APPENDIX A

GUIDELINES ON GNSS VULNERABILITY AND MITIGATION METHODS INCLUDING TERRESTRIAL, AIRBORNE AND PROCEDURAL SOLUTIONS

1. INTRODUCTION

1.1 GNSS is being progressively introduced throughout the world and has the potential to meet performance requirements for all phases of flight, obtaining safety and efficiency benefits through the navigation domain. As GNSS operations become prevalent, it is essential that the service providers identify the vulnerabilities of this system and develop the necessary mitigations. This paper identifies the vulnerabilities of GNSS and the corresponding mitigations that can be applied when appropriate. In developing this paper, several other vulnerability studies have been considered and their concerns and recommendations addressed. Most vulnerabilities discussed are common to other navigation systems providing aeronautical radio navigation service, but those systems are outside the scope of this paper.

2. GNSS SIGNAL VULNERABILITIES

2.1 Interference

2.1.1 GNSS core satellite constellations and satellite-based augmentation system (SBAS) signals are vulnerable due to their relatively low received signal power since GNSS signals originate from satellites and each satellite's signal covers a large fraction of the Earth's surface. While the very high frequency (VHF) data broadcast of a ground-based augmentation system (GBAS) is more difficult to interfere (its signal power is similar to that of terrestrial navigation aids), GBAS service depends on the core satellite signals. Interfering signals are limited to line-of-sight propagation. For example, the interference region at 600 m (2 000 ft) above ground level is inherently limited to approximately 110 km (60 NM) for a ground-based interferer.

2.1.2 The GNSS Standards and Recommended Practices (SARPs) require a specified level of performance in the presence of levels of interference as defined by the receiver interference mask. These interference levels are generally consistent with the International Telecommunication Union (ITU) regulations. Interference at levels above the mask may cause loss of service but such interference is not allowed to result in hazardous or misleading information.

2.1.3 *Unintentional interference*. The majority of reported GNSS interference events have been traced to on-board systems, and experience with GNSS installation has identified several sources of unintentional interference (e.g. spurious emissions or harmonics of VHF communications equipment and the out-of-band and spurious emissions from satellite communications equipment). Portable electronic devices can also cause interference to GNSS and other navigation systems.

2.1.3.1 Ground-based sources of interference currently include mobile and fixed VHF communications, point-to-point radio links operating in the GNSS frequency band, harmonics of television stations, certain radar systems, mobile satellite communication systems and military systems. The likelihood of such interference depends on State spectrum regulation, frequency management and enforcement within each State or region.

2.1.4 *Intentional interference.* Because of the low power of GNSS signals, it is possible for low power transmitters to jam the GNSS signal. While there have been no recorded instances of intentional jamming directed at civil aircraft, the possibility of intentional interference must be considered and evaluated as a threat.

2.2 **Spoofing**

2.2.1 Spoofing is the intentional corruption of the navigation signals to cause aircraft to deviate and follow a false flight path. Spoofing of satellite-based GNSS signals is technologically much more complex than spoofing of conventional ground-based navigation aids. Spoofing of the GBAS data broadcast is as difficult as spoofing conventional landing aids.

2.2.2 While spoofing can theoretically cause misleading navigation for a particular aircraft, it is very likely to be detected through normal procedures (e.g. by monitoring of flight path and distance to waypoints and by radar surveillance). Ground proximity warning systems (GPWS) and aircraft collision avoidance systems (ACAS) provide additional protection against collision with the ground and with other aircraft. In view of the difficulty in spoofing GNSS and the fact that unique operational mitigations are not deemed necessary, spoofing is not further addressed in this paper.

2.3 **Ionospheric and other atmospheric effects**

2.3.1 Heavy precipitation attenuates GNSS satellite signals by only a small fraction of 1 dB and does not impact operations. Tropospheric effects are addressed by system design and do not represent a vulnerability issue. There are two ionospheric phenomena that must be considered: rapid and large ionospheric changes, and scintillation. Ionospheric changes result in range errors that must be accounted for in system design. Scintillation may result in temporary loss of GNSS signals from one or more satellites.

