

GPS Jamming/Spoofing Guidance for Mid-Cabin Gulfstream Aircraft with Collins Aerospace Flight Management Systems

Introduction

GPS interference, whether it is jamming alone or jamming along with deceptive data input to the navigation system - referred to as “spoofing” - has become a significant concern for all operators. There are reports of these events occurring daily around the World, and persistently in areas of conflict.

There are several global locations that have consistent reports of GPS signal interference. In other cases, reports of unexpected events occur from operations far from conflict zones that seem to coincide with local military activity. This article is intended to provide guidance for both situations for Mid-Cabin Gulfstream aircraft equipped with Collins Aerospace FMS, i.e., G150, late production G200 and G280.

GPS Jamming vs. GPS Spoofing

So, what is the difference between GPS jamming and GPS Spoofing? GPS jamming occurs when the GPS signal is lost or is blocked. This is similar to the condition in Fig. 1, in which the GPS was depowered when the FMS was powered-up in a G280. For these instances, the navigation system will recognize the loss of input and revert to secondary navigation references per design, DME/DME or VOR/DME and IRS, if installed.

GPS spoofing occurs when a counterfeit GPS signal is substituted for the true GPS signal in such a way that the navigation system does not recognize the substitution. It will not revert to the secondary sources but will use the counterfeit signal as if it were reliable because it does not recognize that the signal is illegitimate.



Fig. 1. Collins FMS-6200 CDU at power-up with no GPS input. Note that the power-up default time and date is 00:00 UTC on 01 Jan 1970, GNSS NOT AVAILABLE is displayed in the message line, and the actually valid active database is shown as invalid per the amber display due to the incorrect system date and time.

GPS/GNSS signals are weak because they involve communications with orbital satellites at considerable distance from our aircraft. As such, these signals can be overpowered by ground-based interference at closer distances. However, the systems are designed to reject signals that are not considered reasonable, based on a comparison between where the airplane was and where it interprets its position to be. This process occurs continuously.

Therefore, “spoofing” of a GPS receiver must be preceded by a jamming event in which the previous position information is gradually removed from the system logic. At that point, the incorrect position, time, or altitude information can be applied to the GPS because there is no way for the GPS receiver to determine if the signal is reasonable or not.

Indications of GPS Interference

GPS interference can be identified in several ways. There may be sudden changes in distance to the next waypoint in the flight plan or in time required to get there. The MAP may “shift” laterally very rapidly. GPS time in the CDU may become stationary and inaccurate, as may position and altitude information. ATC may start inquiring about having you switch transponders or verifying position, based on the erroneous ADS-B data that they are receiving.

In addition to FMS, other systems rely on GPS to function properly; including ADS-B Out, SVS (G280, if installed), EGPWS/TAWS, Electronic Charts (if installed, for geosynchronous indications), and SMS/TLAF (G280, if installed). ATN/CPDLC may be logged-off due to erroneous time information. Systems in the cabin may also be affected. DU MAP displays may show close proximity to terrain while at cruise with associated TAWS alerts. Ka-Band or other internet systems in the cabin that rely on accurate position data for communication will likely be unavailable.



Fig. 2. FMS-6200 CDU LRN POS DATA page. This page may show that the FMS and GNSS positions are frozen during a spoofing event, while the IRS will continue to update, if installed.

ADS-B Out Fail SVS Fail

Fig 3. CAS messages that may appear in the G280. G150 and G200 will have illuminated annunciator lights for ADS-B anomalies.

There may also be indications on the PFD and CDU itself, including “GNSS NOT AVAILABLE”, “CHECK POSITION,” or “LOW POS ACCURACY” in the CDU message line. The removal of SVS graphical information with an “SVS” cyan flag may appear in the PFD.

As stated in ALL-MOL-23-0015 and ALL-MOL-23-0018, and guidance from the FAA and EASA, it is important to notify ATC as soon as the crew becomes aware that GPS interference is occurring and to request vectors or other assistance as needed to navigate the aircraft on the desired path. It is also important to communicate to ATC that ADS-B information coming from your aircraft could be inaccurate. If the crew receives an alert from EGPWS or TCAS and is unable to immediately determine that the alert is erroneous, the crew should follow the published procedures for responding to the given alert. Do not hesitate to respond appropriately to one of these alerts if it occurs, as it cannot be assumed that it is false.

More generalized information from the FAA and EASA can be found at the following:

[FAA Safety Alert For Operators \(SAFO\) 24002, Recognizing and Mitigating Global Positioning System \(GPS\)/Global Navigation Satellite System \(GNSS\) Disruptions.](#)

[EASA Safety Information Bulletin \(SIB\) 2022-02R3, Global Navigation Satellite System Outage and Alterations Leading to Communication / Navigation / Surveillance Degradation.](#)

These publications have been updated periodically over the last several months. Crews are advised to reference the most current versions of these documents.

Mitigation or Avoidance Procedures

Mitigating the effects of GPS interference depends on the conditions under which the event occurred. The best mitigation, of course, is to avoid the area where interference has been occurring. There are industry sources and government notices that indicate areas that are at risk. Fight crews are encouraged to find alternate routes between destinations that avoid areas of known GPS interference. However, Gulfstream recognizes that this is not always feasible or possible, so the following mitigations are recommended.

Scenario 1: Unexpected GPS Interference During Normal Operations

If the crew encounters GPS interference unexpectedly during the execution of a normal flight, the crew should first do the immediate notifications and make requests for assistance from ATC as described above. This unexpected event poses the most workload for the crew to reestablish navigation capability of the scenarios discussed.

The second step, if the course line is displayed on the MAP near where the airplane is thought to actually be, is to select a VOR from the MAP display near that line and tune it into NAV1 and NAV2. Select the bearing pointers for these VORs on the MAP and HSI displays for an RMI indication. This can be accomplished through the SMCs on G280 and there are also provisions for these displays in the G150 and G200. It is important not to tune a VOR near the MAP aircraft position, because it may be outside the usable service volume of the actual nearest VOR.

Selecting these options for the HSI can be accomplished during preflight setup, so only the VOR would need to be tuned if the aircraft is out of the usable service volume of an automatically tuned VOR. VOR frequencies can be tuned using 3-letter identifiers for VORs that are contained in the Navigation Database.



Fig. 4. SMC HSI Configuration page. LSK 2R and 3R can then be used to select navigation sources for the RMI bearing pointers on the HSI. For mitigation against loss of positional awareness during GPS interference, VOR 1 and VOR 2 are recommended.



