technology Management & Innovation*)

Navigation: the ability to determine current and desired position (relative or absolute) and apply corrections to course, orientation, and speed to attain a desired position anywhere around the world, from subsurface to surface and from surface to space. (www.pnt.gov)

Network: a group of components that share information or interact with each other in order to perform a function. (*DHS Lexicon, 2010*)

NRE Estimate Phase: the comprehensive literature review, development of a Terms of Reference document, consultation with an NRE Advisory Group comprising senior government experts, and preliminary coordination with SMEs to identify scenarios leading to GPS disruptions of various magnitude and severity. HITRAC conducted data calls and workshops to elicit SME input in a structured manner on the likelihood of these scenarios and their mission disruption consequences for each highlighted critical infrastructure sector. Mission disruption consequences were considered as a function of time and severity. *(2011 National Risk Estimate)*

NRE Integration Phase: an interagency effort to review the NRE for soundness, consistency, and accuracy. This phase helped identify key GPS disruption risk trends visible from research and workshop results as well as potential risk mitigation strategies that could be adopted by the public or private sectors. *(2011 National Risk Estimate)*

NRE Outlook Phase: consultation with SMEs through alternative futures development workshops to identify the key strategic uncertainties that could define future risks of GPS disruptions over the next 20 years, as well as the milestones and indicators that alternative futures are unfolding. The methodology underpinning the alternative futures development was drawn from a 2008 U.S. National Intelligence Council *Disruptive Civil Technologies* report. *(2011 National Risk Estimate)*

Patriot Watch Program: a system-of-systems approach to provide real-time monitoring (preparedness), location, and notification (response) of GPS interference for protecting the Nations CIKR Sectors. Joint effort of several USG entities led by DHS. *(U.S. Coast Guard Navigation Center Presentation, http://www.navcen.uscg.gov/pdf/cgsicMeetings/USSLS/Apr_2011_Groton/BPenick_SLGSC_Patriot_Watch.pdf)*

Positioning: the ability to accurately and precisely determine one's location and orientation two dimensionally (or three dimensionally when required) referenced to a standard geodetic system (such as World Geodetic System 1984). *(www.pnt.gov)*

Precise Time: a time requirement accurate to within 10 milliseconds. *(2010 Federal Radio Navigation Plan)*

Private Sector: individuals, and entities, including for-profit and nonprofit, which are not part of any government. *(DHS Lexicon, 2010)*

Radio Line-of-Sight (Radio LOS): a direct, nonguided path between a transmitting antenna and a receiving antenna. The criticality of LOS is sensitive to the radio frequency (RF) employed. Very low frequency (VLF) and low frequency (LF) signals tend to be travel between the Earth and the ionosphere. LF and medium frequency (MF) signals propagate as ground waves, which tend to follow the curvature of the Earth. Signals at the high end of the MF range and in the high frequency (HF) range benefit from ionospheric refraction, a phenomenon in which the density gradient in the atmosphere acts like a lens and tends to bend radio beams back toward the Earth. At very high frequencies (VHF) and above, true optical LOS is considered essential. *(Webster's New World Telecom Dictionary 2010)*

Recovery: the development, coordination, and execution of service- and site-restoration plans; the reconstitution of government operations and services; individual, private-sector, nongovernmental, and public-assistance programs to provide housing and to promote restoration; long-term care and treatment of affected persons; additional measures for social, environmental, and economic restoration; evaluation of the incident to identify lessons learned; post incident reporting; and development of initiatives to mitigate the effects of future incidents. (*National Disaster Recovery Framework, 2010*)

Redundancy: additional or alternative systems, subsystems, assets, or processes that maintain a degree of overall functionality in case of loss or failure of another system, sub-system, asset, or process. (*DHS Lexicon, 2010*)

Reliability: the probability of performing a specified function without failure under given conditions for a specified period of time. (*2010 Federal Radio Navigation Plan*)

Resilience: the ability to adapt to changing conditions and prepare for, withstand, and rapidly recover from disruption. The ability of systems, infrastructures, government, business, communities, and individuals to resist, tolerate, absorb, recover from, prepare for, or adapt to an adverse occurrence that causes harm, destruction, or loss. (*DHS Lexicon, 2010*)

Risk: the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences. (*DHS Lexicon, 2010*)

Risk Assessment: a product or process that collects information and assigns values to risks for the purpose of informing priorities, developing or comparing courses of action, and informing decisionmaking. (*DHS Lexicon, 2010*)

Risk Management: a process of identifying, analyzing, assessing, and communicating risk and accepting, avoiding, transferring, or controlling it to an acceptable level at an acceptable cost. (*DHS Lexicon, 2010*)

Risk Management Strategy: a course of action or actions to be taken in order to manage risks. (*DHS Lexicon, 2010*)

Risk Mitigation: the application of measure or measures to reduce the likelihood of an unwanted occurrence and/or its consequences. (*DHS Lexicon, 2010*)

Risk Mitigation Option: a measure, device, policy, or course of action taken with the intent of reducing risk. (*DHS Lexicon, 2010*)

Scenario: a hypothetical situation comprising a hazard, an entity impacted by that hazard, and associated conditions including consequences when appropriate. (*DHS Lexicon, 2010*)

Sector: a logical collection of assets, systems, or networks that provide a common function to the economy, government, or society. The National Infrastructure Protection Plan addresses 18

CIKR sectors, identified by the criteria set forth in HSPD-7. (*National Infrastructure Protection Plan, 2009*)

Sector-Specific Agency (SSA): Federal departments and agencies identified in HSPD-7 as responsible for CIKR protection activities in specified CIKR sectors. (*National Infrastructure Protection Plan, 2009*)

Sector-Specific Plan (SSP): augmenting plans that complement and extend the NIPP Base Plan and detail the application of the NIPP framework specific to each CIKR sector. SSPs are developed by the SSAs in close collaboration with other sector partners. (*National Infrastructure Protection Plan, 2009*)

Severity: the extent of the harm caused by the disruption to the service, and it reflects a consideration of three parts: capacity, substitutability, and extent (geographic and functional). (*2011 National Risk Estimate*)

Spoofing: the surreptitious replacement of a true satellite signal with a manipulated satellite signal. (*Los Alamos National Laboratory, A Simple Demonstration that the Global Positioning System (GPS) is Vulnerable to Spoofing, 2002*)

Strategic Surprise: an unanticipated incident or event that causes or results in significant disruption or damage to a critical infrastructure sector and/or its supply chain. (*U.S. National Intelligence Council, Disruptive Civil Technologies, 2008*)

Subject Matter Expert: an individual with in-depth knowledge in a specific area or field. (*DHS Lexicon, 2010*)

Syntonization: the process of setting the frequency of one oscillator equal to that of another. The term *synchronization* is commonly used in place of *syntonization* to mean the same thing. (*Alliance for Telecommunications Industry Solutions, ATIS Telecommunications Glossary 2011*)

System: any combination of facilities, equipment, personnel, procedures, and communications integrated for a specific purpose. (*DHS Lexicon, 2010*)

Threat: a natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property. (*DHS Lexicon, 2010*)

Time: the expected length of a GPS service disruption. (*2011 National Risk Estimate*)

Timing: the ability to acquire and maintain accurate and precise time from a standard (Coordinated Universal Time, or UTC), anywhere in the world and within user-defined timeliness parameters. Timing includes time transfer. UTC is used for telecommunications, network synchronization, secure military communications, bank transactions, power grids, and transportation systems. There is a growing need in sectors for accurate time and frequency services to operate more efficiently and to maintain safety and security. (*www.pnt.gov; DoD,*

Global Positioning System (GPS) 2008: A Report to Congress, 2008; GPS Timing Criticality Update: Final Report)

Transportation Sector: the Nation's transportation system quickly, safely, and securely moves people and goods through the country and overseas. The Transportation Systems Sector consists of six key subsectors, or modes:

- **Aviation:** includes aircraft, air traffic control systems, and approximately 450 commercial airports and 19,000 additional airfields. This mode includes civil and joint-use military airports, heliports, short takeoff and landing ports, and seaplane bases.
- **Freight Rail:** consists of hundreds of railroads, more than 143,000 route-miles of track, more than 1.3 million freight cars, and roughly 20,000 locomotives.
- **Highway and Motor Carrier:** encompasses more than 4 million miles of roadways and supporting infrastructure. Vehicles include automobiles, buses, motorcycles, and all types of trucks.
- **Maritime:** consists of about 95,000 miles of coastline, 361 ports, over 10,000 miles of navigable waterways, 3.4 million square miles of Exclusive Economic Zone to secure, and intermodal landside connections, which allow the various modes of transportation to move people and goods to, from, and on the water.
- **Mass Transit:** includes multiple-occupancy vehicles, such as transit buses, trolleybuses, vanpools, ferryboats, monorails, heavy (subway) and light rail, automated guideway transit, inclined planes, and cable cars designed to transport customers on local and regional routes.
- **Pipeline:** include vast networks of pipeline that traverse hundreds of thousands of miles throughout the country, carrying nearly all of the Nation's natural gas and about 65 percent of hazardous liquids, as well as various chemicals. (*National Infrastructure Protection Plan – Transportation Sector Snapshot, 2009*, http://www.dhs.gov/xlibrary/assets/nipp_snapshot_transportation.pdf)

Uncertainty: the areas that will be of significant importance to a CIKR sector in the future. (*NRE Scenario Workshop Guidance, 2010*)

Unintentional Disruption: may occur from malfunctions or accidents due to aging GPS constellation issues, space debris hitting satellites, errors by GPS constellation operators, defective software, and failures in uplink stations, among other causes. Others may result from Federal and non-Federal radio communications systems operating in close frequency or geographic proximity to a GPS receiver. (*DoD, Global Positioning System (GPS) 2008: A Report to Congress, 2008; GPS Backup for PNT Transition Strategy for Navigation and Surveillance, 2006; Recommendation on GNSS Vulnerability and Mitigation Measures, 2004*)

Vulnerability: a physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard. (*DHS Lexicon, 2010*)

Vulnerability Assessment: the product or process of identifying physical features or operational attributes that render an entity, asset, system, network, or geographic area susceptible or exposed to hazards. Vulnerability assessments can produce comparable estimates of vulnerabilities across a variety of hazards or assets, systems, or networks. (*DHS Lexicon, 2010*)

Wide Area Augmentation System (WAAS): a system of ground stations to provide necessary augmentations to the GPS navigation signal. The WAAS is designed to provide the additional accuracy, availability, and integrity necessary to enable users to rely on GPS for all phases of flight, from en route through approach for all qualified airports within the WAAS coverage area. WAAS also provides the capability for increased accuracy in position reporting, allowing for more uniform and high-quality worldwide Air Traffic Management. (*FAA, http://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/techops/navservices/gnss/faq/waas/#2*)

~~(U)~~ Annex C. NRE Risk Assessment and Monte Carlo Simulation Methodology

~~(U)~~ Overview

~~(U//FOUO)~~ The risk analysis underlying this NRE draws on data elicited from SMEs at sector consequence and scenario likelihood workshops. For purposes of this analysis, risk is calculated as the product of each scenario's consequence score multiplied by its estimated frequency of occurrence.

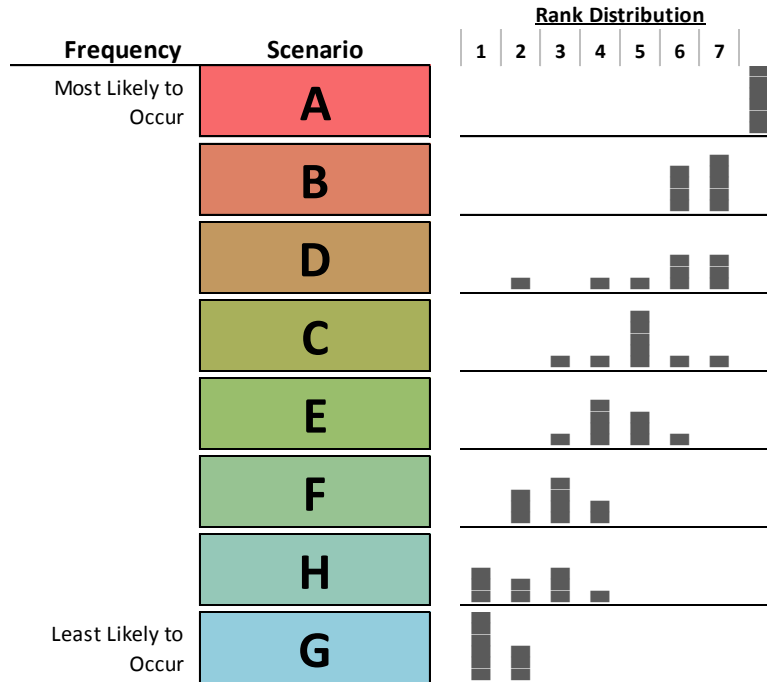
~~(U//FOUO)~~ An initial analysis was calculated on the raw data to produce a series of risk scores for each sector and scenario. These results were then optimized through a multistep process, including running a series of Monte Carlo simulations using the Crystal Ball⁸⁶ software package produced by Oracle. In all, a total of four different risk results were calculated:

- 1) ~~(U)~~ Risk calculated with the raw data.
- 2) ~~(U)~~ Risk calculated with Monte Carlo using the raw data and normal distributions.
- 3) ~~(U)~~ Risk calculated with Monte Carlo using non-outlier data and normal distributions.
- 4) ~~(U)~~ Risk calculated with Monte Carlo using non-outlier data and optimized distributions.

~~(U)~~ Evaluating Frequency

~~(U//FOUO)~~ Using a two-step process, the frequency values were captured from SMEs during a workshop on May 6, 2011. SMEs were first tasked with rank ordering the eight scenarios from mostly likely to least likely to occur, given a 1 to 8 scale, with 8 being "most likely to occur." These results were aggregated and reviewed by the SMEs, and a group consensus rank order was formed through an open discussion period (see Figure C-1). During this period, SMEs were allowed to resubmit their results if the open discussion swayed their judgments.

⁸⁶ ~~(U)~~ Crystal Ball is a Monte Carlo simulation add-in to Microsoft Excel that allows analysis of risks and uncertainties associated Excel spreadsheet models. The software's functionality includes sensitivity analysis, correlation, and historical data fitting. Graphics and reports facilitate the presentation of results of analysis.

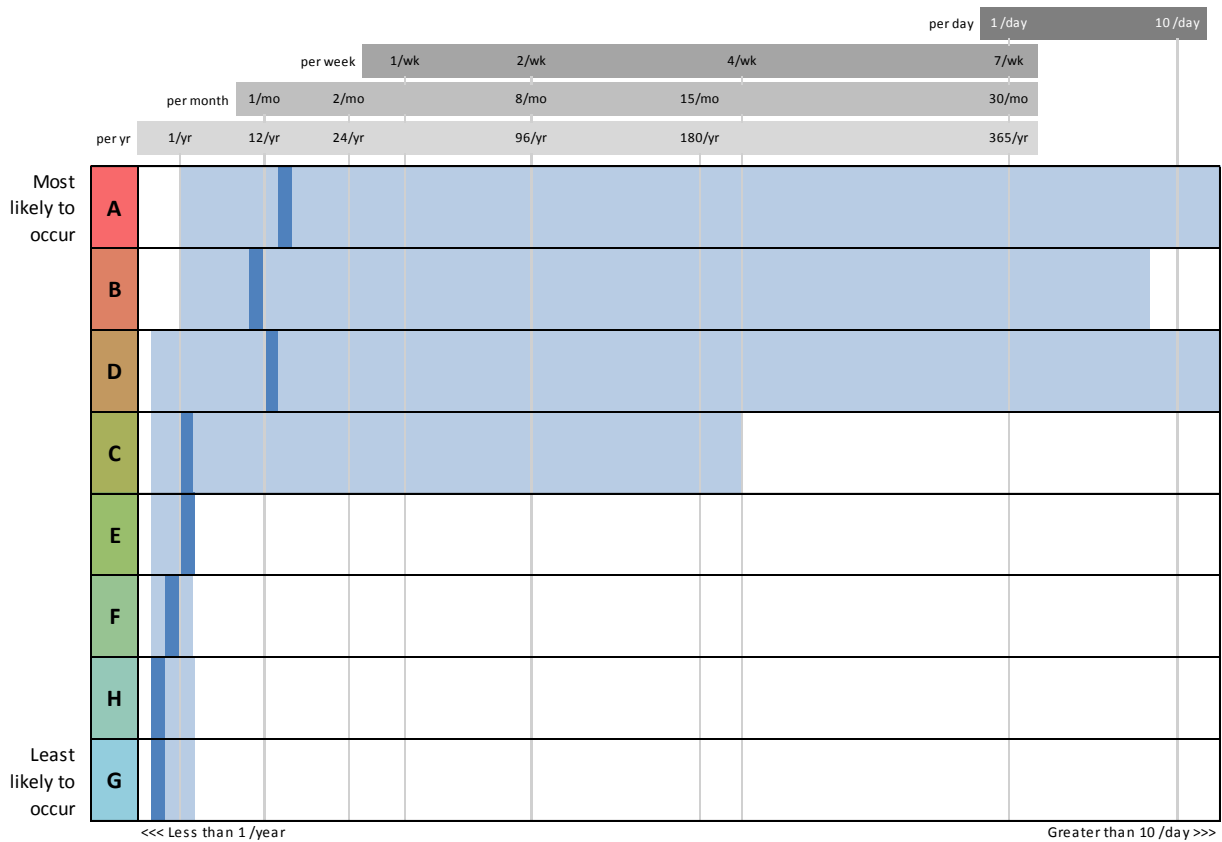


~~(U//FOUO)~~ Figure C-1: Frequency Rank Order Results

~~(U//FOUO)~~ In the second phase of the frequency workshop, SMEs were given a form to enter their estimated range of occurrences for each scenario (see Figure C-2). For calculation purposes, these values were converted into a common unit and aggregated to show the minimum, maximum, and median scores based on all the SME inputs (see Figure C-3). A group discussion period was used to develop a consensus frequency estimate for each scenario. This final group consensus frequency range was used in the risk calculation.



~~(U//FOUO)~~ Figure C-2: Example of Filled-in SME Frequency Form



~~(U//FOUO)~~ Figure C-3: Final Aggregate Results of SME Frequency Elicitation

(U) Evaluating Consequence

(U//FOUO) Consequence values were elicited from SMEs via six sector-specific workshops. In each workshop, SMEs were asked to fill out a consequence lookup table given a 1 to 10 scale, with 10 being the most consequential score (see Figure C-4). This lookup table represented their consequence judgments given the intersection of time (y-axis) and severity (x-axis).

Time	> 30 days					
	< 30 days					
	< 7 days					
	< 1 day					
	< 1 hr					
		No degradation or disruption of sector mission	Isolated degradation of sector mission	Widespread degradation of sector mission	Isolated outage	Widespread outage
		Severity				

(U//FOUO) **Figure C-4: Example of Blank SME Consequence Table Form**

(U//FOUO) The median value and distribution of scores for each cell in the table were calculated and presented to the SMEs for review and discussion. If their judgment was swayed during the discussion process, SMEs were allowed to resubmit their scores for recalculation. Through this process, a group consensus consequence lookup table was developed (see Figure C-5).

Time	> 30 days	2	4	7	9	10
	< 30 days	2	4	6	8	9
	< 7 days	2	3	5	6	7
	< 1 day	1	3	3	4	4
	< 1 hr	1	1	2	2	2
		No degradation or disruption of sector mission	Isolated degradation of sector mission	Widespread degradation of sector mission	Isolated outage	Widespread outage
		Severity				

~~(U//FOUO)~~ Figure C-5: Example of Consensus Consequence Table

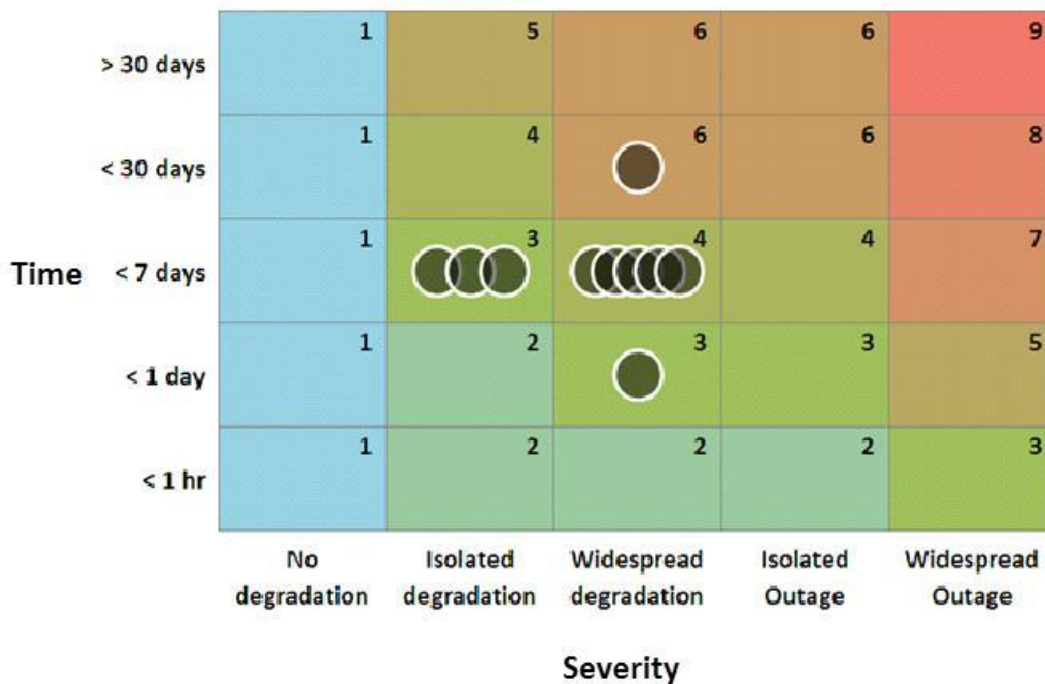
~~(U//FOUO)~~ In the second step of the consequence workshops, SMEs were asked to judge where on the consequence lookup table each scenario belonged by evaluating it using both the time and severity criteria (see Figure C-6).

Time	> 30 days	2	4	7	9	10
	< 30 days	2	4	(B) (D) 6	(E) 8	9
	< 7 days	2	3	(F) 5	(C) 6	7
	< 1 day	1	3	(A) 3	4	(G) 4
	< 1 hr	1	1	2	2	(H) 2
		No degradation or disruption of sector mission	Isolated degradation of sector mission	Widespread degradation of sector mission	Isolated outage	Widespread outage
		Severity				

~~(U//FOUO)~~ Figure C-6: Example of SME Scenario Scoring Form

~~(U//FOUO)~~ For each scenario, all of the individual results were anonymously presented to the SMEs for group discussion, with the intended purpose of driving toward a consensus (see Figure

C-7). The scenario's final consequence score is the calculated median of the values derived from the consensus lookup table. In the example below, the scenario's median consequence score is 4.



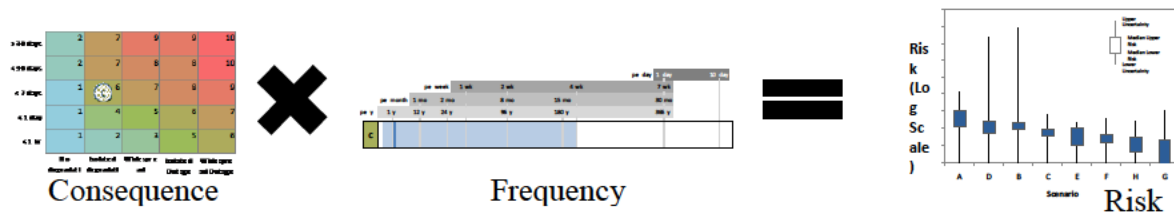
(U//FOUO) Figure C-7: Example of a SME Scenario Results Presented Anonymously

(U) Monte Carlo Simulation

(U//FOUO) A Monte Carlo simulation uses a random sampling of data to calculate results based on a probability distribution. It is often used to simulate mathematical models and is ideal for models with small sample sizes. For this reason, a Monte Carlo simulation was chosen to further analyze the risk results. For this risk model simulation, each cell of the consequence lookup table and the likelihood of occurrence were used as inputs (see Figure C-3 and Figure C-5). Probability distributions were assigned to these inputs, and Crystal Ball ran a total of 1,000 trials for each simulation to produce results for each sector and scenario.

(U) Risk Calculated with Raw Data

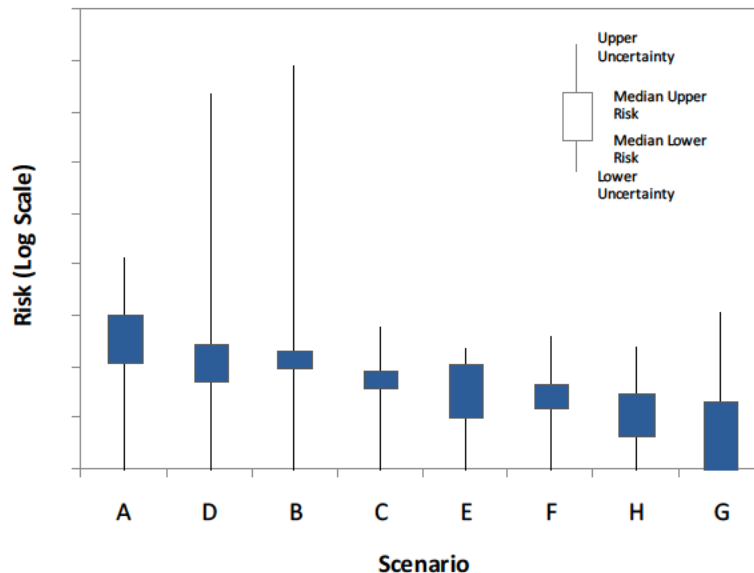
(U//FOUO) The initial risk score was a simple function of the consequence and frequency of occurrence scores (see Figure C-8). In order to reduce the impact of outlier data, the median values for each sample data set were used. The consequence value for each sector and scenario was based on the median scores elicited from the SMEs. This was multiplied by both the median minimum and median maximum frequency values derived from the threat/likelihood workshop. A risk score range was then calculated for each sector and scenario.



~~(U//FOUO)~~ Figure C-8: Methodology to Calculate Risk Scores

~~(U)~~ Monte Carlo using Raw Data and Normal Distributions

~~(U//FOUO)~~ In the first Monte Carlo simulation, each input of the model was given a normal distribution based on the mean and the standard deviation of the data sample. By using a Monte Carlo simulation, we were able to expand the relatively small data sample size to produce a more refined result. In this first model run, all SME data values were used to calculate the mean and the standard deviation. The results of this Monte Carlo simulation were fairly similar to the previously calculated risk scores. However, by using all of the data and a normal distribution, outliers were able to produce a noticeable impact when calculating the mean and the standard deviation. This resulted in a wide range of risk scores for the scenarios in each sector (see Figure C-9).⁸⁷



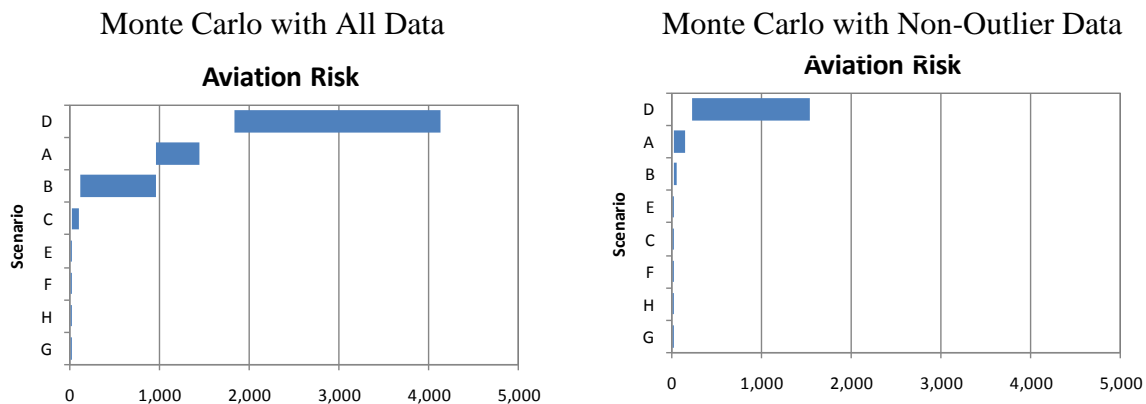
~~(U//FOUO)~~ Figure C-9: Range of Risk Scores for the Aviation Sector

⁸⁷ In Figure C-9, risk scores are represented on a logarithmic scale (log scale) because the risk scores vary widely and the range of associated uncertainty (vertical lines) is substantial, extending to very large numbers. Note that, in a log scale, the line segments between tick marks are not equal. For the vertical scale in Figure C-9, each tick mark represents a value 10 times the value of the preceding tick mark.

~~(U)~~ **Monte Carlo using Non-Outlier Data and Normal Distributions**

~~(U//FOUO)~~ In order to reduce the large range of risk scores produced in the first Monte Carlo simulation run, the underlying frequency data was reviewed. Due to the high uncertainty of the frequency of occurrence for each scenario, the SMEs produced a very wide range of values based on their knowledge and experience (see Figure C-3).

