# Annex B Normative Functional Requirements

## B.1 Tasking Agent Requirement

Tasking Agents accessing a distributed SCOS system will require access to one or more spectrum sensor devices situated at a remote location through an Internet-connected interface.

This interface must expose all of these functions to the SCOS system user through a defined, standardised interface

* The TA can discover the availability and capability of sensor devices connected to a Sensor Management System
* The TA can request the performance of a scan task according to chosen parameters, or in a more advanced system request a recurring scan to be scheduled that will be executed automatically by the SCOS system
* The TA can define where the data generated in the scan should be transmitted to once complete
* The TA must be given diagnostic or performance information relating to the execution of their scan task

The user must be able to access their scan data and associated metadata describing the scanner’s environment, hardware and software configuration and scan settings.

## B.2 Data Quality and Definition

Data acquired must be accompanied by adequate metadata information to allow for duplication of the measurement or assessment of data quality by a subject matter expert. Hardware specification and measurement parameters are to be included in the messaging metadata requirements. Information less amenable to metadata capture should be made available via appropriate and accessible documentation, e.g., algorithm described via written article with source code in Github repository.

## B.3 Regulatory requirements

This standard should provide mechanisms to meet the regulatory requirements of national operators that have defined parameters or requirements for spectrum sensing in various applications. These regulatory requirements would take two forms: the first is technical requirements for sensitivity, resolution, etc. The second is limitations on how and where sensing might be done where there are sensitivities around privacy, military use and other national policies and regulations.

## B.4 Policy Management and Enforcement Requirements

To allow for granularity in what the SCOS systems can do, but also ensure spectrum occupancy or utilization data is not exposed in contravention of national policy or regulation, it is proposed that the SSM would be able to apply policies to allow or disallow certain functionality in the SSDs, or disallow transmission of the data to third party systems.

These policies would be determined by the SSM operator in accordance with their requirements and that of local authorities (e.g. a national regulator or network operator), and cascaded down to any connected SSDs. These policies would allow sensing only according to allowed metrics (e.g. no hi-resolution raw scans in military radar bands), and limit sensing data transmission to certain classes of third party systems.

##

## B.5 Sensor Location-Fixing Requirements

The SCOS device can convey the location of the sensors to the aggregation entity such as the SSM. The instruction to use available location capabilities on the SSD (e.g. GPS location) will be part of the scan schedule instruction from the Tasking Agent requiring the scan. This feature allows the SSM or the aggregation entity to localize the proximity of the signal source location allowing more efficient spectrum management. This location fixing capability will be implemented by the system operator to be in accordance with local regulatory requirements.

Location can be fixed in three ways:

* At scan-time from lat/long co-ordinates from internal GPS, GLONASS or similar system
* Configured at startup-time from lat/long co-ordinates from internal GPS, GLONASS or similar system
* Configured on SSD by authorised/certified installer at commissioning time with accurate lat/long coordinates
* Configured on SSD by authorised/certified installer at commissioning time with street address/location

The type of location fix would be specified in device metadata (NOTE: ADD REFERENCE).

## B.6 Service Level Agreement Requirements

To be completed.

## B.7 Certification Requirements

To be completed.

## B.8 Technical Requirements

### B.8.1 Device classes and complexity

The following sensing device categories may be considered:

* **Energy Efficient Sensing Devices**: This standard should provide mechanisms of energy efficient operations, eg. solar powered or battery operated spectrum sensors for monitoring applications.
* **Small form factor devices**: Devices that can fit the spectrum sensing function within a small form factor (e. g. a USB dongle, cell phone etc.)
* **Advanced Spectrum Sensing Devices**: Advanced Spectrum Sensing Devices with capable Radio Frequency Front Ends (RFFE) and dedicated resources for spectrum sensing may be considered.
* **Non-dedicated Devices with Sensing Capability:** A number of consumer and professional radio devices contain radio receivers that can be used as sensing devices, including mobile phone handsets, Wi-Fi access points (from 802.11ac) and Dynamic Spectrum Access radio systems (including 802.22).

### B.8.2 Number of devices

This standard shall support at least one Spectrum Sensing Device to cover a location or area, communicating with a back-end Spectrum Sensing Management System (SSM), but will extend to describing an architecture and interfaces for multiple SSDs potentially communicating with multiple SSM instances.