Fig. 5. FMS-6200 CDU with NAV1 and NAV2 manually tuned to separate VORs. Note that manually selecting a VOR, either by tuning from the Navigation Database as shown above, or directly entering the frequency, will disable AUTO TUNE (if enabled during power-up) for each NAV receiver that has been manually tuned. This prevents the displayed VOR (or ILS LOC) from changing automatically without crew selection or notification.

GPS Jamming/Spoofing Guidance – Collins FMS



Fig. 6. DU3 indications in G280 with FMS 3 selected using DME/DME, VOR/DME, and IRS only for position reference. Note the RMI bearing pointers showing relative bearings to two VORs as well as DME indications for both stations, and the EPU value is 0.35. This is typical for DME/DME input within the usable service volumes of VORs when GPS is disabled or unavailable.

Ensure that DME/DME and VOR/DME are ENABLED on the CDU FMSX VOR/DME CONTROL page. This is selectable as follows: INDEX > NEXT (2/3) > LSK 1L (FMSX VOR/DME CTL). It is one LSK above the GNSS CTL, as shown in Fig. 7. All sensors will normally default to the ENABLED condition when the aircraft is powered-up, so this is a verification step.

Step three, and most importantly, is to remove the GPS/GNSS input to each FMS and thereby remove the corrupt data. To begin, select each installed CDU GNSS to DISABLD for its associated FMS, as shown in Fig. 9. The path to this page is INDEX > NEXT (INDEX 2/3) > LSK 2L (FMS X GNSS CTL) (Fig. 8).

Removing the GPS/GNSS signal from the FMS will facilitate regaining more accurate navigation data but will do nothing to restore normal operations to other systems that consume GPS/GNSS signals directly. These include EGPWS/TAWS, ADS-B Out, ATN/CPDLC and systems in the cabin.



Fig. 7. FMS3 VOR/DME CONTROL page showing VOR/DME and DME/DME use enabled.



Fig. 8. FMS CDU INDEX page 2/3, showing paths to VOR/DME CTL and GNSS CTL. Note that FMS CTL is also selectable from this page, to be discussed later.

GPS Jamming/Spoofing Guidance – Collins FMS



Fig. 9. FMS CDU showing GNSS CONTROL page with both GNSS receivers disabled (DISABLD, as shown at LSK 1L and 2L). To get all FMS to disregard GPS signals, deselection of GNSS receivers will need to be performed on all installed CDUs, as each is associated with a different FMS.

It may be necessary to request vectors from ATC or use VOR navigation to get to a known VOR location while disabling the GPS receivers. The NAV source can be selected to NAV1 and NAV2 for flight guidance, which will display an HSI with a CDI for easier navigation than the RMI. It is then a matter of keeping up with the passage of VORs and appropriate frequency management.

Once a VOR has been tuned and the crew is comfortable using it as a reference, the FMS position may be updated using the location of the VOR. The path to this page is INDEX > POS INIT > NEXT (POS INIT 2/3). Select the LSK associated with UPDATE FROM NAVAID (5L). It may be necessary to enter a NAVAID identifier in the LSK 5R field first. The radial and distance from the selected VOR will be shown with a CONFIRM POS prompt. This is because the FMS does not have an internal history of how it arrived at the point you are trying to input. The system will not permit UPDATE FROM NAVAID to be performed unless the airplane is airborne. There is also a selection on this page for LAT/LON to be entered, if desired.

Once the FMS position is updated, DME/DME and VOR/DME should be sufficient to provide adequate navigation via FMS, which can then be

reselected, so long as the airplane remains within the usable service volumes of VOR and DME facilities. In LNAV, some systems tend to hunt for a heading when using DME/DME or VOR/DME reference. If observed to do this, it is recommended to track the course using HDG mode for the AFCS.

Most GPS interference activities are relatively local in nature, usually covering 100 to 150 NM, because of the ground-based nature of the equipment that is used for spoofing.

The GPS altitude may be quite close to the ground, which could trigger false EGPWS alerts. Keep in mind that the aircraft cannot meet the RNP requirements for certain procedures when using DME/DME or VOR/DME navigation, so ATC should be advised. If there are no usable VOR/DME facilities in range and there is no optional IRS on the aircraft, the FMS will go into Dead Reckoning navigation mode, using what it was doing before the signal was lost as a reference for what it needs to do next and providing steering inputs without any position updates. If operating in a remote or oceanic environment, this could pose a test of airmanship and navigation skills. It is important to keep up with the oceanic trip log and perhaps observe other aircraft nearby to stay on your desired track (assuming that aircraft is not also having navigational difficulties).

Remember, the portable GPS receiver that you may have on your EFB or other device is probably subject to the same jamming and spoofing activities as the aircraft, so it will not be a reliable source of position information.

Recovery of GPS navigation after exiting an area of GPS interference is discussed below.

GPS Jamming/Spoofing Guidance – Collins FMS

Considerations for Aircraft Equipped with IRS

Inertial Reference Systems (IRS) are not standard but are available as options on Mid-Cabin aircraft. The IRS is the lowest-priority navigation sensor to the FMS and will not be used by the system until DME/DME and VOR/DME solutions are no longer available.

The FMS with IRS installed in Mid-Cabin aircraft uses a different hybrid navigation solution than what is used on Large Cabin Gulfstreams. In normal operations, the FMS position when sourced from the IRS is updated from raw IRU data that is corrected using hybrid algorithms that are heavily weighted in favor of GPS sensor input. It is important to deselect both GPS sensors on the associated FMS as soon as feasible when GPS interference is detected to prevent bias in the hybrid algorithm that could affect IRS data as shown from the associated FMS. Since the corrections are made within the FMS and not the IRU, there are no steps required to deselect Hybrid FMS, only the GNSS sensors.

Once GPS is deselected on the FMS associated with the IRS, the accuracy of position is dependent upon the length of time since position was initialized and the drift rate that is inherent to a given IRU when there is an absence of other types of sensor data. However, in most cases, the IRS is a suitable alternative for short-duration navigation during a period of GPS spoofing if there are no usable VOR/DME facilities in range.

