



Enforcement Subcommittee

July 24, 2018

Subcommittee Members

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

Objective

“Assess the extent to which SAS/ESC systems and technologies may be able to support automated interference prevention, detection, and resolution today and potentially in the future” ...

Response Organization

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

Major Conclusion 1

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.

Major Conclusion 2

A commercial system for the identification of the interferer or source of interference has yet to be developed in a direct manner. Although not an SAS/ESC capability, 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.

Major Conclusion 3

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.

Major Recommendation 1

One legal issue involves liabilities associated with computing or applying the device parameters necessary for prevention. It is recommended that NTIA investigate with the FCC the definition of liability for:

- Harm caused by an interference event if the SAS computed and applied everything correctly;
- Harm caused if the SAS computes the same incorrectly;
- Operations that are suspended to prevent interference where actual interference was unlikely; and
- Interference from rogue, malicious or non-compliant devices.

Major Recommendation 2

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.

It is recommended that NTIA and the FCC develop 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.

Major Recommendation 3

A methodology to validate and accredit a device so that an interference detection function could directly monitor interference events has yet to be developed. It is recommended that NTIA investigate two potential mechanisms:

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

Major Recommendation 4

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?

Major Recommendation 5

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

- The relationships between the increasing capabilities of monitoring equipment and processes and the speed and accuracy of detecting, classifying, identifying, locating and reporting interference incidents;
- Privacy and other issues that are implicated by these increasing capabilities; and,
- The optimum tradeoffs associated with increased technological capabilities and privacy requirements.