APPENDIX B

PART 15 UNWANTED EMISSION SEPARATION DISTANCE ANALYSIS

In the Notice Proposed Rulemaking (NPRM), the Federal Communications Commission (Commission) proposes an in-channel power level of 6 watts or 38 dBm for higher powered unlicensed devices employing cognitive radio technologies.[1] The NPRM also proposes to limit the unwanted emissions for these higher powered unlicensed devices to the levels specified in Section 15.247(c) of the Commission's Rules.[2] Section 15.247(c) specifies that unwanted emissions in any 100 kHz be at least 20 dB below that in the 100 kHz bandwidth within the band that contains the highest level of the desired power. The unwanted emission level based on the Commission's proposal is:

$$38 - 20 = 18 \text{ dBm}$$

Converting this level to a reference bandwidth of 1 MHz results in an unwanted emission level:

$$18 + 10 \text{ Log } (1\text{x}10^6/100\text{x}10^3) = 28 \text{ dBm}$$

The receiver system noise level is computed using the following equation:

$$N = -114 + 10 \text{ Log } (BW) + NF \qquad \text{(B-1)}$$

where:

N = the receiver system noise level (dBm);
BW = the receiver intermediate frequency bandwidth (MHz);
NF = the receiver noise figure (dB).

If the licensed receiver has a bandwidth of 1 MHz and a noise figure of 3 dB, the system noise level computed using Equation B-1 is:

$$N = -114 + 0 + 3 = -111 \text{ dBm}$$

Using an interference-to-noise ratio (I/N) of –6 dB as the criteria, the allowable interference level is:

$$I = N + I/N = -111 + (-6) = -117 \text{ dBm}$$

[1] *Facilitating Opportunities for Flexible, Efficient, and reliable Spectrum Use Employing Cognitive Radio Technologies*, Notice of Proposed Rulemaking, ET Docket No. 03-108, 18 F.C.C. Rcd 26859, at ¶ 38 (2003).

[2] *Id.* at ¶ 42.

The path loss that is required to preclude interference is given by:

$$L_p = P_U + G_T + G_R - I \qquad \text{(B-2)}$$

where:

L_p = the path loss (dB);
P_U = the unwanted power level of the unlicensed device (dBm);
G_T = the transmit antenna gain of the unlicensed device (dBi);
G_R = the receive antenna gain (dBi);
I = the allowable interference level (dBm).

Using 0 dBi for the unlicensed transmit antenna gain and the receive antenna gain, the required path loss to preclude interference computed using Equation B-2 is:

$$L_p = 28 + 117 = 145 \text{ dB}$$

The following equation is used to compute the distance separation that is required to preclude potential interference:

$$10n \text{ Log } D = L_p - 20 \text{ Log } F + 27.55 \qquad \text{(B-3)}$$

where:

F = the frequency (MHz);
D = the separation distance (m);
n = the path loss exponent.

The path loss exponent indicates the rate at which the path loss increases with distance. The value of path loss exponent depends on the specific propagation environment. Table B-1 provides path loss exponents for different propagation environments.[3]

Table B-1. Path Loss Exponents for Different Environments

Propagation Environment	Path Loss Exponent
Free Space	2
Urban Area	2.7 to 3.5
Shadowed Urban Area	3 to 5
In-Building Line-of-Sight	1.6 to 1.8
Obstructed In Building	4 to 6
Obstructed In Factory	2 to 3

As shown in Table B-1 typical values for the path loss exponent are between 2 to 4.

[3] The Institute of Electrical and Electronics Engineers Inc. Press, *Wireless Communications Principles and Practice*, at 104 (1996).

Using Equation B-3 and the path loss required to preclude interference, the required separation distances necessary to preclude interference as a function of frequency and path loss exponent are given in Table B-2.

Table B-2. Summary of Analysis Results

Frequency	Path Loss Exponent	Required Separation Distance
1000 MHz	2	422 km
1000 MHz	3	5.6 km
1000 MHz	4	649 m
2000 MHz	2	211.3 km
2000 MHz	3	3.5 km
2000 MHz	4	469 m
5000 MHz	2	84 km
5000 MHz	3	1.9 km
5000 MHz	4	290 m

As shown in Table B-2, using the unwanted emission limit in Section 15.247(c), large separation distances are necessary to preclude interference, even in environments where obstructions are present (e.g., n = 4).