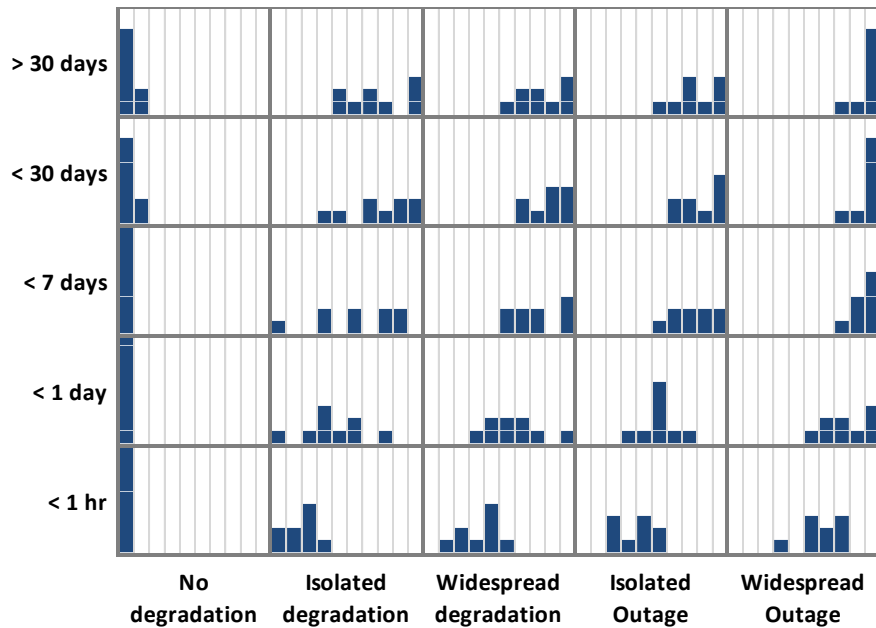
~~(U//FOUO)~~ For the second Monte Carlo simulation, outliers among the likelihood of occurrence scores were removed to produce a cleaner data set. For this model, both the maximum and minimum values were removed from the inputs and the mean and standard deviations were recalculated. Expectedly, the resulting Monte Carlo simulation run produced a set of results with a narrower range of risk scores while maintaining the same order. In the example below (see Figure C-10), the range of risk scores for Aviation Risk decreased dramatically with the outliers removed. These changes were consistent across all the sector and scenario risk scores.



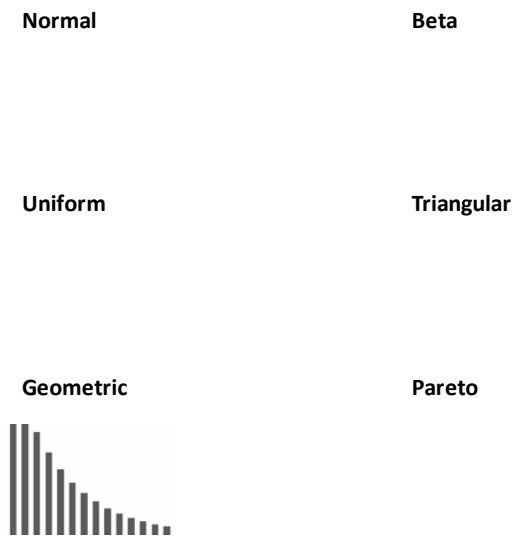
~~(U//FOUO)~~ **Figure C-10: Comparison of All Data vs. Non-Outlier Data Monte Carlo Models**

~~(U)~~ **Monte Carlo using Non-Outlier Data and Optimized Distributions**

~~(U//FOUO)~~ To further refine the risk results, a third Monte Carlo simulation was developed. In the first two simulations, a standard normal distribution was used for input into the model. Unfortunately, a majority of the data produced during the consequence and threat workshops do not fit into a normal distribution but rather a wide range of distribution types, including, but not limited to, a uniform, beta, and geometric distribution (see Figure C-11 and Figure C-12).

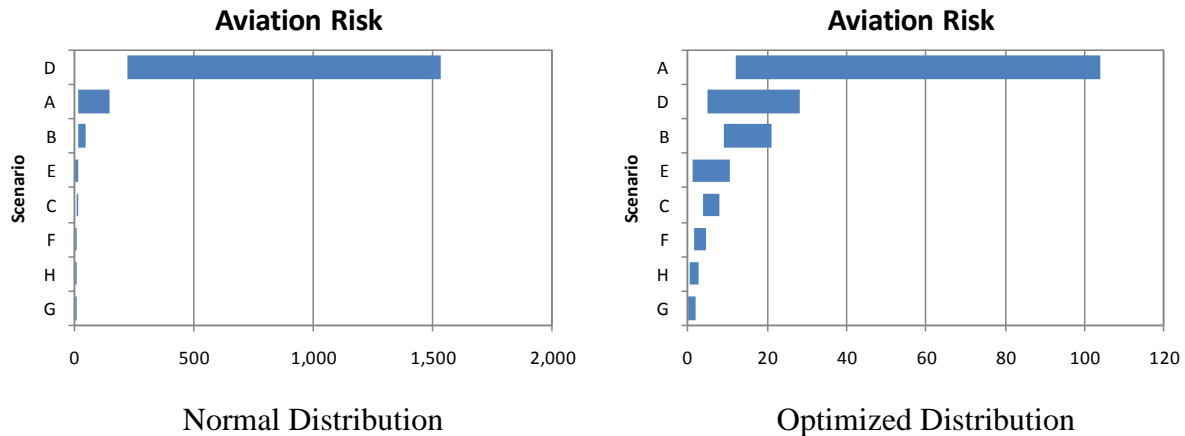


~~(U//FOUO)~~ Figure C-11: Histogram of the Results From a Consequence Workshop Showing the Variety of Score Distributions



~~(U//FOUO)~~ Figure C-12: Examples of Different Probability Distribution Types

~~(U//FOUO)~~ For this third Monte Carlo simulation, Crystal Ball processed the scores for each input and calculated a distribution curve that would best fit the sample data. This was done for each of the consequence and likelihood of occurrence inputs. The resulting output was noticeably different from the first two simulations. This third model produced the narrowest range of risk scores and also re-sorted the order of results (see Figure C-13). Scenario D was no longer consistently the highest scenario and was replaced by Scenario A.



~~(U//FOUO)~~ **Figure C-13: Comparison of Monte Carlo simulations showing results with a Normal Distribution vs. an Optimized Probability Distribution (notice the smaller range on the x-axis)**

~~(U//FOUO)~~ These results can be explained by reviewing the frequency of occurrence data. Although an effort was made to remove outliers by throwing out the minimum and maximum values for each scenario's data set, Scenario D had two values that were noticeably higher than the rest. Throwing out only one of these higher outliers still left the remaining one in, adversely skewing the normal distribution with a weighted mean and standard deviation. By changing from a normal distribution to a more optimized one that more accurately reflected the sample data, the remaining outlier data had less of an impact, resulting in a narrower and smaller range of risk score for Scenario D.

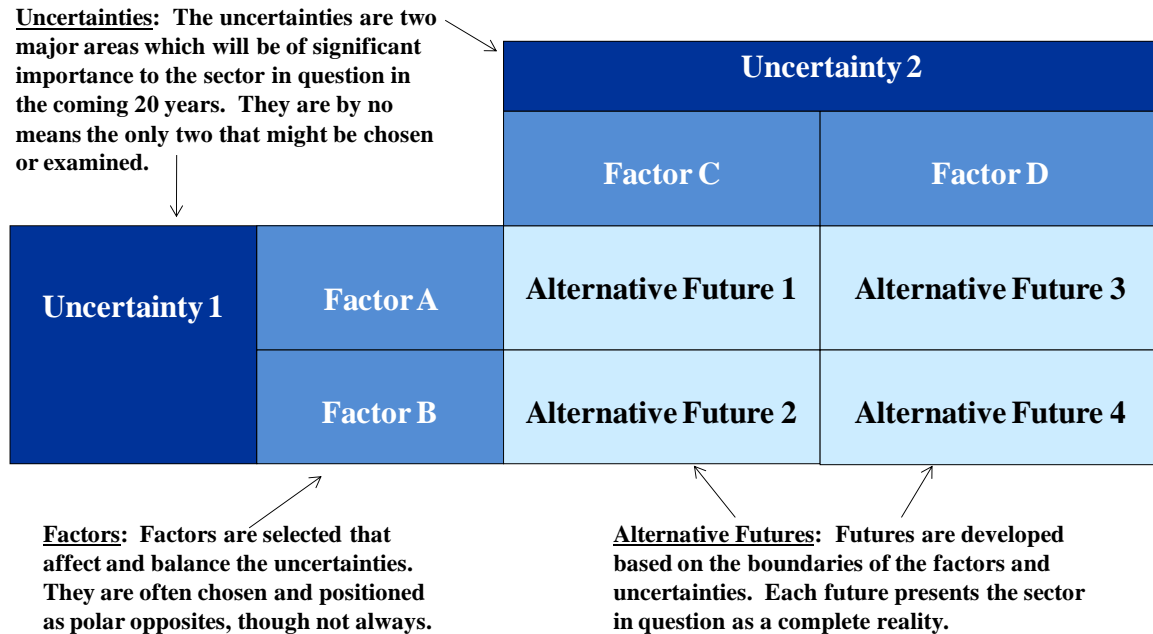
~~(U)~~ Annex D. Alternative Futures Development Methodology

- ~~(U)~~ Alternative futures serve as an analytic approach informing the findings of this NRE. The alternative futures are not predictions of future events. Instead, they are included in this NRE to illustrate possible alternatives concerning the use of GPS by highlighted critical infrastructure sectors—Communications, Emergency Services, Energy, and Transportation—and provide lessons and perspectives about these sectors that may help guide policy and funding decisions.
- ~~(U)~~ Alternative futures analysis is used throughout government and the private sector to facilitate strategic thinking and planning, which enable analysts and decisionmakers to identify possible outcomes and alternatives in a structured manner, consider implications of these outcomes, and assess policy options for addressing these potential futures. Alternative futures are plausible alternative views about how the future may develop based on interpretation of observed trends and data; they are *not*, however, predictions or forecasts.⁸⁸ Alternative futures analysis enables analysts and decisionmakers to consider possible outcomes and alternatives in a structured manner.
- ~~(U)~~ The NRE alternative futures were developed with a methodology that considered a range of key uncertainties for each sector over a 20-year period from 2011 to 2031. The alternative futures development methodology was based in part on a 2008 U.S. National Intelligence Council *Disruptive Civil Technologies* report.⁸⁹ A similar approach was used in the 2010 NRE on Global Supply Chain Security.
- ~~(U)~~ Alternative futures development workshops were conducted in May and June 2011, resulting in the creation of four draft alternative futures for each highlighted critical infrastructure sector. Workshop participants included SMEs from government, academia, and the private sector. At teleconferences prior to the workshops, key strategic uncertainties or major areas that will be of significant importance to the sector and its use of GPS in the coming 20 years were discussed and weighed. These uncertainties were considered as integral parts of the respective sector's future, as well as how they might be combined with other factors to create compelling and illustrative alternative futures.⁹⁰
- ~~(U)~~ At the workshops, factors that would be valuable in highlighting the challenges to the sector by affecting and balancing the uncertainties were identified. Polarizing perspectives were often selected in order to make the alternative futures more distinct. Alternative futures were then built based on the boundaries of the factors and uncertainties.

⁸⁸ (U) U.S. National Intelligence Council, *Disruptive Civil Technologies – Conference Report*, 2008. Accessed 24 July 2010 at http://www.dni.gov/nic/confreports_disruptive_tech.html.

⁸⁹ (U) Ibid.

⁹⁰ (U) The TSS Alternative Futures Scenarios were developed directly with the SSAs and other transportation SMEs in November 2010. First, a conference call was held to discuss and select the uncertainties and factors, then a workshop was held to develop the alternative futures scenarios.



~~(U)~~ Figure D-1: Developing Alternative Futures

- ~~(U)~~ For each sector, two alternative futures were selected as the most critical for further exploration. This decision was based on those alternative futures from which policymakers might draw the most interesting and valuable conclusions.
- ~~(U)~~ SMEs then accomplished four tasks:
 - 1) (U) Considered the two primary alternative futures for each sector and provided thoughts on the potential challenges and opportunities inherent in these alternative futures;
 - 2) (U) Identified case studies, including projects, innovations, and failures from the sector that illustrate issues captured by the alternative futures;
 - 3) (U) Offered strategic thoughts on the milestones and indicators for the sector and supply chain to aid policymakers and other customers in determining whether any of the alternative futures are being realized; and
 - 4) (U) Identified the factors that may not have been accounted for in alternative futures development that could bring chaos to the sector and supply chain.
- ~~(U)~~ The results and findings of these discussions are presented in Annex G.

(U) Annex E. Sector Consequence Workshop Findings

(U) NRE GPS Communications Sector Consequence Workshop Findings Report

(U) Summary of Key Workshop Findings

~~(U//FOUO)~~ HITRAC held a workshop on March 2, 2011, to discuss how the Communications Sector uses GPS and to elicit SME judgment regarding potential sector consequences that could arise if the GPS signal were disrupted in varying ways. (See Annex I for a list of SME participants.)

~~(U//FOUO)~~ SMEs judged the following GPS disruption scenarios to have higher impacts on the Communications Sector:

- ~~(U//FOUO)~~ Scenario A: Continuous, stationary, unintentional interference.
- ~~(U//FOUO)~~ Scenario D: Multiple, low-power, continuous and intermittent, stationary and mobile jammers.
- ~~(U//FOUO)~~ Scenario H: Brief high-power jamming followed by continuous high-power spoofing.
- ~~(U//FOUO)~~ Scenario E: Severe geomagnetic storm.

~~(U//FOUO)~~ SMEs judged the following GPS disruption scenarios to have lower impacts on the Communications Sector:

- ~~(U//FOUO)~~ Scenario G: Continuous multiple spoofers.
- ~~(U//FOUO)~~ Scenario B: Single, low-power, continuous, stationary jammer.
- ~~(U//FOUO)~~ Scenario C: Single, high-power, continuous, stationary jammer.
- ~~(U//FOUO)~~ Scenario F: Continuous single spoofer.

~~(U//FOUO)~~ In addition, SMEs made the following observations regarding the Communication Sector's use of GPS PNT:

- ~~(U//FOUO)~~ A GPS disruption that degrades or stops GPS-derived timing capabilities for under an hour would cause low impacts on the Communications Sector. Both of these low impacts are due to built-in backups (e.g., rubidium vapor or cesium beam oscillators) that would continue functionality.
- ~~(U//FOUO)~~ If the GPS signal is disrupted while power is unavailable and batteries at cell sites run out, it is not possible to reinitialize GPS after power returns. Thus, GPSDOs would have to function in holdover mode.

- ~~(U//FOUO)~~ In the event of an outage, most SS7s will default to Stratum 3 clocks.⁹¹ However, most smaller offices (such as those in rural areas) do not have Stratum 2 or 3 backups in place.
- ~~(U//FOUO)~~ It is noteworthy that a moderate to high degree of difficulty is assumed in an SS7 clock losing operability. In large part, this is because the loss of SS7 assumes a “triple fault”—that is, the GPS signal must fail along with both the primary and secondary reference clocks for SS7s.
- ~~(U//FOUO)~~ The National Outage Reporting System (NORS) is responsible for functioning as a 24/7 watch office for any reported GPS outage or signal disruption. Any disruption to E911 service is reported to NORS, as is any substantial standard signal disruption. When outages or disruptions are large enough, the National Coordinating Center for Telecommunications is notified and involved.
- ~~(U//FOUO)~~ GPS degradation or outage has low to no impact to the Government Emergency Telecommunications System (GETS) because several factors—all unlikely to occur independently or together—must exist. For example, a complete failure of the SS7 must occur as well as damage to multiple switches. Any minor impact to Wireless Priority Service (WPS) may cause users to redial.
- ~~(U//FOUO)~~ Continuity of operations and continuity of government plans based upon GPS signal outage were not considered necessary by the SMEs.
- ~~(U//FOUO)~~ Future developments in GPS technology include improving fortifications against spoofing attacks as well as providing secondary user notifications if a device is being spoofed.
- ~~(U//FOUO)~~ The National Guard is authorized to refill generators that enable oscillators during emergencies. If generators must be prioritized, life-sustaining services will always have first priority, and mobile switching centers and some critical cell sites will receive priority. During Hurricane Katrina, private carriers obtained and maintained their own fuel for generators.

~~(U)~~ Scenario Consequence Summaries

~~(U//FOUO)~~ *Scenario A: An interference source is causing unintentional disruption. Ground receivers within a 30-km GTG radius are affected, and airborne receivers within LOS are affected.*

(b)(7)e, (b)(7)f

(b)(7)e, (b)(7)f

(b)(7)e, (b)(7)f

(U//FOUO) SMEs were divided as to whether the scenario would lead to isolated degradation, widespread degradation, or isolated outage of the network. Poor network performance or outages would mean that cell phones would not function for E911 or general use as time drifts off.

Scenario A			Continuous, stationary, unintentional interference (Gnd: 30km radius, Air: radio LOS)				
Time	E	> 30 days	1	6	8	8	10
	D	< 30 days	1	4	8	8	10
	C	< 7 days	1	4	6	7	9
	B	< 1 day	1	3	5	5	8
	A	< 1 hr	1	2	3	5	7
			No degradation	Isolated degradation	Widespread degradation	Isolated Outage	Widespread Outage
			1	2	3	4	5
			Severity				

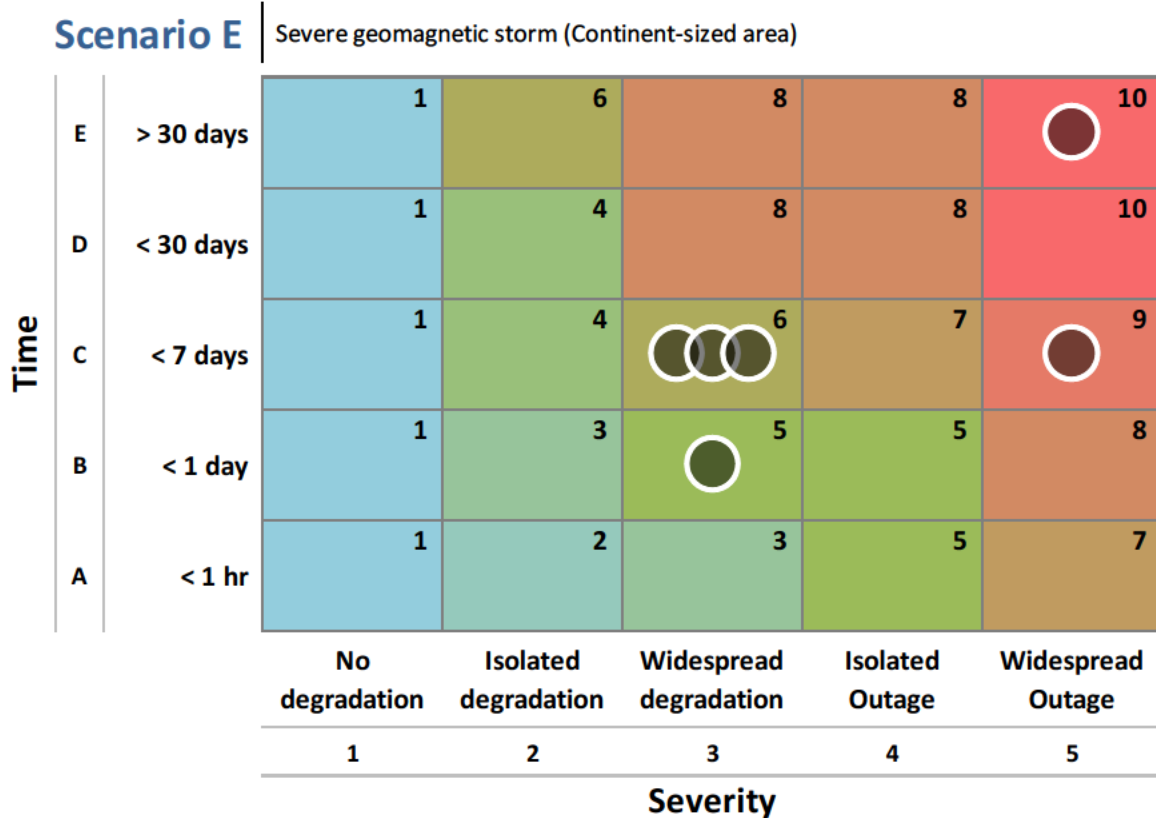
(U//FOUO) **Scenario E: Continent-scale natural disruption caused by a severe geomagnetic storm. Tracking threshold of GPS is reduced significantly.**

(U//FOUO) Most SMEs agreed that this scenario would result in widespread degradation in the Communications Sector and that the effects of the scenario would last for less than seven days. SMEs noted that the severity of the scenario depends on solar wind density: if solar wind is slow or less dense, there are fewer impacts; if solar wind is dense, effects could last for two to three days. Disruption to GPS would be intermittent since the impacts come in waves, which could

(b)(7)e, (b)(7)f

last several hours at a time. Not only would this degrade end-user communications, but it could also affect the operations of the telecom carrier and its ability to respond to emergencies that arise.

~~(U//FOUO)~~ SMEs noted that when moving, the rate at which the GPS signal would fade depends on the direction of travel: for a given speed of travel, east/west fading is more rapid than north/south fading. GPS receivers would go into acquisition/reacquisition phase for the duration of the storm, but they would likely reacquire the GPS signal approximately two hours after sundown in most instances.



~~(U//FOUO)~~ **Scenario C: Jamming disruption from a single multiple-watt stationary jammer. GPS receiver tracking is affected within a three-km GTG radius and a 230-km LOS radius. GPS receiver acquisition is affected within a four-km GTG radius and a 350-km LOS radius.**

(b)(7)e, (b)(7)f

Scenario C

Single, high-power, continuous, stationary jammer (Gnd: 3-4km radius, Air: 230-350km radio LOS)

Time	E	> 30 days	1	6	8	8	10
	D	< 30 days	1	4	8	8	10
	C	< 7 days	1	4	6	7	9
	B	< 1 day	1	3	5	5	8
	A	< 1 hr	1	2	3	5	7
			No degradation	Isolated degradation	Widespread degradation	Isolated Outage	Widespread Outage
			1	2	3	4	5
			Severity				

~~(U//FOUO)~~ **Scenario D: Jamming disruption from multiple low-power jammers on the ground. The jammers are stationary and mobile, with some intermittently active. Pockets of intermittent tracking and acquisition disruption occur across the metropolitan area.**

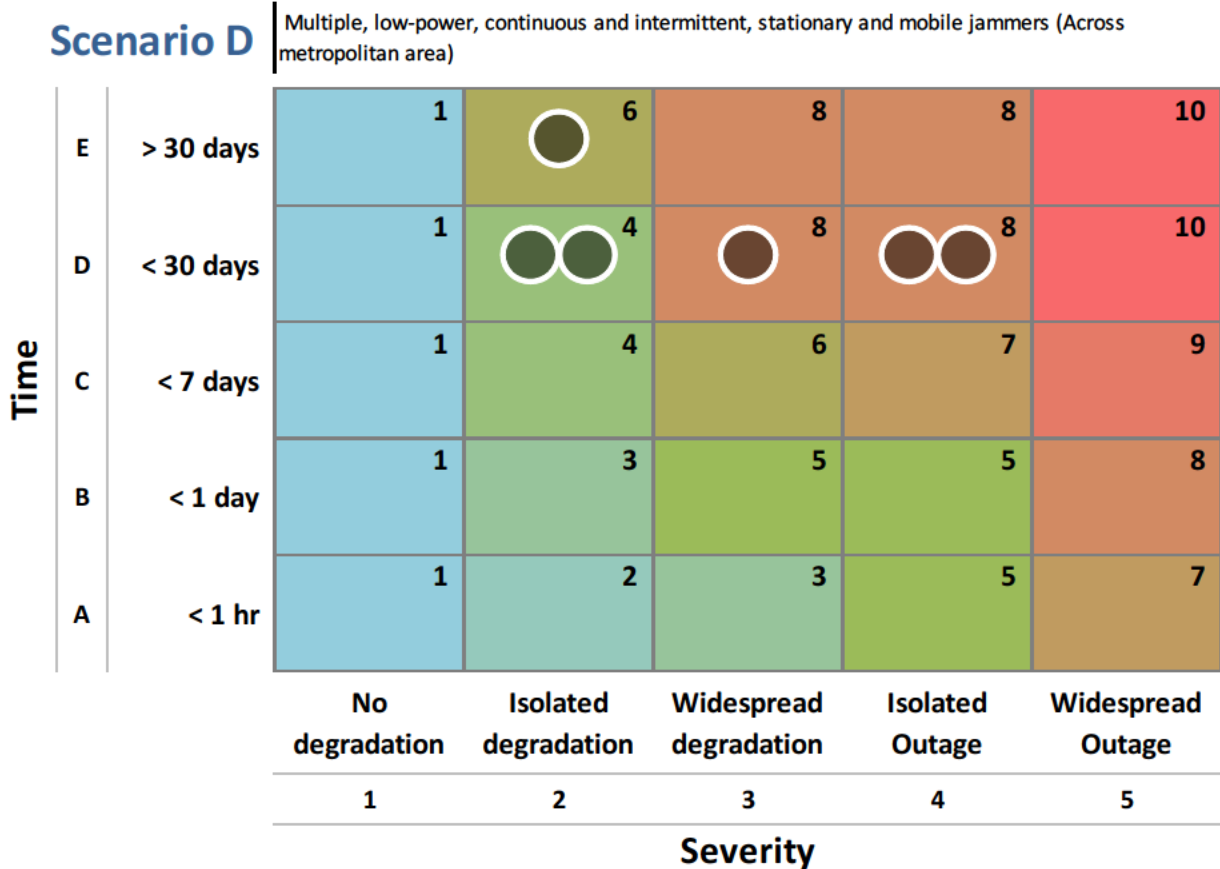
(b)(7)e, (b)(7)f

~~(U//FOUO)~~ One SME suggested that jamming long enough near a central office could isolate an SS7 node,⁹³ which could disable a sizable part of the metropolitan cellular communication

⁹³ ~~(U)~~ SS7 is a telecommunications protocol that links telecos, cellular, and long distance networks and connects disparate telecommunications providers into one common signaling network. "Cisco SS7 Fundamentals,"

http://www.cisco.com/univercd/cc/td/doc/product/tel_pswt/vco_prod/ss7_fund/ss7fun01.pdf, accessed July 15, 2011.

network, but participants disagreed on how plausible such a scenario would be, as it could require multiple systems, which compose key backbone infrastructure with sophisticated architecture, to fail.



~~(U//FOUO)~~ **Scenario H:** *Sophisticated, coordinated “navigation confusion” attack whereby a strategically placed multiple-watt transmitter generates GPS-like signals after an initial interval (several minutes) of jamming. Receivers within a three-km GTG radius and a 230-km LOS radius report a confident timing and position fix, but the timing is wrong by up to hundreds of microseconds and the position fix is wrong by up to tens of kilometers.*

(b)(7)e, (b)(7)f

Scenario H

Single, high-power jammer followed by spoofing (Gnd: 3km radius, Air: 230km radio LOS)

Time	E	> 30 days	1	6	8	8	10
	D	< 30 days	1	4	8	8	10
	C	< 7 days	1	4	6	7	9
	B	< 1 day	1	3	5	5	8
	A	< 1 hr	1	2	3	5	7
			No degradation	Isolated degradation	Widespread degradation	Isolated Outage	Widespread Outage
			1	2	3	4	5
			Severity				

~~(U//FOUO)~~ **Scenario F: Pinpoint spoofing attack against a single target receiver. The spoofer walks off time and position reported by the target receiver without raising alarms.**

~~(U//FOUO)~~ Most SMEs agreed that this scenario would result in isolated degradation for the Communications Sector and that the effects would last for less than seven days. SMEs noted that spoofing could be difficult for users to detect, which means it could take substantial time for authorities to be notified of suspected illicit activity. Carrier technicians would likely pursue many faulty equipment-based hypotheses before considering spoofing as the culprit, and this would delay resolution. Critical nodes for the communication system could be affected by spoofing, but there would be substantial difficulty in causing widespread harm to these communications linkages. It would be possible to spoof a receiver without internal communications alarms being alerted however, since current receivers could fail to recognize spoofing is underway.

Scenario F

Continuous single spoofer

Time	E	> 30 days	1	6	8	8	10
	D	< 30 days	1	4	8	8	10
	C	< 7 days	1	4	6	7	9
	B	< 1 day	1	3	5	5	8
	A	< 1 hr	1	2	3	5	7
			No degradation	Isolated degradation	Widespread degradation	Isolated Outage	Widespread Outage
			1	2	3	4	5

(U//FOUO) *Scenario G: Sophisticated, coordinated pinpoint spoofing attacks against multiple target receivers (one spoofer per targeted receiver). Each spoofer independently walks off the time and position without raising alarms.*

(U//FOUO) SMEs generally agreed that this scenario would result in isolated degradation to the Communications Sector but disagreed on the estimated duration of this degradation. SMEs noted that it would be difficult to locate and eliminate the spoofers, but the extent of disruption would likely stimulate intense effort to find the sources. However, a sophisticated, coordinated spoofing attack would trigger anomalies that would be noticed within the network, and, if such anomalies were indeed noticed, network rerouting would mitigate the attack quickly.

Scenario G

Continuous multiple spoofer

Time	E	> 30 days	1	6	8	8	10
	D	< 30 days	1	4	8	8	10
	C	< 7 days	1	4	6	7	9
	B	< 1 day	1	3	5	5	8
	A	< 1 hr	1	2	3	5	7
			No degradation	Isolated degradation	Widespread degradation	Isolated Outage	Widespread Outage
			1	2	3	4	5

~~(U//FOUO)~~ **Scenario B: Jamming disruption from a single low-power stationary jammer.** GPS receiver tracking is affected within a 500-m GTG radius and a 20-km LOS radius. GPS receiver acquisition is affected within an 800-m GTG radius and 30-km LOS radius.

~~(U//FOUO)~~ Most SMEs judged that the effects of this scenario would last for less than seven days. While the majority of SMEs judged the scenario would result in isolated degradation, some SMEs judged it would result in isolated outage. SMEs noted that the weaker signals from the jammer could complicate locating the device and could likely extend the duration of the jamming. Those investigating disruptions might first suspect faulty equipment rather than jamming.

Scenario B

Single, low-power, continuous, stationary jammer (Gnd: 500-700m radius, Air: 20-30km radio LOS)

Time	E	> 30 days	1	6	8	8	10
	D	< 30 days	1	4	8	8	10
	C	< 7 days	1	4	6	7	9
	B	< 1 day	1	3	5	5	8
	A	< 1 hr	1	2	3	5	7
			No degradation	Isolated degradation	Widespread degradation	Isolated Outage	Widespread Outage
			1	2	3	4	5
			Severity				

~~(U)~~ ***NRE GPS Emergency Services Sector Consequence Workshop Findings Report***

~~(U//FOUO)~~ HITRAC held a workshop on March 5, 2011, to discuss how the Emergency Services Sector uses GPS PNT and to elicit SME judgment regarding potential Sector consequences that could arise if the GPS signal were disrupted in various scenarios. (See Annex I for a list of SME participants.)

