Report of the Enforcement Subcommittee Commerce Spectrum Management Advisory Committee (CSMAC) July 24, 2018

Members

Larry Alder	Mary Brown	Mark Crosby
Mark Gibson	Dale Hatfield	Paul Kolodzy
Mark McHenry	Janice Obuchowski	Rick Reaser
Dennis Roberson	Andrew Roy	Mariam Sorond
Bryan Tramont	Jennifer Warren	Bob Weller

CSMAC
Enforcement Subcommittee
Recommendations/Comments
July 24, 2018

Our objective is to "Assess the extent to which SAS/ESC systems and technologies may be able to support automated interference prevention, detection, and resolution" ("IPDR").[1] The Subcommittee has broken this question into technical, legal, and policy components, namely:

Technical Capabilities *– What are the technical capabilities that are available today, and what can be the technical capabilities available in the near future for interference prevention, detection, and resolution?*

1. **Interference Prevention** is the practical understanding of the impact of one signal on another and the establishment of conditions and techniques that will make those signals compatible. We note that:[2]

    a. Interference prevention includes understanding how the systems are used, their physical and radio frequency environment (emissions and reception by devices), signal propagation (either by *in situ* measurements or by modeling), and waveform compatibility (which includes defining the appropriate interference metric(s) such as SINR, statistical impact on application, etc.).

    b. Current SAS/ESC systems that are under development for the 3.5 GHz band have many well-defined characteristics for one side (commercial) of the interference prevention analysis. These include use of protection/exclusion zones, reception levels of CBSD devices and propagation characteristics as analyzed and managed through the SAS.

    c. The second side of the analysis for SAS/ESC systems (the government system and the impact of non-government systems on them) has been completed through analysis of information from the ESC and the instantiation of that information within a third-party infrastructure (the SAS).

    d. The ESC capabilities being deployed for the 3.5 GHz band (as well as the RF monitoring systems under development for AWS-3) are limited in scope but demonstrate the capacity to create sophisticated environmental monitoring that could be used for both interference protection as well as interference detection.

---

[1] Some members of the Sub-Committee recommended that the automated spectrum enforcement activities should be described as "Detecting, Classifying/Identifying, Locating, Reporting, Mitigating and Remediating."

[2] Multiple-Input, Multiple-Output (MIMO) creates new issues for interference prevention due to the non-homogeneous spatial distribution of RF power. Therefore, it is difficult to predict both the location and the statistical distribution of possible interfering sources as well as the impact of an interferer on a MIMO receiver.

e. The success of the SAS/ESC approach may indicate that highly integrated devices and infrastructure for advanced telecommunications services that enable large-scale single environment measurements (albeit at lesser sensitivities than specific spectrum monitoring systems) may be possible.[3]

2. **Interference Detection** is the inference or direct observation of interference events. A desirable feature of interference detection is the identification of the interferer or source of interference. We note that:

   a. The 3.5 GHz CBRS band is a demonstration of interference detection by inference where an ESC or CBRS device (CSBD) will report potential interference events to the SAS. Other spectrum users will also report potential interference events to the SAS.

   b. A methodology to validate and accredit a device so that an interference detection function could directly monitor interference events has yet to be developed. Two mechanisms could be investigated:[4]

      i. A means to accredit signal level measurements at a device in order to provide evidential characteristics of an interference event; or

      ii. A means to accredit the detected interference event in order that it may be used as evidence. Securing a consensus baseline from the SASs providers is recommended.

   c. As noted above, a desirable feature of interference detection is the identification of the interferer or source of interference.[5] In the latter case, interference detection through monitoring, the equipment and (potentially automated) processes can also be used in classifying/identifying, locating, and reporting the interference to the associated SAS or regulatory authority. The speed and accuracy of accomplishing all or a portion of these steps depends upon the sophistication of the equipment used.

   d. A commercial system for the identification of the interferer or source of interference has yet to be developed in a direct manner. The Radio Frequency Interference Monitoring System (RFIMS) for AWS-3 may be the first attempt in which an automated system is developed for interference identification purposes. This is an area of research in which the space defines the number of signal identification "tags" that would be necessary to enable the identification of an emitter that is creating interference. This assumes, however, that a single emitter is the cause of interference. This program, however, is presently contingent upon AWS licensee cooperation to permit their devices to be controlled by the RFIMS.

---

[3] There are developments in industry and government on how to aggregate distributed spectrum sensing measurements into a coherent spatial map of RF power.

[4] We note that there are policy implications for commercial SAS providers on how to support this level of enforcement that are beyond the scope of this effort.

[5] It will be necessary to identify the policy ramifications for SAS providers to turn off devices to resolve the cause of an interference event.