2.4 **Other vulnerabilities**

2.4.1 The GNSS ground and space segment vulnerabilities also need to be considered. There is a risk of an insufficient number of satellites in a given constellation due to lack of resources to maintain a constellation, launch failure(s) or satellite failure. Constellation control segment failure or human error can potentially cause the failure of multiple satellites within a constellation.

2.4.2 Another risk is service interruption or degradation during a national emergency situation, where each State has the freedom of action as authorized by the Convention on International Civil Aviation (Article 89 refers). If signal denial is limited to a specific area, jamming of all civil GNSS signals would occur but the affected airspace would be closed to civil air traffic regardless. Another less likely situation would involve degradation or denial of core satellite or satellite augmentation signals throughout the coverage area.

3. ASSESSING GNSS OUTAGE RISKS

3.1 There are two principal aspects to be considered in the evaluation of the operational risks associated with GNSS vulnerabilities:

a) the likelihood of GNSS outage; and

b) the impact of GNSS outage.

3.2 By considering these aspects as a function of airspace, air navigation service providers can determine whether mitigation is required and, if so, to what level. Mitigation is required for outages with major impacts having a moderate to high likelihood of occurrence.

3.3 Assessing likelihood of GNSS outage

Interference

3.3.1 *Unintentional interference*. Operational experience is the best way to assess this risk. The likelihood of unintentional interference is often a function of geography. Large cities with significant radio frequency (RF) interference sources, industrial sites, etc., are more prone to the unintentional interference than remote regions. This interference is very unlikely in remote regions.

3.3.2 *Intentional interference*. Each State must consider the motivation to interfere with GNSS in determining the likelihood of intentional interference. The motivation may be driven by potential damage to a region and the operational impact on aviation and non-aviation applications. If there is minimal impact, the threat potential is low since there is no motivation to interfere. The extent of potential impacts may grow as applications using GNSS expand and the dependence on GNSS increases.

Ionospheric effects

3.3.3 Rapid and large changes in the ionosphere are frequently observed near the geomagnetic equator, but their effect is not large enough to impact en-route through non-precision approach operations. For approach with vertical guidance (APV) and precision approach (PA) operations, the effects of these changes can be assessed and mitigated when designing augmentation systems. In equatorial regions, the availability of APV and PA operations using a single GNSS frequency may be limited.

3.3.4 Ionospheric scintillation is insignificant at mid-latitudes. In equatorial regions, and to a lesser extent at high latitudes, scintillation may result in the temporary loss of one or more satellite signals. Operational experience in equatorial regions has shown that the probability of loss of existing GNSS service is remote due to the relatively large number of satellites in view. Scintillation can interrupt reception of broadcasts from a SBAS geostationary orbit (GEO) satellite.

3.4 Assessing impact of GNSS outage

3.4.1 The impact of a GNSS outage on navigation services depends on the following factors:

a) type of airspace: remedial action timing is more critical for a terminal area than for high altitude en-route airspace, and, for en-route airspace, is more critical for airspace where more stringent separation minima is established;

b) air traffic density: in regions with high traffic density, reliance on radar vectoring or pilot procedures may be impractical due to workload;

c) level of service: for less demanding operations dead reckoning may be all that is required to proceed to an area where GNSS service is available;

d) availability and equipage of other navigation systems: aircraft that can navigate with other means will not be affected;

e) radar surveillance: if primary or secondary radar is available, ATC will be able to provide more assistance to assure separation and divert to alternate airports;

f) extent of outage: the geographic extent and duration of a service interruption;

g) outage assessment: the ability of the air navigation service provider to quickly assess the extent of the service outage; and

h) weather conditions: while it is prudent to assume instrument meteorological conditions (IMC) when assessing outage impacts, the geographic extent of IMC and the meteorological parameters assumed in any analysis should be realistic.

3.4.2 The impact of a GNSS outage on other services should also be considered. GNSS is frequently used as a source of precision timing information within communication and radar systems, and may be used for automatic dependent surveillance (ADS) services. Timing vulnerabilities can be addressed through system design, and ADS applications are outside the scope of this paper.

