UNLICENSED SUBCOMMITTEE

Draft Recommendations on Enforcement

Submitted for Adoption: CSMAC Meeting
July 24, 2012

Question 1: Enforcement -- What Procedures Should Federal Agencies Have in Place?

> i. **How should Federal agencies deal with complaints of interference received by unlicensed users?**
>
> **ii. How should Federal agencies deal with interference from unlicensed users in the hands of citizens who don't understand the rules?**
>
> **iii. How should we prevent software modifications that alter the compatibility characteristics of a device?**
>
> **iv. With widely distributed products, what is the best approach to enforcing rules when the number of offenders may be significant?**

Summary of Proposed Recommendations

Proposed Recommendation #1*:* To the extent possible, the National Telecommunications and Information Administration (NTIA) should put in place regulatory requirements, and work with the Federal Communications Commission (FCC) on parallel measures, that reduce reliance on post-hoc regulatory enforcement of interference by turning to technology-based solutions for "connected devices." NTIA, in coordination with the FCC, also should proactively educate policymakers concerning the secondary status of unlicensed devices in shared bands and the obligation of consumers and manufacturers to accept interference.

- As appropriate, similar technology requirements should be established for Federal systems and devices that can be connected.

Proposed Recommendation #2: To meet the objective of Recommendation #1, and to the extent possible, the Committee recommends that NTIA, in coordination with the FCC, require that in all new unlicensed bands, or in shared Federal bands designated for unlicensed access, that devices should be "connected devices," which are required periodically to "call home" to: (1) Renew the authorization to operate in the band (e.g., via a certified database, or directly to the manufacturer), (2) Obtain a firmware update, to be remotely disabled in a particular frequency, and/or (3) Receive direction to move to another frequency band when necessary.

- Under this scenario, the burden of interference mitigation would be on manufacturers to rely on technology solutions, lessening the relative onus on consumer education.

Proposed Recommendation #3: In cases when non-compliant devices do not operate within the rules to prevent interference, or when "avoidance through technology" measures fail, NTIA should consider recommending that the FCC strengthen enforcement measures to provide

stronger deterrents, so that interference mitigation may be addressed more proactively than reactively.

- To this end, the Committee endorses the earlier CSMAC recommendations regarding enforcement measures, summarized below.

Proposed Recommendation #4: In cases when it is not a matter of unlicensed devices intentionally operating outside of the rules, but interference still occurs, manufacturers should increase consumer education efforts about the operating parameters of Part 15. NTIA should work with the FCC and with industry (e.g., manufacturers) to ensure that consumer awareness provides an important counterpart or "backstop" to enforcement and "avoidance through technology" efforts.

Proposed Recommendation #5: The Committee recommends that NTIA, in coordination with the FCC, undertake further study of the regulatory treatment under the current unlicensed framework for "cheap, dumb" devices. The Committee generally recommends that in the future "unconnected" devices should be restricted to legacy bands of spectrum where they are already prevalent (e.g., 900 MHz, 2.4 GHz). Policymakers should consider whether such devices should even be further restricted in the future, phasing out their access to very high-quality bands over an appropriate time period.

Discussion:

i. How should federal agencies deal with complaints of interference received from unlicensed users?

The Committee's proposed recommendations are guided by two types of unlicensed wireless operations, which generally argue for different courses of preventative measures and remedies when it comes to interference, as discussed below:

- Untethered consumer devices and systems, which typically are less expensive and/or legacy devices.
- Connected equipment that can essentially be required to "call home" periodically (e.g., to contact a spectrum management database) and take mitigation steps when interference occurs, including the possibility of automatic shut off or losing access to particular frequencies.

The cases of garage door opener interference, wireless microphones and the TV white spaces band, and 5 GHz consumer devices highlight the differences between unconnected devices and connected equipment when it comes to interference and potential solutions. Manufacturers and operators (e.g., Wireless Internet Service Providers) may face certain requirements, such as through the equipment certification process, which can help anticipate and resolve interference issues through measures such as periodic reauthorization and firmware updates. *(See Appendix A)*

Proposed Recommendation #1*:* To the extent possible, NTIA should put in place regulatory requirements, and work with the FCC on parallel measures, that reduce reliance on post-hoc regulatory enforcement of interference by relying on technology-based solutions for connected devices. NTIA, in coordination with the FCC, should also proactively educate policymakers

concerning the secondary status of unlicensed devices in shared bands and the obligation of consumers and manufacturers to accept interference.

- As appropriate, similar technology requirements should be established for Federal systems and devices that can be connected.

(a) How will consumers recognize degradation and its cause?

Avoidance Through Technology: Regardless of whether they are using "connected" or "unconnected" devices, the challenge for consumers in an increasingly congested spectrum environment is to recognize interference as the source of degradation of performance of an unlicensed device. This requires a consumer to be able to isolate an interference issue from a configuration issue. For many consumer wireless systems, as is the case with WiFi (IEEE 802.11), a consumer must verify and ensure that the plethora of configuration settings are applied correctly prior to pursuing an interference remedy. Additionally, radiofrequency (RF) interference and the resulting degradation of service are not easily detectable by consumer available products and devices.