A recent informal evaluation of IRS-only navigation was performed on a G280 in the fleet. The aircraft was in domestic RNP-2 airspace, using a valid GPS enabled FMS for flight guidance on FMS1. DU3 was set to FMS3 to monitor IRS performance. After the IRS was the only source of navigation information (DME/DME and VOR/DME manually disabled), the EPU gradually increased but stayed within limits for RNP-2 for approximately 15 minutes. Given that most remote airspace has a higher RNP value, there would be a longer time that the IRS could be used for navigation in that airspace. In addition, this IRS was never using GPS previously during the flight, it had been initialized with GPS disabled. Therefore, it was not in a hybrid update state at the beginning of the

evaluation. The IRS may provide adequate navigation until exiting the area of GPS interference and reestablishing a normal navigation configuration and it is certainly a better navigation source than dead reckoning.

Pilots are encouraged to review the AFMS for the specific IRS installed in the aircraft prior to utilizing it as the sole source of navigation information. These supplements are included in the STC Airplane Flight Manual Supplements (AFMS) section in PlaneBook, and hard copies are provided in the Supplements section of the AFM on the aircraft.

GPS Jamming/Spoofing Guidance – Collins FMS



Fig. 10. G280 DU3 with IRS ONLY MSG displayed near HSI. This message occurs when the IRS is the only sensor used by the FMS and other criteria are present as stated in the Gulfstream G280 Pro Line Fusion Flight Management System v3.6.1 Pilot Guide, available in PlaneBook.

EPU in this case has exceeded RNP at approximately 15 minutes, as indicated by the amber digits. The RMI bearing pointers are not presented because a VOR frequency change is in progress, but they will reappear momentarily.

GPS Jamming/Spoofing Guidance – Collins FMS

Scenario 2: Flight Transiting an Area of Known GPS Interference En Route

If flight through an area of known or anticipated GPS interference is unavoidable, there are steps that a crew can take to mitigate the effects of GPS jamming and spoofing.

Plan the flight so as to always remain within the usable service volumes of VOR/DME facilities and positive ATC communication and control. It is best to simply file and fly established airways, which provide the above unless specifically noted otherwise on the charts or by NOTAM. Do not attempt the flight with any inoperative navigation or communication equipment, even if allowed by the MMEL. Attempt to avoid operating in low IMC due to the likelihood of erroneous EGPWS alerts.

When setting up the flight deck, ensure that once the position has been initialized, one FMS has GNSS disabled. For aircraft with the third FMS (IRS), FMS3 should have GNSS disabled. Ensure that DME/DME and VOR/DME are enabled for all FMS installed as shown in Fig. 11. If the aircraft only has two FMS, disable GNSS on FMS2. This can be done prior to entering the area of known or suspected GPS interference and does not have to be the navigation state for the entire flight.

Prior to entering the suspected interference area, the crew should also display VOR and DME information, either with the RMI indications as discussed above or by selecting VOR as the NAV source for the non-coupled side of the cockpit. The crew should also monitor the displays for any anomalous indications, as well as the LRN POS DATA or a GNSS STATUS page for early indications of interference. If interference is encountered, flight guidance can be transferred to FMS 2 or NAV 1 or 2 if proceeding to a VOR. Monitor EPU values, which should stay at approximately 0.35 NM if DME/DME is being used. If GNSS HEIGHT is low, anticipate possible erroneous EGPWS alerts.



Fig. 11. G280 with optional third FMS and IRS set up for flight through an area of suspected GPS interference. Note that FMS1 and FMS2 are using GPS and that FMS3 has GNSS DISABLD. It will use DME/DME, VOR/DME and IRS for position information, in that order.

GPS Jamming/Spoofing Guidance – Collins FMS

Scenario 3: Aircraft Will Depart from or Arrive at an Airport with Known GPS Interference

For an aircraft that will depart an airport with known GPS interference in the vicinity, it is advisable to disable GNSS receivers for all FMS installed prior to takeoff. Check your personal devices. If you have a navigation app on your phone that shows an accurate location for you, you can probably do a POS INIT using GPS while on the ground, then disable the GNSS as described above. This is because the interfering equipment antenna is often pointed skyward and may not affect signals on the ground unless one is very close to it. Ensure all other sensors are enabled for all FMS, and display VOR/DME information for immediate use using bearing pointers.

If it is determined that the GPS signal is invalid at power-up, disable the GNSS to all FMS, then input the correct UTC and DATE on the STATUS page. Follow the prompts, there will be a REQ PEND message on the CDU for several seconds while this data is manually entered. Once correct data is entered, the ACTIVE DATA BASE should change from amber to white.

Next, select POS INIT and select the LAT/LON associated with the airport identifier to set the FMS position. You will be prompted with RESET INITIAL POS on the message line of the CDU if the initialized position is greater than 40 NM from the last known position of the FMS, which could occur if the GPS had been spoofed even though the airplane is still in the same location. Follow the prompts to re-enter the position.

Pressing TOGA without a new flight plan entered and no valid GPS signal will send the aircraft FMS position to the takeoff position of the departure runway that was initialized during the previous flight. This will also be accompanied by a RESET INITIAL POS message on the CDU. Once the new flight plan is entered, pressing TOGA will set the airplane position to the end of the departure runway. When only using DME/DME and VOR/DME for navigation, it is recommended that TOGA or RUNWAY UPDATE (CDU LSK 6L) is pressed while in position on the departure runway to get the most precise FMS location feasible.

Plan to exit the area using conventional VOR/DME navigation and file known routes that can be conducted using these sources. RNP departures are not usable in most cases due to DME/DME restrictions. Monitor EPU during departure. Notify ATC of possible erroneous ADS-B Out information. It is likely that local ATC is knowledgeable of the interference and may have established procedures.

If inbound to an airport with known or suspected interference, set up the aircraft as described in Scenario 2, but attempt to transition to full DME/DME and VOR/DME navigation well before the GPS interference area is entered. Plan to fly conventional ILS, LOC or VOR approach procedures for arrival. Avoid low IMC operations.

Reestablishing GPS Navigation After Exiting the Area of GPS Interference

Monitor the GNSS STATUS page for at least one GPS receiver. Once the data starts to update and the position is no longer static, it is likely that the airplane is exiting the area of interference. Just as an area of jamming was encountered before the area of spoofing, an area of jamming will also be encountered prior to exiting the interference area as the aircraft moves away from the counterfeit signal antenna and back into an area of legitimate GPS satellite signal coverage.