3. **Interference Resolution** is the mechanism that either directly or indirectly modifies transmission and/or reception parameters to mitigate an interference condition.

    a. The SAS currently has the capacity to direct a CBSD to change its operational parameters to resolve potential federal user interference events. In the current framework, SASs have the capability to modify device parameters, *e.g.*, power, frequency, bandwidth, etc., to resolve potential interference.

    b. A mechanism is needed to confirm that the indirect resolution action was undertaken and successful. A cause and effect mapping mechanism is needed and event validation confirmation methods will need to be developed to allow devices to return to their previous operational states as soon as practical.

Legal Issues *– What are the legal issues/challenges that must be addressed to implement automated enforcement prevention, detection, and resolution mechanisms?*

a. CBRS technical rules require that the SAS must provide interference protection through a specific scripted process. The models that must be used and the mechanisms that must be employed to determine interference are well defined either by the FCC technical rules or by an agreed-upon third-party (*i.e.*, WInnForum).

b. One legal issue involves liabilities associated with computing or applying the device parameters necessary for prevention. Liability must be defined for:

    i. Harm caused by an interference event if the SAS computed and applied everything correctly

    ii. Harm caused if the SAS computes the same incorrectly

    iii. Operations that are suspended to prevent interference where actual interference was unlikely, and

    iv. Interference from rogue, malicious or non-compliant devices.

c. The purpose of interference detection within the CBRS band is to both mitigate the interference event and provide feedback to control/prevent further interference. So, the same legal liability issues detailed in (b) probably apply.

d. To the extent an automated system resolves actual interference, there is a need to investigate legal (or policy) precedents for the broader resolution role of SASs.

e. To the extent automated systems are capable of resolution of actual interference, then to the extent regulators wish to access, or act upon (such as in an enforcement proceeding), the facts of the resolved interference event, additional legal questions are raised. Interference detection for evidentiary proceedings is a complicated process associated with a documented chain of custody. Automated systems may permit regulators to utilize data from non-government entities as evidence. The specifics of what data, how it would be

obtained, and how it might be used, should be specified with reference to underlying legal authority.

Policy Issues *– What are the policies that could be implemented to generate support for an automated enforcement prevention, detection, and resolution mechanism, or conversely, cause fears/concerns from participants?*

a. It is recommended that NTIA/Federal Agencies identify desired policy objectives. Specifically, should users of the band be required to forgo certain aspects of anticipated privacy for the benefit of a safer spectrum environment and/or access to the band?

b. It is recommended that the automated enforcement activities be divided between *ex ante* and *ex post* processes as the former can be substantive including matters such as equipment labeling, consumer education, enforcement advisories and aspects of equipment authorization.

c. It is recommended that the certification process for SASs and devices be fully defined. Stakeholders must be confident that SASs and devices will function properly. The roles of the regulators, SAS providers, device providers and operators must be well defined.

d. SASs should continue to retain the proactive capability to allow federal users in bands designated for sharing to claim or reserve channels or bandwidth in support of their superior spectrum rights (to the extent applicable), equal rights with commercial users (to the extent applicable) or future bidirectional rights to the extent specified.

e. Malicious jamming and spoofing, which are increasingly easy to accomplish, would put enormous stress on all of the elements of the SAS/ESC system. It is suggested that NTIA address the adequacy of the CBRS system to deal with such destructive interference, and the role SASs may provide in the future.

f. Whether gathered by an SAS or other responsible entity, it is recommended that NTIA take appropriate steps to ensure that the data collected during the monitoring process is sufficient to provide accurate information on the classification, identification, and location of the interference source.

g. It is further recommended that NTIA undertake, or cause to be undertaken by an appropriate body, a forward-looking study to better understand:

    i. The relationships between the increasing capabilities of monitoring equipment and processes and the speed and accuracy of detecting, classifying, identifying, location and reporting interference incidents;

    ii. Privacy and other issues that are implicated by these increasing capabilities; and

    iii. The optimum tradeoffs associated with increased technological capabilities and privacy requirements.

h. The regulatory authorities should reexamine the extent to which resolution mechanisms can be employed among license holders and the mechanisms to address potential conflicts. Delineation of the duties of the SAS will need to be specified by rule. SAS may operate as (a) a “traffic cop” only, (b) a “traffic cop” + investigator, or (c) a “traffic cop” + investigator + decision-maker with the power to change the way a participant operates in the shared band.

i. It is recommended that a policy framework be developed with a clear delegation of authority to the SAS, detailing the responsibilities and liabilities of the participants, including exempting a SAS from liability when acting in good faith pursuant to its responsibilities. These responsibilities will vary depending on whether the SAS is managed by a regulatory body, if it functions are performed on a commercial basis, or whether the responsibilities are delegated or subcontracted by a federal authority to a private entity.