APPENDIX C
ISSUES RELATED TO GEO-LOCATION COGNITIVE RADIO TECHNIQUES

The positional accuracies available from GPS receivers range from, centimeters for carrier-phase survey grade receivers, to about 40 meters for users operating civilian grade coarse/acquisition (C/A) code tracking receivers in autonomous mode. Satellite availability, which is related to the GPS received signal level and satellite geometry, affects positional accuracy. Satellite augmentation systems such as the Federal Aviation Administration's Wide Area Augmentation System (WAAS)[1] and differential GPS (DGPS),[2] the increased number of in orbit GPS satellites,[3] and the anticipated additional satellites from the European Union's radionavigation satellite system, Galileo, will increase the positional accuracy of GPS receivers. Additional, planned civil-signals also can be used by ground-based GPS receivers to, increase positional accuracy. The Commission adopted accuracy and reliability requirements for Automatic Location Identification as part of its rules for wireless carrier enhanced 911 (E911) service.[4] The accuracy and reliability requirements for E911 Phase II operations for handset-based solutions are 50 meters for 67 percent of calls, 150 meters for 95 percent of the calls. The Commission could adopt positional accuracy requirements for CR devices employing geo-location capabilities that are at least as stringent as the E911 requirements. Many manufacturers are developing GPS chipsets to meet the Commission's December 31, 2005 Phase II deadline, so the technology should be available at a reasonable cost. The Commission's Office of Engineering and Technology has also developed guidelines for testing and verifying these positional accuracy requirements.[5]

In comments filed in response to another rulemaking proceeding, the Institute of Electrical and Electronics Engineers (IEEE) 820.18 Radio Regulatory Technical Advisory Group stated that embedding GPS technology in unlicensed devices is technically feasible and could be used to limit the device so it does not transmit when located in or near an area where interference to a fixed receiver is likely.[6] The IEEE also states that unlicensed devices that employ GPS technology in conjunction with an on-line

[1] WAAS is a system of satellites and ground stations that provide GPS signal corrections. A WAAS-capable GPS receiver can provide a positional accuracy of better than 3 meters 95 percent of the time.

[2] DGPS provides corrections to the GPS signal via a datalink from base stations. Using DGPS the accuracy of GPS for instantaneous positioning is reduced from 40 meters 95% of time to typically 3 meters 95% of the time.

[3] There are currently 29 GPS satellites in orbit including spares.

[4] *Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems*, Third Report and Order, CC Docket No. 94-102 (released October 6, 1999).

[5] Federal Communications Commission, OET Bulletin No. 71, *Guidelines for Testing and Verifying the Accuracy of Wireless E911 Location Systems* (April 12, 2000).

[6] Institute of Electrical and Electronics Engineers Comments ET Docket No. 02-380, at 10 (April 17, 2003).

database of the fixed site locations can be used to prohibit that device from operating in those areas.[7] To implement this technique, for example, the unlicensed device could connect to the Internet to receive updated fixed site location information. Such updates could be accomplished over-the-air or through a computer with a wired connection, such as by attaching to a universal serial bus port through a cradle as currently is done for personal data assistants (PDAs) and cell phones. Issues related to the accuracy and integrity of the on-line databases of the fixed site locations are critical to successfully implementing geo-location techniques. When implementing geo-location techniques in non-government frequency bands, the Commission's Universal Licensing Service (ULS) can be used to create and maintain the fixed site location information. The ULS can be updated on a daily basis to ensure that it contains the most accurate information. The ULS is being successfully used today for non-government public safety and non-public safety frequency bands. If geo-location techniques are implemented in government frequency bands, NTIA can develop and maintain a web-based capability that could be used to provide the location information. The database of the fixed site locations would have to be downloaded to the geo-location equipped unlicensed device on a weekly basis in order to ensure that all fixed sites are adequately protected.