Select FMS CONTROL to INDEP while reestablishing GNSS input to the FMS. One at a time, select one GNSS to ENABLE on one FMS CDU, then repeat for the other GNSS on the other CDUs after verifying the signal is correct. If the GPS has been significantly spoofed, the GPS may not find the current location to be reasonable and may not recover on its own. If this is the case, check the time and date on the STATUS page for accuracy and reset to correct values.

If this does not work, for the G150 and G280 it is permissible to pull and reset the associated GPS CB, one at a time. For the G280, these are located at M17 and M18 on the OHP. For the G150, they are located at E10 and F10 on the OHP. This should re-initialize the GPS receiver as if powering up the airplane. In the G280, the GPS 1 Fail and GPS 2 Fail amber CAS messages will assert while the associated CB is pulled.

For G200 installations, there is variance in the CB panels and all aircraft may not have specific GPS circuit breakers. Ensure that you know what other systems may be affected by pulling a CB that is not specific to a GPS receiver.

Once valid GPS navigation has been reestablished and verified for all installed FMS, the FMS CONTROL can be reset to SYNC and the flight may resume normally. However, some GPS-dependent systems may not recover for the duration of the flight.

When configuring the G280 for normal operations, it may be necessary for the copilot to select FMS2 after using FMS3. Note that this typically places both pilots on FMS1 momentarily

during the transition. If landing performance has been initialized, it may drop out of the FMS and need to be reinitialized. There may also be a loss of VSD for several seconds. Crews are encouraged to stay alert for such dropouts of information in the G150 and G200 as well when switching between navigation sources.

Conclusion

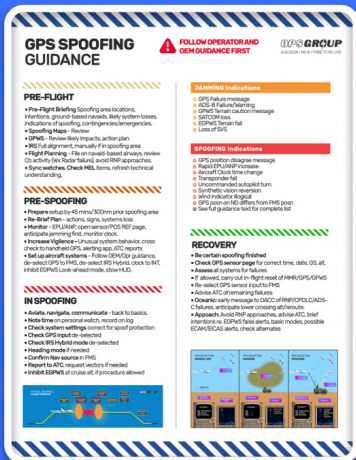
Aircraft can be safely operated within areas of GPS interference using conventional navigation sources, ATC services, and good airmanship. The most workload-intensive GPS interference situation is one in which the GPS is rendered unreliable with no prior notice or expectation. These recommendations provide guidance for the crew to maintain or regain situational awareness during such an event. If an area of known or anticipated GPS interference is to be operated within, use this guidance and recommended practices to avoid loss of positional awareness during these operations, should such an event occur.

Regardless of the conditions under which the aircraft is subjected to GPS interference, crews need to adhere to procedures regarding alerts that may be activated by erroneous GPS signals, unless it can be immediately determined that the alert is triggered in error.

Systems that rely on GPS/GNSS signals may be rendered unreliable or inoperative during the event and may remain so for the duration of the flight.

Crew Guidance

GPS SPOOFING



Best practices for spoofing regions

Actions before, during and after spoofing

Typical spoofing flight profile

GPS SPOOFING GUIDANCE



**FOLLOW OPERATOR AND
OEM GUIDANCE FIRST**

OPS GROUP
AUG 2024 / NO © / FREE TO RE-USE

PRE-FLIGHT

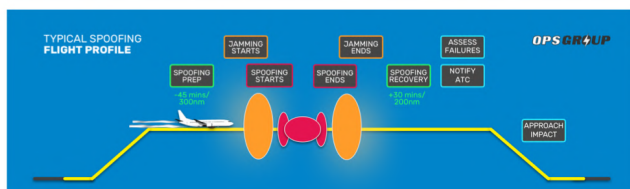
- **Pre-Flight Briefing** Spoofing area locations, intentions, ground-based nav aids, likely system losses, indications of spoofing, contingencies/emergencies.
- **Spoofing Maps** - Review
- **GPWS** - Review likely impacts, action plan
- **IRS** Full alignment, manually if in spoofing area
- **Flight Planning** - File on nav aid-based airways, review Cb activity (Wx Radar failure), avoid RNP approaches.
- **Sync watches, Check MEL** items, refresh technical understanding,

PRE-SPOOFING

- **Prepare** setup by **45 mins/300nm** prior spoofing area
- **Re-Brief Plan** - actions, signs, systems loss
- **Monitor** - EPU/ANP, open sensor/POS REF page, anticipate jamming first, monitor clock.
- **Increase Vigilance** - Unusual system behavior, cross check to handheld GPS, alerting app, ATC reports
- **Set up aircraft systems** - Follow OEM/Opr guidance, de-select GPS to FMS, de-select IRS Hybrid, clock to INT, inhibit EGPWS Look-ahead mode, stow HUD.

IN SPOOFING

- **Aviate, navigate, communicate** - back to basics.
- **Note time** on personal watch, record on log
- **Check system settings** correct for spoof protection
- **Check GPS input** de-selected
- **Check IRS Hybrid mode** de-selected
- **Heading mode** if needed
- **Confirm Nav source** in FMS
- **Report to ATC**, request vectors if needed
- **Inhibit EGPWS** at cruise alt, if procedure allowed



JAMMING Indications

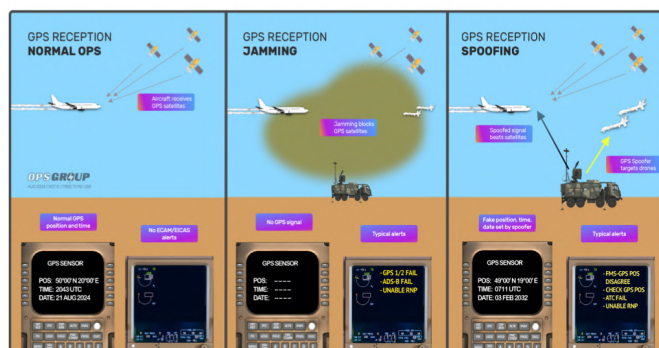
- GPS Failure message
- ADS-B Failure/Warning
- GPWS Terrain caution message
- SATCOM loss
- EGPWS Terrain fail
- Loss of SVS

SPOOFING Indications

- GPS position disagree message
- Rapid EPU/ANP increase
- Aircraft Clock time change
- Transponder fail
- Uncommanded autopilot turn
- Synthetic vision reversion
- Wind indicator illogical
- GPS posn on ND differs from FMS posn
- See full guidance text for complete list

RECOVERY

- **Be certain spoofing finished**
- **Check GPS sensor page** for correct time, date, GS, alt.
- **Assess** all systems for failures
- If allowed, carry out in-flight reset of MMR/GPS/GPWS
- Re-select GPS sensor input to FMS
- Advise ATC of remaining failures
- **Oceanic:** early message to OACC of RNP/CPDLC/ADS-C failures, anticipate lower crossing alt/reroute.
- **Approach:** Avoid RNP approaches, advise ATC, brief intentions re. EGPWS false alerts, basic modes, possible ECAM/EICAS alerts, check alternates






Crew Guidance

If you are operating a flight into a spoofing area **tomorrow**, this guidance will help to mitigate the impact of GPS Spoofing.

