

JSP 602 Instruction	1041	Applicability	Applications, Data/Information, Infrastructure, Integration, Network/Communications
Configuration Identity	Version: 01.01 Amended: 2009-03-10 Reviewed: 2009-03-10	Epoch Applicability	2008 - 2013

JSP 602: 1041 – Procurement of Navstar GPS Receiving Equipment to provide Position Velocity and Timing Data for use by UK Defence Forces

Outline

Description: This leaflet defines the policy covering the provision and use of GPS Navstar receiving equipment within UK Defence for all position, velocity, and timing applications. It is inclusive of any equipment capable of receiving signals supporting either or both of the GPS Standard Positioning Service (SPS) and the Precise Positioning Service (PPS). The GPS Navstar satellite constellation is controlled and operated by the US DoD, who have offered access to the authorised PPS restricted access service to their NATO allies via a multilateral MOU. The US endorsed definitions of SPS and PPS are:

- SPS GPS. The SPS is a civil service provided by signals transmitted on the GPS L1 frequency and modulated using an unencrypted coarse acquisition code (C/A-code). Most legacy PPS User Equipment also uses the C/A code as an aid to acquire the Precision code (P-code) which, when encrypted, is referred to as Y-code; or P(Y)-code.
- PPS GPS. The PPS is a military service provided by signals transmitted on GPS L1 & L2 frequencies, modulated using encrypted codes. Currently, PPS is supported by the Y-code. A new encrypted Military code (M-Code) is in development. M-code uses a technique to spectrally separate the energy from the civil frequencies centred at L1 and L2. Both Y-code and M-Code provide a more robust signal structure than the C/A-code used with SPS.

Reasons for Implementation: This policy shall be implemented to avoid the known vulnerabilities associated with SPS GPS. It is also necessary to maintain uniformity of information across the UK MoD and with our NATO and other allies to aid interoperability and delivery of coherent capability.

Issues: Failure to follow policy will result in vulnerabilities and may result in interoperability issues with our NATO Allies and in particular US Armed Forces.

Guidance: This policy is consistent with UK EW Policy and our NATO commitments under NATO MOU IV concerning Navstar GPS. In accordance with the MOU, the UK GPS Project Office (PO) (DE&S AirS2P2 IPT) has been identified to the US Authorities as the single UK focal point for PPS GPS issues.

The default for all UK MoD use of GPS shall be PPS GPS unless it can be clearly demonstrated that to do so will be operationally more limiting.

Policy

Strategic

1041.01: General MoD GPS Policy

1041.01.01 The UK MoD Policy on GPS, stipulates that; UK Forces shall be equipped and undertake military operations with PPS GPS User Equipment because of the increased signal robustness, unless to do so can be clearly demonstrated to be operationally more limiting. Neither shall they operate with PPS equipment in the SPS mode (i.e. a PPS capable receiver not loaded with a valid operational cryptographic key). Overall responsibility for platform capability remains with the platform-owner DEC.

1041.02: GPS PPS Cryptographic Requirements

1041.02.01 Although PPS GPS equipment employ cryptographic processes and require loading with cryptographic keys they are not themselves controlled cryptographic items. The requirements of JSP 602, Leaflet 1032 with respect to the generation of a GPS Key Management Plan (KMP) have been met by the UK GPS PO's own overarching Key Management Plan for the UK GPS Project. However, individual programmes employing PPS GPS remain responsible for developing a programme specific Appendix to the overarching GPS KMP detailing key material and data loader requirements. Programmes that have crypto requirements over and above those of simply PPS GPS may prefer to include all their crypto requirements in a single programme specific KMP and therefore will not need to produce an Appendix for the GPS PO's KMP. Copies of the UK GPS Project KMP and sample Appendices are available from the UK GPS PO website.

1041.03: Waiver Process for Policy Non-Compliance

1041.03.01 The above general policy foresees the possibility that in certain special circumstances it might be operationally more limiting to use PPS GPS. If the responsible DEC and procuring IPT believe this to be the case they shall contact the JSP 600 Secretariat who will direct them to the relevant Subject Matter Experts to examine the case and explain the process and additional requirements.

