In the Matter of
Amendment of the Commission’s Rules with Regard to Commercial Operations in the 3550-3650 MHz Band

To: The Commission

COMMENTS OF TELCORDIA TECHNOLOGIES, INC. D/B/A ICONECTIV

Telcordia Technologies, Inc., doing business as iconectiv (“Telcordia” or “iconectiv”), is pleased to submit these comments in response to the Federal Communications Commission’s (“FCC”) Further Notice of Proposed Rulemaking (“NPRM”) in the above-referenced proceeding.

iconectiv provides market-leading solutions, including number portability clearinghouses and databases, that enable operators to interconnect networks, devices, and applications critical to evolving the global telecommunications marketplace. The U.S. has an opportunity to add 150 MHz of new spectrum for wireless broadband services and to maintain its global leadership position in mobile broadband. To make the most of this spectrum, the Commission should adopt rules that will encourage private sector investment and deployment in a shared Federal/commercial framework in the 3.5 GHz band.
DISCUSSION

REGULATORY ENVIRONMENT FOR SPECTRUM ACCESS SYSTEMS

MULTIPLE SAS ADMINISTRATORS

The proposed rules assume that multiple SAS administrators would be authorized to operate in the 3.5 GHz band, just as multiple databases are authorized to operate in the television white space (“TVWS”) band.¹ iconectiv supports the authorization of multiple competing SAS operators in the 3.5 GHz band. We believe this will benefit the overall ecosystem by providing a choice of SAS system providers to stakeholders in the band. This approach will promote innovation in SAS development and operation and will result in a more robust SAS ecosystem.

The FCC is interested in determining whether it is feasible for multiple SASs to operate effectively in the 3.5 GHz band. Just as TVWS databases synchronize information with each other in near real-time using secure web service techniques, so could SAS operators achieve near real-time synchronization and information interchange. Techniques for information interchange using web services are both mature and secure. Endpoints can be authenticated using certificate authentication techniques to prevent unauthorized access and the information interchange can be secured from eavesdropping through use of HTTP on top of the SSL/TLS transport protocol.

The SAS Administrator qualification procedure defined in the Further Notice² closely reflects the procedures used to qualify and govern the operation of TVWS databases currently in service in the TV bands. We believe these requirements are reasonable and sufficient to qualify and govern SAS Administrators.

¹ See Further Notice, 29 FCC Rcd at 4300 ¶ 91, 4337 (definition of Spectrum Access System), 4349 (proposed Rule Section 96.48).
² See id., 29 FCC Rcd at 4304-05 ¶¶ 105-108, 4349-50 (proposed Rule Section 96.48).
The proposal to allow SAS Administrators to collect fees for PAL and GAA users for associated services in a similar manner to rules adopted for TVWS\(^3\) is reasonable and appropriate. iconectiv believes that limiting fees to PALs is overly restrictive and unduly limits the flexibility of the SAS Administrator to develop business models required to operate services in the 3.5 GHz band. The Commission should refrain from prescribing regulations regarding business models. The database enables use of spectrum in this band and SAS operators should have the option to be compensated through a nominal fee for enabling use of this spectrum.

**SAS PURPOSES AND FUNCTIONALITY**

The proposed core SAS functions put forward in the *Further Notice* assume that the SAS will interact directly with all CBSDs.\(^4\) However, the Commission should differentiate treatment applicable to CBSDs operating in a managed network from that applied to CBSDs operating on a stand-alone, opportunistic basis. Managed networks, whether operating in GAA or PAL spectrum, are subject to network planning where power limits, transmitter frequencies, neighboring cell information and physical cell identities are set. The emissions within a managed network are carefully controlled under the carrier’s supervisory framework, consistent with regulatory limits. In the managed network scenario, the SAS could interact at the network management function level within the mobile broadband network instead of at the level of the individual CBSDs. Such an assignee would be certified differently from a GAA CBSD that interacts directly with the SAS.

In an operator-managed network, the SAS should not assign specific frequencies to individual CBSDs. Instead, the SAS should provide a frequency block range to the managed network’s operational support system (“OSS”). In the case of PAL, the frequency block range

---

\(^3\) See id., 29 FCC Rcd at 4305 ¶ 109, 4349 (proposed Rule Section 96.49).

\(^4\) See id., 29 FCC Rcd at 4302 ¶ 95, 4347 (proposed Rule Section 96.43).
would be defined as part of the license agreement, \textit{i.e.}, the 10 MHz spectrum assigned for a specific PAL. The SAS would not provide specific frequency allocations to each separate transmitter. Furthermore, for managed networks, the SAS can oversee the network’s OSS by providing a set of restrictions stemming from the rules the Commission adopts. This would allow for flexibility and innovation within those constraints, as opposed to the SAS managing the CBSDs within a managed network.

This type of alternate SAS-OSS operation could additionally be supported by defining OSS areas of operations specified by polygonal geographic regions with associated maximum allowed power threshold levels at the boundaries of the assigned area. The OSS within the mobile broadband network could then determine how to allocate those channels to each individual CBSD. The network’s OSS would be free to assign channels to individual CBSDs within the area and would also be free to assign power levels to these devices, as long as the power levels do not exceed the proscribed maximum received values at the area boundaries. It is feasible for the SAS to specify signal levels at the license area boundary (or the boundary of multiple license areas operated together as a network under common control), so as to avoid interference to incumbent users and to adjacent PAL users.