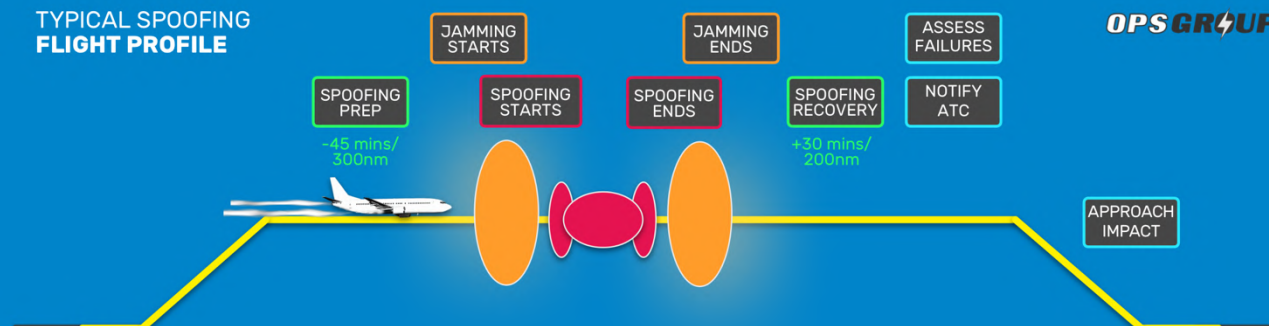
This is based on best practices collected from the flight crew participating in the GPS Spoofing Workgroup, as well as OEM and other expert input.

Nothing here is intended to replace or override company procedures, OEM advice, or legal requirements.



TYPICAL SPOOFING FLIGHT PROFILE

OPS GR4UP



Pre Flight

- Refresh systems knowledge
- Crew Briefing: Spoofing plan
- IRS alignment

Pre-Spoofing

- Rebrief plan, signs of jamming/spoofing
- System prep (eg. GPS Off)
- Monitor sensors
- Consider contingencies

Spoofing

- Expect jamming, then spoofing
- May be multiple cycles
- Conventional nav
- Report to ATC

Recovery

- Be certain GPS interference finished
- Re-select GPS sensors
- Assess failed systems and impact

Enroute

- Oceanic: advise ATC early of failures
- CPDLC, ADS-C, Wx Radar, may remain failed
- Review EGPWS actions
- Consider contingencies

Approach

- Anticipate system issues, false EGPWS, EICAS warnings
- Check RNP capability
- Brief spoofing impact on app.

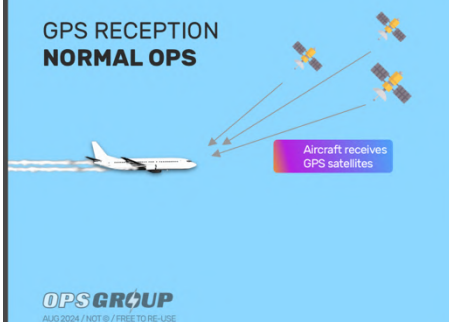
Post Flight

- Report spoofing
- Tech log
- Maint: GPS hard reset may be req'd

GUIDANCE OVERVIEW

REFER TO FULL MITIGATION LIST
GPS SPOOFING WORKGROUP 2024

GPS RECEPTION NORMAL OPS



OPS GR4UP
AUG 2024 / NOT 10 / FREE TO RE-USE

Normal GPS position and time

No ECAM/EICAS alerts



GPS RECEPTION JAMMING

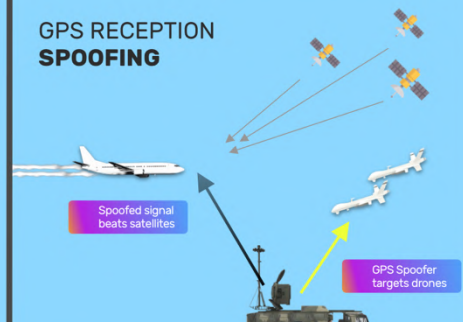


No GPS signal

Typical alerts



GPS RECEPTION SPOOFING



Fake position, time, date set by spoofer

Typical alerts



Pre Flight

Pre-Flight Briefing

For flights into known spoofing areas, include GPS Spoofing as a full briefing item. Consider:

- Likely entry and exit points of spoofing areas
- Intentions before, during, and after spoofing
- Availability of ground-based Navaids
- Likely system downgrades/losses (e.g. EGPWS, Weather radar, CPDLC, RNP)
- Expected indications of jamming, indications of spoofing
- Contingency planning (e.g. Engine failure, depressurization) in spoofing area
- Impact of spoofing on RNP requirements later in flight

Spoofing Maps

Check online spoofing map for latest locations of active spoofing. Knowing where the spoofing is happening is the best mitigation. (e.g. SkAI Live GPS Spoofing Tracker Map)

GPWS

Specifically review likely EGPWS impact, brief actions for EGPWS alerts in cruise, use of Terrain Override, EGPWS alerts on approach below MSA. Plan action in case of repeated EGPWS alerts on second approach in case of EGPWS response. Review difference between basic GPWS alerts and enhanced/Look-Ahead alerts. Be fully prepared for unusual EGPWS behavior.

IRS

Perform a full IRS Alignment for each flight into known spoofing areas. If departing from an airport within a spoofing area (e.g., LCLK, LLBG, OLBA), perform manual IRS alignment. Caution risk of IRS automatically taking GPS position.

Flight Planning

If practical, file airways associated with ground based nav aids. Review GPS required routes, RNP-1 or -2 airways. Consider alternate routes further from the spoofing area. Review forecasted Cb activity, considering Weather Radar failure is possible. Consider if destination requires RNP approaches.

