Motorola Solutions, Inc.
1455 Pennsylvania Avenue, NW
Suite 900
Washington, DC 20004

January 03, 2014

Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, S.W.
Washington, DC 20554

Re: GN Docket No. 12-354 – Amendment of the Commission's Rules with Regard to Commercial Operations in the 3550-3650 MHz Band

Dear Ms. Dortch:

Motorola Solutions, Inc. ("Motorola Solutions") hereby submits the attached document in response to the Commission's Public Notice[1] seeking information on proposed spectrum access system for the 3.5 GHz band.

Please contact me if there are any questions on this filing.

Respectfully submitted,

*/s/ Chuck Powers*
Chuck Powers
Director,
Engineering and Technology Policy
Motorola Solutions, Inc.
1455 Pennsylvania Avenue, N.W.
Washington, DC 20004
(202) 371-6900

[1] Wireless Telecommunications Bureau and Office of Engineering and Technology Call for Papers On The Proposed Spectrum Access System For The 3.5 GHz Band, GN Docket No. 12-354, *Public Notice*, 28 FCC Rcd 15843 (2013).

## Introduction

Motorola Solutions supports the Commission's efforts to enable a multi-tiered Spectrum Access System (SAS) in the 3.5 GHz band. A wide variety of services can be accommodated through the SAS, and spectrum can be dynamically managed via databases to realize highly efficient and flexible use of the band. Some examples of spectrum users include commercial service providers (e.g., priority access licensees), critical access users (e.g., public/life safety, critical infrastructure, etc.) and general authorized access users (e.g., consumer WiFi). The SAS offers the opportunity to adaptively adjust spectrum allocations, through dynamic assignment of spectrum that can vary based on geography and time. We expect to have further discussions about the development details of SAS databases in the future. Motorola Solutions encourages the Commission to deploy a robust and flexible SAS database system.

## Responses

*Focus Area A: General Responsibilities and Composition of SAS*

*A.1. What should be the scope of the SAS's responsibilities for enabling and de-conflicting use of the 3.5 GHz Band? How should these responsibilities manifest within a given tier (e.g., Priority Access, GAA) or between the different tiers? Should the SAS identify the available spectrum to authorize use in a particular location/frequency/time (similar to, but more expansive than the TV White Spaces approach) or should the SAS also manage the use of the band (i.e., configure and/or set limits on various radio parameters to maximize efficient use of the band)?*

The SAS should be responsible for generally de-conflicting use of the 3.5 GHz band. Specifically, this function includes providing spectrum access information to the various tiers, as well as assuring non-interference to higher priority tiered (i.e., priority access licensee, critical access, and incumbent) users. The SAS database should be aware of all active system deployments in the band, including cases where a priority access licensee (PAL) has exclusive access rights to a portion of the spectrum, in order to effectively manage the overall (e.g., co, adjacent and alternate channel) interference environment. This also allows the SAS to most effectively and efficiently manage overall spectrum usage.[1] The SAS should convey spectrum opportunities to Authorized Users (AUs) of the various tiers through spectrum usage permits, that specify the allowed operating frequency/bandwidth, operating location/area, permissible transmit power levels and usage times (see below).

The required SAS computations include predicting the interference levels throughout the system for the various active users (based on their operating frequencies, location, transmit power levels,

[1] For example, depending on the size of PAL license areas, and the particular operating restrictions for the portion of the band, there may be certain locations where even the PAL licensee is not utilizing the spectrum, which could be used by other users (e.g., GAA or PA/critical access) at the appropriate transmit power levels to avoid interference. Of course, such use could be revoked at any time (subject to the SAS database update rate, e.g., on the order of 15 minutes) if the PAL user wants to actively utilize the spectrum in the particular area.

equipment class,[2] etc.), and determining usable frequencies and maximum transmit power levels for newly active systems to avoid interference to other users. AU systems should not generally be expected to be synchronized, or utilize the same type of modulation. Priority Access (PA) users (including PALs and critical access users) should generally be allowed to transmit at their authorized full transmit power levels (for each respective class) if desired. Actual system transmit power levels should be tracked in the database, as further described below (see Focus Area D). In cases where there is a conflict between two equal priority level systems, the first arriving system should be allowed to operate at full power, and the subsequent arriving systems should generally reduce their power to avoid interference, based on their operating location and proximity. Priority Access users from the same system (e.g., operator) should be allowed to tolerate (i.e., self-manage) interference within their system. Different types of uses (e.g., LTE small cells of various sizes, WiFi hotspots, incident scenes, wider area networks, backhaul, etc.) should be supported in the database. Higher power uses may be segregated from the rest of the band to simplify interference management.[3] In general, interference avoidance could be accomplished on a best-effort basis for General Authorized Access (GAA) tier devices.[4] Further description on interference management techniques is given below.