Another factor is the complexity of performing the spectral analysis to identify the offending signal. Furthermore, given the widespread – and growing – consumer adoption of these wireless systems, the problem of interference and performance degradation will only worsen. Therefore, the best approach to managing degradation due to interference is avoidance through technology. Technology is capable of detecting signal clarity and can hop to another clearer channel to transmit. Additional evolution of technologies should further refine the ability to manage around noisy RF spectrum without the knowledge of the consumer.

The committee recommendation is for NTIA, in coordination with the FCC, to encourage adoption of technologies that:

- Have been designed to operate in a shared spectrum environment; and
- Avoid contentious noisy channels through auto-sensing and channel management capability.
    - This could include, but is not limited to, Frequency Hopping Spread Spectrum type technologies.

ii. How should Federal agencies deal with interference from unlicensed users in the hands of citizens who don't understand the rules?

(a) Is it possible to do prevention/education at the consumer level?

Possible scenarios for which Federal government spectrum users may have to address complaints from unlicensed users largely fall into two categories: (1) Legacy, "untethered" Part 15 systems that do not reflect the current state of technology, and generally do not have the flexibility to respond quickly when primary users change operating conditions in a band (e.g., garage door openers.). (2) Newer unlicensed technologies (e.g., database-dependent cognitive radios) for which the implications of Part 15 rules to Federal users may require real-world operating experience to fully understand (e.g., 5 GHz Dopplers).

Relative Lessening of Onus on Consumers: Both the cases of garage door opener interference and interference from unlicensed devices into 5 GHz weather radar bands underscore the limitations of consumers' ability to identify, in real-time, sources of interference. Given the extent to which even less expensive unlicensed equipment is now connected to the Internet, consumer education per se will become less important if connected equipment has requirements to, for example, "call home" to proactively manage interference issues and thus prevent performance degradation in the first place. Under this scenario, technology-based solutions mean that the onus for identifying interference would not be on the consumer. In the case of garage door openers, the interference was relatively easy to identify given the volume of complaints and proximity to military installations.

However, on a going forward basis, sources of interference are likely to be more dispersed, complex and difficult to pinpoint. Garage door openers highlight the extent to which – even when a source of interference is known – the implications to users may not be easy to anticipate. A 2005 FCC Public Notice on the garage door issue said: "It is not possible to predict in advance which specific users or locations near military bases may experience interference, because of the variety of technical characteristics of garage door controls and configuration of the mobile radio systems."[1] Regarding the 5 GHz Doppler radar scenario, this interference case also points to the challenges of enforcement when – intentionally or inadvertently – unlicensed users are creating interference for authorized Federal users.

Increasing Connectedness of "Things": While consumer education is always useful in reducing unexpected behaviors, a better approach may be to make sure that a consumer is not required to be in the loop for mitigation efforts when problems occur. Looking forward, the vast majority of sharing opportunities are likely to involve devices that are inherently connected to the Internet in some way, or at least capable of connecting. The demand for spectrum is driven largely by the desire to provide higher bandwidth and more ubiquitous communications solutions, which means that use cases like the legacy garage door opener problem are not likely to be the primary reason to do future sharing. (Indeed, even for garage doors, future whole home management solutions are likely to use real communications rather than signaling to do things like opening doors. For example, multi-purpose and connected devices such as smart phones could replace garage door openers, locks, and security system enabling.)

Manufacturer Responsibility: Once we assume that interesting future cases will involve connected devices, it becomes easier to put the heaviest burden of mitigation on manufacturers, where the expertise to understand the issues exists. For example, certification might require that a device reauthorize itself by contacting its manufacturer over the network every so often (e.g., once per week). Failure to do this (allowing reasonable margin for network outages) would, by rule, require the device to disable sharing sensitive spectrum until such reauthorization can be done. Combining this reauthorization with the ability to force firmware updates would give the manufacturer and the regulator the tools to do complete and timely mitigation.

---

[1] FCC Public Notice, Office of Engineering & Technology, Feb. 15, 2005, hraunfoss.fcc.gov/edocs_public/attachmatch/DA-05-424A1.pdf. While the Notice said DoD was making reasonable efforts with NTIA, and the FCC was working with the garage door opener industry, it added: "For security reasons, the Department of Defense cannot make information broadly available in advance as to the deployment of the new mobile radio systems."

In the 5 GHz Doppler Radar case, the first step after identifying the problem might have been to cause all certified units to disable any access to the sensitive band, thus immediately mitigating the interference. After this, engineering analysis that demonstrated most manufacturers' equipment was not creating problems would have allowed those manufacturers to reauthorize their units, while problematic systems would have been forcibly updated to corrected firmware before reauthorization. Had this type of mechanism been available, the entire Doppler Radar issue could have been addressed with virtually no consumer exposure to degradation issues and rapid mitigation for the radars using the band.