Contingencies/Emergencies

Consider the impact of spoofing on a diversion while in the spoofing area, or afterwards. Conventional arrival and approach / missed available or daylight VMC from MSA down. Review safe altitudes enroute (MEA/MORA) and at destination/alternate on approach (MSA).

Refresh Technical Understanding

Review difference between GPS Spoofing and GPS Jamming. Know which aircraft systems use GPS (long list!). Loss of ADS-B, SVS, GPWS etc. is not possible to be avoided. Refresh conventional navigation skills, be aware that most enroute airspace isn't actually RNP airspace. Spoofing takes place in areas with low Navaid coverage - may be many hundreds of miles between DMEs and VORs. Understand difference between Conventional/Standalone IRS and Hybrid IRS (B787, G650 etc.).

Synch watches

Synch mechanical watch to known source (e.g. iPhone) at dispatch, in preparation for aircraft clock failure.

NO-TAMS

Don't rely purely on NOTAMs to give comprehensive warnings of spoofing locations.

Crosscheck MEL items

Consider the impact of any MEL (Minimum Equipment List) items. Review impact of unserviceable system items in light of expected GPS Spoofing impacts, especially any inoperative radio navigation items.

Operations at airports WITHIN spoofing areas

- Expect on-ground spoofing, which creates greater risk of system impacts
- **IRS Alignment:** Turn off the GPS receiver via the FMC prior to aligning the IRS, and carry out a manual alignment. Be vigilant for automatic capturing of the spoofed GPS position during alignment.
- Do not plan GPS/RNP approaches, SIDs, STARs, into/out of known spoofing areas



Pre-Spoofing

Prepare for spoofing

Commence preparation and system setup well prior to first expected spoofing location.
Spoofing area ETA -45 minutes, or 300 nm is suggested.

- Consider declining direct routings to remain on airway, especially if airway is based on NavAids.
- Evaluate emergency descent and diversion options with regard to spoofing impact on systems

Re-Brief plan

A quick re-brief of actions when spoofing is encountered. Intentions, and expected systems loss, e.g. ADS-B, CPDLC. Re-brief EGPWS actions in event of alert in cruise.

Monitor

Monitor EPU (Estimated Position Uncertainty) and ANP (Actual Navigation Performance) values. Open Sensor/Pos Ref page for GPS status. Anticipate jamming to commence before spoofing: the typical spoofing encounter now commences with a period of GPS jamming, which makes the GPS receiver more vulnerable to spoofing. Monitor aircraft clock for jumps or changes.

Increase vigilance

- Keep an eye on all aircraft systems for unusual behavior.
- Monitor aircraft position and navigation system status using all available means, including use of a handheld GPS e.g. Bad Elf, Garmin, iPad/iPhone, EFB. Keep the antenna of the external GPS system in sight of satellites but as shielded from the

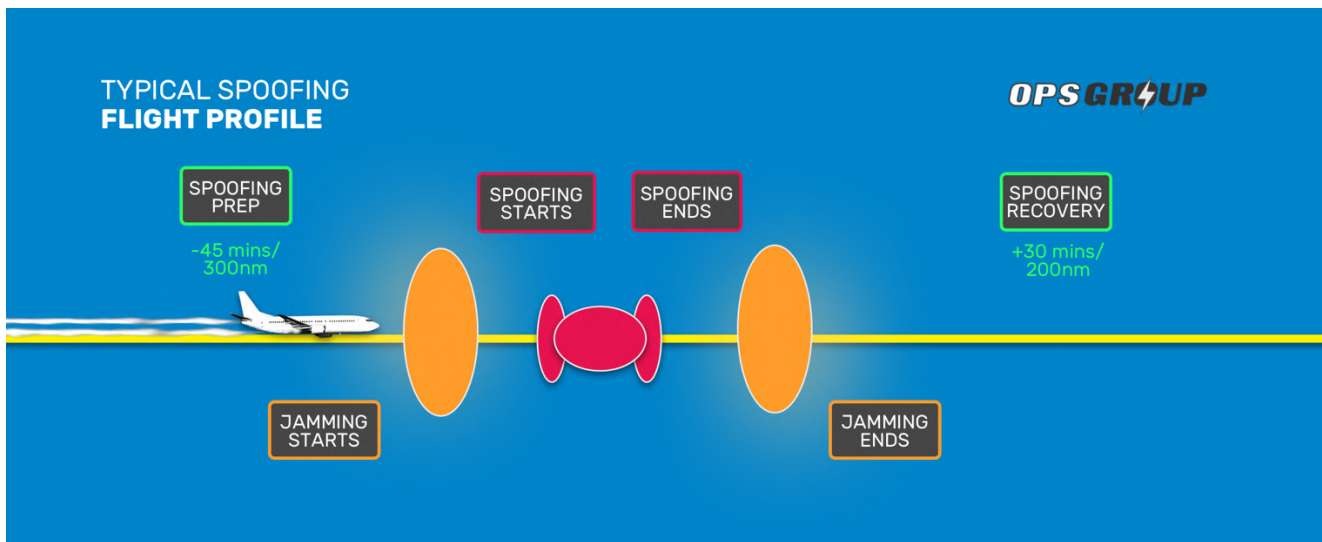
horizon as possible, using glareshield or aircraft frame. Any disagreement between aircraft GPS and external GPS will suggest spoofing.

- Use an alerting App such as APG's NaviGuard. Regularly cross-check aircraft system indications to standalone systems (e.g. Watch, VOR/DME position, EFB/External GPS) to detect spoofing early.
- Listen out for ATC or other aircraft reports of spoofing
- Be ready to apply systems setup as soon as typical initial warnings occur, in case of surprise/early spoofing encounter.
- Have Nav Log (OFP/CFP) tracks, times, distances ready to assist with manual/DR navigation.
- Keep an eye on GPS date (in sensors page). A date change is a strong indicator of likely problems recovering the GPS receiver post-spoofing.

Set up aircraft systems

- Always follow OEM and Operator Procedure as primary spoofing setup guidance.
- **De-select GPS input to FMS.** Note that this will only prevent the FMS position from including spoofed GPS values, but will not protect other systems e.g. EGPWS, Weather Radar.
- **Deselect "IRS HYBRID" mode** if applicable.
- **Set the aircraft clock to "Internal" (INT)** / manual, if possible, to protect CPDLC and other datalink functions.
- If procedure approved - **Inhibit EGPWS Look Ahead mode** to prevent false alerts at cruise altitude.
- Stow **Head Up Display** and do not use.

