# APPENDIX H

# SAMPLE TECHNOLOGY ASSESSMENT/CONTROL PLAN

**TECHNOLOGY ASSESSMENT/CONTROL PLAN**

**MEMORANDUM OF AGREEMENT (MOA)**

**BETWEEN DOD AND [COUNTRY X]**

**FOR ACCESS TO**

**GLOBAL POSITIONING SYSTEM (GPS) PRECISE POSITIONING SERVICE**

## I. PROGRAM CONCEPT

A. **Scope:** This program offers access to the military signals from the United States (U.S.) Department of Defense (DoD) Navstar Global Positioning System (GPS) to **Country X** for mutual military purposes. It formally designates **Country X** as an authorized user of the GPS military signals, called the Precise Positioning Service (PPS). In accordance with established U.S. DoD GPS policy, prior to becoming an authorized military user of GPS-PPS, any foreign nation must conclude a formal agreement with the U.S. DoD covering access to and security of the PPS. In general, authorized users of PPS may be the military organizations of allied and friendly nations with which the U.S. promotes interoperability or may plan to conduct joint military operations. Where, under previous programs with NATO, some co-development was involved, under this program all GPS-PPS equipment will be procured from the U.S.

B. **GPS Description:** The GPS is a space-based positioning and navigation system developed by the DoD. It is intended to provide precise, three-dimensional position and velocity, as well as time, to an unlimited number of users possessing receive-only equipment. GPS information is continuously available on a worldwide basis, at any altitude, and in any weather. The GPS provides two services, or levels of accuracy, the PPS and the Standard Positioning Service (SPS). The PPS provide the best accuracy and is designed for military use. It is directly available to the DoD and other authorized users and is denied to others through cryptography. The SPS provides a lesser degree of accuracy and is available to all users. SPS accuracy levels will be set by the U.S., consistent with U.S. national security interests.

## II. NATURE AND SCOPE

A. **Scope:** This MOA permits the military organizations of **Country X** to become military users of the U.S. DoD GPS-PPS. The MOA covers terms and conditions, security visits, and the provisions pursuant to which **Country X** may acquire and operate GPS-PPS user equipment.

B. **Countries Participating:** The United States and **Country X.**

C. **Program Phases:** This program covers access to, and security and availability of, GPS military signals and equipment. Acquisition of GPS-PPS user equipment from the U.S. is authorized. The program does not have separate phases. **Country X** may purchase up to X,XXX units, at an estimated total value of approximately $XXX million.

D. **Summary of Projected Benefits: Country X** is required to provide to the U.S. DoD access to GPS program information, technical data, planning data, test results and reports, GPS applications, integration designs, differential applications, and any additional system improvements as a result of its participation in the GPS Program. Some foreign technology benefit may accrue to the U.S., especially in miniaturizing functions using less costly, commercial devices or in applications technology, through program flow-back provisions and through our direct military interaction. Of more importance, however, is the benefit that the U.S. will attain greater military interoperability with **Country X** during joint exercises and joint operations under wartime conditions.

E. **Points of Contact:**

| | | | |
|---|---|---|---|
| Mr. David Apple | OASD(C3I) | Pentagon | (703) 695-0000 |
| Maj Patricia Homer | SAF/AQSS | Pentagon | (703) 693-0000 |

F. **Major Milestones:** GPS is a continuing program. Milestones for access to PPS are not applicable.

## III. TECHNOLOGY ASSESSMENT

A. **Sensitive Technical Data/Technologies:**

1. Civil GPS-SPS equipment is an international commodity. GPS-PPS equipment may be similar to civil equipment, except for the addition of security components described below. The GPS was designed as a force multiplier for military war fighting missions requiring delivery of troops or munitions, including operations with diverse types of forces, while maintaining common references for positioning, navigation, and time. Access to GPS-PPS user equipment promotes interoperability among forces and directly enhances the efficiency and effectiveness of joint operations. The countries to participate will acquire GPS receivers and PPS devices in the receivers. Without the PPS devices and implementing software, the receivers are standard and not sensitive. The aspects of GPS-PPS to be protected are described in the following paragraphs.