A similar approach makes sense for cases of sharing based upon band/location databases for such things as higher power white spaces applications. Again, if devices are required to reauthorize periodically, then so long as the appearance of a new licensed user (e.g., new TV station) can be anticipated in the database update early enough to guarantee that all devices will reauthorize before the new station deploys, sharing can be accommodated.

The lesson to be drawn here is that since the demand for spectrum is arising from the explosion of smart devices that need to communicate, we should use those same "smarts" to enable safer sharing scenarios. The continued decrease in product costs makes this approach feasible even for very low end or low cost devices. Further, such low cost, less sophisticated devices already have significant access to existing unlicensed spectrum allocations, without requirements to rely on technology to renew an authorization to address interference issues or firmware upgrades.

Finally, if this approach to primarily allowing sharing via smart devices is to take hold, the U.S. may need to take a leadership position in the international community to advance this more holistic approach to sharing controls.

***Proposed Recommendation #2*:** To meet the objective of Recommendation #1, and to the extent possible, the Committee recommends that NTIA, in coordination with the FCC, require that in all new unlicensed bands, or in shared Federal bands designated for unlicensed access, that devices should be "connected devices" that are required periodically to "call home" to renew the authorization to operate in the band (e.g., via a certified database, or directly to the manufacturer), to obtain a firmware update, to be remotely disabled in a particular frequency, and/or to receive direction to move to another frequency band when necessary.

- Under this scenario, consumers would not face the burden of awareness of interference mitigation options, for which the responsibility would lie with manufacturers to rely on technology solutions.

The previous CSMAC adopted recommendations on enforcement measures in a report from the Interference and Dynamic Spectrum Access Subcommittee.[2] That report recommended: "The NTIA, the FCC and government entities with spectrum management responsibilities need to shift from an interference prevention only approach to both prevention and rapid resolution of problems that occur." To that end, the current Committee's work endorses and builds on those recommendations by focusing on the "prevention" side of the equation via an "avoidance through technology" approach when possible.

[2] See Subcommittee Report at http://www.ntia.doc.gov/advisory/spectrum/meeting_files/11082010/CSMAC_11082010doc_BLACK.pdf.

While prophylactic technology solutions can increase the cost of devices at the margin, unlicensed devices and users typically benefit from zero or low costs for spectrum access, which presumably will continue on bands shared with primary Federal or other licensed services. As a condition for unlicensed access to bands shared with sensitive Federal systems in particular, such devices can be required periodically to renew the authorization to operate, and/or update the "terms of use" governing access to a band, by connecting to a spectrum management database (e.g., the TV bands geolocation databases certified by the FCC to govern access to vacant TV channels).

Even when technology-based requirements make such avoidance measures possible, industry still requires the reinforcement of meaningful enforcement provisions and consumer education to provide a strong incentive to prevent such measures from being poorly executed.

The Dynamic Database Approach to Device Reauthorization and Updates: On a going-forward basis, a requirement that devices and systems sharing a band on an unlicensed basis should be "connected" devices seems particularly feasible considering the potential use of geolocation databases to enforce permissions and terms-of-use updates on an automated basis. The use of databases to control cognitive radios in shared-spectrum environments has been the key aspect of the FCC's TV White Space (TVWS) proceeding. One indication of the potential embodied in this concept is the fact that the FCC has conditionally certified ten TVWS database administrators (including Google and Microsoft). In addition, several other regulators are considering a similar approach to opening TV spectrum for unlicensed use, including Ofcom in the UK and Industry Canada. The concept of database-enabled cognitive radios can lend itself to many applications, including ultimately sharing spectrum with Federal users. (*See Appendix B for a detailed example of how an unlicensed device reauthorization via database could work.)*

For TVWS, the databases contain information on all incumbent operations, including certain unlicensed wireless microphones. The majority of these data are for licensed facilities that are managed through the FCC's licensing systems (i.e., the Universal Licensing System and the Consolidated Broadcast Data Base System). Other data not in the FCC's licensing systems are entered directly into the databases by the users, including temporary frequency reservations by licensed wireless microphone operators.

The database calculates the list of available channels based upon the specific information provided by the device upon a query. A query request includes location information, antenna height, device type, FCC certification information, device serial number as well as other data. Upon a device query, the database calculates the list of available frequencies and sends this information back to the device. No raw data is device-facing.

TVWS devices must check with the database whenever they move more than 50 meters (for nomadic devices) or within at least 48 hours (for both fixed and nomadic devices). Devices that fail to check with the database within the prescribed time frame can be de-registered. De-registered devices must contact the database administrator to re-establish their permissions.

The current U.S. framework calls for the TVWS database to serve several roles, including both permission to transmit (based on geolocation) and enforcement. Given that the FCC certification

ID and device serial number are part of a device query, the FCC requires database administrators to verify the validity of the device's certification ID against the FCC's Equipment Authorization System. In addition, the FCC will establish procedures to disable either single devices via device serial number or whole classes of devices via the FCC certification ID based upon enforcement procedures.