Within Spoofing Area



Typical indications of Jamming

It is common for jamming to precede spoofing. Jamming will result in the loss of GPS Signal only. The time from jamming to spoofing varies.

- **GPS Failure message**
- **ADS-B Failure/Warning**
- **GPWS Terrain caution message**
- **Loss of Ka SATCOM**
- **EGPWS Terrain fail**
- **Loss of SVS**

Typical indications of Spoofing

Unlike jamming, a GPS signal is present, but it has fake information. False GPS position, time, and date information will be processed by the GPS receiver as being valid. As soon as this is fed to other systems, failure messages will begin.

- **Rapid EPU or ANP increase**
- **GPS position** and IRS or FMS position disagree caution message
- **Aircraft Clock time changes**, or difference between Capt/FO clocks
- **Transponder failure**: EICAS/ECAM "ATC FAIL"
- **Autopilot turns aircraft unexpectedly**
- **ADS-B Failure/Warning**
- **Synthetic Vision** reverting to blue over brown
- **Loss of enhanced display**, such as display of terrain on PDI
- **Wind indication** on ND is illogical or has a major shift - erratic groundspeed
- **GPS position symbol** on ND drifts away from the FMS and the IRS symbols
- **Datalink** (CPDLC, ADS-C) failure warning
- **GPS information on sensor page** shows unusual values: altitude, etc.
- **Handheld GPS** (e.g. Garmin, iPad) **disagrees** with aircraft GPS position
- **EGPWS** audible warning ('Pull Up')
- **GPS 1 and 2 dramatically different** i.e. more than 100 meters, which may also give an ECAM/EICAS GPS miscompare warning.
- **Spoofing Alerting app** e.g. Naviguard gives alert
- **ACARS message** from ground/ops advises of spoofing (based on aircraft downlink message with unusual values).

Actions following confirmation of active spoofing

- **Aviate, navigate, communicate** – back to basics.
- Note the time on personal watch, record on log.
- Check system settings are correct for spoofing protection. Also applies to unexpected "surprise spoofing".
- **Check GPS input de-selected**
- **Check IRS Hybrid mode de-selected**
- **Heading mode**: Consider selecting heading mode to keep the aircraft on track during troubleshooting
- Confirm Nav Source in FMS: DME/DME, IRS, etc.
- **Report to ATC**. Advise ATC of spoofing encounter ASAP. Include position so that other crew on frequency are aware.
- **Request ATC vectors** or confirmation of correct position and track if required.

- If company procedures allow, **inhibit EGPWS at cruise altitude** (TERR OVRD). This avoids false "PULL UP" etc. warnings triggered by spoofed altitude data.
- Use **Conventional Navigation**
- Check Aircraft Clock Time and compare to current time.
- Check **GPS Date** on sensors page. A change of date, especially forward in time, is likely to create greater GPS receiver problems after spoofing.
- **FMS Auto-tune** may not function correctly (uses GPS to check Navaid position).
- **Set reminders** based on waypoint or coordinates (not time) to reverse all system settings changed for spoofing.



Recovery

Most spoofing encounters can be fully recovered from in flight. However, an increasing number of aircraft are left with severe impacts to navigation, communications, and safety systems (e.g. EGPWS) that are not recoverable before reaching destination.

Before beginning recovery, be certain that spoofing has finished. Double check known spoofing location map, and be alert to the possibility that another round of spoofing may occur. Allow a time period of normal GPS readings, e.g. 10 minutes.

Indications that spoofing is complete

The following items may be helpful to identify the end of GPS Spoofing:

On Sensors/Pos Ref page, GPS shows:

- Correct UTC time and date, **and**
- GS (Ground Speed) consistent with TAS, ND, **and**
- Consistent position and altitude

Actions after exiting spoofing area

- **Re-select GPS** sensor input to FMS
- **Assess** all systems for failures, especially Weather Radar, CPDLC/Datalink,
- If required, and if procedure exists/allows, carry out **in-flight reset of MMR/GPS Receiver**
- If required, and if procedure exists/allows, carry out **in-flight reset of GPWS computer**



ATC

- Advise ATC of any relevant systems remaining failed, e.g. Nav, CPDLC, ADS-C and impact on navigation (e.g. Unable RNP)
- Disregard any CPDLC mandate for domestic FIR's – airspace entry will not be denied.
- **If planning an oceanic crossing** with degraded RNP or Comms systems, advise the first oceanic ACC well before Oceanic Entry. For example, Shanwick requests a freetext remark in the RCL message at OEP -90, "RMK/RNP 10 ONLY DUE GPS INTERFERENCE / NO CPDLC"
- **For the NAT HLA**, note that RNP4 is required for PBCS tracks, as well as CPDLC and ADS-C for the RCP/RSP requirement. Elsewhere in the HLA, RNP 10 is the minimum, but RNP4 is often used for tactical separation outside the NAT PBCS Tracks. If you are RNP10 only, **expect lower crossing altitudes and reroutes**.
- Request to follow STARs (/SIDs) based on conventional nav aids.
- Avoid/decline RNP approaches.



Destination/Alternate Approach considerations

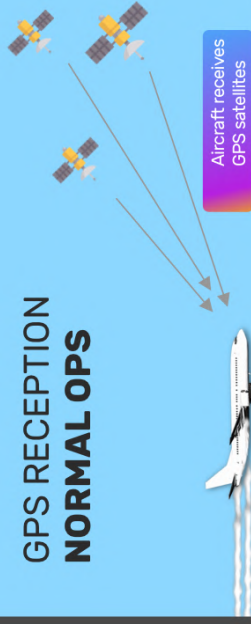
- **Even if the GPS receiver appears normal** after spoofing, there is a risk of later failure or incorrect behavior. This is because the spoofing may have contaminated the receiver settings. In most cases, only a hard reset will guarantee receiver integrity.
- **Avoid RNP approaches** unless there is certainty that all systems are operating normally. Check missed approach for any RNP/RNAV requirement.
- **Advise ATC** of your earlier GPS interference, e.g. "Due to earlier GPS interference, unable xxx approach, request xxx approach". This will also give ATC a heads-up to monitor your tracking more closely.
- **Brief intentions re. GPWS responses.** Expect false EGPWS alerts, but re-brief to be clear on difference between GPWS basic mode alerts (Radio Altimeter based) and EGPWS alerts (GPS altitude based). Ensure all basic GPWS mode alerts are followed without delay, as these are not affected by spoofing. Brief intentions for different alert types.