4. REDUCING THE LIKELIHOOD OF GNSS OUTAGES

4.1 Installation and operation

4.1.1 On-aircraft interference can be prevented by proper installation of GNSS equipment, its integration with other aircraft systems (e.g. shielding, antenna separation, out-of-band filtering) and restrictions on the use of portable electronic devices on board aircraft.

4.2 Spectrum management

4.2.1 *Spectrum management*. Effective spectrum management is the primary means of mitigating unintentional interference from man-made transmitters. Operational experience has indicated that the threat of unintentional interference can become a rare event if effective spectrum management is applied. There are three aspects of effective spectrum management:

a) creation of regulations/laws that control the use of spectrum;

b) enforcement of those regulations/laws; and

c) vigilance in evaluating new RF sources (new systems) to ensure that they do not interfere with GNSS.

4.2.2 *Interference location and termination*. The ability to locate the interferer and terminate the interference to GNSS without delay is a critical aspect. The primary method of detecting interference is through pilot reporting. As many aircraft may experience outage simultaneously when interference first occurs, an automated method of reporting the outage (e.g. an automatic data link message) would reduce workload and facilitate defining the outage area and locating the interferer. Interference detection systems may be implemented in aircraft and on the ground.

4.3 New signals and constellations

4.3.1 New signals and core satellite constellations will significantly reduce the vulnerability of GNSS. The use of the stronger signals and diverse frequencies planned for GPS, GLONASS and Galileo will effectively eliminate the risk of unintentional interference, since it is highly unlikely that such an interference source would simultaneously affect more than one frequency. Additional satellites (including multiple constellations) will eliminate the risk of the complete outage of GNSS due to scintillation, and multiple frequencies will mitigate the impact of ionospheric changes. Future GEO satellites will mitigate the effect of ionosphere on SBAS by using satellites which lines of sight are separated by at least 45°. More robust GNSS signals and new frequencies make it more difficult to intentionally interfere with all GNSS services. Additional core satellite constellations mitigate the risk of system failure, operational errors or discontinuance of service. They may also continue to provide global service in the unlikely event that a provider of one GNSS element modifies or denies service due to a national emergency situation.

4.3.2 Robust system management and funding are essential to continued operation of GNSS services and mitigate the system vulnerabilities identified in paragraph 2.4, except for the potential for global interruption of service due to a national emergency. An effective means of avoiding a global interruption of service is for service providers to adopt a policy of specific area denial in the event of national emergency.

5. MITIGATING THE EFFECTS OF GNSS OUTAGES

5.1 Introduction

5.1.1 There are three principal methods currently available to mitigate the effects of GNSS outages on aircraft operations:

a) by taking advantage of inertial navigation systems and GNSS receiver technologies;

b) by employing procedural (pilot or ATC) methods; and

c) by taking advantage of terrestrial radio navigation aids used as a backup to GNSS or integrated with GNSS.

5.1.2 By adopting an effective strategy using one or more methods identified in this section, a service provider will not only ensure safe aircraft operations in case of GNSS outages but will also discourage the attempts of intentional interference by reducing the potential effects of these attempts.

5.2 Inertial navigation systems and receiver technologies

5.2.1 Inertial navigation system (INS) provides a short-term area navigation capability after the loss of GNSS or other position updating. Many air transport aircraft are already equipped with INSs and inertial systems become more affordable and accessible to operators with smaller, regional aircraft. This capability should therefore be considered when evaluating the need for terrestrial aids as mitigations for GNSS outages.

5.2.2 There are also technologies that add robustness to GNSS receivers to mitigate interference. Anti-jam technologies include advanced antennas (e.g. spatial nulling) and receiver signal processing techniques. As the cost of these technologies decreases, they may become more affordable alternatives to inertial navigation systems for small aircraft.