As mentioned above, the concept of database-enabled cognitive radios can be applied to sharing spectrum with Federal systems. The fact that no data are device facing helps to maintain the integrity of the Government Master File, which is the database of all the Federal frequency assignments managed by the NTIA. The safeguarding of classified data should also be considered within this framework. The enforcement concerns can be studied and expanded upon as necessary. As mentioned within this report, regular and frequent database interaction can also be used to update device firmware. The take-away is that database-enabled devices allow for much more robust and real-time spectrum sharing whether in commercial, Federal, or shared allocations.

The discussion of the use of a data base presupposes the availability of information about existing interference problems and patterns, as well as the available solutions. One of the challenges highlighted in the case studies in Appendix A is identifying these problems and patterns. A tool that may help address this challenge is the establishment of a voluntary Interference Clearinghouse website to leverage the power of "crowd sourcing." This idea will be explored in more detail during the next CSMAC cycle.

Proposed Recommendation #3: As a fallback, in cases when non-compliant devices are knowingly not operating within the rules to prevent interference, or when "avoidance through technology" measures fail, NTIA should consider recommending that the FCC strengthen enforcement measures to provide better deterrents, so that interference mitigation may be addressed more proactively than reactively.

To this end, the Committee endorses the earlier CSMAC recommendations regarding enforcement measures, summarized below.

- Put in place streamlined interference reporting tools to complement "spot monitoring" of new operations.
- Increase penalties for violations. There should be a tiered series of penalties for violations of existing spectrum management rules that cause interference, with increased penalties, especially for incidents that put safety-of-life systems at risk.
- Increase budgetary resources for monitoring and enforcement. Budgetary funding should be increased to facilitate increased laboratory testing and field monitoring by the FCC and NTIA after new rules are implemented for advanced wireless technologies. Several sources of funding should be explored.
- Per the FCC's Fiscal Year 2011 budget proposal language to resolve "100% of non-emergency interference complaints" in one month, NTIA should encourage the FCC to expand this to a broader "shot clock" approach to responding to interference complaints so that licensees and operators of unlicensed devices have certainty on the timetable.
- Develop tools for Temporary Restraint of Interference (TRI). Government entities responsible for spectrum management should establish a process, similar to a temporary restraining order, to address egregious interference complaints immediately. Upon a bona

fide showing of interference from a specific device, class of devices or service, an entity receiving such interference should be able to file a complaint with the appropriate government agency. Upon an appropriate showing, the device or entity causing the interference shall cease such harmful transmissions, while the case is being examined by the appropriate agency.

- Develop and explore the use of remote shut-off technologies for resolving interference problems.
- Increase assessments/Test-Bed approach. The ability of cognitive radio (software defined radio) technology to sense the surrounding RF spectrum environment can be harnessed to assist in reporting cases of "bad actors" in which nearby RF emitters are operating outside of their permissible parameters and causing interference.
- More stringent equipment authorization will be an important tool in facilitating spectrally efficient equipment. It may be appropriate for the FCC and NTIA to review equipment authorization practices, such as spot checking, to ensure incentives to manufacture and distribute spectrally efficient equipment consistent with the FCC and NTIA rules.
- Establish a streamlined process for the maintenance and retention of interference reporting and enforcement data. Such data should include documentation of interference that may be caused by legally authorized operations. Analyzing these data will provide an ongoing assessment of FCC and NTIA spectrum management and enforcement policies.
- Explore through legislation, regulations or industry/government agreements, the ability of the Federal government to expand its enforcement of spectrum interference rules, especially as it may relate to public safety and law enforcement.

Proposed Recommendation #4: In cases when it is not a matter of unlicensed devices intentionally operating outside of the rules, but interference still occurs, manufacturers should increase consumer education efforts about the operating parameters of Part 15. NTIA should work with the FCC to ensure that in such cases they work with industry (e.g., manufacturers) to ensure that consumer awareness provides an important counterpart or "backstop" to enforcement and "avoidance through technology" efforts.

The Work Plan for the current CSMAC asked a series of questions about Federal agency responses to interference, including: (1) How should Federal agencies deal with complaints of interference received by unlicensed users? (2) How should Federal agencies deal with interference from unlicensed users in the hands of citizens who don't understand the rules? (3) How should we prevent software modifications that alter the compatibility characteristics of a device?

Voluntary coordination on education, would entail Federal users who receive complaints referring consumers to industry groups, companies and Federal regulators who could provide information about Part 15 limitations and the operating strictures under which their own devices operate.[3] However, this approach would entail the private sector developing awareness efforts and understanding upfront the limits of Part 15 rules.

As discussed in further detail in Appendix A, both the interference case studies of garage door openers and 5 GHz Doppler Radar provide "lessons learned" concerning how coordination efforts have resulted in the past in greater consumer awareness of why interference was occurring and

[3] Among the resources available are a 1993 FCC Office of Engineering and Technology Handbook, "Understanding the FCC Regulations for Low-Power, Non-Licensed Transmitters," http://transition.fcc.gov/Bureaus/Engineering_Technology/Documents/bulletins/oet63/oet63rev.pdf.

what steps they (or others) could take to mitigate it. As discussed above, however, consumer awareness/education is an effective supplement to, but not a substitute for, more forward-looking measures, such as avoidance through technology and stronger enforcement tools.