The IEEE has stated that it is feasible to incorporate GPS chipsets within unlicensed devices. As discussed earlier, GPS chipsets are being incorporated in handsets to meet the Commission's E911 mandate. Incorporating the geo-location hardware in the unlicensed device is the only practical way to effectively, from an interference protection standpoint, implement geo-location technology. If the Commission permits geo-location technology to facilitate sharing with other fixed receivers, the location positioning technology should be incorporated within the unlicensed device.

GPS signal failures can occur in urban canyons, indoors, or in shaded areas where there is too much noise or the received signals are too attenuated or distorted by multipath to be received and used reliably in ranging. Under such conditions, demodulating the navigation data included in the satellite broadcast becomes practically impossible.[8] These difficulties can be somewhat compensated for by providing additional data through a cellular network. This technique is referred to as network or assisted GPS (AGPS).[9] The network must be able to supply at least the satellite orbital parameters and exact time to enable position calculation from attenuated signals. GPS receivers in autonomous mode are capable of providing position information during momentary losses of the satellite signals, which occurs frequently in urban environments. The time between when this momentary loss of satellite signals occurs and when the receiver can no longer provide position information depends of the GPS receiver

[7] *Id.* The exclusion areas where unlicensed device operation is prohibited would be determined based on the characteristics and operational scenarios for the licensed service and the unlicensed devices.

[8] A minimum of three to four satellites are necessary for a GPS receiver to determine a position location.

[9] The data provided by AGPS can come in the form of sensitivity assistance designed to aid satellite acquisition or as assistance with time and timing functions.

architecture, application, and manufacturer implementation. Since unlicensed devices that employ geo-location techniques require a position location to control device transmissions, it is important to determine how much time should be permitted after the position location is lost and when the device must cease all transmissions. For example, if a distance of 100 meters (330 feet) is assumed as the critical distance and a person is walking at 4 miles per hour, the time required to cover this distance is 56 seconds. Therefore, using 60 seconds after position information is no longer available as the upper limit for unlicensed devices employing geo-location techniques to cease transmissions seems reasonable. However, larger separation distances between unlicensed devices and the fixed receivers could accommodate longer periods of time when the geo-location capability is not available.

Geo-location technology used in conjunction with an on-line database of sites that require protection holds promise for facilitating sharing between unlicensed devices and radio services using receivers at fixed locations. GPS-based technology incorporated within the unlicensed device is capable of providing position locations with the necessary accuracy. However, many issues related to the accuracy and integrity of the on-line database as well as the integrity of the data downloaded to the unlicensed device must be addressed. If the geo-location device is unable to obtain a location, or the database is not successfully downloaded, the unlicensed device should not be permitted to transmit. In a separate rulemaking, the Commission is proposing to implement geo-location techniques to permit sharing between unlicensed devices and fixed-satellite earth station and radar receivers operating in the 3650-3700 MHz band. The experience gained with implementing geo-location technology in the 3650-3700 MHz band can be used to address the issues related to the interface with the on-line database.

APPENDIX D
ISSUES RELATED TO DEVICES EMPLOYING MESH NETWORKING

Wireless networks have long embraced a centralized model that holds the potential for bottlenecks and a single point of failure. However, wireless mesh networks are emerging as an alternative to wireless switching. Mesh networks distribute intelligence from switches to access points by incorporating a grid-like topology. The development of this topology parallels the architecture evolution in the computer industry. First, computing environments were stand-alone mainframes; these were followed by client/server and then peer-to-peer. Network architecture inevitably will evolve to a distributed, dynamic wireless architecture.

Mesh networking is typically implemented in two basic modes: infrastructure and/or client meshing. In order to gain the maximum benefit that mesh networks have to offer, both modes need to be supported simultaneously and seamlessly in a single network.[1] Infrastructure meshing creates a wireless backhaul mesh among wired access points and wireless routers. This reduces system backhaul costs while increasing network coverage and reliability. Client meshing enables wireless peer-to-peer networks to form between and among client devices (e.g., end users) and does not require any network infrastructure to be present. In this case, clients can hop through each other to reach other clients in the network.