- **Brief possible ECAM/EICAS alerts** on descent and approach, especially ones that may occur on final approach but can be disregarded, e.g. RNP related warnings.
- **Check alternate** non-GPS approach availability.

Post Flight

- **File an Air Safety Report** for tracking of the GPS Spoofing problem.
- **Tech Log:** Note any GPS Spoofing in the aircraft tech log each flight, to ensure a hard reset of the GPS / MMR is carried out
- For any unusual system impacts, send data to avionics manufacturers e.g. Honeywell, Collins.

GPS RECEPTION NORMAL OPS

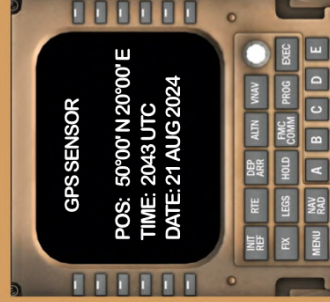


Aircraft receives
GPS satellites

OPS GROUP
AUG 2024 / NO © / FREE TO RE-USE

Normal GPS
position and time

No ECAM/EICAS
alerts



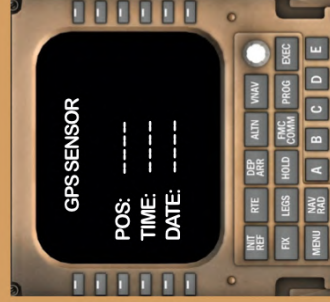
GPS RECEPTION JAMMING



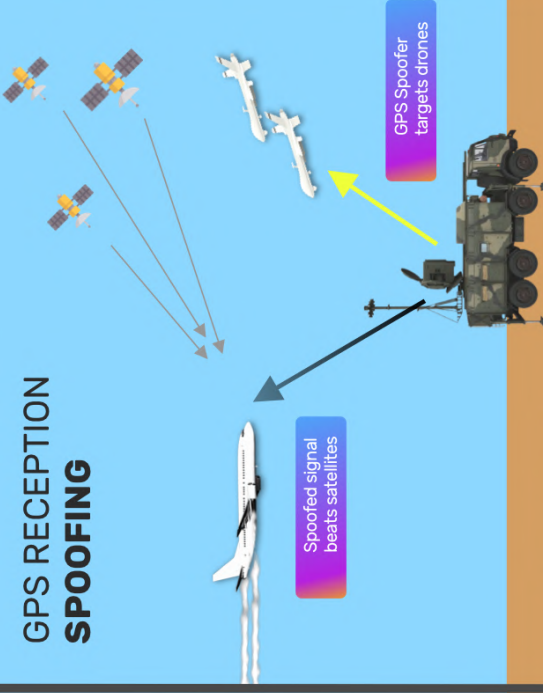
Jamming blocks
GPS satellites

No GPS signal

Typical alerts



GPS RECEPTION SPOOFING



Spoofed signal
beats satellites

GPS Spoofer
targets drones

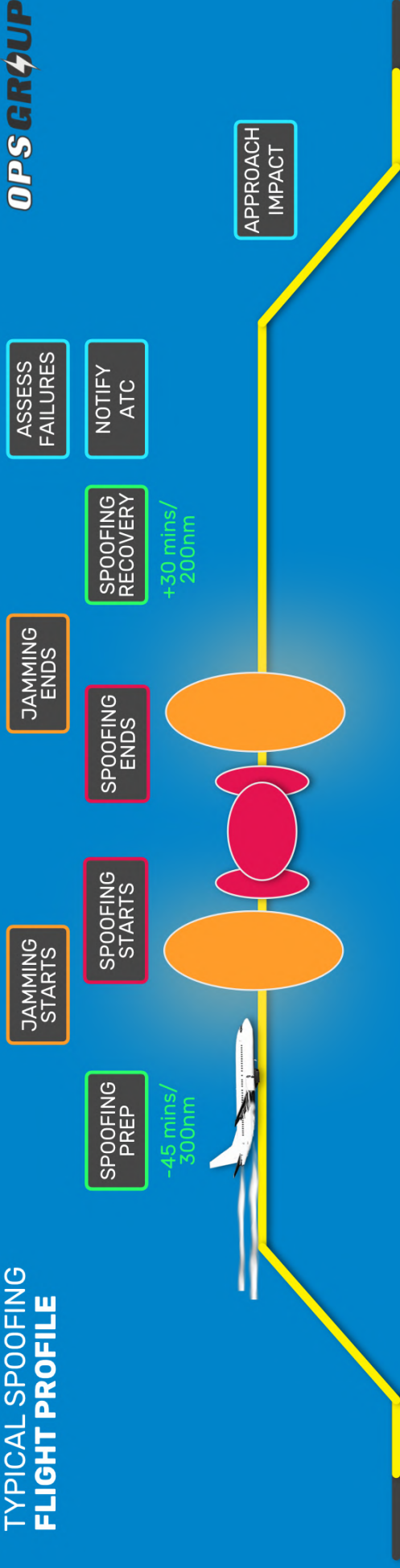
Fake position, time,
date set by spoofer

Typical alerts



TYPICAL SPOOFING FLIGHT PROFILE

OPS GR4UP



Pre Flight

- > Refresh systems knowledge
- > Crew Briefing: Spoofing plan
- > IRS alignment

Pre-Spoofing

- > Rebrief plan, signs of jamming/spoofing
- > System prep (eg. GPS Off)
- > Monitor sensors
- > Consider contingencies

Spoofing

- > Expect jamming, then spoofing
- > May be multiple cycles
- > Conventional nav
- > Report to ATC

Recovery

- > Be certain GPS interference finished
- > Re-select GPS sensors
- > Assess failed systems and impact

Enroute

- > Oceanic: advise ATC early of failures
- > CPDLC, ADS-C, Wx Radar, may remain failed
- > Review EGPWS actions
- > Consider contingencies

Approach

- > Anticipate system issues, false EGPWS, EICAS warnings
- > Check RNP capability
- > Brief spoofing impact on app.

Post Flight

- > Report spoofing
- > Tech log
- > Maint: GPS hard reset may be req'd

GUIDANCE OVERVIEW

REFER TO FULL MITIGATION LIST
GPS SPOOFING WORKGROUP 2024