~~(U//FOUO)~~ SMEs judged the following GPS disruption scenarios to have the highest impact on the Emergency Services Sector:

- ~~(U//FOUO)~~ Scenario D: Multiple, low-power, continuous and intermittent, stationary and mobile jammers.
- ~~(U//FOUO)~~ Scenario G: Continuous multiple spoofers.
- ~~(U//FOUO)~~ Scenario E: Severe geomagnetic storm.
- ~~(U//FOUO)~~ Scenario F: Continuous single spoofer.

~~(U//FOUO)~~ SMEs judged the following GPS disruption scenarios to have lower impacts on the Emergency Services Sector:

- ~~(U//FOUO)~~ Scenario H: Brief high-power jamming followed by continuous high-power spoofing.
- ~~(U//FOUO)~~ Scenario A: Continuous, stationary, unintentional interference.
- ~~(U//FOUO)~~ Scenario B: Single, low-power, continuous, stationary jammer.
- ~~(U//FOUO)~~ Scenario C: Single, high-power, continuous, stationary jammer.

~~(U//FOUO)~~ In addition, SMEs made the following observations regarding the Emergency Services Sector's use of GPS PNT:

- ~~(U//FOUO)~~ Most GPS disruption scenarios would result in disruption rather than outages of the Emergency Service Sector. The Sector could typically revert to workarounds in the event of a GPS disruption, but these workarounds would likely result in reduced efficiency.
- ~~(U//FOUO)~~ For example, GPS is used for synchronizing signals. GPS keeps the clock within radio equipment stable, and the clock keeps the frequencies stable. In order to use simulcast, multiple towers need identical synchronized frequencies. Without GPS to synchronize, communications abilities would deteriorate. Without simulcast ability, parts of the Emergency Services Sector would have to fall back on less sophisticated means of communications, such as reverting to a standard single frequency repeater, which does not require GPS to operate. An entire department would have to share a single channel, which would likely cause chaos.

- ~~(U//FOUO)~~ Although many jurisdictions still have conventional systems in place that do not rely on GPS, fewer legacy systems will be in use each year as reliance on GPS-based systems grows.
- ~~(U//FOUO)~~ A longer lasting effect of disruption in GPS to the Sector could be the erosion of public confidence in GPS-supported services.
- ~~(U//FOUO)~~ Spoofing scenarios are of particular concern to the Sector, which is reliant on accurate positioning and navigation features in order to respond to emergency incidents. The Emergency Services Sector uses Standard Positioning Service (SPS) GPS, available to civilians, not Precise Positioning Service, available to the military, which leaves it more vulnerable to spoofing.

~~(U)~~ Scenario Consequence Summaries




~~(U//FOUO)~~ *Scenario A: An interference source is causing unintentional disruption. Ground receivers within a 30-km GTG radius are affected, and airborne receivers within radio LOS are affected.*

~~(U//FOUO)~~ The SMEs judged this scenario would result in either isolated or widespread degradation, and most SMEs agreed the degradation would last for less than seven days. SMEs noted that the stationary nature of the interference would make it easy to locate within a short timeframe. In addition, because this scenario would affect ground and airborne systems, both the FCC and FAA would be involved in finding and mitigating the cause of the interference, likely increasing the amount of resources devoted to the issue.

~~(U//FOUO)~~ During the degradation, fire and rescue, police, and 911 call centers could have to find manual workarounds, which would minimize disruption somewhat but increase inefficiencies. This would result in increased response time from first responders. Airborne emergency services would be impacted as well, as they might require visual landmarks or maps to respond to incidents.

Scenario A



Continuous, stationary, unintentional interference (Gnd: 30km radius, Air: radio LOS)

Time	E	> 30 days	1	5	8	8	10
	D	< 30 days	1	4	7	7	10
	C	< 7 days	1	 3	 6	7	9
	B	< 1 day	1	 3	5	5	8
	A	< 1 hr	1	2	3	5	7
			No degradation	Isolated degradation	Widespread degradation	Isolated Outage	Widespread Outage
			1	2	3	4	5
			Severity				

~~(U//FOUO)~~ *Scenario E: Continent-scale natural disruption caused by a severe geomagnetic storm. Tracking threshold of GPS is reduced significantly.*

~~(U//FOUO)~~ All SMEs agreed that this scenario would cause widespread degradation; however, they were split on whether the effects would last less than seven days or less than one day, with most leaning toward less than one day.

~~(U//FOUO)~~ A severe geomagnetic event would degrade the command and control, location-based service, and airborne activities of the Emergency Services Sector. However, with this type of disruption, and with the effects and source known, there may be advance notice of degradation, allowing emergency services to plan and mitigate with possible countermeasures accordingly, as well as alert and educate the public. In addition, any degradation effects could be equipment specific; for example, according to one SME, this scenario could cause less disruption in A-GPS systems, e.g., cell phone GPS receivers assisted by cell phone towers, which use data from non-satellite sources, such as networks, to allow GPS devices to obtain GPS satellite measurements to determine their positions more quickly using much weaker GPS signals than conventional GPS receivers can obtain.

Scenario E		Severe geomagnetic storm (Continent-sized area)					
Time	E	> 30 days	1	5	8	8	10
	D	< 30 days	1	4	7	7	10
	C	< 7 days	1	3		7	9
	B	< 1 day	1	3		5	8
	A	< 1 hr	1	2	3	5	7
			No degradation	Isolated degradation	Widespread degradation	Isolated Outage	Widespread Outage
			1	2	3	4	5
			Severity				




~~(U//FOUO)~~ **Scenario C: Jamming disruption from a single multiple-watt stationary jammer.** GPS receiver tracking is affected within a three-km GTG radius and a 230-km LOS radius. GPS receiver acquisition is affected within a four-km GTG radius and a 350-km LOS radius.

~~(U//FOUO)~~ SMEs generally agreed that the effects of this scenario would last less than seven days, and most judged the scenario would cause isolated degradation, although a few thought it could lead to isolated outages.

~~(U//FOUO)~~ SMEs determined that this scenario would cause both navigation and communication disruptions within the Emergency Services Sector. For instance, without GPS navigation, fire and rescue crews could have trouble finding unfamiliar addresses. Although this could be mitigated, such as with paper maps, those resources may not be readily available to crews who have come to rely on GPS. This scenario could also impact communications, as the GPS degradation would begin to affect radio systems, in turn affecting CAD systems and voice communications. Although many jurisdictions still have conventional systems in place that do not rely on GPS, fewer legacy systems will be in use each year as reliance on GPS-based systems grows.

Scenario C

Single, high-power, continuous, stationary jammer (Gnd: 3-4km radius, Air: 230-350km radio LOS)

Time	E	> 30 days	1	5	8	8	10
	D	< 30 days	1	4	7	7	10
	C	< 7 days	1		6		9
	B	< 1 day	1		5	5	8
	A	< 1 hr	1	2	3	5	7
			No degradation	Isolated degradation	Widespread degradation	Isolated Outage	Widespread Outage
			1	2	3	4	5
			Severity				

~~(U//FOUO)~~ **Scenario D: Jamming disruption from multiple low-power jammers on the ground. The jammers are stationary and mobile, with some intermittently active. Pockets of intermittent tracking and acquisition disruption occur across the metropolitan area.**

~~(U//FOUO)~~ SMEs were divided about the severity and timing of the effects from this scenario. A plurality of SMEs agreed the scenario would result in widespread degradation for greater than 30 days across the Sector; however, an equal number of SMEs judged the effect would be isolated degradation, although timing varied from less than 1 day to more than 30 days. A single SME judged the scenario would lead to widespread outages lasting less than 30 days. Because some of the jammers are mobile, there would be intermittent pockets of disruptions that could be very difficult to track, hampering mitigation efforts.

~~(U//FOUO)~~ As with other scenarios, this situation would cause disruptions for police, fire, and EMS, and force them to revert to older systems as a workaround (assuming they still had the capability). Several SMEs noted that one of the greatest consequences from this scenario could be an erosion of the public's trust in GPS reliability and capabilities.

Scenario D

Multiple, low-power, continuous and intermittent, stationary and mobile jammers (Across metropolitan area)

Time	E	> 30 days	1	5	8	8	10
	D	< 30 days	1	4	7	7	10
	C	< 7 days	1	3	6	7	9
	B	< 1 day	1	3	5	5	8
	A	< 1 hr	1	2	3	5	7
			No degradation	Isolated degradation	Widespread degradation	Isolated Outage	Widespread Outage
			1	2	3	4	5
			Severity				

~~(U//FOUO)~~ **Scenario H: Sophisticated, coordinated “navigation confusion” attack whereby a strategically placed multiple-watt transmitter generates GPS-like signals after an initial interval (several minutes) of jamming. Receivers within a three-km GTG radius and a 230-km LOS radius report a confident timing and position fix, but the timing is wrong by up to hundreds of microseconds and the position fix is wrong by up to tens of kilometers.**

~~(U//FOUO)~~ Half the SMEs judged the effect from this scenario would be isolated degradation for less than seven days. The remaining SMEs generally agreed there would be widespread degradation but disagreed as to whether it would last less than seven days or less than 30 days.

~~(U//FOUO)~~ The most notable consequence for the Emergency Services Sector seen emerging from this scenario is the effect spoofing would have on location data for emergency services. For instance, police, fire, and EMS could receive a wrong fix for their location and go to the wrong address, possibly resulting in damaging or life-threatening consequences for those waiting on emergency help. A situation like this would depend on dispatchers and other backup technology to mitigate consequences.

Scenario H

Single, high-power jammer followed by spoofing (Gnd: 3km radius, Air: 230km radio LOS)

Time	E	> 30 days	1	5	8	8	10
	D	< 30 days	1	4	7	7	10
	C	< 7 days	1	3	6	7	9
	B	< 1 day	1	3	5	5	8
	A	< 1 hr	1	2	3	5	7
			No degradation	Isolated degradation	Widespread degradation	Isolated Outage	Widespread Outage
			1	2	3	4	5
			Severity				

~~(U//FOUO)~~ **Scenario F: Pinpoint spoofing attack against a single target receiver. The spoofer walks off time and position reported by the target receiver without raising alarms.**

~~(U//FOUO)~~ All SMEs judged that isolated degradation would result from this scenario; however, estimated durations varied, with most SMEs believing the degradation would last more than 30 days, but the remaining SMEs split between various durations, all of which were of less than 30 days. SMEs generally agreed that the duration would be greater than 30 days because pinpointed spoofing that attacks a single, possibly isolated, target could take a good deal of time to detect and/or diagnose and could necessitate a lengthy physical search for the spoofer.

~~(U//FOUO)~~ Although this scenario involves a single target, SMEs agreed upon various ways disruptions to the Emergency Services Sector could result. A spoofer could take control of a target receiver but apply zero error functions to it for a time, leaving the Sector unaware the receiver has been compromised. At a later date, perhaps during a crisis or some other vulnerability, the spoofer could spoof the system, affecting public safety in various ways. For instance, instead of shifting the location, the spoofer could slowly drag the time off, disrupting the communications capability. If the Emergency Services Sector is using a synchronous station and that station's timing is off, the station would essentially be taken off the air, degrading communications.

Scenario F

Continuous single spoofer

Time	E	> 30 days	1	5	8	8	10
	D	< 30 days	1	4	7	7	10
	C	< 7 days	1	3	6	7	9
	B	< 1 day	1	3	5	5	8
	A	< 1 hr	1	2	3	5	7
			No degradation	Isolated degradation	Widespread degradation	Isolated Outage	Widespread Outage
			1	2	3	4	5
			Severity				




~~(U//FOUO)~~ Scenario G: Sophisticated, coordinated pinpoint spoofing attacks against multiple target receivers (one spoofer per targeted receiver). Each spoofer independently walks off the time and position without raising alarms.

~~(U//FOUO)~~ Most SMEs agreed that this scenario would result in widespread degradation for more than 30 days; with many SMEs believing consequences could last much longer than that. After the lengthy time required to discover the cause of the disruption, the presence of multiple spoofers means that it could take a significant period of additional time to locate those spoofers and affected devices.

~~(U//FOUO)~~ SMEs discussed effects on the Emergency Services Sector, depending on various ways this scenario could occur. The Sector is often divided into municipalities, so whether these multiple spoofing attacks target multiple receivers in a single jurisdiction or receivers across multiple jurisdictions would determine the scope of the impact to emergency services. Smaller attacks across a wider area could erode public confidence in the Sector.

Scenario G

Continuous multiple spoofer

Time	E	> 30 days	1	5	 8	8	10
	D	< 30 days	1	4	 7	7	10
	C	< 7 days	1	3	6	 7	9
	B	< 1 day	1	3	5	5	8
	A	< 1 hr	1	2	3	5	7
			No degradation	Isolated degradation	Widespread degradation	Isolated Outage	Widespread Outage
			1	2	3	4	5
			Severity				

~~(U//FOUO)~~ **Scenario B: Jamming disruption from a single low-power stationary jammer.** GPS receiver tracking is affected within a 500-m GTG radius and a 20-km LOS radius. GPS receiver acquisition is affected within an 800-m GTG radius and 30-km LOS radius.

~~(U//FOUO)~~ SMEs mostly agreed this scenario would result in isolated degradation for less than seven days. SMEs generally judged the jammer could be detected and located in a short timeframe owing to its stationary nature and the limited area in which it could be located, which would quickly create a known “dead zone.” However, because of the small scope of the jamming, it could take some time before the issue was noticed and a response triggered.

~~(U//FOUO)~~ One SME mentioned that this kind of degradation likely would affect the operations of the Emergency Services Sector, requiring the use of workarounds in order maintain the Sector’s services, and another mentioned that this sort of incident might only lead to an issue with a component of the Sector (because of the size of the affected area), rather than the Sector itself.

Scenario B

Single, low-power, continuous, stationary jammer (Gnd: 500-700m radius, Air: 20-30km radio LOS)

Time	E	> 30 days	1	5	8	8	10
	D	< 30 days	1	4	7	7	10
	C	< 7 days	1	3	6	7	9
	B	< 1 day	1	3	5	5	8
	A	< 1 hr	1	2	3	5	7
			No degradation	Isolated degradation	Widespread degradation	Isolated Outage	Widespread Outage
			1	2	3	4	5
			Severity				

~~(U)~~ **NRE GPS Energy Sector Consequence Workshop Findings Report**

~~(U)~~ **Summary of Key Workshop Findings**

~~(U//FOUO)~~ HITRAC held a workshop on March 24, 2011, to discuss how the Energy Sector uses GPS PNT and to elicit SME judgment regarding potential subsector consequences that could arise if the GPS signal were disrupted in various scenarios. (See Annex I for a list of SME participants.)

~~(U//FOUO)~~ SMEs judged the following GPS disruption scenarios to have the highest impact on the Energy Sector:

- ~~(U//FOUO)~~ Scenario G: Continuous multiple spoofer.
- ~~(U//FOUO)~~ Scenario D: Multiple, low-power, continuous and intermittent, stationary and mobile jammers.
- ~~(U//FOUO)~~ Scenario F: Continuous single spoofer.
- ~~(U//FOUO)~~ Scenario H: Brief high-power jamming followed by continuous high-power spoofing.

~~(U//FOUO)~~ SMEs judged the following GPS disruption scenarios to have lower impacts on the Energy Sector:

- ~~(U//FOUO)~~ Scenario A: Continuous, stationary, unintentional interference.
- ~~(U//FOUO)~~ Scenario B: Single, low-power, continuous, stationary jammer.
- ~~(U//FOUO)~~ Scenario C: Single, high-power, continuous, stationary jammer.
- ~~(U//FOUO)~~ Scenario E: Severe geomagnetic storm.

~~(U//FOUO)~~ In addition, SMEs made the following observations regarding the Energy Sector's use of GPS PNT:

- ~~(U//FOUO)~~ SMEs considered the current mitigation measures in effect or planned for the next three to five years in the Energy Sector and recognized that baseline operations for the Energy Sector can include occasional degradation of services.
- ~~(U//FOUO)~~ The electricity subsector of the Energy Sector relies on GPS for efficient operations to a greater degree than the other subsectors (petroleum or natural gas).
- ~~(U//FOUO)~~ The electricity subsector use of GPS timing through PMUs is still not prevalent throughout the power grid. Industry has been hesitant to install PMUs, especially for operational control of the grid.
- ~~(U//FOUO)~~ The modernization of the power grid – certain aspects of which are known as the “Smart Grid” – relies heavily on PMUs. Going forward, it is a national priority to

make the power grid more reliable and efficient, and distributed networks of PMUs are a tool well suited for making that happen.

- ~~(U//FOUO)~~ Spoofing attacks against multiple targets could cause significant service outages.
- ~~(U//FOUO)~~ The sources of continuous or higher powered GPS disruption can be more readily located than the sources of intermittent or lower powered GPS disruption. Locating and disabling these sources requires timely coordination across multiple government agencies.






~~(U)~~ Scenario Consequence Summaries

~~(U//FOUO)~~ *Scenario A: An interference source is causing unintentional disruption. Ground receivers within a 30-km GTG radius are affected, and airborne receivers within radio LOS are affected.*

~~(U//FOUO)~~ Most SMEs agreed that this scenario would result in isolated or no degradation and that the degradation would last for less than seven days. SMEs noted that it could take up to seven days (and perhaps longer) for authorities to detect, locate, and disable the jammer, although continuous interference sources are easier to identify. SMEs noted that within the Energy Sector, this scenario could affect a single substation, assuming there is no backup to a terrestrial clock. The device that loses clock synchronizing will provide erroneous measurement, such as frequency and phase angle, resulting in erroneous power flow calculations. This could cause overheating to some elements of the grid in the affected area, such as overloaded lines or overloaded transformers. If the device is used for adaptive protection, in the case of a fault, coordination of the protection system could be disrupted and backup protection might operate to isolate the fault before the local protection device operates. SMEs agreed that outages are not likely to occur because of the redundancy in the power grid system and similar redundancy in other Energy subsectors.

Scenario A

Continuous, stationary, unintentional interference (Gnd: 30km radius, Air: radio LOS)

Time	E	> 30 days	1	5	7	8	10
	D	< 30 days	 1	 4	 7	7	9
	C	< 7 days	 1	 3	6	7	8
	B	< 1 day	1	2	4	4	5
	A	< 1 hr	1	2	2	2	4
			No degradation	Isolated degradation	Widespread degradation	Isolated Outage	Widespread Outage
			1	2	3	4	5
			Severity				

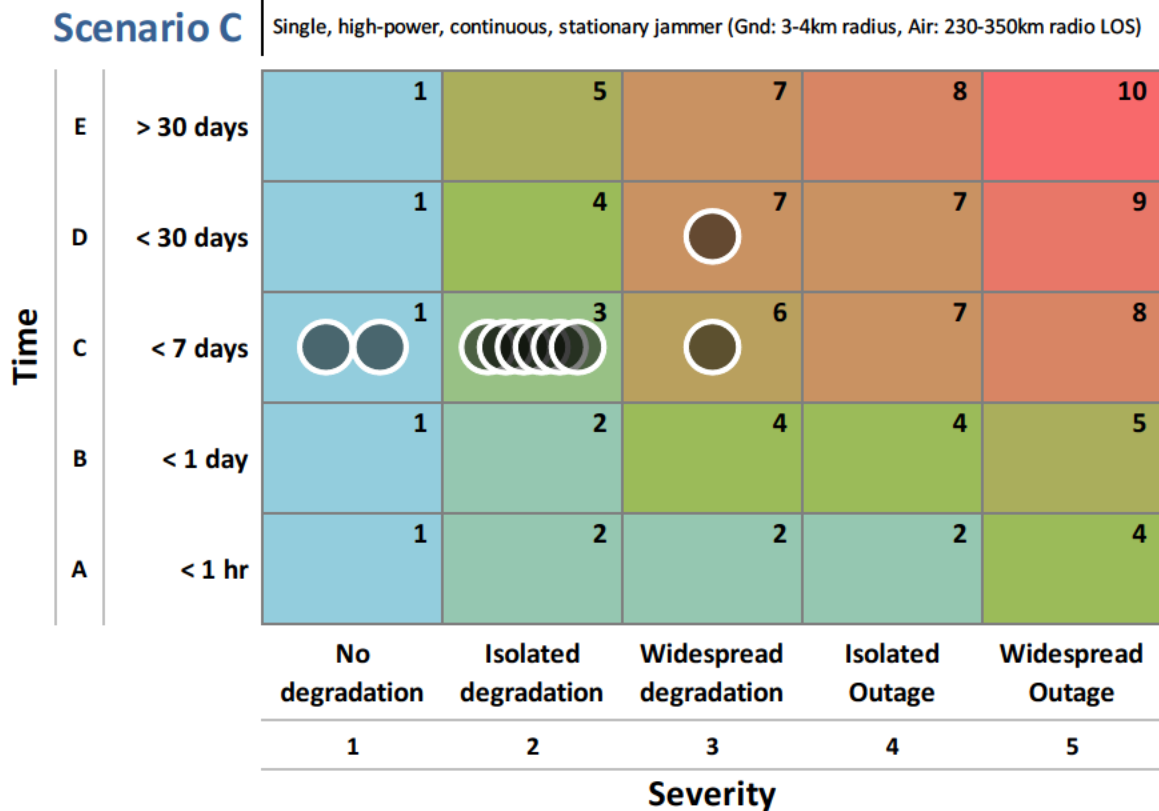
~~(U//FOUO)~~ **Scenario E: Continent-scale natural disruption caused by a severe geomagnetic storm. Tracking threshold of GPS is reduced significantly.**

~~(U//FOUO)~~ SMEs judged that the effects of this scenario would last between less than one day and less than seven days, depending on the duration and geographic area most impacted by the geomagnetic storm. Most SMEs judged the effects of the scenario on the Energy Sector would be either widespread degradation or isolated degradation. SMEs noted that the penetration of PMUs within the power grid is still relatively small and that PMUs are used to monitor, not control, the stability of the power grid. Assuming the event is affecting the ability of the GPS receiver to receive the signal continuously and timing is intermittently received, the device would resynchronize and run on an internal clock during the loss of the signal until it receives the signal again and resynchronizes. Therefore, it is likely that this scenario would cause little degradation of services as there is sufficient robustness in the Sector. SMEs noted that the most significant effects to the Energy Sector would stem from the electrical currents generated by the geomagnetic storm impacting electrical transmission equipment, not from the effects of the geomagnetic storm on GPS utilized by the Sector.

Scenario E		Severe geomagnetic storm (Continent-sized area)					
Time	E	> 30 days	1	5	7	8	10
	D	< 30 days	1	4	7	7	9
	C	< 7 days	1	3	6	7	8
	B	< 1 day	1	2	4	4	5
	A	< 1 hr	1	2	2	2	4
			No degradation	Isolated degradation	Widespread degradation	Isolated Outage	Widespread Outage
			1	2	3	4	5
			Severity				

~~(U//FOUO)~~ **Scenario C: Jamming disruption from a single multiple-watt stationary jammer.**
GPS receiver tracking is affected within a three-km GTG radius and a 230-km LOS radius.
GPS receiver acquisition is affected within a four-km GTG radius and a 350-km LOS radius.

(b)(7)e, (b)(7)f







~~(U//FOUO)~~ **Scenario D: Jamming disruption from multiple low-power jammers on the ground. The jammers are stationary and mobile, with some intermittently active. Pockets of intermittent tracking and acquisition disruption occur across the metropolitan area.**

~~(U//FOUO)~~ SMEs were divided as to whether the effects of this scenario would persist for less than or more than 30 days. The presence of multiple intermittent jammers would be difficult to identify, locate, and disable, thus enabling effects to persist for up to or more than 30 days. Most SMEs judged the scenario would result in isolated degradation of services in the Energy Sector, although some SMEs thought the degradation would be widespread and could result in isolated outages. SMEs judged that electrical services would be degraded because when operators cannot depend on the better observability provided by GPS, they adopt safer operating conditions, which means less efficiency. If the intermittent jamming is longer than 15 seconds, time synchronization might be lost, affecting the state parameters calculation used for load flow and system stability and line carrying margin. In that case, the time-stamped data would be ignored by operators and they would consider the state estimation algorithm in order to detect faults and undesirable states that require that remedial action to be taken.⁹⁵

⁹⁵ ~~(U//FOUO)~~ NASA Ames Research Center, "State Estimation," www.nasa.gov/centers/ames/research/technology-onepaggers/state-estimation.html, 29 March 2008, accessed September 22, 2011.

Scenario DMultiple, low-power, continuous and intermittent, stationary and mobile jammers
(Across metropolitan area)





Time	E	> 30 days	1	 5	 7	8	10
	D	< 30 days	1	 4	7	 7	9
	C	< 7 days	1	3	6	7	8
	B	< 1 day	1	2	4	4	5
	A	< 1 hr	1	2	2	2	4
			No degradation	Isolated degradation	Widespread degradation	Isolated Outage	Widespread Outage
			1	2	3	4	5
Severity							

~~(U//FOUO)~~ **Scenario H:** *Sophisticated, coordinated “navigation confusion” attack whereby a strategically placed multiple-watt transmitter generates GPS-like signals after an initial interval (several minutes) of jamming. Receivers within a three-km GTG radius and a 230-km LOS radius report a confident timing and position fix, but the timing is wrong by up to hundreds of microseconds and the position fix is wrong by up to tens of kilometers.*

~~(U//FOUO)~~ SMEs were divided as to whether the scenario would result in isolated degradation or isolated outage. Most SMEs agreed that the duration of the effects from the scenario would be less than seven days, although detection could be challenging, particularly if the spoofer operates below the thermal noise level. The resulting change in phase values of a region relative to the rest of the power grid would be apparent. This “movement” of the substation could cause an alarm, but none of the present GPS clocks are designed to alarm on unexpected movement. If the movement is sudden, some manufactures may report a phase or frequency shift on the clock. Further investigation should lead the operator to determine the GPS signal was the cause. If the movement is subtle, the GPS clock will likely steer out what it thinks is an error. The disruption would result from the inability to coordinate power transfer between the affected region and the non-affected region. An outage could occur if synchrophasor measures drift due to spoofing, causing transformers to overload and overheat. While the jamming could persist for weeks, SMEs noted that operators would learn to discard phasor measurements once they realize the measurements are no longer reliable.







Scenario H

Single, high-power jammer followed by spoofing (Gnd: 3km radius, Air: 230km radio LOS)

Time	E	> 30 days	1	5	7	8	10
	D	< 30 days	1	4	7		9
	C	< 7 days	1		6		8
	B	< 1 day	1	2	4		5
	A	< 1 hr	1	2	2	2	4
			No degradation	Isolated degradation	Widespread degradation	Isolated Outage	Widespread Outage
			1	2	3	4	5
			Severity				

~~(U//FOUO)~~ **Scenario F: Pinpoint spoofing attack against a single target receiver. The spoofer walks off time and position reported by the target receiver without raising alarms.**

~~(U//FOUO)~~ Most SMEs agreed that this scenario would result in isolated degradation and that the effects of this scenario would last for less than seven days. Effects would be localized to the targeted generator. Some SMEs noted that power companies would not allow an outage to persist for more than a few days. If capture time for the receiver is walked off significantly enough, it would be noticed. The affected PMU would be identified as unreliable and ignored by the state estimator. A single synchronized measurement that is inaccurate has limited impact on system operation and system stability. A significant challenge could be that maintenance personnel might not identify spoofing as the cause of the disruption in their standard troubleshooting procedures.

Scenario F		Continuous single spoofer					
Time	E	> 30 days	1	 5	7	8	10
	D	< 30 days	1	 4	7	7	9
	C	< 7 days	 1	 3	 6	 7	8
	B	< 1 day	1	2	4	4	5
	A	< 1 hr	1	2	2	2	4
			No degradation	Isolated degradation	Widespread degradation	Isolated Outage	Widespread Outage
			1	2	3	4	5
			Severity				

~~(U//FOUO)~~ **Scenario G: Sophisticated, coordinated pinpoint spoofing attacks against multiple target receivers (one spoofer per targeted receiver). Each spoofer independently walks off the time and position without raising alarms.**

~~(U//FOUO)~~ Most SME judged that this scenario would result in widespread outage of a duration ranging from less than seven days to more than 30 days. This scenario could cause significant damage to the power grid due to the degradation of numerical data. Certain generators could erroneously detect an oscillating signal and attempt to dampen that oscillation. In this case, generators would automatically try to dampen an oscillation that did not exist, leading to a potential outage. SMEs noted that this scenario could cause a major and widespread outage. It would take a long time to locate the spoofers because they do not need to radiate power to track the victim antennas (because they are stationary).





Scenario G		Continuous multiple spoofer					
Time	E	> 30 days	1	5	7	8	10
	D	< 30 days	1	4	7	7	9
	C	< 7 days	1	3	6	7	8
	B	< 1 day	1	2	4	4	5
	A	< 1 hr	1	2	2	2	4
		No degradation	Isolated degradation	Widespread degradation	Isolated Outage	Widespread Outage	
		1	2	3	4	5	
Severity							

~~(U//FOUO)~~ **Scenario B: Jamming disruption from a single low-power stationary jammer.** GPS receiver tracking is affected within a 500-m GTG radius and a 20-km LOS radius. GPS receiver acquisition is affected within an 800-m GTG radius and 30-km LOS radius.

~~(U//FOUO)~~ Most SMEs judged that this scenario would result in isolated degradation lasting less than 30 days. SMEs noted that the duration of the scenario effects would depend on the length of time it takes to detect, locate, and disable the jammer. It is more difficult to detect and locate low-power stationary jammers than high-power stationary jammers. However, SMEs indicated that the range of the low-power jammer is so short that it would probably cause limited degradation to the Energy Sector because of the redundancy in the systems.