5.3 Procedural methods

5.3.1 If there is no other navigation system available in case of GNSS outage in non-radar airspace, aircraft can revert to dead reckoning, as most new aircraft navigation systems include an automatic dead reckoning capability. When possible, pilots can revert to visual navigation, exit the affected area or land at a suitable airport. In the event the GNSS capability is lost, ATC can assess the potential for loss of lateral separation and, where possible, use vertical separation instead.

5.3.2 The same procedures can be used in radar airspace, with the additional possibility for ATC to vector aircraft through the affected area, depending on the ATC workload and the number of impacted aircraft. For many current terminal operations, aircraft are already radar vectored to intercept a precision approach path.

5.3.3 In uncontrolled non-radar airspace, pilots can communicate with each other via air-to-air channel to maintain separation and attempt to determine the geographical extent of the outage.

5.3.4 Successful reliance on procedural means to assure separation and diversion depends upon all of the factors in paragraph 3.4. The most significant consideration is the extent to which aircraft are equipped with another means of navigation, such as inertial navigation.

5.3.5 Procedures and training for pilots and air traffic controllers should address the vulnerability of GNSS and identify how to respond effectively to interference and implement alternative procedures, and to report interference occurances and their location.

5.4 **Terrestrial radio navigation aids**

5.4.1 Currently, one of the most effective means of mitigating a GNSS outage is for aircraft to revert to using terrestrial navigation systems. As the transition to GNSS is accomplished and the terrestrial infrastructure is reduced, increased reliance will be placed on the other mitigation techniques. The operational capability required from a terrestrial infrastructure will evolve as GNSS operations become predominant and airspace and procedures rely increasingly on area navigation (RNAV) operations. A DME infrastructure can be used to provide an area navigation service for en-route and terminal operations for aircraft equipped with flight management systems that use multiple DMEs. This same capability can be used for RNAV approach operations if the DME coverage is sufficient.

5.4.2 For those cases where reversionary navigation does not provide an RNAV capability, the workload to transition to alternative routes and procedures must be considered. However, once the operations on these alternative routes are established, operations can continue as long as required in the event of sustained interference.

5.4.3 If it is determined that an alternate precision approach service is needed, instrument landing system (ILS) or microwave landing system (MLS) may be used. This would likely entail retaining a minimum number of such systems at an airport or within an area under consideration.

6. **CONCLUSIONS**

6.1 *Unintentional interference*. The likelihood and operational effect of interference varies with the environment. Unintentional interference is not considered a significant threat provided that States exercise proper control and protection over the electromagnetic spectrum for both existing and new frequency allocations. Furthermore, the introduction of GNSS signals on new frequencies will ensure that unintentional interference does not cause the complete loss of GNSS service.

6.2 *Intentional interference*. The risk of intentional interference depends upon issues that must be addressed by States. For States that determine that the risk is unacceptable in specific areas, safety and efficiency can be maintained by adopting an effective mitigation strategy through a combination of on-board mitigation techniques (e.g. use of INS), procedural methods and terrestrial navigation aids.

6.3 *Ionosphere*. Scintillation can cause loss of GNSS satellite signals in the equatorial and auroral regions, but is unlikely to cause complete loss of GNSS service and will be mitigated with the addition of new GNSS signals and satellites. Ionospheric changes may limit the SBAS and GBAS services that can be provided in the equatorial region using a single GNSS frequency, and must be considered when designing the augmentation systems.

6.4 *Other vulnerabilities*. Independently managed constellations, funding, and robust system design will significantly mitigate system failure, operational errors, and discontinuance of service.

6.5 States should assess the GNSS vulnerability for their airspace and select appropriate mitigations depending on the airspace in question and the operations that must be supported. These mitigations can ensure safe operations in transition to GNSS and enable States to avoid the provision of new terrestrial navigation aids, reduce existing terrestrial navigation aids, and discontinue them in certain areas.

ATTACHMENT

EXAMPLE GNSS VULNERABILITY ASSESSMENT

Guidelines for evaluating the impact and likelihood of a GNSS outage is provided in section 3 of this paper. This appendix provides two examples of how this methodology can be applied to existing GNSS operations. These examples do not take into account future GNSS signals or constellations.