### B.8.3 Real-time applications

The sensing devices will be performing spectrum sensing functions according to its scheduler (which is managed by its SSM), which can be updated in near-real time (dependant on speed of communication between Tasking Agent, SSM and SSD), or perform scans at scheduled intervals based on pre-configured schedules. However, the spectrum sensing reporting of data is out on a Best Effort basis, since the SCOS System uses the chosen available transport mechanism (e. g. 802.11, 802.22, Ethernet, Cable, Cellular etc.).

The SCOS system will benefit if sensing reports from various sensors are provided on a reasonable time-scales (e. g. minutes) so that the information is not stale. However, this is not a mandatory requirement. Also, the messaging format may be defined such that it does not produce excessive overhead penalty on the transport layer being used.

It is envisioned that real-time streaming will be provided for in future drafts of 802.22.3.

### B.8.4 Channelization

This standard may specify a Spectrum Manager entity that can command various sensors to go and sense in certain bands, or it may even specify the spectrum sensors to ignore certain bands from sensing, and impose channelization maps for sensors to meet local regulations or technical requirements.

Specific channelization maps may be provided in future drafts of 802.22.3.

## B.9 Security Requirements

This standard mandates secure authentication and authorisation between Tasking Agent and SSM, SSD and SSM, SSM and Data Manager, and Data Manager and DRP. Traffic between these components must also be encrypted. The specific security technology to be used is not mandated in this standard, but recommended best practices are described in Annex B. Note that the security model does not extend past transmission to the DRP. Responsibility for securing the spectrum data at destination remains the responsibility of the operator of that store.

The technology model is designed to ensure that data derived from SCOS devices and SSM are not used as an attack vector against White Space Databases, regulator spectrum management databases, etc. It is also designed to ensure that only authorised Tasking Agents can make use of the SCOS resources, and that they are correctly identified to enable correct application of the relevant system policies.

In each case, the security model must address:

(1) Data categorization (i.e. sensitivity/confidentiality of scan data)

(2) Access control - authorization and authentication (of each element when interacting with another)

(3) Logging and auditing (of instructions, tasks, access control)

(4) Data encryption (within devices and in transmission)

(5) System and information integrity (validation of device configuration, storage system)

(NOTE: Section to be developed further)

### B.9.1 Intra-device Layer Security (physical interfaces)

This standard defines security mechanisms to ensure integrity of sensing chain from antenna to DRP.

* Antenna to amplifier/filters: physical security of device in terms of cable/connectors (tampering such as substituting antenna, physical such as connector corrosion)
* Amplifier to SDR: cable connectors or PCB connections
* SDR to processing unit: cable connectors or PCB connections
* Enclosure for active elements: Protection against moisture, dust ingress. Screening against RFI from external sources. Screening to protect antenna elements against RFI from active elements.

(NOTE – this section needs considerable attention)

### B.9.2 Inter-Layer Security

#### B.9.2.1 Network Layer

Since this standard uses any available transport mechanism for data transmission, it will not recommend its own security mechanisms, but will use the existing security mechanisms of the transport mechanism being used (e.g. network 802.11 using Transport Layer Security,

#### B.9.2.2 Application Layer

Data transmissions should be secured on the application layer using mechanisms to guarantee the integrity and confidentiality of sensing and control data transmissions. This standard does not specify the technology used, but recommended implementation practices are noted in Annex B: **Error! Reference source not found.**.

### B.9.2 Security of sensed data

This Standard shall not support mechanisms that expose data of radio system users that are modulated onto signals that are examined by the 802.22.3 SCOS System. For example, any kind of demodulation of the signals that may interfere with the privacy of the radio system users shall not be not be supported. However, the SCOS system shall support sophisticated spectrum sensing methods such as cyclostationary processing that can detect signals and characterize their modulation type.

### B.9.3 Security of analyzed or characterized spectrum data

This Standard shall support security mechanisms to ensure that spectrum characterization data is transmitted to the destination DRP in a secure way. This Standard shall not specify the security mechanisms used to protect this data once received by the DRP – this is implementation and system user specific.