*A.2. What are the key system elements of the SAS (e.g., database, signaling entities, etc.)? Who should have responsibility for each of these elements? Which system elements of the SAS require direct control by the Commission and which elements can be managed by third-party SAS provider(s) or other third parties? What level of oversight should the Commission exert over the functions of the SAS?*
*A.3. What are the key architectural decisions that could be affected by rules governing the SAS? To what extent should the SAS architecture be centralized or distributed? Are there specific enabling technologies that should be contemplated within the rules?*
*A.4. How can interoperability be ensured (between multiple SASs provided by multiple vendors and between SASs and Authorized Users (AUs) while leaving room for technological innovation and differentiation?*
*A.5. How would the SAS interact with incumbent systems?*

The Commission should authorize multiple user-facing (3rd party) SAS database service providers, for similar reasons as in TVWS (e.g., to encourage innovative services, improve redundancy

[2] Equipment class should contain information about the receiver interference protection requirements (e.g., co- and adjacent channel D/U interference protection ratios), the transmit spectral mask (OOBE) employed by the equipment (for use in interference computations), and the expected duty cycle of the transmissions.
[3] This concept is somewhat similar to the High Power Operation Zones in the 3.5 GHz NPRM, and would allow band selection (front-end filtering) of stronger interferers.
[4] GAA devices are expected to be relatively low power (e.g., less than 24dBm, and typically less than 20dBm), and may be able to operate on a best-effort basis in the presence of interference (similar to unlicensed WiFi devices). Once again, actual transmit power levels should be conveyed to the SAS to track the interference environment.

and overall system reliability, etc.).[5] The Commission, along with industry, should specify the minimum required interference protection methods and standards to be followed by the various SAS database service providers (further described below).[6] Frequent synchronization of user registration data should be enforced among multiple databases, as is currently possible (though not necessarily required) in TVWS. Due to privacy concerns about some of the incumbent, PAL and critical access user data, such data should not be readily available to other system users. All such data should be transferred utilizing industry standard encryption techniques. Sensitive military user data can be contained in a centralized and isolated (unified) database, of which only authorized SAS database providers would have limited access to, in order to protect incumbent operations.[7] Other incumbent users (e.g., FSS receivers) should be required to register with at least one of the authorized database service providers (in a mechanism similar to cable headend receiver or wireless microphone protection in TVWS). Alternatively, a registration clearinghouse could be stood up by the database service providers to serve this function.

User-facing SAS database access techniques should be governed by industry bodies. One example of industry-driven database access techniques can be found in the IETF PAWS group, which addresses encryption and authentication techniques for white space database access. The Commission should employ implementation requirements to ensure that a prescribed level of consistency is maintained among the databases (similar to TVWS, see also below). Multi-stakeholder groups can be employed to work on low level implementation details in many of these areas.[8]

As in TVWS, AU devices should be allowed to obtain database access through a proxy or master device. Such devices can broadcast beacon signals to dynamically control their member network.[9] In this manner, a base station will be able to manage the user equipment in a small cell deployment (i.e., control the operating frequencies, operating times and transmit power levels), and not significantly impact user equipment requirements. As mentioned, many systems, including LTE-based systems, already have provisions built in to control such parameters (e.g., power control, etc.).

---

[5] There was broad industry support for having multiple database providers in TVWS. This should include the ability for equipment providers to field an authorized database, if desired. All database providers would be required to meet minimum performance requirements to be authorized providers by the Commission.

[6] 3GPP is an example of an industry body that can provide interference tolerance information for LTE systems. IEEE is another example of an industry body that can provide interference tolerance requirements for WiFi systems.

[7] Sensitive incumbent users in the 3.5 GHz band, such as the DoD, would have full control and access to the unified incumbent database. SAS database providers would have highly limited and fully secured access to such data.

[8] Multi-stakeholder groups could also be extended to address acceptable interference levels for different system types/equipment classes (in conjunction with the aforementioned standards bodies), along with the administration of Interference Limits Policy, as recommended by the FCC TAC Spectrum and Receiver Performance working group.

[9] Many systems, including LTE and WiFi (802.11af) support these types of beacon or control functions.

