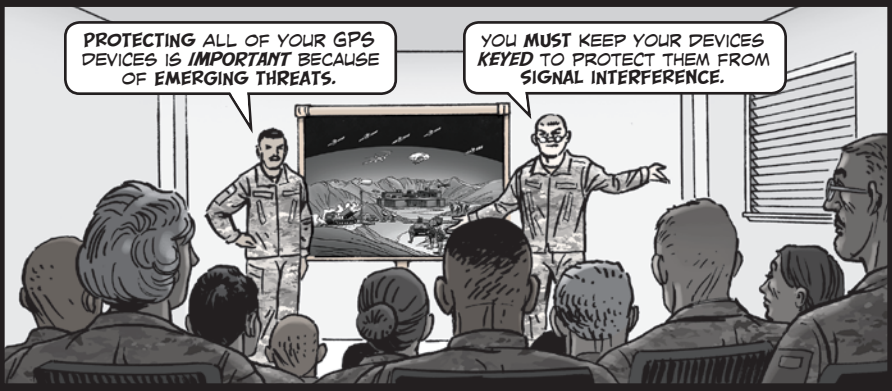
Keying is the Key to GPS Protection!



Keying is the Key

For maximum performance for military operations, you need to ensure that every selective availability anti-spoofing module (SAASM)-equipped GPS device is always COMSEC keyed. This includes the well-known DAGR, as well as the embedded receivers "hidden" inside many other weapon systems.

Emerging threats make the electromagnetic environ-ment more challenging than ever for low-power radio signals like GPS. Loading all SAASM receivers with COMSEC key materials is your best defense against signal interference. When keyed, your GPS receiver provides the highest possible level of anti-spoofing protection, including positioning, navigation and timing (PNT) accuracy. When your GPS receiver is keyed, it tracks the military GPS signal, Precise Positioning Services (PPS).

An unkeyed SAASM-based GPS receivers are no better than standard commercial GPS receivers. When your GPS receiver is unkeyed, it is only tracking the commercial GPS signal, Standard Positioning Service (SPS). And that presents an increased risk to military operations.

All units with SAASM-based GPS devices ***must*** have current COMSEC keys loaded before their receivers are used in combat, combat support or combat service support operations. That means you must perform pre-combat checks (PCCs) and pre-combat inspections (PCIs) to ensure that your equipment is keyed. There are two types of SAASM-based GPS: embedded and stand-alone.

Keep DAGR keyed for maximum performance

Embedded SAASM Devices

Some line replaceable units (LRUs) with embedded GPS cards aren't routinely opened at the unit level. These systems are required to provide access points for key-fill.

Check your equipment carefully. If it has a key-fill device, review the TMs to determine if the GPS key-fill is required. If so, follow the TM instructions to maintain the key.

Stand-alone GPS Receiver

The primary stand-alone device is the AN/PSN-13A defense advanced GPS receiver (DAGR), NSN 5825-01-526-4783. Units must maintain keys in all DAGRs regardless of how they're used.

DAGRs have a custom key-fill connector interface that requires a special key-fill adapter cable, NSN 5995-01-521-3185, to connect with the fill device. You can quickly verify the current key by checking the DAGR display screen.

Note About DAGR GPS Keys

Maintaining the DAGR COMSEC key can be a burden for operators. To relieve that hardship, the GPS system offers over-the-air key distribution (OTAD). That reduces the need for physical keying to just once a year. The OTAD software was released under MWO 11-5820-1172-23-1. You can get a copy of the MWO and the software at the PNT website:

https://www.pmpnt.army.mil

For help with keying your DAGRs, contact PM PNT's Stephen Morrissey at (478) 926-9511 or by email: **stephen.r.morrissey.civ@mail.mil**

If you need help with keying other stand-alone or embedded GPS systems, contact the project/program/product manager or the sustainment agency responsible for the end item.

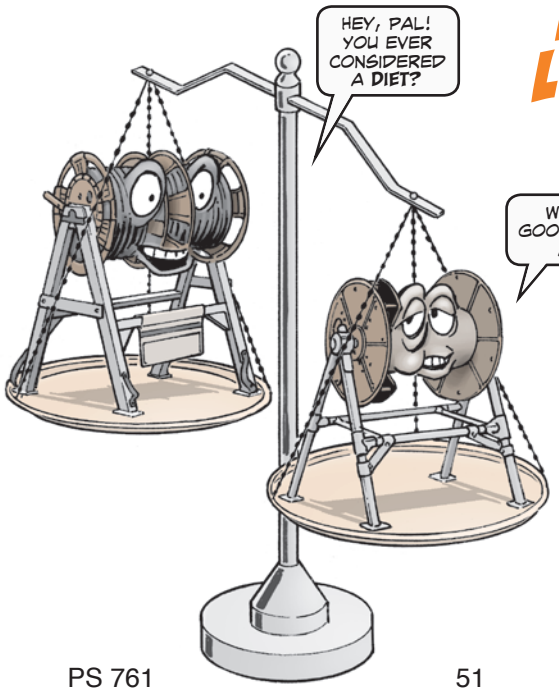
To use OTAD, your DAGR must have MWO 11-5820-1172-50-1 applied. The MWO covers turning in the obsolete AN/PSN-13 DAGRs that cannot use latest operating software (OS) or the OTAD signal. It also details upgrading the affected AN/PSN-13A DAGRs. The details of that MWO are addressed in CECOM Maintenance Advisory Message 2014-07-0002 (6 May 14), which can be found on the PNT website.

More information about how to confirm OTAD is working on your device is in the latest change to the DAGR's TM 11-5820-1172-13&P (May 14/Ch 1, Aug 15). You'll find it on the LOGSA ETM website: **https://www.logsa.army.mil/etms**

PS END

RL-309/U Cable Reel Stand...

NEW STAND LIGHTER FOR LUGGING



When it's time to lay or recover commo cable, using the old RL-31 cable reel stand can provide quite a workout. When you combine the stand's 59 pounds with body armor, a backpack and weapons, you're lugging a heckuva lot of weight!

PS MORE