Scenario B

Single, low-power, continuous, stationary jammer (Gnd: 500-700m radius, Air: 20-30km radio LOS)

Time	E	> 30 days	1	5	7	8	10
	D	< 30 days	 1	 4	7	7	9
	C	< 7 days	 1	 3	6	7	8
	B	< 1 day	1	2	4	4	5
	A	< 1 hr	1	2	2	2	4
			No degradation	Isolated degradation	Widespread degradation	Isolated Outage	Widespread Outage
			1	2	3	4	5
			Severity				

~~(U)~~ **NRE GPS Transportation Systems Sector (Aviation) Consequence Workshop Findings Report**

~~(U)~~ **Summary of Key Workshop Findings**

~~(U//FOUO)~~ HITRAC held a workshop on March 14, 2011, to discuss how the aviation subsector uses GPS PNT and to elicit SME judgment regarding potential subsector consequences that could arise if the GPS signal were disrupted in various scenarios. (See Annex I for a list of SME participants.)

~~(U//FOUO)~~ SMEs judged the following GPS disruption scenarios to have the highest impact on the aviation subsector of the Transportation Systems Sector:

- ~~(U//FOUO)~~ Scenario G: Continuous multiple spoofers.
- ~~(U//FOUO)~~ Scenario F: Continuous single spoofer.
- ~~(U//FOUO)~~ Scenario D: Multiple, low-power, continuous and intermittent, stationary and mobile jammers.
- ~~(U//FOUO)~~ Scenario H: Brief high-power jamming followed by continuous high-power spoofing.

~~(U//FOUO)~~ SMEs judged the following GPS disruption scenarios to have lower impacts on the aviation subsector of the Transportation Systems Sector:

- ~~(U//FOUO)~~ Scenario A: Continuous, stationary, unintentional interference.
- ~~(U//FOUO)~~ Scenario C: Single, high-power, continuous, stationary jammer.
- ~~(U//FOUO)~~ Scenario E: Severe geomagnetic storm.
- ~~(U//FOUO)~~ Scenario B: Single, low-power, continuous, stationary jammer.

~~(U//FOUO)~~ In addition, SMEs made the following observations regarding aviation's use of GPS PNT:

- ~~(U//FOUO)~~ The SMEs considered the current mitigation measures in effect or planned for the next three to five years in the aviation subsector and recognized that baseline operations for the subsector are not perfect but routinely involve an element of mission degradation. In other words, jamming would certainly not be welcome and would have operational impacts, but the aviation operations would probably compensate for any known electromagnetic threat or danger.
- ~~(U//FOUO)~~ SMEs noted that it is highly unlikely that there could be a long-term, widespread degradation or outage of service for all transportation modes in a single incident. In other words, aviation operations may be degraded by jamming or spoofing, but these threats are unlikely to have a lasting and simultaneous impact on maritime and road transportation. However, a GPS disruption incident will have long-term

implications for the FAA because the Next Generation Transportation System (NextGen) will be dependent on timing.






- ~~(U//FOUO)~~ The sources of continuous GPS disruption can be more readily located than the sources of intermittent GPS disruption. Locating and disabling these intermittent sources requires timely coordination across multiple government agencies.
- ~~(U//FOUO)~~ In most scenarios, disruption of GPS would result in degradation, not outages, in the aviation subsector. This is due to the sufficient backup systems already in place. These backup systems are based on the terrestrial navigation aids that were used before satellite navigation became available (VOR, DME, ILS).
- ~~(U//FOUO)~~ The extent to which GPS disruptions currently occur is not fully known as pilots do not always report incidents.
- ~~(U//FOUO)~~ A significant degradation of aviation services could affect the Postal and Shipping Sector, which relies on next-day delivery of goods such as medical supplies.
- ~~(U//FOUO)~~ The aviation industry depends on the Communications and Energy Sectors and would be affected by GPS disruptions affecting any of these sectors.
- ~~(U//FOUO)~~ In the future, aviation will be increasingly reliant on GPS for navigation and surveillance, especially through the increasing use of ADS-B for GPS-derived position and collision avoidance. However, the development of multi-frequency receivers could make aviation more resilient to GPS disruptions. These receivers are not expected to be widespread until after 2020. The new multi-frequency signals could also be jammed, but the jammers would need to be more powerful and thus easier to detect.

~~(U)~~ **Scenario Consequence Summaries**

~~(U//FOUO)~~ *Scenario A: An interference source is causing unintentional disruption. Ground receivers within a 30-km GTG radius are affected, and airborne receivers within radio LOS are affected.*

(b)(7)e, (b)(7)f

degradation of GPS at a high-traffic airport would have broader impacts on the subsector than would a similar degradation at a low-traffic airport.

Scenario A			Continuous, stationary, unintentional interference (Gnd: 30km radius, Air: radio LOS)				
Time	E	> 30 days	1	 5	6	6	8
	D	< 30 days	1	 4	5	6	8
	C	< 7 days	1	 3	 4	 4	7
	B	< 1 day	1	2	3	3	5
	A	< 1 hr	1	2	2	2	3
			No degradation	Isolated degradation	Widespread degradation	Isolated Outage	Widespread Outage
			1	2	3	4	5
			Severity				

~~(U//FOUO)~~ **Scenario E: Continent-scale natural disruption caused by a severe geomagnetic storm. Tracking threshold of GPS is reduced significantly.**

~~(U//FOUO)~~ The majority of SMEs judged that this scenario would result in widespread degradation and that this degradation would last for less than one day. Effects would be widespread because they likely would extend beyond a single metropolitan area. These events cannot be reliably predicted. Fortunately, the WAAS is designed with a built-in reversionary mode. If a strong ionospheric storm occurs, WAAS discontinues support for precision approach but continues support for non-precision approach as well as terminal area and en route navigation. The majority of SMEs thought the effects would be limited to a day as these natural events typically do not last longer. However, some SMEs noted that the effects could be felt nationwide and it could take the aviation industry several days to return to normal operations. SMEs also noted that there is limited historical precedence for geomagnetic storms significantly affecting aviation.

Scenario E

Severe geomagnetic storm (Continent-sized area)

Time	E	> 30 days	1	5	6	6	8
	D	< 30 days	1	4	5	6	8
	C	< 7 days	1	3	4	4	7
	B	< 1 day	1	2	3	3	5
	A	< 1 hr	1	2	2	2	3
			No degradation	Isolated degradation	Widespread degradation	Isolated Outage	Widespread Outage
			1	2	3	4	5
			Severity				

~~(U//FOUO)~~ **Scenario C: Jamming disruption from a single multiple-watt stationary jammer. GPS receiver tracking is affected within a three-km GTG radius and a 230-km LOS radius. GPS receiver acquisition is affected within a four-km GTG radius and a 350-km LOS radius.**

~~(U//FOUO)~~ The majority of SMEs agreed that the duration of effects of this scenario on the aviation mode would be less than seven days because multiple-watt stationary jammers are relatively easy to locate. Most SMEs judged the scenario would result in widespread degradation, although some thought the effects would be an isolated degradation. Arrival precision would be lost, and aircraft would have to rely on ground-based navigation aids along fixed flight paths, resulting in local inefficiency but perhaps more widespread flight delays. SMEs noted that if the jammer is on continuously, it is easier to locate than if it is turned on and off intermittently by a hostile actor.

Scenario C

Single, high-power, continuous, stationary jammer (Gnd: 3-4km radius, Air: 230-350km radio LOS)

Time	E	> 30 days	1	5	6	6	8
	D	< 30 days	1	4	5	6	8
	C	< 7 days	1	3	4	4	7
	B	< 1 day	1	2	3	3	5
	A	< 1 hr	1	2	2	2	3
			No degradation	Isolated degradation	Widespread degradation	Isolated Outage	Widespread Outage
			1	2	3	4	5
			Severity				

~~(U//FOUO)~~ **Scenario D: Jamming disruption from multiple low-power jammers on the ground. The jammers are stationary and mobile, with some intermittently active. Pockets of intermittent tracking and acquisition disruption occur across the metropolitan area.**

~~(U//FOUO)~~ Most SMEs agreed that the effects of this scenario would last for more than 30 days and that these effects would be isolated degradation of the aviation mode, although some SMEs judged the effects to be widespread degradation. SMEs noted that it would be challenging to track down jammers that are dispersed and operating intermittently. However, the effects would be more of a nuisance to the aviation subsector. Mitigation exists with legacy ground-based navigation aids, although capacity at affected airports could be reduced. One SME noted that there would need to be at least three WAAS reference stations out to have a widespread effect on WAAS services provided at locales other than those directly affected by jamming. In this scenario, aviation may not be the primary target of hostile actors but would suffer collateral effects.

Scenario D

Multiple, low-power, continuous and intermittent, stationary and mobile jammers (Across metropolitan area)

Time	E	> 30 days	1	5	6	6	8
	D	< 30 days	1	4	5	6	8
	C	< 7 days	1	3	4	4	7
	B	< 1 day	1	2	3	3	5
	A	< 1 hr	1	2	2	2	3
			No degradation	Isolated degradation	Widespread degradation	Isolated Outage	Widespread Outage
			1	2	3	4	5
			Severity				

~~(U//FOUO)~~ **Scenario B: Jamming disruption from a single low-power stationary jammer.** GPS receiver tracking is affected within a 500-m GTG radius and a 20-km LOS radius. GPS receiver acquisition is affected within an 800-m GTG radius and 30-km LOS radius.

~~(U//FOUO)~~ Most SMEs agreed that this scenario would result in isolated degradation to the aviation mode and that this degradation would last for less than seven days. Service would be degraded, but legacy systems would provide sufficient services to preclude an outage. Aircraft would still be able to land but airport capacity would be reduced. SMEs noted that is easier to locate stationary jammers than moving ones, and the FAA has a seven-day self-imposed deadline for locating them, which is usually sufficient for ensuring necessary cross-agency coordination.

Scenario B

Single, low-power, continuous, stationary jammer (Gnd: 500-700m radius, Air: 20-30km radio LOS)

Time	E	> 30 days	1	5	6	6	8
	D	< 30 days	1	4	5	6	8
	C	< 7 days	1	3	4	4	7
	B	< 1 day	1	2	3	3	5
	A	< 1 hr	1	2	2	2	3
			No degradation	Isolated degradation	Widespread degradation	Isolated Outage	Widespread Outage
			1	2	3	4	5
			Severity				

~~(U//FOUO)~~ **Scenario H:** *Sophisticated, coordinated “navigation confusion” attack whereby a strategically placed multiple-watt transmitter generates GPS-like signals after an initial interval (several minutes) of jamming. Receivers within a three-km GTG radius and a 230-km LOS radius report a confident timing and position fix, but the timing is wrong by up to hundreds of microseconds and the position fix is wrong by up to tens of kilometers.*

~~(U//FOUO)~~ Most SMEs agreed that the effects of this scenario would be widespread degradation but there was some disagreement on the duration of the effects, with estimates ranging from less than 1 day to more than 30 days. SMEs agreed that there would be malicious intent behind implementation of this scenario and that it would require some sophistication to execute. In general, spoofing is much more complex than jamming, although there are multiple levels of detection in avionics. Pilots would start using conventional navigation until the spoofing is shut down. One SME noted that it could take more than 30 days to locate the spoofing device unless military-grade equipment was used because the jamming portion is too brief for the FAA to find it. However, once GPS is declared unreliable, alternative navigation and surveillance systems would be used at the expense of airport capacity and system efficiency.

Scenario H

Single, high-power jammer followed by spoofing (Gnd: 3km radius, Air: 230km radio LOS)

Time						
		No degradation	Isolated degradation	Widespread degradation	Isolated Outage	Widespread Outage
		1	2	3	4	5
E	> 30 days	1	5	6	6	8
D	< 30 days	1	4	5	6	8
C	< 7 days	1	3	4	4	7
B	< 1 day	1	2	3	3	5
A	< 1 hr	1	2	2	2	3
		Severity				

~~(U//FOUO)~~ **Scenario F: Pinpoint spoofing attack against a single target receiver. The spoofer walks off time and position reported by the target receiver without raising alarms.**

~~(U//FOUO)~~ Most SMEs agreed that the effects of this scenario would be isolated degradation of services lasting for more than 30 days. SMEs noted that the aviation subsector might not realize there is a spoofing incident until an airplane crash had occurred, and then public confidence would be lost. Effects would be isolated, because the FAA would switch to an alternative navigation system—VOR—if spoofing is detected. SMEs agreed that a sophisticated hostile actor would perpetrate this scenario. It would be challenging to locate the spoofing source and terminate its operation. However, such an attack is generally only effective against one aircraft at a time.

Scenario F

Continuous single spoofer

Time	E	> 30 days	1	5	6	6	8
	D	< 30 days	1	4	5	6	8
	C	< 7 days	1	3	4	4	7
	B	< 1 day	1	2	3	3	5
	A	< 1 hr	1	2	2	2	3
			No degradation	Isolated degradation	Widespread degradation	Isolated Outage	Widespread Outage
			1	2	3	4	5
			Severity				

~~(U//FOUO)~~ **Scenario G: Sophisticated, coordinated pinpoint spoofing attacks against multiple target receivers (one spoofer per targeted receiver). Each spoofer independently walks off the time and position without raising alarms.**

~~(U//FOUO)~~ SMEs generally agreed that this scenario would result in widespread degradation to the aviation mode with effects lasting for more than 30 days. If spoofing was suspected or detected, aviation would no longer use GPS, WAAS, or GBAS. The scenario could particularly affect the general aviation industry, which relies more heavily on GPS and WAAS. Degradation would be widespread, but there likely would not be a mission outage because alternative systems like VOR are currently available. However, airspace performance and efficiency would be adversely affected.

Scenario G

Continuous multiple spoofer

Time	E	> 30 days	1	5	6	6	8
	D	< 30 days	1	4	5	6	8
	C	< 7 days	1	3	4	4	7
	B	< 1 day	1	2	3	3	5
	A	< 1 hr	1	2	2	2	3
			No degradation	Isolated degradation	Widespread degradation	Isolated Outage	Widespread Outage
			1	2	3	4	5
			Severity				

~~(U)~~ ***NRE GPS Transportation Systems Sector (Maritime, Mass Transit, Highway, Freight Rail, and Pipeline) Consequence Workshop Findings Report***

~~(U)~~ **Summary of Key Workshop Findings**

~~(U//FOUO)~~ HITRAC held a workshop on March 28, 2011, to discuss how the Transportation Systems Sector uses GPS PNT and to elicit SME judgment regarding potential subsector consequences that could arise if the GPS signal were disrupted in various scenarios. (See Annex I for a list of SME participants.)

~~(U//FOUO)~~ SMEs judged the following GPS disruption scenarios to have the highest impact on the maritime, mass transit, highway, freight rail, and pipeline modes of the Transportation Systems Sector:

- ~~(U//FOUO)~~ Scenario G: Continuous multiple spoofer.
- ~~(U//FOUO)~~ Scenario H: Brief high-power jamming followed by continuous high-power spoofing.
- ~~(U//FOUO)~~ Scenario D: Multiple, low-power, continuous and intermittent, stationary and mobile jammers.
- ~~(U//FOUO)~~ Scenario E: Severe geomagnetic storm.

~~(U//FOUO)~~ SMEs judged the following GPS disruption scenarios to have lower impacts on the maritime, mass transit, highway, freight rail, and pipeline modes of the Transportation Systems Sector:

- ~~(U//FOUO)~~ Scenario A: Continuous, stationary, unintentional interference.
- ~~(U//FOUO)~~ Scenario B: Single, low-power, continuous, stationary jammer.
- ~~(U//FOUO)~~ Scenario C: Single, high-power, continuous, stationary jammer.
- ~~(U//FOUO)~~ Scenario F: Continuous single spoofer.

~~(U//FOUO)~~ In addition, SMEs made the following observations regarding the maritime, mass transit, highway, freight rail, and pipeline modes' use of GPS PNT:

- ~~(U//FOUO)~~ The SMEs considered the current mitigation measures in effect or planned for the next three to five years in the Transportation Systems Sector and recognized that baseline operations for the respective subsectors are not perfect and routinely involve an element of mission degradation. SMEs noted that there are new and emerging GPS-dependent technologies that could be implemented in the Sector in the next five years, such as connected vehicle technology for cooperative, active safety.
- ~~(U//FOUO)~~ SMEs noted that it is highly unlikely that there could be a long-term, widespread degradation or outage of service for all transportation modes in a single incident.

- ~~(U//FOUO)~~ The impact of a disruption of GPS on the Transportation Systems Sector could last longer than the technical disruption given potential loss of confidence in the GPS signal by users.
- ~~(U//FOUO)~~ There is significant economic appeal for industry to develop technologies that rely on GPS because the signal is free and receivers are small, low power, and low cost.
- ~~(U//FOUO)~~ While transportation modes could resort to manual methods of navigation, this would come at a loss of efficiency within the transportation system.
- ~~(U//FOUO)~~ Research and development of alternative, non-satellite-based navigation and vehicle tracking systems for transportation applications is needed to supplement and serve as a backup to satellite-based systems.
- ~~(U//FOUO)~~ There is a need to educate GPS users on the risks associated with dependencies on GPS-enabled technologies before a disruption occurs.

~~(U)~~ Scenario Consequence Summaries

~~(U//FOUO)~~ *Scenario A: An interference source is causing unintentional disruption. Ground receivers within a 30-km GTG radius are affected, and airborne receivers within radio LOS are affected.*

~~(U//FOUO)~~ Most SMEs judged the effects of this scenario would be isolated degradation of services of the Transportation Systems Sector lasting for less than seven days. SMEs noted that the duration of the outage would depend on the length of time it took to detect, locate, and disable the interference source. They referenced the San Diego incident, which was resolved in a matter of hours, as well as other instances that took much longer. Given that the interference source is stationary and continuous, it should be relatively easy to locate within seven days. SMEs emphasized that this scenario would only have an isolated impact because the Transportation Systems Sector is diverse, with multiple conveyance options. However, one SME noted that all modes are not alike—while rail could pick up some elements of highway transit or vice versa, the services provided by the maritime shipping industry in moving large quantities of goods into ports could not be readily replicated by other modes. Mariners would have to revert to manual methods of navigation, degrading the efficiency of services provided. For surface transport, remote traffic control systems and right-of-way controls at rail-highway interfaces could be disrupted.

Scenario A

Continuous, stationary, unintentional interference (Gnd: 30km radius, Air: radio LOS)

Time	E	> 30 days	1	4	6	5	10
	D	< 30 days	1	4	5	6	8
	C	< 7 days	1	3	4	4	7
	B	< 1 day	1	2	3	3	4
	A	< 1 hr	1	1	2	2	3
			No degradation	Isolated degradation	Widespread degradation	Isolated Outage	Widespread Outage
			1	2	3	4	5
			Severity				

~~(U//FOUO)~~ **Scenario E: Continent-scale natural disruption caused by a severe geomagnetic storm. Tracking threshold of GPS is reduced significantly.**

~~(U//FOUO)~~ SMEs generally agreed that the effects of this scenario would be widespread degradation of services across the Transportation Systems Sector. For example, one SME indicated that the scenario would result in intermittent disruptions of GPS reception, causing degradations in transportation efficiency. Mariners might have to resort to manual methods of navigation until the GPS signal is again reliable. In addition, portside maritime operations (e.g., terminal facilities, intermodal connections) would be impacted. There could be some disruptions to surface transportation until backup systems and procedures are established. SMEs were divided on the estimated duration of this degradation—ranging from less than one day to less than 30 days. SMEs noted that there could be cascading effects on the Sector lasting longer than the duration of the storm itself.





Scenario E		Severe geomagnetic storm (Continent-sized area)					
Time	E	> 30 days	1	4	6	5	10
	D	< 30 days	1	4	5	6	8
	C	< 7 days	1	3	4	4	7
	B	< 1 day	1	2	3	3	4
	A	< 1 hr	1	1	2	2	3
			No degradation	Isolated degradation	Widespread degradation	Isolated Outage	Widespread Outage
			1	2	3	4	5
			Severity				

~~(U//FOUO)~~ **Scenario C: Jamming disruption from a single multiple-watt stationary jammer.** GPS receiver tracking is affected within a three-km GTG radius and a 230-km LOS radius. GPS receiver acquisition is affected within a four-km GTG radius and a 350-km LOS radius.

~~(U//FOUO)~~ SMEs generally agreed that the effects of this scenario would last for less than seven days. Most SMEs judged the effects of the scenario to be isolated degradation, although other SMEs judged the effects to be isolated outage. SMEs noted that the scenario would result in degradation and not outage, because the Sector comprises so many modes of transportation and not every mode is dependent on GPS. There would be outages in transportation components but there would not be outages across the entire Sector. Maritime operations would shift to manual methods while GPS is unavailable. Surface transportation would still function, although disruptions and component outages may occur in SCADA control nodes that depend on GPS reception to function, such as pipeline and port dockside operations. As in Scenario A, the challenge would be detecting, locating, and disabling the jammer in a timely manner, but a single, stationary jammer likely could be disabled within seven days. SMEs noted that adding power does not make the jamming worse but expands the reach of the jamming.

Scenario C

Single, high-power, continuous, stationary jammer (Gnd: 3-4km radius, Air: 230-350km radio LOS)






Time	E	> 30 days	1	4	6	5	10
	D	< 30 days	1	4	5	6	8
	C	< 7 days	1		4		7
	B	< 1 day	1		3		4
	A	< 1 hr	1	1	2	2	3
			No degradation	Isolated degradation	Widespread degradation	Isolated Outage	Widespread Outage
			1	2	3	4	5
			Severity				

~~(U//FOUO)~~ **Scenario D: Jamming disruption from multiple low-power jammers on the ground. The jammers are stationary and mobile, with some intermittently active. Pockets of intermittent tracking and acquisition disruption occur across the metropolitan area.**

~~(U//FOUO)~~ SMEs judged that the effects of this scenario could last for more or less than 30 days but were divided on the severity of the outage. Most SMEs judged that the effects would be isolated degradation, while others judged isolated outage or widespread degradation. Affected maritime operations would shift to manual methods of navigation, reducing efficiency. One SME noted the effects could be widespread if a critical transportation node, such as the Chicago rail hub, was targeted and effects cascaded across the rail system. Other SMEs noted that this scenario would affect trucking more than rail because there is less dependency on GPS in rail. Another SME raised the point that intermodal connection points—such as where maritime and rail meet—could be adversely affected. SMEs noted the duration of the scenario's effects would be lengthy as it would be challenging to detect, locate, and disable multiple mobile jammers and cited examples of lengthy or ongoing GPS jamming incidents. One SME mentioned that there also could be psychological impacts from the scenario—GPS users might lose confidence in the reliability of GPS, and it is uncertain when they would regain it.

Scenario D

Multiple, low-power, continuous and intermittent, stationary and mobile jammers (Across metropolitan area)

Time	E	> 30 days	1	 4	 6	5	10
	D	< 30 days	1	 4	 5	 6	8
	C	< 7 days	1	3	4	4	7
	B	< 1 day	1	2	3	3	4
	A	< 1 hr	1	1	2	2	3
			No degradation	Isolated degradation	Widespread degradation	Isolated Outage	Widespread Outage
			1	2	3	4	5
			Severity				

~~(U//FOUO)~~ **Scenario H:** *Sophisticated, coordinated “navigation confusion” attack whereby a strategically placed multiple-watt transmitter generates GPS-like signals after an initial interval (several minutes) of jamming. Receivers within a three-km GTG radius and a 230-km LOS radius report a confident timing and position fix, but the timing is wrong by up to hundreds of microseconds and the position fix is wrong by up to tens of kilometers.*

~~(U//FOUO)~~ Most SMEs agreed that the effects of this scenario would be isolated outage and that the effects would last either less than 30 days or less than seven days. SMEs indicated that short jamming intervals followed by spoofing would be difficult to detect and disable. SMEs noted that the scenario has the potential to result in the outage of one subsector (such as maritime) but not the entire Transportation Systems Sector. SMEs noted the potential for catastrophe if a ship carrying hazardous cargo navigated off course but emphasized that a ship’s licensed pilot should be well trained in alternative methods of navigation to avert an accident. Erroneous timing could cause disruptions of SCADA nodes with loss of function until reset by human intervention. Public confidence in the reliability of the GPS signal also could be adversely affected.

Scenario H

Single, high-power jammer followed by spoofing (Gnd: 3km radius, Air: 230km radio LOS)

Time	E	> 30 days	1	4	6	5	10
	D	< 30 days	1	4	5	6	8
	C	< 7 days	1	3	4	4	7
	B	< 1 day	1	2	3	3	4
	A	< 1 hr	1	1	2	2	3
			No degradation	Isolated degradation	Widespread degradation	Isolated Outage	Widespread Outage
			1	2	3	4	5
			Severity				

~~(U//FOUO)~~ **Scenario F: Pinpoint spoofing attack against a single target receiver. The spoofer walks off time and position reported by the target receiver without raising alarms.**

~~(U//FOUO)~~ SMEs were divided about whether this scenario would result in isolated degradation or isolated outage. SMEs noted the effects could depend on the specific receiver targeted by the adversary. For example, in the maritime mode, a high-value vessel could be sent off track, potentially running aground and shutting down a port. SME judgments diverged on the duration of this scenario's effects, ranging from less than 30 days to less than one day. Some SMEs indicated the duration of the scenario could be lengthy because incremental changes in timing would have to accumulate to have noticeable effects, particularly if the receiver is moving. Other SMEs were confident transportation operators would promptly notice drifts in positional or timing accuracy.

Scenario F

Continuous single spoofer

Time							
			No degradation	Isolated degradation	Widespread degradation	Isolated Outage	Widespread Outage
			1	2	3	4	5
E	> 30 days		1	4	6	5	10
D	< 30 days		1	4	5	6	8
C	< 7 days		1	3	4	4	7
B	< 1 day		1	2	3	3	4
A	< 1 hr		1	1	2	2	3

~~(U//FOUO)~~ **Scenario G: Sophisticated, coordinated pinpoint spoofing attacks against multiple target receivers (one spoofer per targeted receiver). Each spoofer independently walks off the time and position without raising alarms.**

~~(U//FOUO)~~ SMEs disagreed as to whether the effects of this scenario would last more or less than 30 days because it would be difficult to locate and disable all spoofers. In addition, the adversary could activate the spoofers at different times over the course of an extended period of time. There could also be longer-term loss of confidence in the GPS signal by users. SMEs were divided on the severity of the consequences of the scenario—it ranged from isolated degradation to widespread outage. One SME noted that if an adversary was in possession of sophisticated spoofers, they would use them for maximum effect. Other SMEs emphasized that it would not be likely that a spoofing attack could disable the entire Transportation Systems Sector, but rather that cascading effects on the efficiency of the transportation system could extend beyond a metropolitan area. Some SMEs judged the effects could be widespread because the spoofers are located throughout the country. SMEs noted that it is challenging to convey messages about suspected GPS disruptions throughout the Transportation Systems Sector; there are mechanisms in place to inform mariners if they are using equipment that has integrity monitoring (such as DGPS) but not the trucking industry, for example.

Scenario G

Continuous multiple spoofer

Time	E	> 30 days	1	4	6	5	10
	D	< 30 days	1	4	5	6	8
	C	< 7 days	1	3	4	4	7
	B	< 1 day	1	2	3	3	4
	A	< 1 hr	1	1	2	2	3
			No degradation	Isolated degradation	Widespread degradation	Isolated Outage	Widespread Outage
			1	2	3	4	5
			Severity				

~~(U//FOUO)~~ **Scenario B: Jamming disruption from a single low-power stationary jammer.** GPS receiver tracking is affected within a 500-m GTG radius and a 20-km LOS radius. GPS receiver acquisition is affected within an 800-m GTG radius and 30-km LOS radius.

~~(U//FOUO)~~ SMEs mostly agreed that this scenario would result in isolated degradation lasting less than seven days. This jammer might be somewhat more challenging to locate than jammers in other scenarios because it is a lower power jammer. The effects would be isolated given the short range of the jammer. SMEs judged that the effectiveness of the Transportation Systems Sector would be slightly degraded but not significantly disrupted.

Scenario B

Single, low-power, continuous, stationary jammer (Gnd: 500-700m radius, Air: 20-30km radio LOS)

Time	E	> 30 days	1	4	6	5	10
	D	< 30 days	1	4	5	6	8
	C	< 7 days	1	3	4	4	7
	B	< 1 day	1	2	3	3	4
	A	< 1 hr	1	1	2	2	3
			No degradation	Isolated degradation	Widespread degradation	Isolated Outage	Widespread Outage
			1	2	3	4	5
			Severity				

~~(U)~~ Annex F. Likelihood Workshop Findings

~~(U)~~ Overview

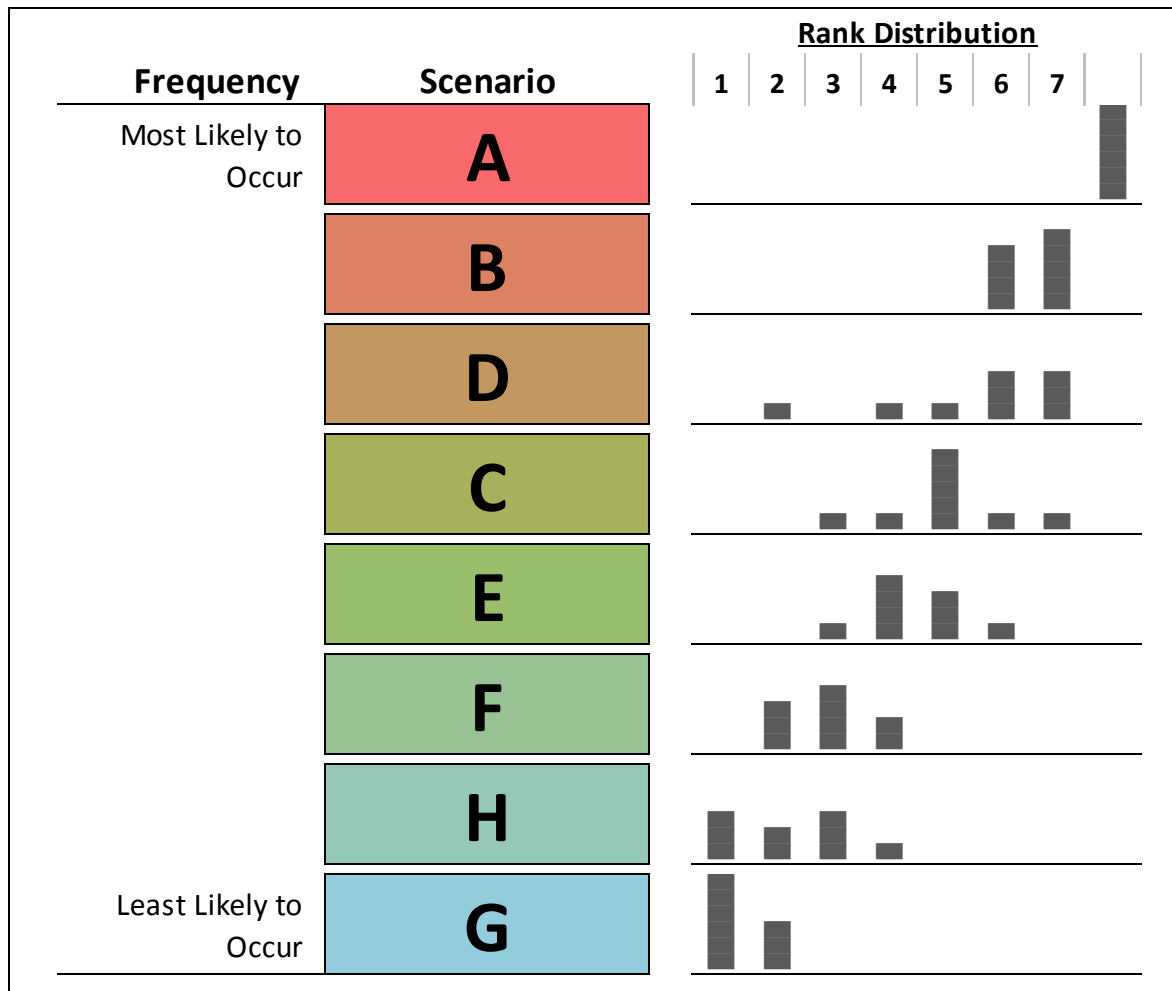
~~(U//FOUO)~~ HITRAC held a workshop on May 6, 2011, to discuss and assess the likelihood of occurrence for the eight scenarios defined for the purpose of the 2011 NRE on GPS Disruption Risks to Critical Infrastructure. SMEs first developed a rank order of scenarios based on the relative frequency of occurrence of GPS disruptions associated with each scenario. After reaching a consensus relative ranking for the scenarios, SMEs estimated the frequency of occurrence of the GPS disruptions for each scenario.