Once the network’s OSS assigns channels to individual CBSDs, information regarding channel use at locations within the assigned operational area can be reported back to the SAS with any information regarding the identity of the CBSD end-user removed to preserve the privacy of individuals using such devices. This information will be used by the SAS to reserve use of the channels and prevent GAA access in the area now assigned to a Priority Access Licensee (PAL). The information can also be used by the SAS to allow grouping of multiple GAA sites within the census tract into a common management framework, so that the SAS can
attempt to serve the requirements of the service provider, e.g., by assigning the same channel across the network. This information could also be used by the FCC in the event of interference problems experienced by incumbents.

Although the Commission proposes to allow PAL and GAA users to coexist in all parts of the band from the outset, a transitional band approach, as proposed by Verizon and others, could also be accommodated by the SAS, using a different initial set of rules that allows a partitioned band operation (PAL in one sub-band, GAA in a separate sub-band, and experimentation with multi-tiered operations in a third sub-band). Once the interim trial period is over, the SAS could then change the rules to allow PAL/GAA coexistence within the same band. Through use of geospatial rules in the SAS, it is even possible to allow PAL/GAA spectral coexistence only in limited initial trial areas to assess any interference issues. However, any changes in operational characteristics must be done only after extensive testing and verification.

As described in the Further Notice, the FCC describes an SAS-to-CBSD interaction where the SAS interacts directly with all CBSDs, whether PAL or GAA devices. In the case of CBSD devices that are managed by mobile network operators, the SAS should support interaction with an OSS that is owned and operated by the mobile network operator to allow operator-managed frequency assignment within their network instead of communications directly between the SAS and individual CBSDs. An SAS can provide a description of allowed channels and maximum power limits on those channels to the network’s OSS within a defined area of operation. The OSS can then choose appropriate frequency assignments and power levels for each of the CBSDs within that area and report back to the SAS the channels, power levels, and locations of the CBSDs (with personal identifying information stripped to protect end-user privacy). The Further Notice describes the case where CBSDs that are thought to be

---

5 See Further Notice, 29 FCC Rcd at 4304 ¶ 103, 4348 (proposed Rule Section 96.46).
causing harmful interference are deactivated or reassigned upon request. The method of
operation described above allows for this possibility with the SAS directing any offending
CBSDs through the intermediate OSS.

**INFORMATION GATHERING AND RETENTION**

The *Further Notice* proposes that the SAS retain information on all operations within the
3.5 GHz band.\(^6\) A certain amount of information protection between device level information
and network level information should be allowed due to competitive concerns regarding the
collection of deployment characteristics such as antenna sectors, design characteristics, *etc.*, that
must be safeguarded. The *Further Notice* also proposes that the SAS collect information
regarding location and look-angles of FSS operators so as to create FSS geographic exclusion
zones and geographic coordinates necessary to create exclusion zones for protect Federal
incumbent users. iconectiv believes this exclusion-based methodology is sound, as it has been
shown to be effective in protecting incumbents in TVWS operation thus far. However, as stated
above, the size of the Exclusion Zones for protecting federal incumbents along the coasts of the
U.S. as proposed in the *Further Notice* is currently so large as to discourage use of this spectrum
by commercial entities.

Additional knowledge regarding use of the 3.5 GHz band by Federal users, such as time
of use or general location of use, could allow more efficient sharing of this spectrum with
commercial users, through the use of coordination zones. If Federal users are uncomfortable
with sharing the necessary information with commercial SAS providers, we support the
incorporation of a separate Federal SAS to maintain this sensitive information in a secure manner
and provide obfuscation of the actual locations and times of use of these Federal systems.

\(^6\) *See id.*, 29 FCC Red at 4303 ¶¶ 99-101, 4348 (proposed Rule Section 96.44).
Use of spectrum sensing information could be helpful in validating assumptions used to provide protection to incumbent users from PAL and GAA users. Spectrum sensing information could be collected by managed networks and GAA CBSDs during periods of inactivity or through the use of a secondary radio receiver. This information could be used by the SAS for evaluation of protection criteria and to support management functions performed by SAS, but sensing should not be required for operation.

**REGISTRATION AND AUTHORIZATION OF CITIZENS BROADBAND RADIO SERVICE DEVICES**

The SAS can verify the identity of CBSDs (or an OSS supervising a network of CBSDs) through use of certificate based authentication or through verification of a shared secret between a device/network controller and the SAS. Since there would need to be a commercial arrangement between a device and a SAS, the SAS provider and device manufacturer can share a set of information known only to the two and embed this shared secret into the two systems for use by an authentication/validation process. When a device contacts the SAS for the first time, it includes this shared secret in the interchange and the database validates the shared secret content through a lookup that associates the devices serial number/FCC ID pair (or ESN) with the shared secret message. If a certificate based approach is used, a third party certificate authentication service can be used to provide identity validation/authentication.

**SECURITY**

iconectiv supports a system in which the communication between SAS and CBSDs (or OSSs) are protected using standard Internet security procedures; specifically, encrypted

---

7 See id., 29 FCC Rcd at 4303 ¶ 102, 4348 (proposed Rule Section 96.45).
communications to prevent eavesdropping and certificate based authentication of the endpoints to verify identity of the end nodes.  

**CONCLUSION**

Based on the foregoing discussion, iconectiv recommends that the Commission adopt rules consistent with the positions set forth in our Comments.

Respectfully submitted,

/S/ John P. Malyar  
John P. Malyar  
Chief Architect  
iconectiv  
444 Hoes Lane  
Piscataway, New Jersey 08854  
(T) 732-699-7192  
jmalyar@iconectiv.com

/S/ Anthony A. Triolo  
Anthony A. Triolo, Ph.D.  
iconectiv  
444 Hoes Lane  
Piscataway, New Jersey 08854  
atriolo@iconectiv.com

Dated: July 14, 2014

---

8 See *id.*, 29 FCC Rcd at 4304 ¶ 104, 4348-49 (proposed Rule Section 96.47).