As one example cited below, after garage door opener interference cases began to be documented following the rollout of authorized DoD Land Mobile Radio (LMR) systems, NTIA established a work group that resulted in:

(1) DoD providing LMR rollout locations to manufacturers and the ranges of spectrum affected through FY 2010.
(2) DoD conducting analyses on the likely extent of potential interference from LMR systems in several areas to provide the findings to major manufacturers.
(3) Manufacturers offering retrofit kits to change the frequencies of existing openers. For new devices, one manufacturer moved away from the 390 MHz range, and another announced plans for a multi-frequency approach to minimize potential interference.

Proposed Recommendation #5: The Committee recommends that NTIA, in coordination with the FCC, undertake further study of the regulatory treatment under the current unlicensed framework for "cheap, dumb" devices. The Committee generally recommends that in the future "unconnected" devices should be restricted to certain bands of spectrum where they are already prevalent (e.g., 900 MHz, 2.4 GHz). Policymakers should consider whether such devices should even be further restricted in the future, phasing out their access to very high-quality bands over an appropriate time period. At the same time, the Committee recognizes that for the foreseeable future one or more unlicensed bands should remain accessible for untethered, single-band or otherwise "dumb" devices.

To address legacy devices that may not be connected to the Internet with enough frequency for an effective "call home" technology-based approach, the Committee discussed several potential options for consideration. These options were informed, in part, by a recognition that untethered devices will continue to be available in significant volumes in the future given the disproportionate cost trade-offs that would be entailed in requiring every device to be able to phone home (e.g., wireless picture frames). These options were discussed with regard to how to manage the expansion of unconnected devices in the future:

(1) Designated band: Under this approach, unlicensed bands such as 2.4 GHz and/or 902-928 MHz could be designated as the only spectrum where unconnected devices could operate.

- *Pros*: This would be a direct way to limit devices that are not frequency hopping or capable of autonomously receiving firmware updates to a particular band designated for systems with similar characteristics.
- *Cons*: The challenge is that this approach would not per se lead to a reduction in less sophisticated unlicensed devices on certain very high-quality spectrum bands.

(2) Designated band with deadline: Under this approach, a deadline would be set by which unconnected devices would be restricted to a particular band (e.g., 2.4 GHz.), which would raise the technology bar for new certifications for devices in other unlicensed bands to account for requirements such as device connectivity and control.

- *Pros*: This provides a migration strategy for grouping together types of unlicensed devices and provides an incentive for devices to meet technology requirements.

- *Cons*: It remains a challenge as to how to address legacy devices in bands that would be reserved in the future for connected devices. Also, Committee members raised for awareness the issue of international coordination, in that the global market for electronics, which is focused on low-cost models, makes it challenging for the U.S. to be a sole determinant of standards baselines. If certain devices are banned in certain bands in the U.S., but they proliferate in the international market, import controls would be hard-pressed to control for certain regulatory outcomes.

As noted above, cross-border marketing issues of unlicensed devices present challenges across the global marketplace regarding compliance with equipment certification and effective interference prevention and enforcement measures, particularly when equipment is manufactured in one country and operated in countries with different regulatory restrictions. The ability of administrations to track noncompliant equipment, in terms of tracing back the source of interference to devices designed or manufactured offshore, is difficult. Another challenge is presented when consumers have the ability to manually override operating restrictions (e.g., flipping a switch for dynamic frequency selection [DFS]) as part of designs to ensure compliance within a certain country's regulatory framework. Collectively, these challenges underscore the importance of preventative, rather than post-hoc, compliance efforts.

Among commonly recognized tools for addressing cross-border issues for equipment certification, testing and compliance are Mutual Recognition Agreements (MRAs). The European Union, for example, has MRAs between the Union and countries such as the U.S., New Zealand and Canada, which address reciprocal acceptance of testing, certification and approval of products in different countries based on EU requirements. A recent Communications Regulators' Association of Southern Africa report noted: "Manufacturers in these countries can therefore certify their products in their home countries based on the EU rules, which is sufficient for placing such equipment on the EU market. MRAs could be considered by individual countries for those involved in manufacturing [Short-Range Devices] SRD devices for the export market."[4]

At the same time, European Market Surveillance Authorities have issued reports as part of a Joint Cross Border R&TTE (Radio Equipment and Telecommunications Terminal Equipment) Market Surveillance Campaign that point to challenges of post-hoc enforcement. The scope of the campaign included the assessment of compliance of products with the administrative requirements, including Technical Documentation, and the technical requirements of the R&TTE Directive regarding EMC and radio spectrum." Of note, it found a low level of compliance in the European market with the products surveyed, which included 2.4 GHz products.[5]

Other markets also face similar challenges regarding compliance of cross-border marketing of license-exempt devices. An ITU primer on spectrum use, for example, has noted that Hong Kong has encountered the use of low-power devices that do not conform to local regulations (e.g.,

[4] Communications Regulators' Association of Southern Africa, Framework For The Harmonisation Of Frequencies For Short-Range Devices (SRDs) In SADC, 29 March 2011.