*Focus Area B: Key SAS Functional Requirements*

*B.1. What is the minimum set of information that must be exchanged among different elements of the SAS ecosystem in general and in particular between AUs and the SAS?*
*B.2. Which configuration and radio parameters (such as applying initial power level, power adjustment, initial frequency assignment, channel switch over, interference mitigations, etc.) would be defined as required obligations of the SAS?*
*B.4. What specific capabilities would need to be specified for the network nodes devices to provide information needed by the SAS (e.g., location capability, dynamic power adjustment, tuning range, etc.)?*
*B.5. What mechanisms should be used for updates (from network devices to SAS and from SAS to Network devices)? How frequently should these updates take place?*
*B.6. How can the SAS best ensure information security and privacy across the entire ecosystem?*
*B.7. If there are multiple Spectrum Access Systems, how could they be synchronized to deal with rapid changes in access to spectrum and the radio environment?*

At a minimum, authorized users should provide the SAS with an operating location/area, equipment class (as noted above)[10], equipment ID[11], requested bandwidth and time of operation. The request could also contain additional/optional information (e.g., antenna height/height above average terrain (HAAT), antenna pattern, an expected transmission duty cycle, etc.) that could be used to further define the interference environment. The SAS should respond to authorized users with a potential operating frequency, an associated maximum allowed transmit power level for the given operating location(s), and an allowed time duration of operation. The AU should then confirm usage of the spectrum by responding with a utilized transmission power level. Optionally, the AU equipment may also report interference environment measurements (for comparison to database predictions and use in interference management and compliance – see below). By the expiration of the allowed time duration of operation, the AU would need to query the database again to receive permission to continue to operate on the channel (or to move off the channel, possibly to another channel, to accommodate a higher priority user, or otherwise adjust its operating parameters). Typically, the database update rate could be on the order of 5-15 minutes, resulting in a minimum database query time of the same order. In some cases, where the environment is more static, longer time durations of operation may be permitted (e.g., daily, as in TVWS databases).[12]

---

[10] For example, an FCC ID could serve as a descriptor for the equipment class (describing the service priority/tier, transmit spectral mask/OOBE, required interference protections, equipment tier/priority level, etc.). Optionally, service priority could be communicated separately.
[11] This may include any necessary authentication information. The SAS may also have the authority to deny service to particular units or equipment classes, as in TVWS.
[12] Similarly, some allowances could be made for missed database access before AU operation must cease. For example, fixed TVWS equipment must query the database every 24 hours, and must cease operation if the database is not accessed for 48 hours. Worst case update rate allowances must be able to accommodate high priority users (e.g., Federal incumbents, sporadic public safety incident scenes).

In general, 3.5 GHz band devices would need to be highly frequency agile,[13] have some type of geo-locating capability (either at a network or device level), and support a limited power control range.[14] Those devices that have extensive capabilities (e.g., extended frequency agility or power control range) would naturally be allowed to operate at more locations and times, due to the database control mechanism. This forms an inherent incentive for manufacturers and users to support these extended capabilities. Device or network geo-location could be acquired through GPS or professional installers, as is allowed in TVWS. In addition, the use of operating location regions should be fully supported. This allows an operational area to be specified for all users within a system (e.g., within 100 meters of a base station/AP), and the operating parameters of the overall system are limited for the particular area through the SAS database. The SAS database in this case assumes that an AU could operate from anywhere within the specified region, and computes maximum allowed transmit power levels accordingly to avoid interference in all possible scenarios.[15] This approach adds a great deal of flexibility into implementing the locating means for an AU device or system (e.g., it would allow low cost or indoor devices with fairly coarse locating capability to successfully operate, albeit at a potentially lower power levels). Once again, this type of performance trade-off could be made to simplify equipment design.

As mentioned above, typical required database update/query rates could be on the order of 5-15 minutes, to support higher priority users (e.g., military incumbents, short term critical access users, etc.). Also as mentioned above, industry standard secure data transfer mechanisms (e.g., TLS 1.2) can be utilized for AUs to interact with the database. Synchronization across databases can also occur via secure links, as is accomplished in minutes today in TVWS.

*Focus Area C: SAS Monitoring and Management of Spectrum Use*

*C.1. What techniques could be used for the SAS to detect use (and misuse) of the spectrum in specific locations/frequencies/times? What criteria should be used to determine whether the spectrum is being used?*
*C.2. What techniques should the SAS employ to detect, locate, measure, and report inter-AU interference problems? What capabilities should be included in AU devices to facilitate these functions? What should be the basis for determining what constitutes interference? For example, should it be based on parameters established by the service that is being offered or some signal threshold? How should the SAS deal with intermittent or transient interference?*
*C.3. What enforcement mechanisms can be implemented in the SAS and authorized devices to ensure*

[13] Depending on the final band plan/band segmentation among users. For example, GAA use may not be permitted in portions of the commercial PAL or critical access user spectrum, and higher powered uses of the spectrum may be confined to particular portions of the band (e.g., 3650-3700 MHz).
[14] If user equipment does not support the required power control dynamic range (i.e., if a device is only able to reduce its transmit power to X dBm, and the SAS database computes that the allowable transmit power level is less than X dBm to avoid interference), then that particular equipment would not be allowed to operate at the given location and time.
[15] This approach was termed as supporting location uncertainty in TVWS, and relies on determining an upper bound on transmit power level for an operating region. Further details are available on these techniques.