1. **Congested airspace — Mid-latitudes.** The following example applies to the existing GNSS operations in airspace with a high density of aircraft operations, and a mid-latitude region with effective spectrum management.

1.1 *Unintentional interference.* Unintentional interference has been encountered in North America and Europe. In North America, there have been seven confirmed cases of interference to GPS in the last few years. Based on operational experience, unintentional interference is unlikely but cannot be neglected.

1.2 *Intentional interference.* For current operations, there is no significant motivation to deliberately interfere with GNSS. No case of intentional interference in civil environment has been reported so far. The likelihood of this interference is negligible for existing operations. The threat of intentional interference may change over time as reliance on GNSS increases.

1.3 The impact of interference is to cause a GNSS outage within the line of sight of the interferer. The majority of air carrier operators in these regions are equipped with inertial navigation and/or an FMS with a DME/DME RNAV capability. DME facilities are available in the majority of airspace. While some aircraft are not equipped with an independent RNAV capability, safety for these aircraft can be maintained and operations can continue, perhaps with reduced efficiency. Therefore, a unintentional and intentional interference have a moderate impact.

1.4 *Spoofing*. There is no significant threat due to spoofing, and the impact would be moderate.

1.5 *Ionospheric effects*. For mid-latitudes, ionospheric scintillation that causes loss of GNSS positioning has never been experienced, so the likelihood of occurrence is negligible. There would be no operational impact due to the short duration of the event and the available terrestrial navigation aids and high level of equipage to use those aids.

1.6 *Summary*. Table 1 summarizes the likelihood and operational impact of the vulnerabilities that have been identified. The table maps the likelihood of occurrence against the operational impact. The State should mitigate any vulnerability that is remote and has a severe impact, or probable and has any impact. In addition, consideration should be given to vulnerabilities that are remote and have a moderate impact.

2. **Remote areas — Equatorial.** The following example applies to the existing GNSS operations in remote airspace with a low density of aircraft operations in an equatorial region with effective spectrum management.

2.1 *Unintentional interference.* Most sources of unintentional interference are less likely in remote regions. With effective spectrum management, the likelihood of interference in these areas may be negligible. The impact of outage may be moderate to severe due to unavailability of radar services.

2.2 *Intentional interference.* Intentional interference has not been encountered, and there is no significant motivation to deliberately interfere with GNSS given the low density of operations and the remote areas. The likelihood of this interference is considered to be negligible for existing operations. The threat of intentional interference may change over time as reliance on GNSS increases. The impact of intentional interference is the same as unintentional interference.

2.3 *Spoofing.* There is no significant threat due to spoofing, and the impact would be moderate.

2.4 *Ionospheric effects.* For equatorial regions, ionospheric scintillation that impacts GNSS performance is likely to occur. The operational effect is moderate, since it is typically a degradation in performance and not a complete loss of navigation capability. In the event that a complete loss of positioning occurs, it does not persist for very long and the low density of operations ensures continued safety.

2.5 *Summary.* Table 2 summarizes the likelihood and operational impact of the vulnerabilities that have been identified. The most significant issue is the potential for ionospheric scintillation. States should take action to reduce the impact of this effect. This can be accomplished through:

a) operational procedures that ensure continued operation during brief GNSS outages; and

b) continued research on the duration and likelihood of severe scintillation.

Table 1. Congested airspace — Mid-latitudes

		Operational impact		
		No impact	Moderate impact	Severe impact
Likelihood	Negligible	Ionospheric effects	Intentional interference; Spoofing;	
	Remote		Unintentional interference	
	Probable			

Table 2. Remote areas — Equatorial

		Operational impact		
		No impact	Moderate impact	Severe impact
Likelihood	Negligible		Unintentional and Intentional interference; Spoofing	
	Remote			
	Probable		Ionospheric effects	

3. When the analysis shows there is no critical vulnerabilities, implementation of spectrum management measures is still essential to reduce, as much as possible, the occurrences of service interruptions.

— — — — — — — —