[5] Report on the Third Joint Cross Border R&TTE Market Surveillance Campaign by the European Market Surveillance Authorities in 2008/2009.

requirements for use of a particular frequency), a dilemma that "arises because it is not possible to require overseas equipment suppliers to manufacture to Hong Kong's specifications, nor to prevent people buying from overseas and bringing these devices back to Hong Kong. Banning such devices and prosecuting users would be a harsh reaction in cases where the potential for interference was very low, yet OFTA [Office of the Communications Authority] cannot allow such devices to be used by placing them on the Exemption Order because they can cause interference in some situations."[6]

Possible questions for further study in 2013

(1) How to pay for Federal system relocation or other costs related to facilitating shared access for users?

(2) What methods could be used to "inventory" or identify where in the spectrum specific unlicensed devices are operating?

(3) Further consideration of pros and cons of setting aside new spectrum exclusively for unlicensed, and/or whether additional Federal bands should be made available for unlicensed use on a purely secondary or tertiary basis (as a non-interfering underlay)?[7]

(4) Ability of unlicensed devices to operate in Federal spectrum on a shared, non-interfering basis with Federal systems where that unlicensed access may be temporary or contingent.[8]

(5) Issues regarding international coordination – in an increasingly globalized economy for devices, how do you address requirements to "turn off" if interference is caused when you are talking about devices manufactured and sold beyond US borders?

(6) The establishment of a voluntary Interference Clearinghouse website to leverage the power of "crowd sourcing" by creating a tool for consumers or government operators to file reports of interference to create a "snapshot" of where such incidents may be occurring and when.

---

[6] ITU, Telecom Research Project, Spectrum Management Module, Hong Kong: http://www.elearning.trpc.com.hk/spectrum/section4.php.

[7] At the November meeting Mr. Nebbia said a further question is whether to set aside spectrum for unlicensed, noting that as part of the search for 500 MHz, should other bands be identified for increased use by unlicensed, including in new ways (e.g., higher power levels or increased duty cycles). He noted that unlicensed spectrum such as 900 MHz and 2.4 GHz, have supported both ISM and radar operations "and those things work pretty well together. But, we allowed unlicensed an increased or different operating parameters than the normal across the spectrum types of things. We still do need feedback." With regard to the emphasis of recommendations in areas such as dumb devices, and how are future issues addressed, he noted the issue of key fobs that open cars and whether such devices should require a relationship with a service provider to allow for occasional updates. So he asked, in areas of such devices, what should the government response be?

[8] Greg Rosston noted at the last meeting, per the scope of the committee's work, the importance of thinking about unlicensed devices that would work in Federal spectrum not unlicensed spectrum: "We sort of want to focus on rules that at least for some period of time would be in the Federal Government spectrum. it's possible with the unlicensed devices that operate in federal government spectrum or the Federal Government agencies may ultimately leave the spectrum, so we may set the road path for that. But for right now we're thinking of it as unlicensed devices and how they would interfere or not interfere with that."

Appendix A
"Classic Cases" of Interference

Classic Case #1 – Garage door opener interference: DoD, in 2004, began to deploy new Land Mobile Radios (LMR) that operate in the same range (380 MHz to 399.9 MHz) as many unlicensed low-powered garage door openers were already operating. (Many of these devices had used this spectrum for numerous years prior to the LMR rollout although DoD had been the authorized user on a primary basis for decades and the Part 15 devices – by definition – could not cause, and were required to accept, interference.)[9] Communities around bases where the new LMR systems were being deployed, including Eglin Air Force Base, Florida and Ft. Detrick, Md., complained to manufacturers of interference in 2005. (One manufacturer said distributors received 10,000 complaints.)[10] The garage door openers had been programmed to operate at 390 MHz, but because they used a wide receiver bandwidth, they were susceptible to interference in other parts of the 380-399.9 MHz range, particularly 387-393 MHz. As the authorized user of 380-399.9 MHz, DoD did not have an obligation under Federal rules to identify or mitigate potential interference with Part 15 devices in that spectrum.

Key factors:

All Players Acting Within the Rules: This was a case in which all players were acting within Federal requirements but interference occurred. As a result, the question was not one of enforcement per se but of adjusting consumer expectations and increasing awareness/education about the operating limits of Part 15.

- Further, DoD was deploying new LMR systems in response to a government requirement for narrowbanding.

Interference Hard to Quantify: GAO noted interference was difficult to quantify because problems "may not be reported or may be reported to several different organizations, including device manufacturers and retailers, government agencies, or congressional representatives.)

Interference Varied by Location: There was not interference reported around every site at which DoD was rolling out new systems, with no interference at some sites and different problems when it did occur (e.g., intermittent inoperability to garage door openers not working at all). When complaints decreased, the GAO report said it was attributable to consumer awareness of the problem and the winding down of LMR testing at various sites.)