~~(U)~~ Summary of Key Workshop Findings

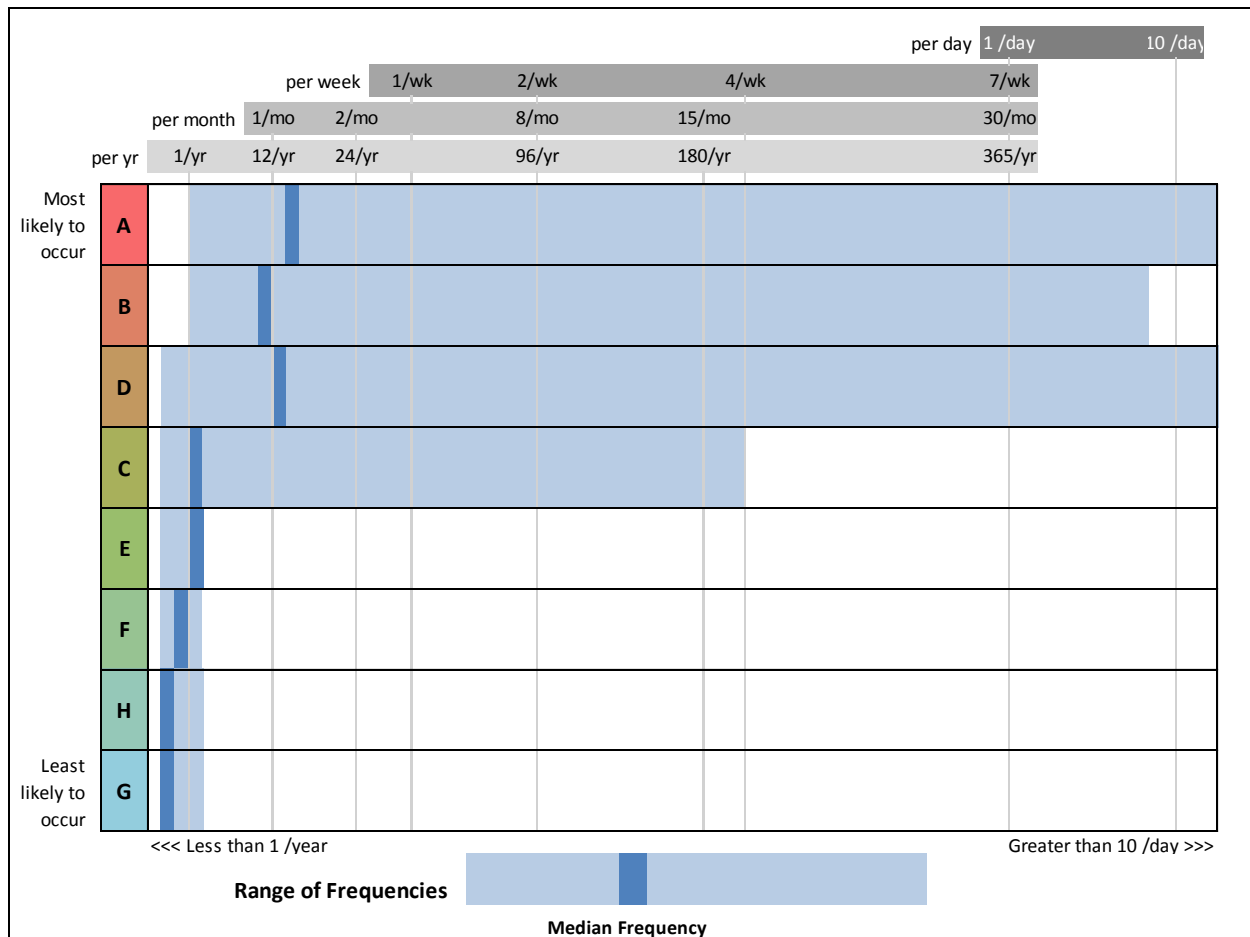
~~(U//FOUO)~~ There was an overall trend in the scenario rankings, with those scenarios that involved jamming disruptions to GPS placing higher (more frequently occurring) in the rank order than those scenarios that involved spoofing. Jamming is far easier to accomplish, and takes less skill and expertise, than spoofing, and jamming can often be an unintentional consequence of other actions or devices. In addition, there is more historical data on jamming occurrences (both intentional and unintentional) than for the other GPS disruption scenarios. SMEs noted that the absence of accurate data about incidents of GPS disruption made it challenging to estimate the likelihood of these scenarios. In many instances, users of GPS may attribute signal disruption to equipment failure and therefore not report to authorities what could be actual instances of jamming or spoofing.

~~(U)~~ Rank Order and Frequency

~~(U//FOUO)~~ SMEs ranked the eight scenarios in relative order of their likelihood to occur, with a score of eight being the scenario most likely to occur and one being the least likely. After the eight scenarios were ranked using a consensus based on the individual rankings (see Figure F-1), SMEs estimated how often they believed each scenario would occur and provided numerical estimates for both minimum and maximum occurrences per year. A median annual frequency was calculated for each scenario (see Figure F-2). The results of rank order are below.



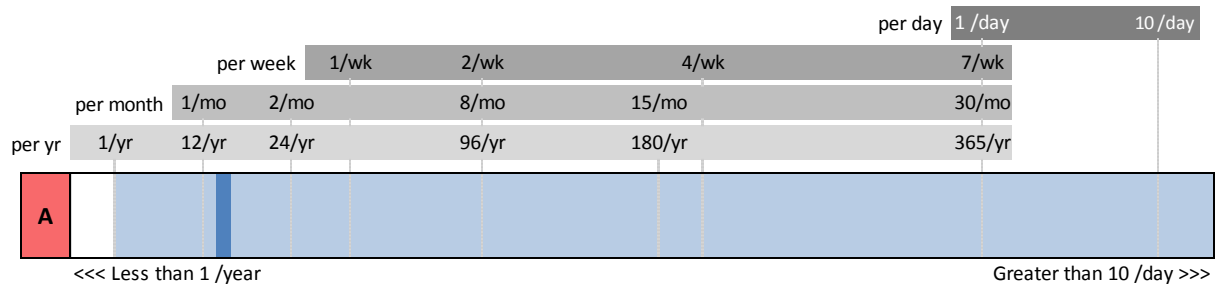
~~(U)~~ Figure F-1: Relative Likelihood of Occurrence for All Scenarios



~~(U)~~ Figure F-2: Estimated Ranges of Frequency of Occurrence for All Scenarios

~~(U//FOUO)~~ **Scenario A: An interference source is causing unintentional disruption. Ground receivers within a 30-km GTG radius are affected, and airborne receivers within radio LOS are affected.**

~~(U//FOUO)~~ All SMEs rated this scenario an eight and agreed that it is the most likely to occur. Two reasons were cited most often for this high ranking. First, there are many types of devices not intended for jamming that can, under the correct circumstances, become “accidental jammers.” These include active TV antennas with preamplifiers that can radiate harmonics and are in-band to GPS, and old or malfunctioning microwave systems. The second cause for the high frequency of this scenario is accidental jamming from authorized or licensed users of jamming technology. For instance, there are facilities—such as doctors’ offices, hospitals, schools, courthouses, and prisons—that employ types of radio-frequency disruption devices that, while not specifically aimed at GPS frequencies, can radiate harmonics that disrupt GPS signals.

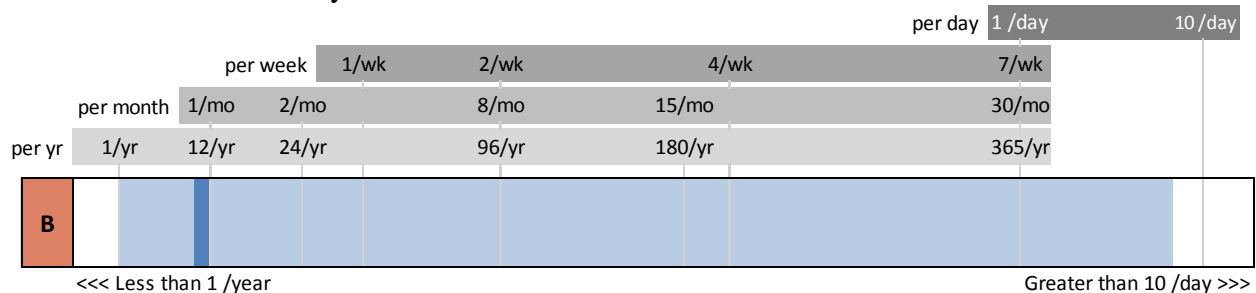


(U//FOUO) SMEs came up with a wide range of frequency estimates for this scenario. The minimum and maximum frequency estimates across all SMEs were one and 5,475 occurrences per year, respectively, although with the outlier of 5,475 occurrences removed, the maximum was 208. However, the median score was 15 times per year. Several SMEs noted (including the one with the outlier score of 5,475) that this type of scenario likely happens multiple times per day but is only rarely reported.

(U//FOUO) Some SMEs cautioned that this scenario's high frequency ranking is not an indication of high risk or impact to critical infrastructure. While situations such as this may occur frequently, they are generally minor and localized.

(U//FOUO) **Scenario B: Jamming disruption from a single low-power stationary jammer. GPS receiver tracking is affected within a 500-meter GTG radius and a 20-kilometer LOS radius. GPS receiver acquisition is affected within an 800-meter GTG radius and 30-kilometer LOS radius.**

(U//FOUO) The consensus ranking for this scenario was seven, with slightly more than half the SMEs scoring it a seven, and the rest a six. As with some instances within Scenario A, many SMEs ranked this scenario high because of historical cases of intentional, authorized jammers having unintended consequences. SMEs also believed this scenario would have a high rank because the kind of low-power jammer in this scenario is a relatively easy, low-cost jammer for individuals to build or buy.

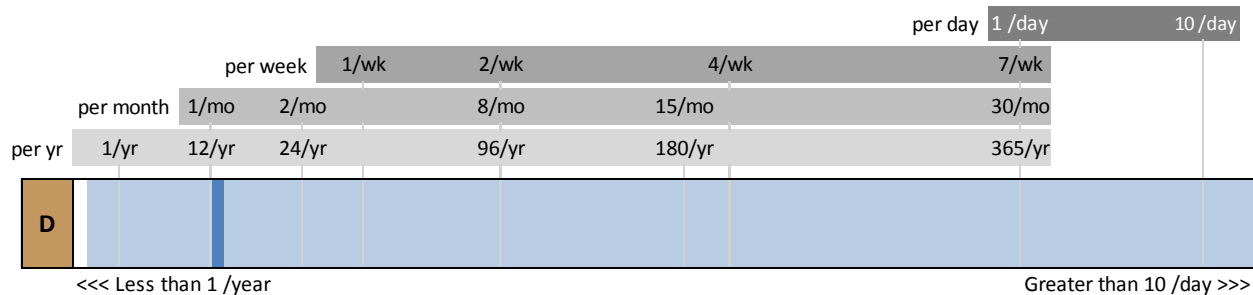


(U//FOUO) Annual frequency estimates for this scenario ranged from one to 3,285, with a median frequency of 12 occurrences per year. With the outlier removed, the maximum estimate was 50 occurrences. Reasons for these estimates included the ready availability of low-cost jammers and their appeal to criminals or those looking to do mischief, as well as their utility in probing detection and response capabilities in various environments. However, as with Scenario A, frequency does not especially imply the degree of impact.

~~(U//FOUO)~~ **Scenario D: Jamming disruption from multiple low-power jammers on the ground. The jammers are stationary and mobile, with some intermittently active. Pockets of intermittent tracking and acquisition disruption occur across the metropolitan area.**

~~(U//FOUO)~~ Although the consensus ranking for this scenario was six, a majority of SMEs were evenly split between six and seven, and the remaining SMEs gave rankings of two, four, and five. The relatively high consensus ranking is based on the increase in commercially available jammers, the ease of acquiring them (such as through the Internet), and their falling cost.

~~(U//FOUO)~~ The SME from the FAA estimated for Scenario D the highest frequency of occurrence on the scale – 10 per day in CONUS, indicating that the proliferation of mobile jammers makes this the scenario that will occur most frequently. Because the median frequency of occurrence was selected for each scenario, this scenario's ranking was much lower than the FAA's estimate.



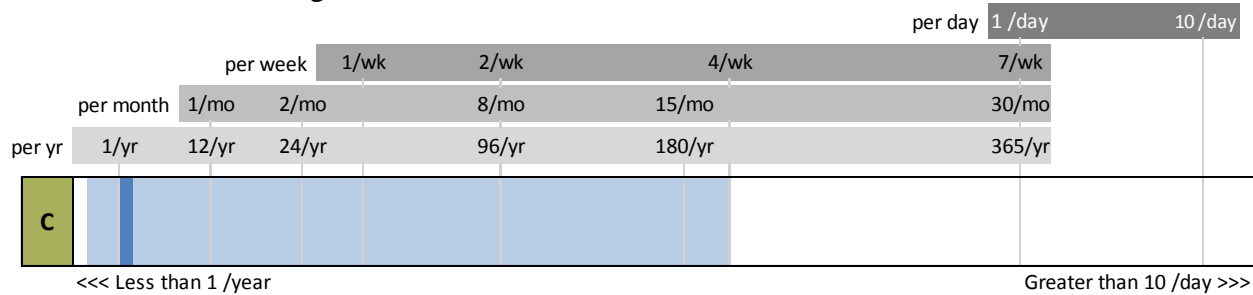
~~(U//FOUO)~~ SMEs estimated a wide range of frequencies for this scenario. The overall minimum and maximum frequencies for the entire group were zero and 4,380, respectively. There was a median likelihood of 13.5 occurrences per year. The wide disparity in estimates was based on individual SMEs' interpretations of the scenario; those SMEs who viewed this scenario as the result of the proliferation of inexpensive mobile jammers, also known as personal protection devices, tended to the high end of the estimated range of frequencies. Those SMEs who interpreted the scenario as a coordinated, malicious event scored it much lower, for reasons including the assumption that an event like this has never occurred and that there are more effective, less complicated means of attack.

~~(U//FOUO)~~ The SME from the FAA noted that in the near term, possibly within the next 12 to 24 months, this sort of scenario could become the most frequently occurring because of the increasing numbers of mobile jammers and our current lack of mitigation options.

~~(U//FOUO)~~ **Scenario C: Jamming disruption from a single multiple-watt stationary jammer. GPS receiver tracking is affected within a three-km GTG radius and a 230-km LOS radius. GPS receiver acquisition is affected within a four-m GTG radius and a 350-km LOS radius.**

~~(U//FOUO)~~ This scenario received a consensus ranking of five, which was selected by a majority of the SMEs. No other rank received more than a single SME vote. The likelihood ranking for Scenario C was in the middle, reflecting the idea that the threat from this type of jammer—which

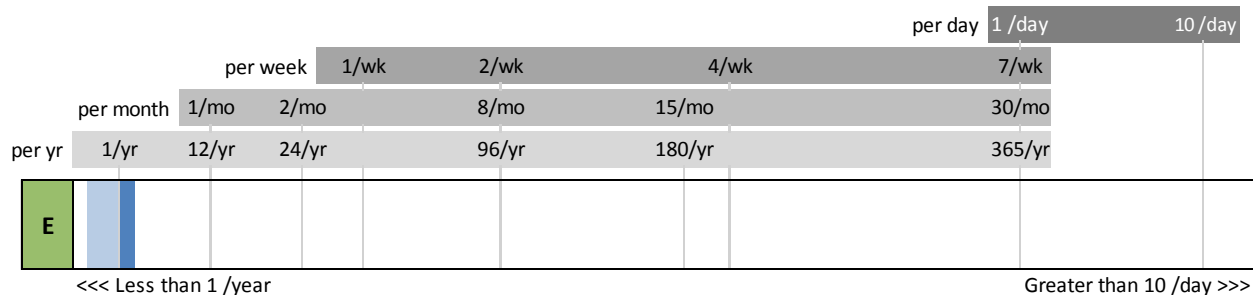
is easily constructed and concealed—would be relatively easy to locate, lessening the probability of the scenario occurring.



(U//FOUO) The estimated frequency of occurrence for this scenario ranged from 0.1 to 208 episodes per year, with a median score of two occurrences per year. With the outlier of 208 removed, the maximum frequency estimate was six annual occurrences.

~~(U//FOUO)~~ **Scenario E: Continent-scale natural disruption caused by a severe geomagnetic storm. Tracking threshold of GPS is reduced significantly.**

(U//FOUO) The consensus ranking for this scenario was four, putting it in the bottom half of the likelihood rankings. SMEs generally agreed that the effects from a scenario like this are unpredictable⁹⁷, typically short lived, and would target areas locally before passing. In addition, most degradation could occur in frequencies below those of GPS.



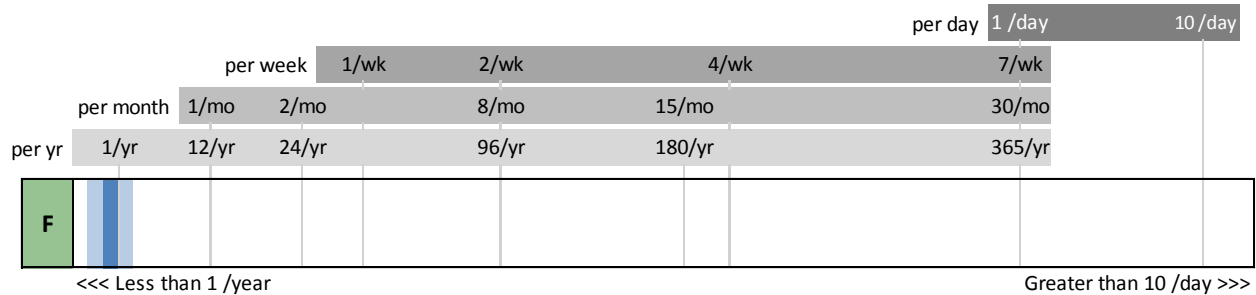
~~(U//FOUO)~~ All SMEs concurred that the approximate frequency for a G4 event (severe geomagnetic storm) is 3.5 per year. The approximate frequency for a G5 event (extreme geomagnetic storm) is 0.33 per year.

~~(U//FOUO)~~ **Scenario F: Pinpoint spoofing attack against a single target receiver. The spoofer walks off time and position reported by the target receiver without raising alarms.**

~~(U//FOUO)~~ SMEs reached a consensus score of three for this scenario. Slightly more than half the SMEs ranked the scenario three, and the others SMEs split between rankings of two and four.

⁹⁷(U) The American Meteorological Society Policy Workshop (March 2011) on *Satellite Navigation and Space Weather: Understanding the Vulnerabilities and Building Resilience* indicates that one reason the effects of severe space weather are unpredictable is because of differences in GPS receiver standards between various user groups.

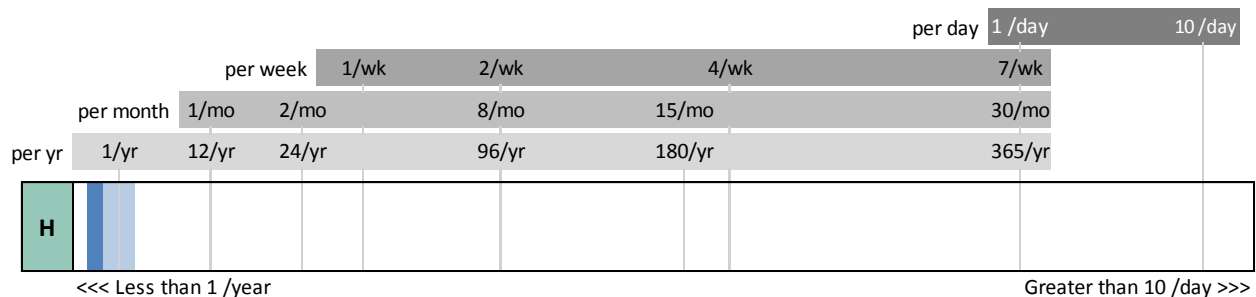
Although it was ranked near the bottom in terms of likelihood of occurrence, Scenario F was assigned the highest likelihood of the spoofing-related scenarios because it was the most simplistic. The spoofing scenarios, in general, received low likelihood rankings for various reasons, most notably because spoofing is a sophisticated type of attack that requires a level of skill not needed for jamming. Although schematics and instructions for constructing spoofers are available online, engineering or other technical ability would generally be needed to successfully construct and operate devices.



~~(U//FOUO)~~ Because of the level of skill needed to successfully implement a spoofing attack, the estimated frequency of occurrence was low and ranged from zero to three times per year, with a median frequency of 0.8 occurrences annually.

~~(U//FOUO)~~ **Scenario H: Sophisticated, coordinated “navigation confusion” attack whereby a strategically placed multiple-watt transmitter generates GPS-like signals after an initial interval (several minutes) of jamming. Receivers within a three-km GTG radius and a 230-km LOS radius report a confident timing and position fix, but the timing is wrong by up to hundreds of microseconds and the position fix is wrong by up to tens of kilometers.**

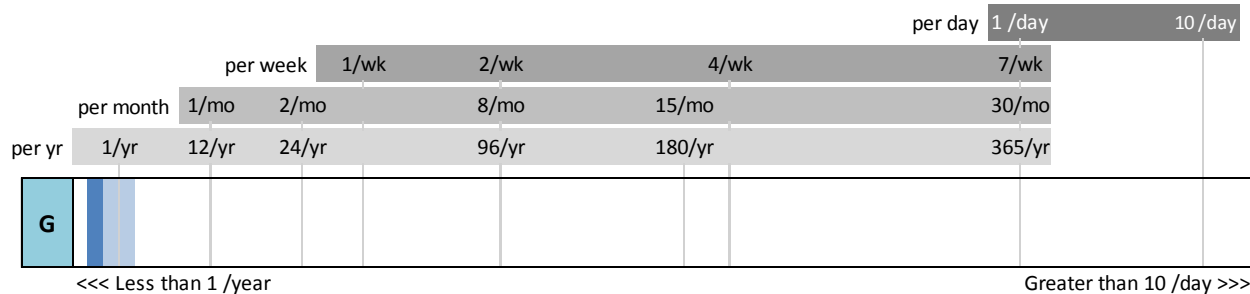
~~(U//FOUO)~~ The consensus ranking for this scenario was tow, although individual SME scores ranged from one to four. As with Scenario F, SMEs concurred that this scenario was one of the least likely to occur, relative to the other scenarios, because it involves a very sophisticated attack requiring advanced technical skills.



~~(U//FOUO)~~ Annual frequency estimates were small, ranging from zero to two occurrences annually, and a median of 0.3 occurrences. One SME pointed out that although numbers for this type of scenario are low now, they are likely to increase over time as individuals acquire the necessary technical skills.

~~(U//FOUO)~~ *Scenario G: Sophisticated, coordinated pinpoint spoofing attacks against multiple target receivers (one spoofer per targeted receiver). Each spoofer independently walks off the time and position without raising alarms.*

~~(U//FOUO)~~ This scenario received a consensus ranking of one, least likely to occur of all eight scenarios. A majority SMEs selected one, and the rest ranked it as two. As with other spoofing scenarios, SMEs agreed it was least likely to occur because of the difficulty in constructing and implementing a spoofing device, as well as the high level of complex coordination needed for the multiple spoofing devices used in this scenario.



~~(U//FOUO)~~ The frequency range estimates for this scenario were identical to Scenario G: zero to two occurrences annually, and a median of 0.3 occurrences. Several SMEs explained that the United States has not seen an attack like this, to date, and so gave zero as both their minimum and maximum annual frequency of occurrence. However, many SMEs suggested that a scenario like this will become increasingly likely in the long term.

~~(U//FOUO)~~ Just as a high frequency ranking does not always correlate to high risk, the opposite is true as well. With this scenario, as with other low-ranked scenarios, some SMEs cautioned that although we may not have seen an attack of this nature before, if one were to occur and succeed, the impact could be severe. Therefore, the low ranking should not be misleading. In addition, this scenario might not be detectable for long periods of time. Often, one-off attacks (September 11, 2001, for instance) cause the most damage.

~~(U)~~ **Limitations**

~~(U//FOUO)~~ The findings from the Likelihood Threat Workshop had one major limitation, which was found in the frequency of occurrence ranges. SMEs agreed that their estimated frequency ranges were speculation or expert opinions based on their knowledge, judgment, and experience, and hard data was often quite limited. There were various reasons for this. There is no deployed suite of sensors that can detect and characterize interference with the GPS signal. Moreover, there is currently no one single repository for reports of GPS jamming or spoofing incidents, and companies and agencies often do not share information about occurrences. The repository problem may be somewhat or fully mitigated when DHS's searchable PNT Incident Portal goes into use.

~~(U//FOUO)~~ SMEs' estimated frequency ranges were also limited because jamming or spoofing incidents are either not reported or are classified. And when incidents are reported, they are not

always publicized. Among incidents that are not reported, it is often because of a lack of awareness that jamming or spoofing is occurring. When there is a problem with GPS, the technology itself is frequently blamed.

~~(U//FOUO)~~ The likelihood of GPS disruption scenarios was identified independent of a specific sector that might be impacted, despite the knowledge that disruptions are dependent upon user equipment characteristics which vary across sectors. This was due to the absence of information on the frequency of a *successful* attack against an individual sector. Furthermore, some threats are not targeted at any one sector, but could result in collateral damage to all sectors.

~~(U)~~ For a list of SME who participated in this workshop, see Annex I.

~~(U)~~ Annex G. Sector Alternative Futures Workshop Findings

~~(U)~~ NRE GPS Communications Sector Alternative Futures Workshop Findings Report - June 20, 2011

~~(U)~~ Introduction

~~(U//FOUO)~~ Alternative future generation serves as a primary analytic approach informing the NRE. A workshop was held on June 20, 2011, to elicit SME judgment to develop and refine alternative futures that could present challenges and opportunities for the Communications Sector's use of GPS PNT (see Annex I for a list of SME participants). Sector Growth/Dependency on GPS and GPS/PNT served as the two uncertainties facing the Sector that defined the four alternative futures (see Figure G-1).

~~(U//FOUO)~~ Workshop participants made the following assumptions concerning the Communications Sector alternative futures; each assumption is intended to be viable over the 20-year outlook of the alternative futures themselves:

- ~~(U//FOUO)~~ Communications Sector growth will be high, regardless of its level of dependence on GPS.
- ~~(U//FOUO)~~ The proliferation of PPDs, such as cigarette lighter jammers, and other jammers will continue to increase.
- ~~(U//FOUO)~~ There will be no backups for GPS that, on their own, offer all the services and functions of GPS that the Communications Sector needs.

~~(U//FOUO)~~ **Key judgments** concerning the future of the Communications Sector's use of GPS PNT raised at the workshop include:

- ~~(U//FOUO)~~ Because GPS is and will continue to be a reliable system, decision makers may be unwilling to reprioritize money and resources to address potential GPS issues and mitigation strategies for disruption scenarios that have not yet occurred.
- ~~(U//FOUO)~~ The Communications Sector will need a backup capability for GPS, especially for timing.
- ~~(U//FOUO)~~ Many communications systems will become increasingly reliant on GPS services because of their need for synchronous networks.
- ~~(U//FOUO)~~ Because GPS is accurate, available, reliable, and free, an alternative PNT system would likely have trouble gaining traction in the Communications Sector and other infrastructure sectors unless it also had those characteristics.

~~(U)~~ Alternative Futures

~~(U//FOUO)~~ **Sector Growth/Dependency on GPS and GPS PNT** served as the two uncertainties facing the Sector that defined the four alternative futures (see Figure G-1).