1041.04: Provision for Accounting for PPS GPS equipment and Security Devices

1041.04.01 All PPS GPS equipment contain security devices that have been bought from the US through a foreign military sales (FMS) process. These security devices are accountable items and equipment containing PPS GPS receivers are controlled accountable items. All losses including those arising from expending GPS guided munitions are to be notified to the UK GPS PO via the procuring/managing IPT. Full details of accounting requirements are contained in the Joint Services Policy and Procedures for the use of GPS NAVSTAR by UK MoD and Defence Contractors (Latest Issue). Types of devices and accounting requirements are:

1041.04.01.01 The PPS Security Module and Auxiliary Output Chip (AOC) based legacy GPS equipment have the marking "(SM)" adjacent to the part number, these components are accountable by quantity.

1041.04.01.02 The current Selective Availability Anti-Spoofing Module (SAASM) based equipments can be identified by the marking "(Contains ASD)" adjacent to the part number, these equipments are accountable by individual SAASM multi chip module linked to the unique equipment serial number. Special accounting rules apply when SAASM based PPS GPS equipment is in the possession of MoD contractors.

Strategic (Continued)

1041.05: <u>Planning for PPS GPS Equipment Disposal</u>

1041.05.01 As PPS GPS equipments are controlled accountable items they cannot be locally scrapped or sent for disposal through normal Defence Sales channels. IPTs managing PPS GPS equipment should make contract provision for recovery of the security devices contained within the PPS receiver via a procedure approved by UK GPS PO as part of the Through Life Management Plan (TLMP). This will apply both to mid-life upgrades as well as final disposal. The UK GPS PO will arrange return of security devices to the US for authorised destruction.

Deployed

As for Strategic Domain

Tactical

As for Strategic Domain

Remote

As for Strategic Domain

Responsibility for Implementing the Policy

Implementation of this policy shall be the responsibility of all MOD Projects and their suppliers.

Procedure

All PPS GPS equipment integrations are subject to the GPS Host Application Equipment (HAE) Certification procedure to be performed by the UK GPS PO.

All MoD Contractors handling SAASM based PPS GPS equipment will be subject to site inspections and audits by UK GPS PO for compliance with SAASM accounting procedures.

Relevant Links

UK Joint Electronic Warfare Policy, CDS Policy 01/06, D/DJtCap/13/J5/EW1, dated 23 Dec 05

Memorandum of Understand Number IV Among the NATO Nations Concerning the Navstar Global Positioning System (including Addendum 3)

[DCI GEN 305/04 UK MoD Global Positioning System \(GPS\) Project Office](#)

[JSP602: 1032 – Cryptography and Key Management](#)

UK MoD Navstar Global Positioning System Programme Key Management Plan - KMP Number 03010A dated May 2003

Joint Services Policy and Procedures (JS P&P) for the use of GPS NAVSTAR by UK MoD and Defence Contractors (Latest Issue)

A glossary of terms and abbreviations used within this document is available [here](#).

Instructions on how to read a JSP602 leaflet are available [here](#).

Compliance

Stage	Compliance Requirements
Initial Gate/DP1	SPS/PPS GPS <ul style="list-style-type: none">• Possibility of solution containing GPS capability identified• Engagement with UK GPS Office to ensure availability of expert advice is planned during Assessment• Draft TLMP recognises possibility of PPS GPS accountability and disposal requirements
Main Gate/DP2	<ul style="list-style-type: none">• Confirm the capability is likely to contain GPS PPS GPS <ul style="list-style-type: none">• Involve UK GPS PO in the tender evaluation team• TLMP includes details of accountability and disposal requirements• Procurement Strategy recognises FMS case is required for PPS security components• SRD refers to JS P&P document SPS GPS <ul style="list-style-type: none">• Waiver request raised via JSP 600 Secretariat• Case for SPS GPS use endorsed by UK GPS PO• DEC Risk Owner accepts the limitations of SPS GPS• SRD includes requirement to output a warning that data source is SPS GPS• Acceptance Trials include NavWar assessment
Release Authority/DP5	PPS GPS <ul style="list-style-type: none">• TLMP requirements for accountability and disposal enacted SPS GPS <ul style="list-style-type: none">• Results of NavWar acceptance testing reflected in Training/Manuals