*automatic compliance with any technical and service rules adopted in this proceeding?*

As discussed above, AUs should report a utilized power level as part of the query process when accessing one of the SAS databases. This would allow the SAS to compute expected interference levels throughout the system. Optionally, it would be useful for AUs to report back to the SAS database any persistent (external and actual) interference issues in their system (e.g., loss or severe degradation of service), and possibly periodic measured interference levels.[16] These measures could be utilized to help determine cases of unauthorized use of the band. In addition, the SAS system could be aware of the types of modulations (e.g., LTE, 802.11af, etc.) employed by each system, to further help in determining unauthorized users. AUs may wish to report any unexpected modulations observed in the band. This capability is yet another reason to keep track of all AUs in the band. Advanced SAS capabilities, such as interference tracking and enforcement, can be supported at a later date. These types of services may also be considered as value-added (not required) services.

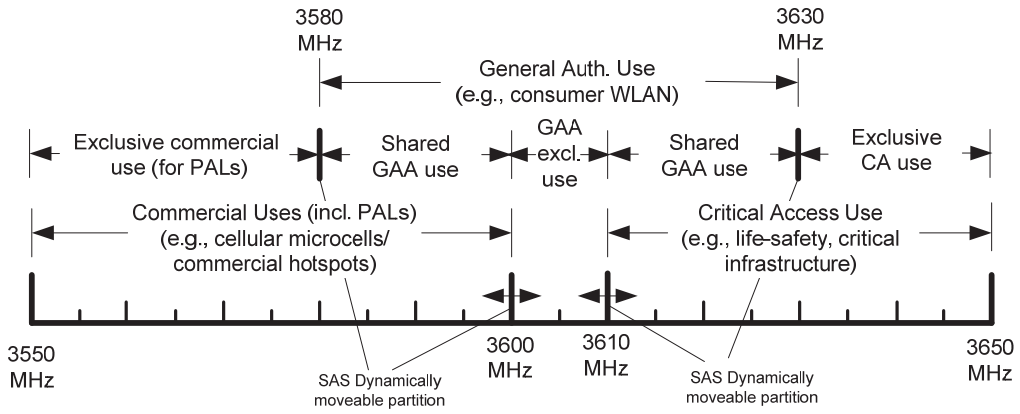
*Focus Area D: Issues Related to Initial Launch and Evolution of SAS and Band Planning*

*D.1. What functions should be required at launch? How should the SAS's capabilities evolve over time? What functions can be added later? How would such an evolution path anticipate backward compatibility of deployed equipment?*
*D.2. What are the key network deployment topologies the SAS should support at launch (e.g., low-power small cells, backhaul, higher-power rural uses)? Can the SAS be designed to support multiple wireless technologies? Please provide technical details to distinguish various use and technology cases as they might, in turn, generate different requirements for the SAS.*
*D.3. Should there be a phased approach to flexible partitioning of the band between different use cases (e.g., low power small cells vs. wireless backhaul or between PA and GAA)? What are the tradeoffs and how we can ensure backward compatibility of devices as the band plan evolves?*
*D.4. How can we ensure that the SAS and band plan evolution maximize flexibility to accommodate multiple spectrum uses / topologies going forward while maintaining backward compatibility?*

The SAS system should support dynamically segmented spectral allocations, as previously described by Motorola Solutions, in order to provide the highest degree of flexibility during system roll-out.[17] This allows each class of user (commercial/PAL, GAA, and critical access) to have some guaranteed minimum amount spectrum, to best support market development in varying regions. An example illustration of the concept is provided below:

---

[16] Measurements would need to be taken during quiet periods on the system. Care must be taken so as not to over-burden the SAS databases with sensing information. This approach would generally call for a standardized suite of interference measurement tests to calibrate the reported results for various types of equipment. In addition, the antenna height, gain and nominal polarization should be reported to the SAS for further refinement of interference measurement results.
[17] Comments of Motorola Solutions, Inc., GN Docket No. 12-354 (filed Dec. 5, 2013).