~~(U//FOUO)~~ **Sector Growth/Dependency on GPS** includes:

- ~~(U//FOUO)~~ Sector growth includes:
 - ~~(U//FOUO)~~ The pace and extent of growth of communications services for which GPS is an enabler.
 - ~~(U//FOUO)~~ The pace and extent of continued expansion of services requiring high capacity, synchronized transmission of wireless data (pictures, video, mobile users).
 - ~~(U//FOUO)~~ Industry willingness to adopt communications/navigation requirements that place burdens on communications services (transmit precise time, aiding information).
 - ~~(U//FOUO)~~ Communications demands for tighter timing synchronization.
- ~~(U//FOUO)~~ Sector growth implies dependency on GPS and includes:
 - ~~(U//FOUO)~~ The degree to which the Sector depends on GPS, such as acceptance and prevalence of GPS-enabled components and systems in the Sector.
 - ~~(U//FOUO)~~ The availability of alternatives, such as nationwide systems (e.g., a land-based backup), Sector-embedded systems (e.g., chip-scale atomic clocks, anti-jam antennas, and inertial navigation systems), and alternative signals of opportunity or better autonomous communications network timing sources.
 - ~~(U//FOUO)~~ The ability to function with interference/loss.
 - ~~(U//FOUO)~~ The ability of the Sector to recognize interference/loss of GPS and thereby enable rapid localization of interference sources.

~~(U//FOUO)~~ **GPS PNT** includes:

- ~~(U//FOUO)~~ The likelihood of a successful attack on GPS signal availability.
- ~~(U//FOUO)~~ The likelihood of a successful disruption of GPS signal availability and its impact on the Communications Sector (e.g., GPS attack, significant geomagnetic storm).
- ~~(U//FOUO)~~ PNT robustness realized through continued U.S. GPS program improvements, such as signal diversity and civil signal integrity monitoring, availability of accurate geospatial information, and enhancement of the National PNT architecture, including the provision of user notifications for any degradation.
- ~~(U//FOUO)~~ Interference threat mitigation capability, such as the ability to enforce technology controls and detect, respond to, and negate interference; practical defenses against spoofing and jamming; and the ability of government to sustain the RNSS radio frequency environment used by GPS; and the ability of GPS manufacturers to design receivers that are less susceptible to spectrum interference.

		GPS PNT	
		Robust GPS system/resource	Vulnerable GPS system/resource
Sector Growth / Dependency on GPS	High growth, increasing GPS dependence	Low Maintenance Sports Car	High Maintenance Hot Rod
	High growth, decreasing GPS dependence	Reliable Minivan	Multi-fuel Jalopy

(U) Figure G-1: Communications Sector Alternative Future Matrix

~~(U//FOUO)~~ **Alternative Future 1: Low Maintenance Sports Car**

~~(U//FOUO)~~ The Low Maintenance Sports Car future is characterized by high growth, along with increasing GPS dependence. Because of the high level of GPS dependence in this future, the Communications Sector planned ahead, acknowledged its dependence, and did everything possible to ensure robust GPS resources were available, including paying attention to the policy elements of interference and mitigation problems and deploying mitigation techniques. The Sector's GPS dependence is also protected by improved border interdictions of interference devices (e.g., PPDs like cigarette lighter jammers) from overseas, as well as enhanced monitoring, reporting, and mitigating of any interference that does occur. Because GPS is fairly ubiquitous in this future, it is exploited to its fullest by the Sector, resulting in higher and faster throughput and efficiency; increased location-based services, especially in the automotive industry; safer, faster, more reliable, cost-efficient, and potentially new communications services; and tighter standards for receivers. The Communications Sector is also proactive in innovating new ways to disable jamming and spoofing on its own. This future may also be marked by the development of a separate secure GPS signal for critical infrastructure or an upgrade to current signals that makes them less susceptible to GPS spoofing.

~~(U//FOUO)~~ **Alternative Future 2: Reliable Minivan**

~~(U//FOUO)~~ The Reliable Minivan future will be marked by high growth in the sector, but with low dependence on GPS, along with a robust GPS system. In this future, time, attention, and money have been spent to ensure GPS robustness; however, because complete robustness cannot be ensured, there have been some moves toward other PNT services, possibly to a worldwide non-GPS standard. PRS, Galileo's service for military and police, is successful and may become the industry standard, allowing the Sector freedom from GPS dependence. Alternatively, the costs associated with IEEE 1588⁹⁸ may be reduced significantly, driving the market to that

⁹⁸ (U) IEEE 1588: A protocol enabling precise synchronization of clocks in measurement and control systems implemented with technologies such as network communication, local computing, and distributed objects. The protocol is applicable to systems communicating by local area networks supporting multicast messaging including but not limited to Ethernet. The protocol enables heterogeneous systems that include clocks of various inherent precision, resolution, and stability to synchronize. The protocol supports system-wide synchronization accuracy in the sub-microsecond range with minimal network and local clock computing resources.

option. The widespread use of IEEE 1588 in this future will lead to the loss of the ability to locate in some applications and the loss of some bandwidth and throughput because asynchronous networks will result in less accurate timing than synchronous ones. With the loss of GPS location services, positioning is disabled or extremely hampered, and E911 services are affected. There may also be some interoperability issues in this future as some communications products or subsectors continue to rely on GPS while others do not.

~~(U//FOUO)~~ **Alternative Future 3: High Maintenance Hot Rod**

~~(U//FOUO)~~ The High Maintenance Hot Rod future encompasses high growth and an increasing dependence on GPS but a vulnerable GPS system and resources. In this future, the Sector decision makers did not proactively implement policy, take technology changes into account, or pay attention to data indicating interference would continue, and also paid insufficient attention to a mitigation strategy. Instead, they were forced into a reactive posture in response to the proliferation of PPDs, issues with unintentional interference, spectrum conflicts and pressure, and possibly a coordinated attack on a metropolitan area, or some other significant, compelling event. Because this future leaves the Communications Sector open to a full range of periodic GPS outages, it has learned to live with nuisance-level impacts but is still open to a dire scenario. Networks serving large numbers of customers are affected more quickly than base/macro stations, and persistent flywheeling⁹⁹ quickly causes problems for major service providers.

~~(U//FOUO)~~ **Alternative Future 4: Multi-Fuel Jalopy**

~~(U//FOUO)~~ The Multi-Fuel Jalopy future is characterized by high growth but with a decreasing dependence on GPS and a vulnerable GPS system and resources. In this future, it was clear that there was a need for an alternative to GPS, and the Communications Sector responded by installing a nationwide backup system, which likely includes fiber and IEEE 1588. The potential for synchronous Ethernet as a backup also exists. Other alternatives in this future include the Sector moving to the Galileo PRS system as the industry standard and depending on GPS only as the backup system. Although the Sector was proactive in this future, the various backups and alternatives to GPS lead to lower performance and higher costs.

~~(U)~~ **Challenges and Opportunities**

~~(U//FOUO)~~ Two alternative futures (Reliable Minivan and High Maintenance Hot Rod) were selected for in-depth examination and discussion. For these two alternative futures, workshop participants were asked to identify the opportunities as well as the challenges and threats that exist in each alternative future for the United States.

⁹⁹ (U) Flywheeling (also called the *flywheel effect*): In this context, flywheeling means relying on the native stability of the oscillator within a GPS-Disciplined Oscillator (GPSDO) device. In other words, when GPS signals are not available, the GPSDO is no longer disciplined to GPS but runs open-loop, with accuracy depending only on the stability of the device's native frequency reference.

~~(U)~~ **Table G-1. Communications Sector Challenges and Opportunities**
 The contents of this table are ~~U//FOUO~~

Alternative Future	Challenges	Opportunities
Reliable Minivan	<ul style="list-style-type: none"> ▪ Finding a cost effective alternative for E911 and other GPS dependent systems. ▪ Finding a way to decrease cost of IEEE 1588-compliant capability. ▪ Finding alternative navigation methodologies. ▪ Maintaining a high throughput without synchronization. ▪ Ensuring necessary infrastructure to implement alternative PNT systems. 	<ul style="list-style-type: none"> ▪ Partnering with other GNSS systems for civil services. ▪ Seeing different ways to look at systems and drive technology in a different direction. ▪ Using multiple available GPS frequencies.
High Maintenance Hot Rod	<ul style="list-style-type: none"> ▪ Maintaining communications under conditions of a severe geomagnetic storm or terrorist attack scenario that lasts more than two days and could result in nationwide/metropolitan area outage. ▪ Explaining to the public how this situation was reached and that the system was left unprotected. ▪ Overcoming a single-point-of-failure scenario when the GPS system is stressed. ▪ Overcoming simultaneous electric power and communications loss as we move toward the smart grid. ▪ Trying to achieve cost effective, multi-frequency GPS receivers. 	<ul style="list-style-type: none"> ▪ Implementing U.S. policy to detect and disable an interference. ▪ Increasing effectiveness of clocks, which will, in turn, increase the flywheel time/effectiveness. ▪ Developing improved disciplining and learning algorithms for backup oscillators. ▪ Developing special, protected signals for critical infrastructure.

~~(U)~~ **Potential Milestones and Variables**

~~(U//FOUO)~~ Workshop participants identified the following **milestones and variables**, which can be monitored by government and industry and could serve as indicators of the potential direction

of identified uncertainties over the next 20 years. These were divided into two categories: indicators of movement toward these futures indicators of movement away from these futures.

~~(U//FOUO)~~ *Reliable Minivan*

~~(U)~~ **Movement toward future**

- ~~(U//FOUO)~~ Rollout of a communications infrastructure that does not depend on GPS indicates the industry is moving toward a lessening dependence on GPS PNT.
- ~~(U//FOUO)~~ International treaties/agreements on GNSS that promote interchangeability indicate a lessening dependence on GPS as well as acknowledgment of the need for worldwide interoperability.
- ~~(U//FOUO)~~ IEEE 1588 is implemented as an industry standard and cost effective alternative, indicating that its ubiquity and drop in price has made it a viable alternative for timing.
- ~~(U//FOUO)~~ Multisystem receivers used in the Communications Sector, indicating the industry has moved away from total GPS dependence by integrating the use of other systems.
- ~~(U//FOUO)~~ Galileo is successful and becomes the industry standard for PNT services, indicating a lessened or eliminated dependence on GPS.
- ~~(U//FOUO)~~ Policy to promote GPS disruption monitoring, reporting, and mitigation is successful, indicating that policymakers understand the importance of maintaining a robust GPS system.

~~(U)~~ **Movement away from future**

- ~~(U//FOUO)~~ IEEE 1588 technology fails to augment or replace GPS; there is a low uptake of the system. This would indicate that attempts to lessen dependence on GPS PNT were tried but failed.
- ~~(U//FOUO)~~ GPS continues to be an integral part of evolving communications infrastructure, indicating that the Sector has remained highly dependent on GPS.
- ~~(U//FOUO)~~ The NRE does not provoke policymakers to take action, which would likely lead to a lack of robustness of the GPS system because little attention has been paid to its protection.

~~(U//FOUO)~~ *High Maintenance Hot Rod*

~~(U)~~ **Movement toward future**

- ~~(U//FOUO)~~ National policy is ignored and GPS is as vulnerable as ever.

- ~~(U//FOUO)~~ Rollout of a communications infrastructure that is based upon GPS, along with predictions of higher throughput premised on that, indicates an increasing dependence on GPS in a growing sector.
- ~~(U//FOUO)~~ Lack of government analysis of alternatives to GPS as a PNT system would be a sign of increasing unilateral dependence on GPS.
- ~~(U//FOUO)~~ Failure to recognize PNT architecture as the basis for future government investment in PNT systems.
- ~~(U//FOUO)~~ Increased introduction of jammers and spoofers would indicate that the absence of a robust GPS signal has encouraged those interested in interfering with the system.
- ~~(U//FOUO)~~ Continued increase in interference events for privacy, criminal, and unintentional reasons would indicate that the GPS has remained vulnerable.

~~(U)~~ Movement away from future

- ~~(U//FOUO)~~ Demonstrable indication from the U.S. Government that GPS is a vulnerable system (along the lines of a cyber response) would indicate that policymakers understand the weaknesses of the system and are willing to address them.

~~(U)~~ Strategic Surprises

~~(U//FOUO)~~ Workshop participants identified the following strategic surprises, which are low-probability, high-consequence events that could bring chaos to the sector and GPS. In addition, participants also identified several strategic surprises that would have a positive impact on the sector.

~~(U)~~ Negative

- ~~(U//FOUO)~~ A sophisticated terrorist attack using GPS jamming and spoofing. Attackers would black out services in an area prior to an attack, impairing first responder capabilities.
- ~~(U//FOUO)~~ Systemic problem with GPS ground stations from the new delivery of software that is not backed up.
- ~~(U//FOUO)~~ Exploitation of a natural disaster by adversaries by impairing GPS services.
- ~~(U//FOUO)~~ Hiding a spoofing/jamming attack behind a space weather event, thereby exacerbating the damages caused by the event while concealing the existence of an intentional spoofing/jamming attack.
- ~~(U//FOUO)~~ Physical attack on operational command centers.
- ~~(U//FOUO)~~ Insider threat from satellite upload.

- ~~(U//FOUO)~~ A significant solar flare damages the satellite and smart grid systems, leaving temporal and long-term effects.
- ~~(U//FOUO)~~ A high-altitude, non-nuclear EMP.
- ~~(U//FOUO)~~ Half of the GPS constellation wiped out by old age.

~~(U)~~ **Positive**

- ~~(U//FOUO)~~ Technological breakthrough makes GPS obsolete.
- ~~(U//FOUO)~~ Chip-scale atomic clock technology becomes ubiquitous.
- ~~(U//FOUO)~~ Private cellular providers roll out a fiber network that provides positioning, relative timing, and other GPS related services.

~~(U)~~ **Future Analytic Considerations**

~~(U//FOUO)~~ SMEs noted that future analytic considerations should begin with quantifying the real frequency of GPS jamming, including static versus actual loss, as well as tracking trends in criminal GPS-related activity. Because of increasing problems with PPDs, SMEs also recommended exploring the idea of import controls on these types of jamming devices. And with the rise in both tracking and jamming technologies, SMEs suggested a look at the future of personal privacy, including the factors motivating people to disrupt GPS, how prevalent it will become, and how jammers may parallel the rise of hackers. In addition, stress tests on large-scale communications infrastructure for spoofing and jamming would be useful.

~~(U//FOUO)~~ SMEs also discussed the need for a rigorous analysis of alternatives for augmentation and backup of GPS in support of critical infrastructure applications, as per national policy. This would include a look at private enterprises and eLoran-type and other PNT services.

~~(U)~~ **NRE GPS Emergency Services Sector Alternative Futures Workshop Findings Report - June 7, 2011**

~~(U)~~ **Introduction**

~~(U//FOUO)~~ Alternative future generation serves as a primary analytic approach informing the NRE. A workshop was held on June 7, 2011, to elicit SME judgment to develop and refine alternative futures that could present challenges and opportunities for the Emergency Services Sector's use of GPS PNT (see Annex I for a list of SME participants). Complexity of Growth and PNT Disruption Likelihood served as the two uncertainties facing the Sector that defined four alternative future scenarios (see Figure G-2).

~~(U//FOUO)~~ Workshop participants fleshed out each scenario, identified core challenges and opportunities presented by the two scenarios judged to be most critical to decision makers, identified potential mileposts that could indicate a scenario is occurring, and discussed strategic surprises that could significantly change the Sector and its use of GPS. Annex D provides a full description of the alternative futures methodology.

~~(U//FOUO)~~ Workshop participants made the following assumptions concerning the Emergency Services Sector alternative futures; each assumption is intended to be viable over the 20-year outlook of the alternative futures themselves:

- ~~(U//FOUO)~~ The Emergency Services Sector will continue to utilize GPS services to fulfill its mission.
- ~~(U//FOUO)~~ Intentional or unintentional disruptions of GPS will continue to occur, potentially more frequently and with greater severity, and these disruptions will adversely affect the Emergency Services Sector.

~~(U//FOUO)~~ **Key judgments** concerning the future of the Emergency Services Sector's use of GPS PNT raised at the workshop include:

- ~~(U//FOUO)~~ GPS is likely to become increasingly integrated into the Sector's operations, and it is possible that users will not be aware that some applications are supported by GPS. However, the extent to which these technologies are used across the Sector will vary by jurisdiction.
- ~~(U//FOUO)~~ The Sector must be cautious not to overly rely on GPS without sufficient backups in place.
- ~~(U//FOUO)~~ Presently, manual backups to GPS exist in the Sector, but their effectiveness relies on continual training and exercise by sector personnel.
- ~~(U//FOUO)~~ The Emergency Services Sector is often reliant on the GPS-enabled services of the Communications Sector to identify the locations of emergency situations. This reliance will continue with the proliferation of position-based services offered by the

Communications Sector. In addition, emergency personnel rely on GPS timing for simulcast communication systems.

- ~~(U//FOUO)~~ There is a need to educate the user community in the Sector about the vulnerabilities of existing and emerging GPS-enabled technologies.

~~(U)~~ Alternative Futures

~~(U//FOUO)~~ **Complexity of Growth** and **GPS PNT Disruption Likelihood** served as the two uncertainties facing the sector that defined four alternative futures (see Figure G-2).

~~(U//FOUO)~~ **Complexity of growth** includes:

- ~~(U//FOUO)~~ Pace and extent of growth of emergency services for which GPS is an enabler, especially in the emergency services subsectors of law enforcement, fire and emergency services, emergency management, emergency medical services, and public works.
- ~~(U//FOUO)~~ Alternative and/or intermittent emergency services that require automated network control.
- ~~(U//FOUO)~~ Shift of communications technology to IP-based technology (which would still result in GPS dependencies).
- ~~(U//FOUO)~~ Complexity of growth implies dependency on GPS, which includes:
 - ~~(U//FOUO)~~ Degree to which the Sector depends on GPS, such as acceptance and permeation of GPS-enabled components and systems in the sector and increasing reliance on GPS for safe operation of future vehicles.
 - ~~(U//FOUO)~~ Availability of alternatives, such as nationwide systems (e.g., a land-based backup) and/or sector-embedded systems, such as chip-scale atomic clocks, anti-jam antennas, and inertial navigation systems.
 - ~~(U//FOUO)~~ Ability to function with interference/loss, including ability of the Sector to recognize interference/loss of GPS, using a built-in detector in the automatic gain control of each GPS receiver, preparedness of the Sector for GPS outages, inadequate training or loss of Sector fallback operating skills given the loss of GPS.

~~(U//FOUO)~~ **GPS PNT Disruption Likelihood** includes:

- ~~(U//FOUO)~~ The likelihood of a successful intentional attack on GPS signal availability.
- ~~(U//FOUO)~~ PNT robustness realized through continued U.S. GPS program improvements, such as signal diversity and civil signal integrity monitoring; availability of accurate geospatial information; and enhancement of the National PNT architecture, including the provision of rapid user notifications for any degradation.

- ~~(U//FOUO)~~ Interference threat mitigation capability, such as the ability to enforce technology controls and rapidly detect, respond to, and negate interference.

		GPS PNT Disruption Likelihood	
		Mild/Moderate	Severe/Catastrophic
Complexity of Growth / Dependency on GPS	Robust	As Good As It Gets	It Wasn't Pretty But We Did It
	Vulnerable	Should Have Known Better	Knife to a Gun Fight

~~(U)~~ Figure G-2: Emergency Services Sector Alternative Future Matrix

~~(U//FOUO)~~ **Alternative Future 1: As Good As It Gets**

~~(U//FOUO)~~ This future represents the best possible outcome, demonstrating the resilience of the Sector, which is not entirely dependent on GPS, in responding to a mild or moderate GPS disruption. The disruption incident serves as a learning experience that allows the Sector to identify what elements of robustness work or do not work. This future results because there were policy changes requiring robustness in the Sector, including backup systems for GPS-enabled technology. This future requires close coordination among first responder organizations and jurisdictions. This future also hinges on personnel training to support Sector missions in the absence of GPS.

~~(U//FOUO)~~ **Alternative Future 2: Should Have Known Better**

~~(U//FOUO)~~ In this future, the Sector is highly reliant on GPS to fulfill its mission and is faced with a mild or moderate GPS disruption—it is a test the Sector fails. Both GPS-enabled systems and backup manual skills failed. The Sector has become so reliant on GPS that backup manual navigation skills have not been adequately taught and maintained. Some systems that users did not know were tied to GPS also fail. The Sector does not demonstrate redundancy or the imagination to identify and implement alternative solutions. As a result, human life is at risk. Human resources are stretched thin, and budget resources drive dependence on inexpensive technology solutions that are not sufficiently robust. This future represents a teachable moment whereby the Sector can identify lessons learned and invest in mitigations to prevent more severe consequences in the future.

~~(U//FOUO)~~ **Alternative Future 3: It Wasn't Pretty But We Did It**

~~(U//FOUO)~~ In this future, the Sector is not entirely dependent on GPS to fulfill its mission when it is faced with a severe or catastrophic GPS disruption. The Sector had identified and preserved the fundamental human skills and knowledge needed to serve as a backup to GPS and was able to implement them during the GPS disruption. While the Sector is stressed and less efficient, it is able to accomplish its mission and minimize loss of life. In order to reach this future, the

Sector had planned and trained for additional system capabilities other than GPS to provide robustness through alternative PNT sources.

~~(U//FOUO)~~ **Alternative Future 4: Knife to a Gun Fight**

~~(U//FOUO)~~ In this future, the Sector is highly dependent on GPS to fulfill its mission and is faced with a severe or catastrophic GPS disruption. The Sector had put all of its eggs in the GPS basket and is totally unprepared to function in the absence of GPS. Emergency response capabilities are ineffective as there are no adequate human or technical GPS backup systems. In addition to navigation, the Sector also loses dispatch and communications systems. There is significant injury or loss of life due to interrupted emergency response services. Recovery from this situation is dependent on the disruption going away or the Sector finding an adequate workaround. There is substantial public outcry at the failure of emergency response capabilities.

~~(U)~~ **Challenges and Opportunities**

~~(U//FOUO)~~ Two alternative futures (Should Have Known Better and It Wasn't Pretty But We Did It) were selected for in-depth examination and discussion. For these two alternative futures, workshop participants were asked to identify the opportunities as well as the challenges and threats that exist in each alternative future for the United States.

~~(U)~~ **Table G-2. Emergency Services Sector Challenges and Opportunities**
The contents of this table are ~~U//FOUO~~

Alternative Future	Challenges	Opportunities
Should Have Known Better	<ul style="list-style-type: none">▪ Conducting a Sector self-assessment and accurately identifying capability gaps.▪ Avoiding a false sense of security that changes are not necessary since the Sector survived the attack.▪ Detecting and attributing the source(s) of disruption.▪ Promoting public awareness of vulnerability of GPS-enabled systems to disruption.▪ Promoting awareness at the policy level of the need for long-range planning and funding for backups to GPS.	<ul style="list-style-type: none">▪ Providing training and organizing exercises to prepare for potential outages.▪ Recognizing the need for and implementing national policy on GPS backups and mitigations to better prepare for and respond to future, potentially more severe outages.▪ Building synergism with GPS users in other sectors to mitigate vulnerability to GPS disruptions.▪ Finding a system-level approach that decreases expense at the user level.▪ Taking advantage of an emerging marketplace for the development of diverse PNT systems and capabilities.▪ Developing a better understanding of the relationships between

(U) Table G-2. Emergency Services Sector Challenges and Opportunities The contents of this table are U//FOUO		
Alternative Future	Challenges	Opportunities
		emergency responders in an emergency situation.
It Wasn't Pretty But We Did It	<ul style="list-style-type: none">▪ Securing the resources needed to develop and implement backup capabilities.▪ Ensuring a robust training and exercise regimen to maintain adequate backups.▪ Developing warning and notification systems to alert Sector users that GPS is down and backup capabilities need to be employed.▪ Finding cost-effective ways to build appropriate levels of robustness into the Sector.	<ul style="list-style-type: none">▪ Conducting civil preparedness drills for GPS dependencies.▪ Promoting the development and implementation of innovative backup systems and mitigation measures.▪ Building leadership resolve in DHS and the Department of Transportation to implement standing U.S. policy regarding PNT systems.▪ Recognizing the complexity and dependency on GPS/PNT in underlying infrastructure and promoting better awareness among informed users.

~~(U)~~ **Potential Milestones and Variables**

~~(U//FOUO)~~ Workshop participants identified the following **milestones and variables**, which can be monitored by government and industry and could serve as indicators of the potential direction of identified uncertainties over the next 20 years:

~~(U)~~ ***We Should Have Known Better***

- ~~(U//FOUO)~~ The widespread use of GPS-enabled devices by the Sector indicates the Sector is becoming increasingly dependent on GPS services. In addition, the inclusion of GPS systems as built-ins for first responder vehicles and equipment could indicate increased reliance on GPS.
- ~~(U//FOUO)~~ Lack of focus on training and exercise of manual navigation techniques would make the Sector increasingly reliant on GPS services.
- ~~(U//FOUO)~~ Limited resources and lack of resolve to prioritize GPS backups suggest the United States is on the path toward this future.

~~(U)~~ ***It Wasn't Pretty But We Did It***

- ~~(U//FOUO)~~ The dual use of military technology to improve the robustness of commercial GPS technology could foster a more resilient sector.

- ~~(U//FOUO)~~ The proactive identification and implementation of key capabilities to overcome or circumvent disruptions would enable the Sector to adapt to the disruption of GPS.
- ~~(U//FOUO)~~ The inclusion of GPS disruption in emergency response exercises would indicate the Sector is aware of the vulnerability and is taking steps to ensure adequate backup or mitigation measures are in place.
- ~~(U//FOUO)~~ The preponderance of portable jamming devices and information on jamming and spoofing techniques make it more likely that an intentional or unintentional GPS disruption incident could occur.
- ~~(U//FOUO)~~ Increased pressure to accommodate more GNSS systems in RNSS spectrum leaves less spectrum than originally envisioned for individual GNSS systems and could make them more vulnerable to disruption.

~~(U)~~ Strategic Surprises

~~(U//FOUO)~~ Workshop participants identified the following strategic surprises, which are low-probability, high-consequence events that could bring chaos to the Sector and GPS:

- ~~(U//FOUO)~~ A localized or widespread natural disaster coupled with intentional disruption of GPS services could impair the ability of the Sector to fulfill its mission.
- ~~(U//FOUO)~~ A massive solar event that takes out the electric power grid could disrupt the Sector's ability to communicate and employ GPS services.
- ~~(U//FOUO)~~ The Sector adapts a system wherein dependency on GPS services is not widely known.
- ~~(U//FOUO)~~ An intentional software virus disables GPS software.
- ~~(U//FOUO)~~ An alternative PNT system is developed by another country and widely adopted throughout the world. The United States becomes dependent on that system.
- ~~(U//FOUO)~~ The malicious, simultaneous manipulation of international PNT systems would cause havoc for the Sector.

~~(U)~~ Future Analytic Considerations

~~(U//FOUO)~~ SMEs noted that future analytic consideration could include the study of backup capabilities to GPS, such as e-Loran-like systems. To date, a suitable nationwide backup to GPS has not been identified although agencies have been charged to develop such a system. There is no nationwide study of the dependency on GPS and potential mitigation or backup measures that could be employed across sectors. In addition, U.S. policy (NSPD-39) directs the denial of hostile use of GPS but how such denial would be executed has not yet been determined. SMEs also emphasized the need for a study on the extent of the use of GPS-enabled commercial off-the-shelf devices in the Sector and any resulting vulnerabilities.

~~(U)~~ ***NRE GPS Energy Sector Alternative Futures Workshop Findings Report - May 25, 2011***

~~(U)~~ **Introduction**

~~(U//FOUO)~~ Alternative future generation serves as a primary analytic approach informing the NRE. A workshop was held on May 25, 2011, to elicit SME judgments to develop and refine alternative futures that could present challenges and opportunities for the Energy Sector's use of GPS PNT (see Annex I for a list of SME participants). Complexity Growth/Dependency on GPS and GPS Attack served as the two uncertainties facing the sector that defined the four alternative futures (see Figure G-3).

~~(U//FOUO)~~ Workshop participants made the following assumptions concerning the Energy Sector alternative futures; each assumption is intended to be viable over the 20-year outlook of the alternative futures themselves:

- ~~(U//FOUO)~~ The current components of the Energy Sector will become increasingly dependent on GPS-based PNT services. However, increasing development and use of alternative forms of energy may lessen dependence on GPS PNT in those components over the next 20 years.
- ~~(U//FOUO)~~ Over the next 20 years, the operation of energy systems will become increasingly automated.
- ~~(U//FOUO)~~ As the Energy Sector becomes more efficient over the next 20 years, it will lose institutional knowledge and the capability to fall back to less effective systems without degradation.

~~(U//FOUO)~~ **Key judgments** concerning the future of the Energy Sector's use of GPS PNT raised at the workshop include:

- ~~(U//FOUO)~~ Because GPS is and will continue to be a reliable system, decision makers may be unwilling to address potential GPS issues and mitigation strategies for scenarios that are predicated but have not yet occurred.
- ~~(U//FOUO)~~ As with other sectors, the Energy Sector will need a backup capability for GPS, which does not currently exist.
- ~~(U//FOUO)~~ At this time, the Energy Sector has experienced fewer problems from GPS outages than other sectors, potentially resulting in a false sense of security for the Sector.
- ~~(U//FOUO)~~ The Sector could potentially decrease its reliance on GPS PNT by investing in alternative timing methods, such as providing a timing signal over the Internet.

~~(U)~~ Alternative Futures

~~(U//FOUO)~~ **Complexity Growth/Dependency on GPS** and **GPS Attack** served as the two uncertainties facing the sector that defined the four alternative futures (see Figure G-3).

~~(U//FOUO)~~ **Complexity Growth/Dependency on GPS** includes:

- ~~(U//FOUO)~~ The pace and extent of the growth of energy sources for which GPS is an enabler, such as smart grid.
- ~~(U//FOUO)~~ Alternative and/or intermittent energy sources that require enhanced automated network controls.
- ~~(U//FOUO)~~ Exploration, extraction, and transportation approaches that require PNT.
- ~~(U//FOUO)~~ Dependency on GPS also includes:
 - ~~(U//FOUO)~~ The degree to which the Sector depends on GPS, such as acceptance and permeation of GPS-enabled components and systems in the sector.
 - ~~(U//FOUO)~~ Availability of alternatives, such as nationwide systems (e.g., a land-based backup) and/or sector-embedded systems, such as chip-scale atomic clocks, anti-jam antennas, inertial navigation systems, and jamming detection on GPS receivers and software tools.
 - ~~(U//FOUO)~~ The ability to function with interference/loss, including ability of the Sector to recognize the interference/loss of GPS.

