Commerce Spectrum Management Advisory Committee (CSMAC)
Spectrum Management via Databases Subcommittee

Draft Recommendations
October 9, 2014

Question we are addressing:
"How can sensitive and government classified operations be included and protected using a database-driven sharing approach, particularly one that strives toward real-time responses?"

Draft Recommendations:

- **Start Now**
  - Effective sharing can be implemented now on case-by-case basis. For example, reasonable protection zones based on power levels and sensitivity, while not optimal, can be a starting point for sharing that likely doesn't require sensitive information disclosure.
  - Leverage characteristics of federal systems that are sufficient to permit sharing while not compromising their sensitive characteristics. (e.g.; record the characteristics needed for sharing as data elements to be used as a baseline to creating the SAS.)
  - Find solutions that work by band and by system; don't try to find a single solution (e.g.; document the models and simulations used in a repository for later incorporation into the SAS.).
  - Implement the SAS concept in the 3.5 GHz band within 36 months.
  - Monitor current research on sharing methodologies (e.g., DAPRA's Shared Spectrum Access for Radar and Communications (SSPARC) program).
  - See reference document on information needed for sharing (link).

- **Begin path to implement federal SAS/black box technique to address federal data sharing concerns as parallel track to sharing now, but it should not be a constraint to getting started with sharing.**
  - A federal SAS is a black box system where commercial SAS requests are made to use or share specific spectrum and the federal SAS returns a response that allows the sharing to take place without exposing sensitive data on federal systems. This is similar to what was done in 70/90 GHz band. [See Tools section below]
  - Pros: Protects sensitive federal information while permitting sharing through operation of the commercial SAS. Promotes actual sharing (as opposed to protection zones) and draws maximum benefit from SAS.
  - Cons: Lacks sufficient transparency. Will take significant time, effort and budget to implement and industry cannot wait. Federal SAS may need to

interface directly with devices or device controllers, may increase network overhead.
    - *Conclusion*: Black box may be feasible, but should not overused to solve all cases and should not be required to commence sharing.

- **Review data and information classification procedures in light of the requirement for commercial/federal spectrum sharing. Procedures should be updated as necessary to promote spectrum sharing while still protecting the intent of data classification.**
    - The issue of data classification is a barrier to broad-scale spectrum sharing. While proper data classification is imperative to protect national security, this often appears as a means to thwart sharing where otherwise feasible. Designations such as "For Official Use Only" (FOUO) or "Unclassified, Special Handling" seem to be overused.
    - NTIA should study data classification procedures to determine whether these procedures should be revised in light of new approaches to sharing (e.g., SAS).
    - There may also be other ways to provide information sufficient for sharing while not exposing sensitive data. NITA should study data obfuscation techniques to protect sensitive data yet still support bi-directional sharing.

Principles NTIA should follow

1. NTIA should not try to find or promote a single solution
    - Deal with sharing on a case-by-case basis.
    - Find system-specific solutions (e.g., 3.5 GHz ship-borne radar)
    - Ensure constraints are applied only where necessary.
    - Start with a simple, yet scalable approach.
    - Work on confidence-building as we develop sharing approaches for various federal systems in various bands.

2. Look for solutions that reflect current best practices
    - Focus on automating existing process for handling sensitive data in spectrum coordination rather than inventing new policies.
    - Ensure delegated authorities have clear guidelines as to what is sufficient to protect sensitive information. There is a body of academic research on the issues of spectrum assurance, including SAS vulnerabilities that decision makers should become familiar with.

Tools to consider:

- Black box method: Request is made to use/share specific spectrum and black box returns unclassified response, similar to 70/90 GHz. This could also be a Federal SAS that the commercial SAS's could interface with.
- Black Box with obfuscation: To mitigate implied disclosure black box system can obfuscate responses. Pros: Reduces the risk of implied disclosure. Cons: Reduces efficiency of sharing. *Recommendation*: Obfuscating black box responses should be a tool of last resort.

- Leverage characteristics of federal systems that are sufficient to permit sharing while not compromising their sensitive characteristics: There are some characteristics of systems such as radar waveforms that might be sensitive; however, other characteristics such as their location may not be. Pros: Enables sharing of spectrum. Cons: Requires significant engineering analysis and open dialogue among stakeholders to determine what characteristics are non-sensitive and see what level of sharing that allows. ***Recommendation:*** Prioritize bands and systems and find ways for collaboration to leverage non-sensitive characteristics to extent possible. See Government/Industry Collaboration Subcommittee for specifics.

Supporting Information:

- Database system overview which is a generic description of how these types of SAS/dynamic databases work (link) and information on timing considerations for implementing protection (link).
- Discussion document on how to what information is needed for sharing showing that sensitive data is not always needed to be shared (link).
- Jeffrey reed and Jung-Min Park – "Ensuring Operational Privacy of Primary Users in Geolocation Database-Driven Spectrum Sharing (link).