NTIA Response: In 2005, NTIA's Office of Spectrum Management and FCC's Office of Engineering & Technology created a working group with representation from DoD and device manufacturers to discuss short- and long-term solutions to interference reports.

Nonetheless, GAO noted that increased information was not a panacea: "Information available does not always provide a clear course of action to consumers trying to remedy interference problems. Because of potential confusion, consumers receiving intermittent interference may unnecessarily purchase a new opener, not knowing that the interference may be temporary." It

[9] *See* Government Accountability Office, "Potential Spectrum Interference Associated with Military Land Mobile Radios," December 2005.
[10] Id.

said that while DoD provided guidance to local installations for outreach to potentially affected communities, it was largely reactive (e.g., guidance on how to respond to media inquiries).

A set of proposed principles could help reflect lessons learned from the garage door interference issue, which is a more relevant case study for legacy systems that must adjust to changing operating conditions in a band (vice new unlicensed systems for which deployment scenarios – e.g., white spaces – may make interference harder to pinpoint).

Classic Case #2 – 5 GHz Dopplers: The FCC issued an Order in 2003 to make spectrum available for use by Unlicensed National Information Infrastructure (U-NII) devices, including Radio Local Area Networks (R-LANS), under Part 15. To protect Federal radar systems from harmful interference, the Order required that U-NII devices operating in 5.250-5.350 GHz and 5.470-5.725 GHz bands use DFS and transmit power control (TPC).[11] (Leading up to the 2003 World Radiocommunication Conference, NTIA worked with the FCC, NASA, and DoD to open spectrum at 5 GHz to unlicensed applications.)

- Under DFS requirements, before the start of any transmissions, and through constant monitoring, the device monitors for the presence of radar. If it determines a radar signal is present, it either moves to another channel or enters a sleep mode if no channels are available.
- The 2003 WRC enabled the allocation on a worldwide basis, with the U.S. having actively promoted the allocation with the caveat that the new service employ DFS to protect radar operations.
- After three years of bench and field testing prototypes, the FCC finalized DFS rules were finalized in March 2006[12]; the first DFS device certification was granted in August 2006.

Interference Problems: The FAA in early 2009 reported interference to some Terminal Doppler Weather Radars (TDWRs) that use the 5600-5650 MHz band at locations across the U.S. In early 2009, the Federal Aviation Administration (FAA) became aware of interference to their Terminal Doppler Weather Radars (TDWR) that operate in the 5600–5650 MHz band, and provide measurements of weather hazards for improving the safety of operations in and around 45 major airports.[13]

FCC Response: A 2010 FCC memorandum on the interference issues found that they surfaced as strobe lines or lines on the radar display: "While the radar continues to be usable, such interference is unacceptable and must be eliminated"[14] The FCC said interference at each location was generally caused by a few fixed wireless transmitters operated by WISPs and used in

[11] FCC Report and Order, In the matter of Revision of Parts 2 and 15 of the Commission's Rules to Permit Unlicensed National Information Infrastructure (U-NII) devices in the 5 GHz band, ET Docket 03-122, adopted Nov. 12, 2003.
[12] FCC Memorandum Report and Order, In the matter of Revision of Parts 2 and 15 of the Commission's Rules to Permit Unlicensed National Information
Infrastructure (U-NII) devices in the 5 GHz band
[13] See "Case Study: Investigation of Interference into 5 GHz Weather Radars from Unlicensed National Information Infrastructure Devices, Part I," NTIA Technical Report, TR-11-473, November 2010.
[14] *See* FCC Memorandum regarding 5 GHz Outdoor U-NII Network Equipment, from FCC OET and Enforcement Bureau chiefs to Manufacturers and Operators of Unlicensed 5 GHz Outdoor Network Equipment, July 27, 2010.

the vicinity of airports at high elevations within line of site to the TDWR installations. In most cases, the interference was caused by operations in the same band as TDWRs but there were reports of interference caused by adjacent band emissions. The FCC memo noted that interference fell into 2 categories: (1) Cases in which equipment was not certified or otherwise non-compliant with Commission rules;[15] (2) Instances in which the equipment was compliant, but still caused interference, due to factors such as the configuration of the transmitter, its height and azimuth relative to the TDWR and the device's failure to detect and avoid the radar signal.

Test Efforts: Engineers from NTIA's Institute for Telecommunication Sciences (ITS) and FAA performed extensive field measurements at a site of reported TDWR interference in San Juan, Puerto Rico. A recent presentation by NTIA officials at the Tri-Service Radar Symposium noted the test results found that U-NII interference was either co-channel or adjacent channel to the TDWR operating frequency and both conditions caused visible interference artifacts[16]. The testing found that DFS U-NII devices from certain manufacturers did not detect and avoid the TDWR signal. At that point, the Commission stopped certifying 5 GHz DFS 5 GHz U-NII devices. According to the NTIA presentation:

- Out of seven U-NII devices tested, five detected and avoided the TDWR.

- Devices from certain manufacturers did not detect and avoid the TDWR signal, although they passed FCC certification tests with simulated radar waveforms.