~~(U//FOUO)~~ **GPS Attack** includes:

- ~~(U//FOUO)~~ The likelihood of a successful attack on GPS signals availability.
- ~~(U//FOUO)~~ PNT robustness realized through continued U.S. GPS program improvements, such as signal diversity and civil signal integrity monitoring, availability of accurate geospatial information, and enhancement of the National PNT architecture, including the provision of user notifications for any degradation.
- ~~(U//FOUO)~~ Interference threat mitigation capability, such as the ability to enforce technology controls and detect, respond to, and negate interference.

		GPS Attack	
		Limited Impact	Extensive Impact
Complexity Growth / Dependency on GPS	Integrated Dependence	Lights On, Pipes Full	I Might Survive
	Unilateral Dependence	I Will Survive	Lights Off, Pipes Clogged

~~(U)~~ Figure G-3: Energy Sector Alternative Future Matrix~~(U//FOUO)~~ Alternative Future 1: Lights On, Pipes Full

~~(U//FOUO)~~ The Lights On, Pipes Full future will be marked by lowered dependence on GPS because of multiple PNT sources and the willingness of the Energy Sector to mandate and deploy backup systems. In the event of a GPS attack, the Sector will continue to function, either with full efficiency because of independent alternatives or with limited impacts that do not affect critical functionality. Because the Sector has planned ahead, a resilient grid will assist with continuous operations during an outage. Any economic impacts are likely to be minimal and easily mitigated. The oil and natural gas subsectors will have an additional advantage in the event of an outage because of the capacity for storage. The electricity subsector does not have significant storage and it could be impacted more.

~~(U//FOUO)~~ Alternative Future 2: I Will Survive

~~(U//FOUO)~~ In the I Will Survive future, technology evolution will allow for unilateral dependence on GPS because new technologies mitigate against the effects of attacks on GPS. However, because of unilateral dependence, the Sector has anticipated and accepts a level of inefficiency and risk in the system, including isolated, sporadic outages and intermittent energy shortages. Inefficiencies may be exacerbated by the need for islanding, in which parts of the system are not operating in sync with the rest of the system and phase regulation is no longer being controlled. Critical areas such as hospitals; public utilities such as drinking water systems, firefighting hydrants, wastewater treatment plants; and first responders might require their own energy backup systems to mitigate effects from outages. In addition, the anticipated need for more energy emergency backup capabilities will drive up expenses associated with purchasing and maintaining the redundant systems.

~~(U//FOUO)~~ Alternative Future 3: I Might Survive

~~(U//FOUO)~~ The I Might Survive future encompasses integrated dependence on GPS but nevertheless experiences extensive impact from GPS attacks. In this future, the Sector attempted to provide backups for GPS but was ultimately unprepared for various reasons, including that an

effective backup capacity was not achieved, alternative PNT systems did not work out, the technology or Sector went in an unexpected direction, or the Sector misjudged the requirements for energy capacity or the sophistication of an attack. GPS attacks have the potential to last a long time and affect a large geographic area. This future may necessitate falling back on earlier methods in which GPS is not a critical function. Because onsite backup systems are not in place, there is a premium on awareness, responsiveness, and alternative plans in the face of attacks.

~~(U//FOUO)~~ **Alternative Future 4: Lights Off, Pipes Clogged**

~~(U//FOUO)~~ The Lights Off, Pipes Clogged future is characterized by a high degree of dependence on GPS without backups in place, brought about by expedient or ill-considered investment decisions, insufficient regulatory actions, faulty assumptions, and poor risk management based on a myopic view of the future. In this future, although the Sector will achieve efficiencies and sophistication under normal circumstances, it is vulnerable to a full range of attacks from natural, intentional, unintentional, and coordinated attacks, resulting in an unreliable power grid and short- and long-term outages in the oil and gas supply. This is an unacceptable future that will be damaging to the Sector's economy and profitability, as well as detrimental to public health and safety.

~~(U)~~ **Challenges and Opportunities**

~~(U//FOUO)~~ Two alternative futures (I Will Survive and I Might Survive) were selected for in-depth examination and discussion. For these two alternative futures, workshop participants were asked to identify the opportunities as well as the challenges and threats that exist in each alternative future for the United States.

~~(U)~~ **Table G-3. Energy Sector Challenges and Opportunities**

The contents of this table are ~~U//FOUO~~

Alternative Future	Challenges	Opportunities
I Will Survive	<ul style="list-style-type: none">▪ Deciding what level of pain the system can endure and for what length of time.▪ Measuring how many operators have implemented a minimal level of security.▪ Convincing owners and operators to invest in local backups for their facilities.▪ Allowing industry to analyze commonalities, which may help GPS robustness, especially in the timing area.▪ Exerting the right regulatory pressure on the industry to make needed changes.	<ul style="list-style-type: none">▪ Providing opportunity for technology shifts that could change the way the sector does business (e.g., large capacity, long-term storage).▪ Solving problems in other sectors through research for the Energy Sector's backups (first responders, etc.).▪ Using the U.S. Coast Guard's differential timing system (DGPS) to provide support.▪ Three-frequency GPS makes intentional denial of service more difficult.▪ Opportunity for GPS receiver

~~(U)~~ **Table G-3. Energy Sector Challenges and Opportunities**
 The contents of this table are ~~U//FOUO~~

Alternative Future	Challenges	Opportunities
	<ul style="list-style-type: none"> ▪ The availability of an extremely reliable GPS system leads to no incentive to advance other systems. ▪ Including GPS/PNT as a recognized cyber component of the energy industry, which is in need of security—jamming resistant, spoofing resistant. ▪ Developing an authenticated GPS signal. 	<p>manufacturers to make multi-system/-frequency receivers.</p> <ul style="list-style-type: none"> ▪ Getting the right regulatory pressure on the industry to make needed changes. ▪ Requiring testing of systems to demonstrate that energy operations can continue without GPS. ▪ Using of dual-channel, multi-coded receivers.
I Might Survive	<ul style="list-style-type: none"> ▪ Demonstrating independence of backup systems and making sure there is no single point of failure and that the backup could last for a long time or indefinitely. ▪ Knowledge preservation for operations of an alternative technology. ▪ Having the components needed to revert to earlier modes of operation. ▪ Giving government the ability to receive reports of PNT attacks from Energy Sector owners and operators and then putting out a warning to sectors regarding the disruption. ▪ Developing a contingency plan for a “graceful” recovery. ▪ Achieving a model to allow sustained operations with lower efficiencies. 	<ul style="list-style-type: none"> ▪ Developing continuity of operations plans and exercises to demonstrate ability to operate without GPS. ▪ Understanding and dealing with PNT integration within the Sector. ▪ Using more distributed energy sources and establishing a micro-grid system when there is a contingency need. ▪ Managing expectations in the sector that GPS is not a panacea and that it has inherent vulnerabilities. ▪ Developing business cases from companies that have convinced boards of need for backups and publicizing cases for wider use. ▪ Sharing best practices in GPS interference and mitigation. ▪ Implementing current U.S. policy to detect, locate, identify, characterize, attribute, mitigate, and, if necessary, deny GPS interference.

~~(U)~~ Potential Milestones and Variables

~~(U//FOUO)~~ Workshop participants identified the following **milestones and variables**, which can be monitored by government and industry and could serve as indicators of the potential direction of identified uncertainties over the next 20 years:

~~(U//FOUO)~~ *I Will Survive*

- ~~(U//FOUO)~~ The industry accepting more dependency on GPS without mitigations is an indicator the Sector is moving toward unilateral dependence.
- ~~(U//FOUO)~~ NERC designating GPS as a Critical Cyber Asset (CIP-002) shows that the industry recognizes GPS needs to be protected like other cyber assets owing to the unilateral dependence upon it.
- ~~(U//FOUO)~~ Acceptance of nuisance outages by the Sector and public forecast the limited impact of GPS attacks in this future.
- ~~(U//FOUO)~~ Erosion of commitment to protect the GPS portion of L Band satellite services increases potential for GPS disruptions.
- ~~(U//FOUO)~~ Emergence of threats like cigarette lighter privacy jammers and other easily available jammers as well as hackers is an indicator that the Sector could be prone to GPS disruptions.
- ~~(U//FOUO)~~ The shift in use of the PMUs from simple monitoring to a control function would indicate the Sector is increasingly reliant on GPS.

~~(U//FOUO)~~ *I Might Survive*

- ~~(U//FOUO)~~ Investments in GPS backup systems, assuming that alternative sources of PNT become available.
- ~~(U//FOUO)~~ Other sectors (IT, Communications) have impetus to innovate by means other than GPS, especially in precision time transfer.
- ~~(U//FOUO)~~ The use of optical systems instead of GPS for PMUs by other countries.
- ~~(U//FOUO)~~ Increased deployments of PMUs over a wider area.
- ~~(U//FOUO)~~ Other countries (particularly Canada) continue to embrace and quickly deploy PMU technology.
- ~~(U//FOUO)~~ Emergence of new businesses/research and development results that recognize threats to GPS and offer expertise to the Energy Sector to enhance systems' robustness.

- ~~(U//FOUO)~~ International agreements regarding the need to protect GPS in the civilian arena from the production and employment of GPS interference devices, such as privacy jammers.
- ~~(U//FOUO)~~ Effective use of U.S. power lines as a means of data transfer.

~~(U)~~ Strategic Surprises

~~(U//FOUO)~~ Workshop participants identified the following strategic surprises, which are low-probability, high-consequence events that could bring chaos to the Sector and GPS:

- ~~(U//FOUO)~~ Mounting an attack on Energy and GPS in the near term, most likely through a hacker.
- ~~(U//FOUO)~~ A large geomagnetic storm takes out capacity, which could affect both GPS and the Sector.
- ~~(U//FOUO)~~ A September 11, 2001-type attack on a major metropolitan area, such as a vehicle-borne IED in concert with a preemptive GPS jamming attack to exacerbate consequences by introducing confusion to first responders operations.
- ~~(U//FOUO)~~ A kinetic attack against substations and then jamming or spoofing, possibly at the same time a major, widespread weather event is occurring.
- ~~(U//FOUO)~~ Alternating attacks between the east and west coast to exceed spare requirements or move spares in one direction and attack in the other.

~~(U)~~ Future Analytic Considerations

~~(U//FOUO)~~ SMEs discussed that future analytic considerations should include a threat component analyzing the capabilities and intent of terrorist groups and nation-state supporters of terrorism to attack GPS, as well as a clear message about current vulnerabilities. In addition, a study and more sophisticated scenario analyses correlating the loss of GPS and the timing derived from GPS on the Energy Sector would be useful. Carefully planned research studies could simulate effects of GPS loss on power measurement, and for each GPS loss discover the error on line parameter estimation. This would give an idea of what is a significant GPS loss for the Energy Sector. In a related vein, SMEs noted that an analytical end-to-end understanding of the contributions of PNT to the various parts of the systems within the Energy Sector would be extremely useful. SMEs also emphasized that more analytical studies on detecting spoofing are necessary.

~~(U)~~ **NRE GPS Transportation Systems Sector Alternative Futures Workshop Findings Report - May 23, 2011**

~~(U)~~ **Introduction**

~~(U//FOUO)~~ Alternative future generation serves as a primary analytic approach informing the NRE. A workshop was held on May 23, 2011, to elicit SME judgment to develop and refine alternative futures that could present challenges and opportunities for the Transportation Systems Sector's use of GPS PNT (see Annex I for a list of SME participants). Dependency on GPS and Debilitating GPS Attack served as the two uncertainties facing the Sector that defined four alternative future scenarios (see Figure G-4).

~~(U//FOUO)~~ Workshop participants fleshed out each scenario, identified core challenges and opportunities presented by the two scenarios judged to be most critical to decision makers, identified potential mileposts that could indicate a scenario is occurring, and discussed strategic surprises that could significantly change the Sector and its use of GPS. Annex D provides a full description of the alternative futures methodology.

~~(U//FOUO)~~ Workshop participants made the following assumptions concerning the Transportation Systems Sector alternative futures; each assumption is intended to be viable over the 20-year outlook of the alternative futures themselves:

- ~~(U//FOUO)~~ There will be a variety of innovations in all transportation modes that will increase reliance on PNT data.
- ~~(U//FOUO)~~ Over the next 20 years, the human skills for using manual PNT systems will erode due to lack of training and practice.
- ~~(U//FOUO)~~ There will be increased instances of intentional and unintentional disruptions of GPS.

~~(U//FOUO)~~ **Key judgments** concerning the future of the Transportation Systems Sector's use of GPS PNT raised at the workshop include:

- ~~(U//FOUO)~~ The economic drivers for the use of GPS by the Sector are its availability, accuracy, and reliability, and that it is provided by the government at no cost to users.
- ~~(U//FOUO)~~ The consequences to the Sector from the loss of GPS are primarily economic although there could be some safety and security impacts.
- ~~(U//FOUO)~~ There is a need for the Sector to identify the threshold for acceptable economic consequences and to understand the potential economic impacts of a loss of GPS on the Sector.
- ~~(U//FOUO)~~ SMEs expressed concern that the political will for a national backup system to GPS is lacking and that it will take a major GPS disruption to prompt reactive investment in implementing and maintaining a backup system.

- ~~(U//FOUO)~~ It would be useful to coordinate requirements for a GPS backup system across user groups so that solutions benefit the greatest number of users.

~~(U)~~ Alternative Futures

~~(U//FOUO)~~ **Dependency on GPS** and **Debilitating GPS Attack** served as the two uncertainties facing the Sector that defined four alternative futures (see Figure G-4).

~~(U//FOUO)~~ **Dependency on GPS** includes:

- ~~(U//FOUO)~~ The degree to which the Sector depends on GPS, such as acceptance and permeation of GPS-enabled components and systems in the Sector.
- ~~(U//FOUO)~~ The availability of alternatives, such as nationwide systems (e.g., a land-based backup) and/or Sector-embedded systems, such as chip-scale atomic clocks, anti-jam antennas, and inertial navigation systems.
- ~~(U//FOUO)~~ The ability to function with interference/loss, including ability of the Sector to recognize interference/loss of GPS (e.g., with built-in interference detectors in the GPS receivers).

~~(U//FOUO)~~ **Debilitating GPS Attack** includes:

- ~~(U//FOUO)~~ The likelihood of a successful attack that interferes with GPS signal availability.
- ~~(U//FOUO)~~ PNT robustness realized through continued U.S. GPS program improvements, such as signal diversity and civil signal integrity monitoring; availability of accurate geospatial information; and enhancement of the national PNT architecture, including provision of user notifications for any degradation.
- ~~(U//FOUO)~~ Interference threat mitigation capability, such as the ability to enforce technology controls and detect, respond to, and negate interference.

		Debilitating GPS Attack	
		Effective Response	Ineffective Response
Dependency on GPS	Shared Dependency	Blue Sky and Sunshine	Muddle Through
	Unilateral Dependency	High Anxiety	GPS 9/11

~~(U)~~ Figure G-4: Transportation Systems Sector Alternative Future Matrix

~~(U//FOUO)~~ **Alternative Future 1: Blue Sky and Sunshine**

~~(U//FOUO)~~ The Blue Sky and Sunshine future is marked by low dependence on GPS due to available backup systems as well the ability of government and industry to effectively detect, respond to, and mitigate against a debilitating attack on the GPS system. In the event of an attack on the GPS system, the Transportation Systems Sector is able to maintain safety and security but with reduced efficiency. There are some economic losses due to reduced efficiency. The ability of the government and industry to effectively respond to an attack on the GPS system validates planning and investment in GPS and seamless backup PNT systems to ensure safety and security. Government regulations requiring backup systems promote the creation of new markets for GPS alternatives and backups.

~~(U//FOUO)~~ **Alternative Future 2: High Anxiety**

~~(U//FOUO)~~ In the High Anxiety future, the Transportation Systems Sector is dependent on GPS without backup systems, but the government and industry are able to effectively detect, respond to, and mitigate against a debilitating attack on the GPS system. Disruption of GPS leads to economic losses as well as potential safety and security impacts. Aircraft are forced to use alternative navigation systems, and timing disturbances could affect rail and pipelines. The effective response capabilities of government and industry to an attack on the GPS system ensure that the Sector can operate through the attack but at lower efficiency levels. There is a high demand on human operators to take effective actions to back up GPS services.

~~(U//FOUO)~~ **Alternative Future 3: Muddle Through**

~~(U//FOUO)~~ The Muddle Through future is marked by low dependence on GPS due to available backup systems, but government and industry are not able to effectively detect, respond to, and mitigate against a debilitating attack on the GPS system. Investments in backup systems over the previous 20 years ensure PNT functions are still available but at reduced efficiency, leading to some economic losses. However, this future reflects a lack of system robustness and poor planning in building capacity to detect, respond to, and mitigate against GPS disruptions. The government is perceived to be incompetent. A core question for policymakers in this future is how much they are willing to spend on GPS backups to maintain a sufficient level of operations.

~~(U//FOUO)~~ **Alternative Future 4: GPS 9/11**

~~(U//FOUO)~~ In the GPS 9/11 future, the Transportation Systems Sector is dependent on GPS without backup systems, and government and industry are not able to effectively detect, respond to, and mitigate against a debilitating attack on the GPS system. This future is not an acceptable alternative for any transportation mode. In this future, GPS is unusable, and without backup systems the Sector regresses 50 years and operates without the efficiencies that GPS provides. Aircraft may be grounded and trucking operates without remote monitoring. This future might prompt the government to reactively promote the development of backup capabilities, but public confidence in GPS and government competence is greatly diminished.

(U) Challenges and Opportunities

~~(U//FOUO)~~ Two alternative futures (“High Anxiety” and “Muddle Through”) were selected for in-depth examination and discussion. For these two alternative futures, workshop participants were asked to identify the opportunities, as well as the challenges and threats, that exist in each alternative future for the United States.

~~(U)~~ **Table G-4. Transportation Systems Sector Challenges and Opportunities.**

The contents of this table are ~~U//FOUO~~

Alternative Future	Challenges	Opportunities
High Anxiety	<ul style="list-style-type: none"> ▪ Identifying an acceptable threshold for economic losses and determining an adequate response. ▪ Protecting Federal interests in GPS use of the L Band Spectrum. ▪ Providing necessary training in each mode for use of non-GPS systems. ▪ Providing near instantaneous detection and rapid mitigation of GPS disruptions. ▪ Convincing policymakers of the real threat posed by this future and that backups are needed. ▪ Garnering the political will to promote investments in backup systems. 	<ul style="list-style-type: none"> ▪ Promoting research and development for GPS backup systems. ▪ Taking advantage of the available time to develop and implement a plan for avoiding unilateral dependence on GPS. ▪ Focusing investments on backup systems as opposed to response capabilities. ▪ Promoting discussion of the development of GPS alternatives. ▪ Educating government and industry about the danger to transportation modes of using GPS as a sole source for PNT. ▪ Providing inexpensive, highly reliable timing.
Muddle Through	<ul style="list-style-type: none"> ▪ Convincing policymakers to maintain multiple systems to ensure that national GPS operations continue. ▪ Realistically estimating the threat to GPS in terms of duration and sophistication of attack type. ▪ Funding robustness of the GPS system. ▪ Determining the length of time the public will be willing to 	<ul style="list-style-type: none"> ▪ Investing in R&D for alternative systems. ▪ Developing low and medium ground frequencies. ▪ Exploring ways to operate without GPS and practicing operations with alternatives. ▪ Sharing information across modes allows coordination of requirements and developing solutions with the most benefit to the most users.

~~(U)~~ **Table G-4. Transportation Systems Sector Challenges and Opportunities.**
 The contents of this table are ~~U//FOUO~~

Alternative Future	Challenges	Opportunities
	accept a lower quality backup system. ▪ Being able to absorb the economic consequences of GPS disruptions. ▪ Achieving continuity of operations for each transportation mode. ▪ Coping with limited skills of those who are forced to use alternative PNT systems.	▪ Raising an alert if two independent navigation systems are not in agreement. ▪ Allowing for longer response time to attack given shared dependency on GPS and backups.

~~(U)~~ **Potential Milestones and Variables**

~~(U//FOUO)~~ Workshop participants identified the following **milestones and variables** that can be monitored by government and industry and could serve as indicators of the potential direction of identified uncertainties over the next 20 years:

~~(U//FOUO)~~ ***High Anxiety***

- ~~(U//FOUO)~~ A drastic increase in the number of devices sold with GPS-enabled applications, such as smart phones, is an indicator of increased dependence on GPS.
- ~~(U//FOUO)~~ An increase in the international investment in GPS alternatives, including ground-based systems, indicates a recognition that sole reliance on GPS is inadequate.
- ~~(U//FOUO)~~ More regulation requiring use of GPS, such as for mileage taxes or inland river navigation, signals an increased dependence on GPS.
- ~~(U//FOUO)~~ Moves away from backup or redundant systems to save money are another indicator of sole dependence on GPS.
- ~~(U//FOUO)~~ Increased privacy concerns among the public about the location-tracking capabilities of GPS-enabled devices could indicate GPS is ubiquitous.

~~(U//FOUO)~~ ***Muddle Through***

- ~~(U//FOUO)~~ The occurrence of interference events could indicate an increased likelihood of a successful debilitating attack on GPS as well as highlight ineffective response capabilities.
- ~~(U//FOUO)~~ The investigation by individual government agencies of GPS alternatives could indicate a trend toward developing backup systems (shared dependency).

- ~~(U//FOUO)~~ The emergence of U.S. policy requiring GPS backups as a function of government that agencies must implement would also promote a shift toward shared dependency.
- ~~(U//FOUO)~~ Public pressure for a GPS backup system could affect the pace of R&D efforts to enhance response capabilities.
- ~~(U//FOUO)~~ An increase in the international investment in GPS alternatives, including ground-based systems, could signal a growing trend toward a future with available GPS backups.
- ~~(U//FOUO)~~ The continual iterations of GPS robustness plans without actual plan implementation could lead to a future where government and industry are not able to effectively respond to an attack on GPS.

~~(U)~~ Strategic Surprises

~~(U//FOUO)~~ Workshop participants identified the following strategic surprises, which are low-probability, high-consequence events that could bring chaos to the Sector and GPS:

- ~~(U//FOUO)~~ Solar weather takes out a significant portion of satellites, leading to a depleted constellation that would take years to replace.
- ~~(U//FOUO)~~ The confluence of a natural disaster and GPS disruption affecting emergency response, communications systems, etc.
- ~~(U//FOUO)~~ Government issues a license for a ground-based transmitter frequency close to the GPS L Band, leading to disruptions in GPS.
- ~~(U//FOUO)~~ Aging constellations that are well beyond their useful life, leading to a potential cascading GPS failure.
- ~~(U//FOUO)~~ A major HAZMAT incident in the transportation system caused by GPS disruption.
- ~~(U//FOUO)~~ A spoofing incident targeting offshore drilling platforms.
- ~~(U//FOUO)~~ Systemic GPS failure from new software supporting the GPS system.
- ~~(U//FOUO)~~ Lack of confidence in GPS because of repeated disruptions leads to missed economic benefits in areas such as intelligent highways.
- ~~(U//FOUO)~~ A public backlash against GPS because of privacy concerns.
- ~~(U//FOUO)~~ A transfer to a foreign PNT system due to a major loss of confidence in GPS.
- ~~(U//FOUO)~~ A nation-state or terrorist group publicizing an attack on the GPS system.

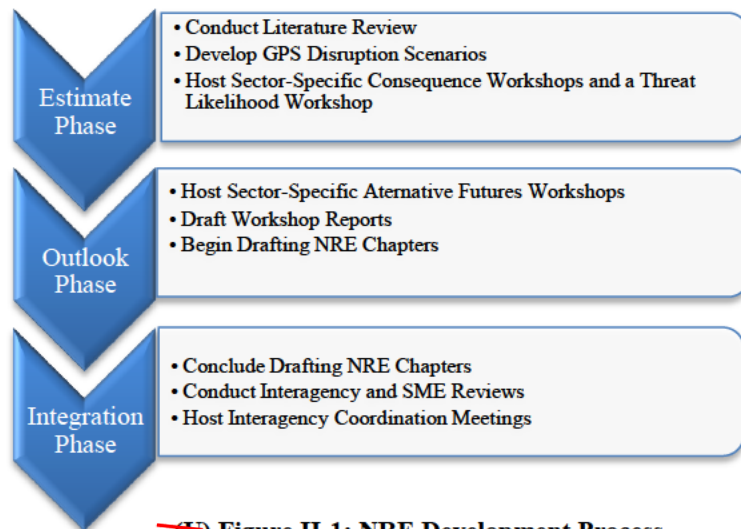
~~(U)~~ **Future Analytic Considerations**

~~(U//FOUO)~~ SMEs discussed that a focus of future analytic considerations could be determining the threshold at which economic losses from GPS disruption are significant enough to warrant investment in a GPS backup. Suggestions for this economic-loss metric included a percentage loss in throughput or a dollar amount. SMEs noted that each sector should analyze the economic benefits of their respective PNT technology applications in order to better understand the economic impact if GPS is disrupted. In addition, SMEs cited the need for further efforts to design and deploy enhanced response capabilities to GPS interference. Finally, they also noted the need to build receivers that can identify jamming and spoofing and alert users to discrepancies.

~~(U)~~ Annex H. NRE Coordination Approach

~~(U//FOUO)~~ Coordination, both internal and external to DHS, has remained a priority throughout the National Risk Estimate: Risks to U.S. Critical Infrastructure from Global Positioning System Disruptions (NRE) development process. During the planning phase of this NRE, HITRAC established a layered outreach approach in order to develop an Interagency coordinated NRE by September 2011. The NRE coordination began in January 2011 by developing an internal NRE writing team and obtaining input and feedback within HITRAC. A Terms of Reference (TOR) document was drafted, and external Departments, Agencies, and other organizations that could provide subject matter expertise on the information requirements driven by the key questions in the TOR were identified.

~~(U//FOUO)~~ Each phase of the NRE development process (Figure H-1) illustrates an additional layer of fidelity in the coordination approach. During the estimate phase, the NRE team conducted a comprehensive literature review, consulted with the Advisory Group, began preliminary coordination with SMEs, and developed GPS disruption scenarios. Then HITRAC hosted five sector-specific (including two subsector-specific) consequence workshops. These one-day workshops, hosted in March and April 2011, consisted of small groups of government and private sector SMEs. In addition, one threat likelihood workshop was held in May 2011. HITRAC produced reports incorporating the SMEs' findings for all workshops that occurred during the estimate phase.



~~(U)~~ Figure H-1: NRE Development Process

~~(U//FOUO)~~ In phase two, the outlook phase, HITRAC hosted four sector-specific alternative futures development workshops. These one-day workshops, hosted in May and June 2011, also consisted of small groups of government and private sector SMEs. HITRAC produced reports incorporating the SMEs' findings for all workshops that occurred during the outlook phase.

~~(U//FOUO)~~ Upon completion of the alternative futures scenarios at the end of the outlook phase and into the beginning of the integration phase, the NRE writing team began drafting the various sections of the NRE, directly incorporating SMEs' findings from the consequence, alternative futures, and threat likelihood workshops.

~~(U//FOUO)~~ HITRAC concluded the final phase of the NRE development process, the integration phase, by hosting two NRE Interagency Coordination Group meetings. These meetings were held to provide an overview of initial analysis, fill information gaps, and coordinate findings

through the Interagency, as well as afford all agencies and participants the chance to provide comments in regard to their particular areas of expertise. The following is a list of Agencies and/or groups that participated in some part of the NRE development or review process.