Under this approach, the Commission would be able to make periodic (e.g., yearly) adjustments to the segments of the spectrum, in order to accommodate the most needed uses in particular areas, while still providing a guaranteed minimum amount of spectrum to users (some of which would be for exclusive use, while a portion would be shared). This would allow the Commission to fine-tune spectral allocations as time passes, and tailor the allocation for a particular area. Once again, it is important for the SAS databases to keep track of all users of the 3.5 GHz spectrum (including PAL, indoor users, etc.) in order to maintain future flexibility for the spectrum. In this manner, spectral allocations can be modified to best suit a changing environment over time, or the particular needs for a given region. For example, using the dynamically segmented spectrum approach above, additional spectrum may be dynamically allocated to commercial users in selected urban areas, without the need for wholesale changes to device operation, lengthy rule-makings or proceedings. Having even moderately frequency agile devices also helps to provide this flexibility.

The SAS can and should support a wide variety of deployments, including predominantly small cell uses (e.g., LTE based commercial and critical access users), WiFi hotspots (e.g., 802.11a/y/af-like commercial and consumer users), and higher powered uses (e.g., WANs, emergency incident scene networks, and wireless backhaul) in portions of the band.[18] As mentioned earlier, industry standards bodies could form a starting point for the expected transmit spectral mask (OOBE) and interference tolerance values required for each class of system.

In general, each PA and incumbent system, depending on the deployment, would have a specified protected area of operation (a cell or protected contour), at which some minimum interference criteria would be met at the cell edge (on at least the co- and adjacent channels).[19]

[18] In general, it is expected that large coverage area users of the spectrum (e.g., PALs) would pay more to use the larger share of resources. Ultimately, the SAS system could track actual usage of spectrum (in area, time and bandwidth utilized) and bill accordingly.

[19] This translates into maintaining some maximum IoT value for LTE systems. Some types of systems (e.g., GAA consumer WiFi hotspots) typically may not have an associated protected contour, and operation would be on a best effort basis (as in the unlicensed band today). In addition, for WAN deployments, a mutually agreed upon propagation (and terrain model) should be determined, preferably in conjunction with the industry. For low power

Incumbents would include naval radar systems, and FSS receivers, which can be protected based on the receiver antenna pattern that is utilized (e.g., taking into account the azimuth and elevation angle of FSS receivers). A maximum allowed transmit power level would be computed for each new user based on the user's operating location(s) and their proximity to other protected users, taking into account the existing interference protection constraints from other (equal and higher priority) users. All required incumbent (and higher priority user) interference protection ratios would be met with the specified maximum allowable transmit power level.[20] If particular AU deployments desired to operate at a location in closer proximity to protected deployments, they would have to reduce their transmit power level, to continuously meet the interference protection requirements of the other users. This method allows the most opportunities for spectrum re-use, and generally results in the highest spectrum utilization efficiency. AU operation should also be allowed on adjacent channels within other users' protected contours, subject to non-interference constraints. Other more simplified methods of maintaining non-interference (based on minimum required separation distances from different classes of services, similar to TVWS) may also be optionally allowed.

In terms of existing equipment in the band (e.g., WISPs in the 3650-3700 MHz portion of the band), equipment should be grand-fathered for a reasonable period of time, and then converted to equipment that follows the new rules for the band. Of course, higher powered uses of the band will naturally require larger protection zones, and larger stand-off distances from co-channel and adjacent channel services. This may serve as further motivation to limit high power usage to particular portions of the 3550-3700 MHz band. In cases where antennas are sectorized, each sector can be treated as an individual transmitter.

*D.5. How should the system be developed and deployed? To ensure a successful launch, what strategies could be employed to test the capabilities of the SAS?*
*D.6. What provisions need to be established to address the possibility of an SAS experiencing a service outage or permanently discontinuing service?*

SAS database providers can be tested using a relatively small set of typical deployment scenarios, to verify proper database computations prior to authorization (in a manner similar to TVWS). Key stakeholders (e.g., incumbents, PAL/critical access users) should have input into the specified set of tests that are administered. It is also possible to perform automated periodic (software based) monitoring of the various active SAS database service providers ensure consistency (within specified limits) across different database vendors. As mentioned above, one particular reason for supporting multiple SAS database vendors is to ensure reliability in the case of service outages (temporary or permanent).

* * * * *

---

small cell applications, a TM-91 propagation model may be appropriate (with a nominal building penetration value applied for indoor networks).

[20] This approach is similar to what was originally proposed for TVWS. *See Unlicensed Operation in the TV Broadcast Bands; Additional Spectrum for Unlicensed Devices Below 900 MHz and in the 3 GHz Band*, ET Docket Nos. 04-186, 02-380, Notice of Proposed Rulemaking, 19 FCC Rcd 10018, n. 50 (2004).