2. Selective Availability/Anti-Spoofing Module (SAASM). This module contains the anti-spoof decryption capability.

a. The SAASM is unclassified but sensitive.

b. Electronic design and manufacturing technology is not sensitive; the cryptographic process is sensitive. The MOA specifies that **Country X** must procure these chips from the U.S. via Foreign Military Sales (FMS) and account by quantity and application for all ships procured. **Country X** is not authorized to build the SAASM and no manufacturing data will be released.

3. PPS reception capability with SAASM (PPS-SAASM). This capability will allow **Country X** to receive/use full military accuracy of GPS directly from the GPS satellites.

a. **Country X** will only be allowed access to PPS through purchase of equipment incorporating the PPS-SAASM. The PPS-SAASM is unclassified.

b. Circuit design and information processing within the PPS-SAASM are sensitive. However, the PPS-SAASM incorporates tamper-resistant features to protect loss of information. The PPS-SAASM is also design to permit unclassified-when-keyed operation.

4. Cryptographic Key Material. Cryptographic keys, classified CONFIDENTIAL CRYPTO, will be needed to operate the GPS equipment in the PPS mode. Provision of keys is through separate arrangement with NSA.

B. **Classification/NDP Category:** As noted above, access to GPS-PPS requires, as a minimum, release of key material classified CONFIDENTIAL CRYPTO. In addition, GPS technical or operational performance/vulnerability information classified up to SECRET, National Disclosure Policy Category 2, may be released to those countries that are approved for access under National Disclosure Policy procedures.

C. **Comparable Foreign Systems:** The only foreign system directly comparable to GPS-PPS is the GLONASS satellite navigation system being fielded by Russia. Availability of GLONASS user equipment is believed to be extremely limited. A more likely alternative for foreign military users who cannot access GPS-PPS is to use a commercially derived differential capability to improve the accuracy of the signal. Differential GPS based upon the civil SPS is highly vulnerable to jamming and spoofing, however, and is not judged useful for military users in active combat.

D. **Active GPS-PPS Foreign Programs:** Authorized GPS-PPS users to date include NATO, Australia, and other allied nations. **[*Note: Full list is classified and would be included in a specific TA/CP.*]**

E. **Impact on U.S./Foreign Military Capability:** The GPS is a force enhancement system covering all military missions. GPS permits direct, common-grid operations for diverse allied

forces. Application of GPS-PPS will substantially improve mission effectiveness for surface, marine, and airborne military activities. Extent of the force enhancement relates to extent of GPS integration in military tactics and doctrine. The U.S. benefits by increasing interoperability with allies and friendly nations during joint exercises and joint operations under wartime conditions.

F. **Risk of Compromise/Damage:** The risk of damage to the U.S. due to loss of GPS equipment or keys is low. The requirement to use PPS-SAASM is intended to limit risk of technology diversion or misappropriation. Risk of compromise by loss of equipment is limited to exploitation of the lost equipment item(s) only. PPS-SAASM equipment is unclassified when keyed, and the key cannot be extracted as it is contained within a physically and electronically tamper-resistant module. In case of loss/compromise of the keys themselves, the keys will only be usable in individual units of keyable GPS equipment. GPS user equipment only operates in a receive mode, and, therefore, compromised keys/equipment cannot be duplicated and proliferated, or widely used, by a potential enemy. In addition, should the situation warrant, suppression of keys may be accomplished by the U.S. operational command.

## IV. TECHNOLOGY CONTROL PLAN

A. **Release of Information:** Information to be released will be limited to technical information necessary for installation, operation, test or maintenance of the GPS-PPS equipment, not including the cryptographic components. This information is unclassified.

B. **Specific Restrictions on Equipment Release:** Foreign nations must procure GPS and PPS-SAASM devices from the U.S. via FMS and specifically account, by quantity and application, for all devices procured. Accountability is maintained at the GPS Joint Program Office, the only source through which devices may be obtained. Foreign nations are not authorized to build the SAASM or to include the SAASM function in any other device. Therefore, no manufacturing data will be released.

C. **Special Security Procedures:** It is expected that standard procedures contained in existing security agreements will be sufficient to control access to restricted GPS material and information. If there are no existing agreements, or existing agreements are not adequate, specific security arrangements must be included in the applicable GPS-PPS MOA.