- The tests found that updated simulated radar waveforms (used for FCC certification) would be required to better protect the TDWR. (The NTIA presentation said: "Simulated radar waveform testing results accurately agree with results from actual TDWR system tests; additional testing does not require an actual TDWR.")

Current Status: The presentation noted that NTIA has created new simulated radar waveforms that more accurately replicate the TDWR for the Commission to use in its certification process; NTIA has tested DFS U-NII devices against these waveforms in a laboratory setting.

- In the meantime, the 5600-5650 MHz TDWR band is not available for use by DFS U-NII devices.

- Manufacturers whose U-NII devices did not detect TDWR signals have altered their detection algorithms and are now able to detect TDWR signals; this functionality can be retroactively deployed to existing legacy devices via firmware updates.

Solutions: The FCC noted in its memorandum last year that stakeholders in the 5 GHz interference issue had agreed to several steps: (1) FAA provided information on the locations of each of the TDWRs. (2) The Wireless Internet Service Providers Association (WISPA)

[15] The Memo noted: "We remind operators and manufacturers of UNII devices that any use or marketing of equipment that has not been certificated as required under the FCC rules or that has been modified such that it no longer complies with the certification requirements will result in FCC enforcement."

[16] *See* "Case Study: Investigation of Interference into 5-GHz Weather Radars from Unlicensed Wireless Devices," presentation to the 2011 Tri-Service Radar Symposium Spectrum Workshop (June 27, 2011, by John Carroll, Frank Sanders, Robert Sole, NTIA.

voluntarily agreed to provide information on the location of the TDWRS relevant to WISP and to encourage operators that install devices within 35 km or the line of sight of the TDWRs to operate at least 30 MHz away from the TDWR operation frequencies. (3) WISPA has voluntarily set up an online database and registry –at http://www.spectrumbridge.com/udrs/home.aspx -- with detailed information about (TDWR systems and registered UNII devices.

Appendix B:
Example: Permissions and Reauthorizations Using a Dynamic Database Approach

There are many technical approaches that would provide the solution to having unlicensed devices certified for certain shared bands automatically reauthorize, but it was clear in our discussions that providing at least one concrete design approach would assist in understanding what is intended and in providing credibility to the approach for the Federal users whose spectrum might be being shared. The following example is provided only as an example and is not intended as a proposed required design:

A device certified to operate in one of these shared bands will be required to reauthorize its compliance with band rules periodically by querying an online database provided by the government (or contractor). Reauthorization will be required every *x* days (this interval can be chosen to be fairly large to limit load on the network and database and still provide real world responsiveness to discovered design errors in devices). If it cannot contact the reauthorization database within *y* days after it is required to reauthorize, or it is refused reauthorization by the database, then it must cease operation on the shared bands until it can again receive authorization, probably after getting a firmware upgrade from its manufacturer. The query to the database will contain the device type (i.e., manufacturer/model), a cryptographic hash of the current firmware and hardware version of the device, as well as (possibly) geo-location information if the band requires such. The government database contains for each licensed device type a list of acceptable hash codes and whatever geo-location limits the band is specified with. The database returns a reauthorization response if the query indicates that the device is operating with acceptable firmware/hardware version in acceptable locations. If the firmware/hardware version is not in the database, then the response so indicates. This permits the device to then query its manufacturer's website for updated firmware, or to otherwise notify its user that it needs servicing. If the location information indicates that the device may not operate based on where it currently is, a different failure code is returned so that the user again can understand the reason for the device becoming non-functional.

The database must provide an online interface to the manufacturer so that he can update it with new firmware hash codes when new firmware is released (after passing whatever certification tests are required by the license). Note that there may well be multiple versions of firmware available for the device, any of which allow authorized use, so the database must support this. If an issue with the proper operation of the device is raised to the manufacturer which requires that certain versions of the device stop working, then the database is updated (by the manufacturer or by the government if necessary) to remove those hash codes.

The result of a system of this sort is that in the event that a post release problem is found in the operation of a device that causes it to interfere with other users in violation of its certification conditions, all such devices in the field will stop operation on the relevant bands within at worst x+y days. If the problem can be fixed with new firmware then a smart device can update itself (or at worst have its user update it) with corrected firmware and resume operation, possibly with virtually no gap in service if the manufacturer's fix is made quickly enough. Devices whose manufacturers have gone out of business before a problem is discovered are handled by the government having a process to simply invalidate their errant versions, possibly with no fix available. In all cases, the government user whose spectrum is being shared is protected within some predefined time guard band agreed to when the spectrum sharing arrangement was created.

It is worth noting that this is a very simple design for illustrative purposes only. A realistic design would probably allow for adjusting the time between reauthorizations based upon experience with versions of a device (a device that has functioned correctly for a few years probably could reauthorize less frequently). It would incorporate more distributed operation (versus this description which suggests centralized operation), handle devices that operate via an access point that may provide surrogate intelligence for authorization, incorporate international operation issues, and probably do many other more sophisticated things.