- (U) Academia
- (U) Chillum-Adelphi (Maryland) Fire Department
- (U) U.S. Department of Commerce, including:
 - (U) National Institute of Standards and Technology
- (U) U.S. Department of Defense
- (U) U.S. Department of Energy
- (U) U.S. Department of Homeland Security components:
 - (U) Office of Intelligence and Analysis
 - (U) U.S. Coast Guard
 - (U) Science and Technology Directorate
 - (U) National Communications System
 - (U) National Protection and Programs Directorate – Office of Infrastructure Protection, Office of Cybersecurity and Communications/National Cyber Security Division, Office of Risk Management and Analysis
- (U) U.S. Department of Transportation, including:
 - (U) Federal Railroad Administration
 - (U) Federal Aviation Administration
- (U) Federal Bureau of Investigation
- (U) Federal Communications Commission
- (U) Federal Deposit Insurance Corporation
- (U) Federal Reserve Bank of the United States of America
- (U) North Carolina State Highway Patrol
- (U) Oak Ridge National Laboratory
- (U) U.S. Naval Observatory

~~(U)~~ Annex I. Subject Matter Expert Contributors

(U) Communications Sector Consequence Workshop, March 2, 2011
Subject Matter Experts

(b)(6)	GPS	(b)(6)
	Communications	
	Communications	
	GPS	
	GPS	
	Comms/GPS	
	Communications	
	GPS Timing	
	Communications	
	Communications	
	GPS	
	Communications	
	Communications	
	Communications	

~~(U)~~ Emergency Services Sector Consequence Workshop, April 5, 2011
Subject Matter Experts

(b)(6)	ESS	(b)(6)
	Communications	
	GPS	
	ESS/Fire	
	ESS	
	GPS	
	GPS	
	GPS	
	ESS/GPS	
	GPS	
	Communications	
	ESS	
	ESS/9-1-1	

~~(U)~~ Energy Sector Consequence Workshop, March 24, 2011
Subject Matter Experts

(b)(6)	Energy	(b)(6)
	Energy	
	GPS	
	Energy	
	Energy	
	GPS	
	GPS	
	Timing/Frequency	
	GPS Timing	
	Energy	
	Energy	
	Energy	
	GPS	

~~(U)~~ Transportation (Aviation) Consequence Workshop, March 14, 2011
Subject Matter Experts

(b)(6)	Aviation	(b)(6)
	Aviation	
	GPS	
	Aviation	
	GPS/Aviation	
	GPS/Aviation	
	Aviation	
	GPS/Aviation	
	Aviation	
	GPS	
	GPS	
	Aviation	
	Aviation	
	Aviation	
	Aviation	

~~(U)~~ **Transportation (Maritime and Surface) Consequence Workshop, March 28, 2011**
Subject Matter Experts

(b)(6)	GPS	(b)(6)
	Transportation	
	Maritime	
	Transportation	
	Transportation	
	GPS	
	GPS	
	GPS	
	Maritime	
	Transportation	
	Transportation	
	GPS	

~~(U)~~ **Likelihood-Threat Workshop, May 6, 2011**
Subject Matter Experts

(b)(6)	GPS	(b)(6)
	Comms	
	GPS	
	GPS	
	Maritime	
	GPS	
	Aviation/GPS	
	ESS/GPS	
	Comms	
	GPS	
	Maritime	
	GPS	

~~(U)~~ **Communications Sector Alternative Futures Workshop, June 20, 2011**
Subject Matter Experts

(b)(6)	GPS	(b)(6)
	GPS	
	Communications	
	GPS	
	GPS	
	GPS	
	Communications	
	GPS	
	Communications	
	Communications	
	Communications	
	Communications	

~~(U)~~ **Emergency Services Sector Alternative Futures Workshop, June 7, 2011**
Subject Matter Experts

(b)(6)	GPS	(b)(6)
	GPS	
	ESS	
	ESS	
	GPS	

~~(U)~~ **Energy Sector Alternative Futures Workshop, May 25, 2011**
Subject Matter Experts

(b)(6)	GPS	(b)(6)
	Energy	
	GPS	
	Energy/GPS	
	Energy	
	GPS	
	GPS Timing	
	Energy	
	Energy	
	GPS	

~~(U)~~ **Transportation Sector Alternative Futures Workshop, May 23, 2011**
Subject Matter Experts

(b)(6)	Rail GPS Transportation Aviation Rail Transportation Aviation GPS GPS Aviation Aviation Maritime Transportation Surface Transportation	(b)(6)
--------	---	--------

~~(U)~~ Annex J. Bibliography

- ~~(U)~~ American Meteorological Society, *Satellite Navigation and Space Weather: Understanding the Vulnerabilities & Building Resilience*, Policy Workshop Report, March 2011, www.ametsoc.org/atmospolicy/documents/AMSSWGPSFinal.pdf.
- ~~(U)~~ Association Internationale de Signalisation Maritime, *Recommendation on GNSS Vulnerability and Mitigation Measures*, 2004.
- ~~(U)~~ Bellows, Charlie, “GPS Operations Center – A User Focused Center of Excellence,” (Date Unknown).
- ~~(U)~~ Berstis, Knute A., “Technologies of Interest to Surveyors in 2025,” National Coordination Office for Space Based PNT, October 16, 2010.
- ~~(U)~~ Berwin, Bob, “LightSquared cell network knocks out first responders’ GPS in tests,” NextGov.com, May 20, 2011, http://www.nextgov.com/nextgov/ng_20110520_9569.php?oref=topstory, accessed August 9, 2011.
- ~~(U)~~ Carroll, James and Kirk Montgomery, “Global Positioning System Timing Criticality Assessment – Preliminary Performance Results,” 40th Annual Precise Time and Time Interval (PTTI) Meeting, December 1, 2008.
- ~~(U)~~ Defense Science Board Task Force, *The Future of the Global Positioning System*, Washington, D.C.: U.S. Department of Defense, October 2005.
- ~~(U)~~ Federal Aviation Administration AJW-19, *GPS L1 RFI Quick Look Report Using Wide Area Reference Station (WRS) Data*, LAAS-229-001414-A, unpublished draft dated November 10, 2010.
- ~~(U)~~ Federal Aviation Administration, *NSTB/WAAS T&E Team, Wide Area Augmentation System Performance Analysis Report*, Report #34, Reporting Period to 1 July – 30 September 2010, October 2010.
- ~~(U)~~ Federal Aviation Administration, *NSTB/WAAS T&E Team, Wide Area Augmentation System Performance Analysis Report*, Report #35, Reporting Period to 1 October – 31 December 2010, January 2011.
- ~~(U)~~ Federal Aviation Administration, *NSTB/WAAS T&E Team, Wide Area Augmentation System Performance Analysis Report*, Report #36, Reporting Period to 1 January – 31 March 2011, April 2011.

- ~~(U)~~ Federal Aviation Administration Web page, “Fact Sheet – Next Generation Air Transportation System 2006 Progress Report,”
www.faa.gov/news/fact_sheets/news_story.cfm?newsId=8336, accessed September 21, 2011.
- (U) Federal Communications Commission: Public Safety and Homeland Security Bureau Web page, “Tech Topic 19: Communications Interdependencies,”<http://transition.fcc.gov/pshs/techtopics/techtopics19.html>, accessed August 22, 2011
- ~~(U)~~ Federal Communications Commission Working Group, *Final Report of the Working Group Established by the FCC to Study Overload/Desensitization Interference on GPS Receivers and GPS-Dependent Applications from LightSquared Terrestrial Broadband Operations*, July 30, 2011, <http://fjallfoss.fcc.gov/ecfs/document/view?id=7021690471>, accessed August 3, 2011.
- ~~(U)~~ Fiske, David, “Federal Communication Commission Enforcement Bureau Steps Up Education and Enforcement Efforts Against Cellphone and GPS Jamming: Targeted Education and Outreach Coupled with Strict Enforcement,”
http://transition.fcc.gov/eb/News_Releases/DOC-304575A1.html, accessed September 29, 2011.
- ~~(U)~~ Fletcher, Jeff, Vivek Vichare, Chaitanya Ganoo, and James Moyne, “Time Synchronization Applications in the Smart Grid and Beyond,” November 4, 2009.
- ~~(U)~~ General Lighthouse Authorities, “GPS Jamming Trial Executive Summary Report,” September 23, 2008.
- ~~(U)~~ Geolocational Privacy Surveillance Act. H.R. 2168, 112th Congress, 1st session, June 14, 2011.
- ~~(U)~~ German Federal Bureau of Maritime Casualty Investigation, “Grounding of the LT CORTESIA on January 2, 2008 on the Varne Bank in the English Channel,” April 1, 2009.
- ~~(U)~~ Global Positioning System Web page, “Global Positioning System Serving the World,” www.gps.gov, accessed January 13, 2011.
- ~~(U)~~ Hambling, David, “GPS Chaos: How a \$30 Box Can Jam Your Life,” *The New Scientist*, March 6, 2011.
- ~~(U)~~ Hart, David G., David Uy, Vasudev Gharpure, Damire Novosel, Daniel Karsson & Mehmet Kaba, “A New Approach to Power Network Monitoring,” *ABB Review*, January 2001.
- ~~(U//FOUO)~~ Homeland Infrastructure Threat and Risk Analysis Center, “GPS Risk to CIKR,” (Pre-Decisional Draft), Washington, D.C.: U.S. Department of Homeland Security, 2010.
- ~~(U)~~ Humphreys, Todd E., Ledvina, Brent L., Kitner, Paul M., Psiaki, Mark I., and O’Hanlon, Brady, “Assessing the Spoofing Threat,” *GPS World*, January 1, 2009.

- ~~(U)~~ Jewell, Don, "GPS Insights-April 2007," *GPS World*, April 2007, <http://www.gpsworld.com/defense/gps-insights-april-2007-8428>, accessed July 6, 2011.
- ~~(U)~~ Khan, Faisal Ahmed and Andrew G. Dempster, "Effects on CDMA Network Performance due to Degradation of GPS based Synchronization," University of New South Wales, 2007.
- ~~(U)~~ Lazar, Steven, et al. "GPS Spectrum: Sharing or Encroachment?" *GPS World*, September 2000.
- ~~(U)~~ Lilley, Robert, Gary Church, and Michael Harrison, "GPS Backup for Position, Navigation and Timing: Transition Strategy for Navigation and Surveillance," Washington, D.C.: Federal Aviation Administration, August 22, 2006.
- ~~(U)~~ Los Alamos National Laboratory, "A Simple Demonstration that the Global Positioning System (GPS) is Vulnerable to Spoofing," *The Journal of Security Administration* 25(2002): 19-28.
- ~~(U)~~ Luo, Ming, et al. "Testing and Research on Interference to GPS from UWB Transmitters," 2001. <http://waas.stanford.edu/~wwu/papers/gps/PDF/mingion01.pdf>.
- ~~(U)~~ Matthews, Michael B., Peter F. Macdorn, Kenn L. Gold, "SCP Enabled Navigation Using Signals of Opportunity in GPS Obstructed Environments," *Journal of Navigation* (58)(2) Summer 2011.
- ~~(U)~~ McNeff, Jules G., "The Global Positioning System," *IEEE Transactions on Microwave Theory and Techniques* 50(3)(March 2002).
- ~~(U//FOUO)~~ MITRE, *GPS Timing Loss Impacts/Backups/Mitigation Report*, October 28, 2010.
- ~~(U)~~ Murfin, Tony, "GNSS Interference: Apparently It's an Issue," *GPS World*, December 15, 2010.
- ~~(U)~~ National Aeronautics and Space Administration Ames Research Center, "State Estimation," <http://www.nasa.gov/centers/ames/research/technology-onepaggers/state-estimation.html>, March 29, 2008, accessed September 22, 2011.
- ~~(U)~~ National PNT Advisory Board, "Comments on Jamming the GPS – A National Security Threat," November 4, 2010.
- ~~(U)~~ National Security Space Office, *National Positioning, Navigation, and Timing Architecture Study Final Report*, September 2008.
- ~~(U)~~ National Security Telecommunications Advisory Committee (NSTAC), *Report to the President on Commercial Communications Reliance on the Global Positioning System (GPS)*, February 28, 2008.

~~(U)~~ National Space-Based Positioning, Navigation and Timing Systems Engineering Forum (NPEF), "Assessment of LightSquared Terrestrial Broadband System Effects on GPS Receivers and GPS-dependent Applications," June 14, 2011.

~~(U)~~ North American Synchrophasor Initiative (NASPI), "Synchrophasor System Benefits Fact Sheet," (Date Unknown).

~~(U)~~ "North Korea Appears Capable of Jamming Receivers," Telemantics, 2010, <http://www.defence.pk/forums/military-forum/76068-north-korea-appears-capable-jamming-gps-receivers.html>.

~~(U)~~ Office of Infrastructure Protection, "National Infrastructure Protection Plan: Banking and Finance Sector," Washington D.C.: U.S. Department of Homeland Security, www.dhs.gov/xlibrary/assets/nipp_snapshot_banking.pdf, accessed August 22, 2011.

~~(U)~~ Office of Infrastructure Protection, "Banking and Finance Sector: Critical Infrastructure and Key Resources Sector-Specific Plan as Input to the National Infrastructure Protection Plan," Washington, DC: U.S. Department of Homeland Security, May 2007, www.dhs.gov/xlibrary/assets/nipp-ssp-banking.pdf, accessed August 22, 2011.

~~(U)~~ Office of Infrastructure Protection, "Communications Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan," Washington, DC: U.S. Department of Homeland Security, 2010, <http://www.dhs.gov/xlibrary/assets/nipp-ssp-communications-2010.pdf>, accessed July 19, 2011.

~~(U)~~ Office of Infrastructure Protection, "Emergency Services Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan," Washington, DC: U.S. Department of Homeland Security, 2010, www.dhs.gov/xlibrary/assets/nipp-ssp-emergency-services.pdf, accessed August 22, 2011.

~~(U)~~ Office of Infrastructure Protection, "National Infrastructure Protection Plan: Energy Sector," Washington, DC: U.S. Department of Homeland Security, http://www.dhs.gov/xlibrary/assets/nipp_snapshot_energy.pdf, accessed August 22, 2011.

~~(U)~~ Office of Infrastructure Protection, "Energy Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan," Washington, DC: U.S. Department of Homeland Security, 2010, www.dhs.gov/xlibrary/assets/nipp-ssp-energy-2010.pdf, accessed August 22, 2011.

~~(U)~~ Office of Infrastructure Protection, "National Infrastructure Protection Plan: Transportation Systems Sector," Washington, DC: U.S. Department of Homeland Security, www.dhs.gov/xlibrary/assets/nipp_snapshot_transportation.pdf, accessed August 22, 2011.

~~(U)~~ Office of Infrastructure Protection, "Transportation Systems: Critical Infrastructure and Key Resources Sector-Specific Plan as Input to the National Infrastructure Protection Plan," Washington, DC: U.S. Department of Homeland Security, May 2007, www.dhs.gov/xlibrary/assets/nipp-ssp-transportation.pdf, accessed 22 August 2011.

~~(U)~~ Papadimitratos and Javanovic, "GNSS-based Positioning: Attacks and Countermeasures," MILCOM, 2008.

~~(U)~~ Royal Academy of Engineering, *Global Navigation Space Systems: Reliance and Vulnerabilities*, March 30, 2011.

~~(U)~~ Salmi, Pekka and Marko Torkeli, "Inventions Utilizing Satellite Navigation Systems in the Railway Industry," *Journal of Technology Management & Innovation* 4(3)(September 2009).

~~(U)~~ Scott, Logan, "911: The Case for Fast Jammer Detection and Location Using Crowdsourcing Approaches," paper presented at ION-GNSS-2011, September 20-23, 2011.

~~(U)~~ Sorrel, Charlie, "Car Thieves Use GPS Jammers to Make Clean Getaway," *Wired*, February 24, 2010.

~~(U)~~ Space-Based Positioning, Navigation & Timing National Executive Committee, "U.S. Space-Based PNT Policy Fact Sheet," December 15, 2004, <http://www.pnt.gov/policy/2004-policy.shtml>, accessed September 29, 2011.

~~(U)~~ Space-Based Positioning, Navigation, and Timing National Executive Committee Web page, www.pnt.gov, accessed January 11, 2011.

~~(U)~~ Stergiou, Paul and David Kalokitis. "Keeping the Lights On: GPS and Power Grid Intermesh," *GPS World*, November 1, 2003

~~(U)~~ Sung-Ki, Jung, "S. Korea Blames North for GPS, Phone Jamming," *Defense News*, March 6, 2011, <http://www.defensenews.com/story.php?i=5883068&c=ASI&s=LAN>, accessed July 7, 2011.

~~(U)~~ Symmetricom, "Timing and Synchronization in WiMAX Networks," October 30, 2006.

~~(FOUO)~~ Szabat, Joel, "FAA Letter to Associate Administrator Karl Nebbia, National Telecommunications and Information Administration, Appendix A," July 21, 2011.

~~(U)~~ Thomas, Keir. "Is GPS About to be Broken?" *PC World*, http://www.pcworld.com/businesscenter/article/221853/is_gps_about_to_be_broken.html, accessed March 20, 2011.

~~(U)~~ U.S. Department of Defense, *Global Positioning System (GPS) 2008: A Report to Congress*, Washington, D.C.: October 31, 2008.

~~(U)~~ U.S. Department of Defense, U.S. Department of Homeland Security, U.S. Department of Transportation, "2008 Federal Radionavigation Plan," Washington, D.C.: 2008.

- ~~(U)~~ U.S. Department of Homeland Security Web page, "Communications Sector: Critical Infrastructure and Key Resources," www.dhs.gov/files/programs/gc_1189102978131.shtm, accessed August 22, 2011
- ~~(U)~~ U.S. Department of Homeland Security Web page, "Emergency Services Sector: Critical Infrastructure and Key Resources," www.dhs.gov/files/programs/gc_1189094187811.shtm, accessed August 22, 2011.
- ~~(U)~~ U.S. Department of Homeland Security Web page, "Energy Sector: Critical Infrastructure and Key Resources," www.dhs.gov/files/programs/gc_1189013411585.shtm, accessed August 22, 2011.
- ~~(U)~~ U.S. Department of Homeland Security, "DHS Positioning, Navigation, and Timing Interference Detection and Mitigation Plan," Washington, D.C.: October 16, 2006.
- ~~(U)~~ U.S. Department of Homeland Security, "DHS Positioning, Navigation, and Timing Interference Detection and Mitigation Plan Implementation Strategy," Washington, D.C.: January 8, 2008.
- ~~(U)~~ U.S. Department of Homeland Security, *DHS Risk Lexicon*, Washington, D.C.: 2010.
- ~~(U)~~ U.S. National Intelligence Council, *Disruptive Civil Technologies – Conference Report*, Washington, D.C.: 2008.
- ~~(U//FOUO)~~ U.S. Department of Transportation, Maritime Administration, "Response to Positioning, Navigation, and Timing Data Call," 2009.
- ~~(U)~~ Vincent, Wilber R., Richard W. Adler, Paul McGill, James R. Clynych, George Badger, Andrew A. Parker, "The Hunt for RFI," *GPS World*, January 1, 2003
http://www.gpsworld.com/gnss-system/signal-processing/the-hunt-rfi-776?page_id=2
- ~~(U)~~ Volpe National Transportation Systems Center, *Global Positioning System Timing Criticality Update Final Report*, September 5, 2008.
- ~~(U)~~ Volpe National Transportation Systems Center, *Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System Final Report*, August 29, 2001.
- ~~(U//FOUO)~~ Ward, K., FAA, e-mail message to Moore, R., HITRAC, February 1, 2011.
- ~~(U)~~ Zeta Associates, "EWR RFI Investigation – Characteristics of RFI between March 25 - April 19," June 9, 2010.
- ~~(U)~~ Zeta Associates - FAA correspondence, 2011.

~~(U)~~ Zeta Associates, "Ongoing EWR RFI Investigation - Two G-II Receivers and Rotating Antenna, TM100402," April 2, 2010.

~~(U)~~ Zeta Associates, "PPD Detections near EWR, TM 110708," July 8, 2011.

~~(U)~~ Annex K. Selected PNT and GPS Regulations, Strategies, Executive Committees, and Working Groups

~~(U)~~ The Nation's PNT systems, including GPS, are managed by multiple jurisdictions and actors. This annex provides examples of key (1) legal authorities and regulations, (2) government strategies, and (3) executive committees and working groups that manage PNT and GPS.

~~(U)~~ Legal Authorities and Regulations

~~(U)~~ The Congress of the United States has mandated that the Federal Government take action toward managing GPS. The key authorities that contribute to government solutions for managing PNT and GPS are as follows:

- ~~(U)~~ The National Defense Authorization Act of 1998¹⁰⁰ grants the Secretary of Defense authority over civil and military GPS; the Secretary is required to coordinate with the Secretaries of Transportation and Commerce on issues concerning civil GPS. The statute requires civil GPS to be continuous, worldwide, and free.
 - ~~(U)~~ The statute requires a Federal Radionavigation Plan (FRP) and biennial reports to Congress from the National Executive Committee for Space-based Positioning, Timing, and Navigation.¹⁰¹
 - ~~(U)~~ The statute instructs the Secretary of Defense to prevent hostile use of GPS without impairing civil GPS uses.
- ~~(U)~~ Title 51, the National and Commercial Space Programs Code,¹⁰² incorporates Section 104 of the Commercial Space Act of 1998 and requires promotion of international agreements that recognizes GPS and its augmentations as an international standard and attempts to eliminate foreign barriers to GPS use worldwide.
 - ~~(U)~~ The statute reiterates that GPS should be provided free of direct user fees.
 - ~~(U)~~ The statute instructs the Assistant Secretary of Commerce to manage and protect the GPS spectrum.
- ~~(U)~~ The Department of Transportation and Related Agencies Appropriations Act¹⁰³ authorizes DGPS and allows the Department of Transportation to integrate former Department of Defense Ground Wave Emergency Network sites with U.S. Coast Guard DGPS stations. The use of DGPS is also encouraged for GPS-based meteorology.

~~(U)~~ Government Strategies

~~(U)~~ Federal strategies provide the key goals and objectives for managing PNT systems. These strategies, in turn, ultimately establish the foundation for subsequent programs and courses of action within the executive branch.

- ~~(U)~~ The 2007 National Strategy for Homeland Security (NSHS) established the President's doctrine for homeland security. The NSHS highlighted the protection of the

¹⁰⁰ ~~(U)~~ 10 U.S. C. §2281.

¹⁰¹ ~~(U)~~ National Defense Authorization for Fiscal Year 2010, Section 1032.

¹⁰² ~~(U)~~ 51 U.S. C. §50112.

¹⁰³ ~~(U)~~ 49 U.S. C. §301.

18 critical infrastructure sectors, many of which depend directly or indirectly on GPS services.

- ~~(U)~~ The National Infrastructure Protection Plan (NIPP) provides the unifying structure for the integration of a wide range of efforts for the enhanced protection and resilience of critical infrastructure and key resources.
 - (U) The NIPP recognizes that PNT and GPS services are integral to several critical infrastructure sectors, including communications, transportation systems, and energy.
 - (U) The NIPP requires that PNT services be “reliable, seamless, resistant, and resilient to unintentional or intentional interference or jamming.”¹⁰⁴
- ~~(U)~~ Homeland Security Presidential Directive (HSPD)-5 serves to enhance the ability of the United States to manage domestic incidents by establishing a single comprehensive national incident management system. This management system is designed to cover the prevention, preparation, response, and recovery from terrorist attacks, major disasters, and other emergencies. The implementation of such a system would allow all levels of government throughout the nation to work together efficiently and effectively.
- ~~(U)~~ HSPD-7—Critical Infrastructure Identification, Prioritization, and Protection—establishes a national policy to identify and prioritize critical infrastructure within the United States and protect them from terrorist attacks. HSPD-7 designates the Secretary of Homeland Security as the lead Federal official in charge of coordinating efforts to protect critical infrastructure, and it identifies roles and responsibilities for additional departments and agencies.
- ~~(U)~~ HSPD-8 establishes policies to strengthen U.S. preparedness in order to prevent and respond to threatened or actual domestic terrorist attacks, major disasters, and other emergencies. The directive requires a national domestic all-hazards preparedness goal, with established mechanisms for improved delivery of Federal preparedness assistance to State and local governments. It also outlines actions to strengthen preparedness capabilities of Federal, State, and local entities.
- ~~(U)~~ NSPD-39 requires each agency with responsibility for GPS PNT to take implementation actions. The respective secretaries are required to accomplish the following:
 - ~~(U)~~ **The Secretary of Defense shall:**
 1. ~~(U)~~ Develop, acquire, operate, realistically test, evaluate, and maintain navigation warfare capabilities and other capabilities required to:
 - a. ~~(U)~~ Effectively utilize GPS services in the event of adversary jamming or other interference;
 - b. ~~(U)~~ Deny adversaries position, navigation, and timing services from GPS, its augmentations, and/or any other space-based PNT systems without unduly disrupting civil, commercial, and scientific uses of these services outside an area of military operations or for homeland security purpose; and
 - c. ~~(U)~~ Identify, locate, and mitigate, in coordination with Departments and Agencies, as appropriate, any interference on a global basis that adversely affects the use of GPS for military operations.

¹⁰⁴ ~~(U)~~ National Infrastructure Protection Plan, 3.2 Identifying Positioning, Navigation, and Timing Services.

2. ~~(U)~~ Train, equip, and exercise U.S. military forces and national security capabilities in operationally realistic conditions that include denial of GPS. In cooperation with the Secretaries of Transportation and Homeland Security, and, as appropriate, with the Secretary of State, develop guidelines that facilitate these activities and navigation warfare training, testing, demonstration, and exercises without unduly disrupting or degrading homeland security and civil services and operations, either internationally or domestically.
 3. ~~(U)~~ Facilitate access to appropriate levels of national security services and user equipment at the Federal level to meet critical requirements for emergency response and other homeland security purposes, and, on an exceptional basis, for civil purposes including State or local emergency response.
- ~~(U)~~ **The Secretary of Transportation shall:**
 1. ~~(U)~~ Have lead responsibility for the development of requirements for civil applications from all U.S. Government civil Departments and Agencies;
 2. ~~(U)~~ Ensure, in cooperation with the Secretaries of Defense and Homeland Security, the performance monitoring of the U.S. civil space-based PNT services;
 3. ~~(U)~~ In cooperation with other Departments and Agencies, promote the use of U.S. civil space-based PNT services and capabilities for transportation safety;
 4. ~~(U)~~ In coordination with the Secretary of Homeland Security, develop, acquire, operate, and maintain backup PNT capabilities that can support critical transportation, homeland security, and other critical civil and commercial infrastructure applications within the United States, in the event of a disruption of GPS or other space-based positioning, navigation, and timing services consistent with HSPD-7.
 - ~~(U)~~ **The Secretary of Commerce shall:**
 1. ~~(U)~~ In coordination with the Secretaries of State, Defense, and Transportation and the National Aeronautics and Space Administration (NASA), seek to protect the radio frequency (RF) spectrum used by GPS and its augmentations through appropriate domestic and international spectrum management and regulatory practices;
 2. ~~(U)~~ In coordination with the Secretaries of Defense and Transportation, and the Administrator of NASA, facilitate cooperation between the U.S. Government and U.S. industry as appropriate to identify mutually acceptable solutions that will preserve existing and evolving uses of space-based PNT services while allowing for the development of other technologies and services that depend on use of the RF spectrum.
 - ~~(U)~~ **The Secretary of Homeland Security shall:**
 1. ~~(U)~~ Identify space-based PNT requirements for homeland security purposes to the Secretary of Transportation and coordinate the use of PNT capabilities and backup systems for homeland security purposes by Federal, State, and local governments and authorities;
 2. ~~(U)~~ In coordination with the Secretary of Transportation, and with other Departments and Agencies, promote the use of the GPS positioning and

timing standards for use by Federal agencies and by State and local authorities responsible for public safety and emergency response;

3. ~~(U)~~ In coordination with the Secretary of Defense, and in cooperation with the Secretaries of Transportation and Commerce, ensure:
 - a. ~~(U)~~ Mechanisms are in place to identify, understand, and disseminate timely information regarding threats associated with the potential hostile use of space-based positioning, navigation, and timing services within the United States; and
 - b. ~~(U)~~ Procedures are developed, implemented, and routinely exercised to request assistance from the Secretary of Defense should it become necessary to deny hostile use of space-based position, navigation, and timing services within the United States;
 4. ~~(U)~~ In coordination with the Secretaries of Defense, Transportation, and Commerce, develop and maintain capabilities, procedures, and techniques and routinely exercise civil contingency responses to ensure continuity of operations in the event that access to GPS is disrupted or denied;
 5. ~~(U)~~ In coordination with the Secretaries of Transportation and Defense and in cooperation with other Departments and Agencies, coordinate the use of existing and planned Federal capabilities to identify, locate, and attribute any interference within the United States that adversely affects use of GPS and its augmentations for homeland security, civil, commercial, and scientific purposes.
 6. ~~(U)~~ In coordination with the Secretaries of Transportation and Defense, and the Director of Central Intelligence, and in cooperation with other Departments and Agencies: (1) develop a central repository and database for reports of domestic and international interference to the civil services of GPS and its augmentations for homeland security, civil, commercial, and scientific purposes; and (2) notify promptly the Administrator of the National Telecommunications and Information Administration, the Chairman of the Federal Communications Commission, the Secretary of Defense, the Director of Central Intelligence, and other Departments and Agencies in cases of domestic or international interference with space-based PNT services to enable appropriate investigation, notification, and/or enforcement action.¹⁰⁵
- ~~(U)~~ Presidential Policy Directive (PPD) 4, the 2010 National Space Policy, requires the United States to maintain leadership in global navigation satellite systems (GNSS) by providing continuous, worldwide access to GPS and its augmentations free of charge. The policy promotes engagement with foreign GNSS providers while allowing for the possibility that they may be used to augment and enhance the resilience of GPS. It also requires investment in domestic capabilities to detect, mitigate, and increase resiliency to GPS interference while identifying and implementing redundant and backup systems as necessary for critical infrastructure and mission-critical functions.
 - ~~(U)~~ The 2010 FRP is the official source of radionavigation policy and planning for the government. It describes the USG's roles, responsibilities, and policies applicable to

¹⁰⁵ ~~(U)~~ National Security Presidential Directive-39 (NSPD-39): U.S. Space-Based Position, Navigation, and Timing Policy. December 15, 2004.

PNT systems. It also describes PNT user requirements, operating plans, and a national architecture for PNT systems that are provided by the USG.

- ~~(U)~~ The National PNT Interference Detection and Mitigation (IDM) Plan 2007 was developed by the Department of Homeland Security and required by the 2004 U.S. Space-Based PNT Policy. The plan identified key national PNT policy directives and responsibilities of departments, committees and working groups throughout the government. The plan recommended coordination of intelligence, incident reporting, and long-term strategies between the relative organizations.

~~(U)~~ **Executive Committees and Working Groups**

~~(U)~~ In 2004, the U.S. Space-Based PNT Policy created a set of interagency committees and working groups, including the National Executive Committee for Space-Based PNT (EXCOM) and the National Coordination Office for Space-Based PNT (NCO). These two entities and their respective working groups are responsible for overseeing and coordinating PNT policy.

- ~~(U)~~ The EXCOM was mandated by presidential directive in 2004 and is a senior-level body tasked with coordinating interdepartmental issues and providing advice to the departments and agencies responsible for the U.S. PNT architecture. The body is co-chaired by the Deputy Secretaries of the Departments of Defense and Transportation and includes representatives at the equivalent levels from the Departments of State, Commerce, and Homeland Security.
 - ~~(U)~~ The Executive Steering Group (ESG) consists of senior officials from each member of the EXCOM and representatives from other key agencies, such as the Federal Aviation Administration and the U.S. Air Force. The ESG provides the mechanism for elevating interagency issues to the level of the EXCOM and attempts to resolve issues that do not rise to that level.
- ~~(U)~~ NCO is responsible for organizing meetings, tracking projects and tasks, and coordinating interagency PNT documents. It is also responsible for developing the annual Five-Year National Plan for Space-Based PNT and overseeing its implementation.
 - (U) The National Space-Based PNT Systems Engineering Forum is a permanent working group under the authority of the NCO and is a forum for discussion and coordination of systems engineering issues and technology development opportunities for GPS-based applications and augmentations.
- ~~(U)~~ The GPS International Working Group was established by the Department of State in the 1990s and is a forum for developing, coordinating, and implementing international PNT strategies and agreements.

~~(U)~~ Annex L. GPS Disruption Threat Assessment [Classified]