on a procedure affected by an expired or unsatisfactory flight inspection, or a procedure that is based upon a recently decommissioned NAVAID.

4. Pilots may not substitute for the NAVAID (for example, a VOR or NDB) providing lateral guidance for the final approach segment. This restriction does not refer to instrument approach procedures with "or GPS" in the title when using GPS or WAAS. These allowances do not apply to procedures that are identified as not authorized (NA) without exception by a NOTAM, as other conditions may still exist and result in a procedure not being available. For example, these allowances do not apply to a procedure with an expired or unsatisfactory flight inspection, or is based upon a recently decommissioned NAVAID.

5. Use of a suitable RNAV system as a means to navigate on the final approach segment of an instrument approach procedure based on a VOR, TACAN or NDB signal, is allowable. The underlying NAVAID must be operational and the NAVAID monitored for final segment course alignment.

6. For the purpose of paragraph c, "VOR" includes VOR, VOR/DME, and VORTAC facilities and "compass locator" includes locator outer marker and locator middle marker.

d. Alternate Airport Considerations. For the purposes of flight planning, any required alternate airport must have an available instrument approach procedure that does not require the use of GPS. This restriction includes conducting a conventional approach at the alternate airport using a substitute means of navigation that is based upon the use of GPS. For example, these restrictions would apply when planning to use GPS equipment as a substitute means of navigation for an out–of–service VOR that supports an ILS missed approach procedure at an alternate airport. In this case, some other approach not reliant upon the use of GPS must be available. This restriction does not apply to RNAV systems using TSO–C145/–C146 WAAS equipment. For further WAAS guidance, see paragraph 1–1–18.

1. For flight planning purposes, TSO-C129() and TSO-C196() equipped users (GPS users) whose navigation systems have fault detection and exclusion (FDE) capability, who perform a preflight RAIM prediction at the airport where the RNAV (GPS) approach will be flown, and have proper knowledge and any required training and/or approval to conduct a GPS-based IAP, may file based on a GPS-based IAP at either the destination or the alternate airport, but not at both locations. At the alternate airport, pilots may plan for applicable alternate airport weather minimums using:

(a) Lateral navigation (LNAV) or circling minimum descent altitude (MDA);

(b) LNAV/vertical navigation (LNAV/VNAV) DA, if equipped with and using approved barometric vertical navigation (baro-VNAV) equipment;

(c) RNP 0.3 DA on an RNAV (RNP) IAP, if they are specifically authorized users using approved baro-VNAV equipment and the pilot has verified required navigation performance (RNP) availability through an approved prediction program.

2. If the above conditions cannot be met, any required alternate airport must have an approved instrument approach procedure other than GPS that is anticipated to be operational and available at the estimated time of arrival, and which the aircraft is equipped to fly.

3. This restriction does not apply to TSO-C145() and TSO-C146() equipped users (WAAS users). For further WAAS guidance, see paragraph 1–1–18.

1–2–4. Recognizing, Mitigating, and Adapting to GPS Jamming and/or Spoofing

a. The low-strength data transmission signals from GPS satellites are vulnerable to various anomalies that can significantly reduce the reliability of the navigation signal. The GPS signal is vulnerable and has many uses in aviation (e.g., communication, navigation, surveillance, safety systems and automation); therefore, pilots must place additional emphasis on closely monitoring aircraft equipment performance for any anomalies and promptly inform Air Traffic Control (ATC) of any apparent GPS degradation. Pilots should also be prepared to operate without GPS navigation systems.

b. GPS signals are vulnerable to intentional and unintentional interference from a wide variety of sources, including radars, microwave links, ionosphere effects, solar activity, multi–path error, satellite communications,