In mesh networks, sophisticated digital modulation schemes, traffic routing algorithms, and multi-hop architectures are employed that use minimal transmission power to increase data throughput over greater distances. With mesh networks, any node within the network can send or receive messages and can relay messages for any one of its neighboring nodes, thus providing a relay process where data packets travel through intermediate nodes toward their final destination. In addition, automatic rerouting provides redundant communication paths through the network should any given node fail. This ability to reroute across other links not only provides increased reliability but extends the network's reach as well. This resilient, self healing nature stems from their mesh networks distributed routing architecture where intelligent nodes make their own routing decisions, avoiding a single point of failure. Because mesh networks are self-forming, adding nodes is also relatively simple. Because mesh networks do not rely on a single access point for data transmissions, users of this technology can extend their communication range beyond that of a typical wireless local area network. Achieving the benefits of self-forming and self-healing, while using minimal power to reduce signal interference within the mesh, involves the implementation of sophisticated routing logic within the software and hardware to enable maximum throughput, as well as maximum reliability.[2]

[1] Mesh Networks homepage at http://www.meshnetworks.com/pages/technology/intro_technology.htm.

[2] National Telecommunications and Information Administration, NTIA Special Publication SP-04-409, *Proceedings of the International Symposium on Advanced Radio Technologies March 2-4, 2004,* at 101 (March 2004).

With low transmission power requirements and a multi-hop architecture, mesh networks can increase the aggregate spectral capacity of existing nodes, providing eater bandwidth across the network. Since mesh networks transmit data over several smaller hops instead of spanning one large distance between hops, mesh network links preserve signal-to-noise ratios (S/N). In terms of scalability, mesh networks can accommodate hundreds or thousands of nodes with control of the wireless system distributed throughout the network, allowing intelligent nodes to communicate with one another without the expense or complication of having a central control point. Furthermore, these networks can be installed in a matter of days or weeks without the necessity of planning and site mapping for expensive cellular towers. As with other peer-to-peer router-based networks, mesh networks offer multiple redundant communication paths, allowing the network to automatically reroute messages in the event of an unexpected node failure.[3]

If traffic is being relayed between a large number of nodes, the latency involved in the relaying can affect time-bounded traffic, such as voice or video. This problem can be addressed in the routing protocols used to implement the mesh, but it is still a potentially serious concern. In addition, if traffic is traveling through intermediate nodes in a mesh (as it most often will), security is an issue. Intermediate nodes might be able to eavesdrop on data not intended for them. This problem could be addressed by employing the end-to-end Virtual Private Network techniques currently used on the Internet, where the same problem exists.[4]

The IEEE 802.15.4 standard specifies a physical layer that could be used for mesh networking devices. The physical layer defines parameters such as the frequency, bandwidth, transmit power, and receiver sensitivity. The frequency bands specified in this standard are: 915 MHz, and 2.4 GHz. The standard specifies the minimum transmit power is 1 milliwatt with a requirement to have transmitter power control (TPC) when higher power levels (greater than 40 milliwatts) are used. The standard is intended to provide reliable data transmission at a range of 100 meters or more.[5]

Given the large number of transmitters in a mesh network that can be operating simultaneously, there is a potential risk for aggregate interference to authorized radio services. As discussed earlier, mesh networks by design transmit data over multiple short paths instead of a single longer path. This means that power levels of the transmitters used in a mesh network can be low and still achieve the necessary S/N for a communications link.[6] The lower power levels of the mesh network transmitters also

[3] *Id.* at 103.

[4] Article on http://wireless.itworld.com, *The importance of wireless mesh networks*, at 2 (February 3, 2004).

[5] The ZigBee Alliance employs the IEEE 802.15.4 standard for low power wireless data communications. The ZigBee Alliance is an association of companies working together to enable reliable, cost effective, low power, wirelessly networked monitoring and control products based on an open global standard.

[6] Lower transmit power also conserves battery life, which is important for mesh network devices because for the network to be effective the individual nodes must remain on.

reduce interference to other mesh network receivers. Currently, the IEEE 802.15.4 standard is implemented in the 902-928 MHz and 2400-2483.5 MHz ISM bands. Because these bands are used primarily by unlicensed devices there is no impact on federal government operations if mesh network operations are implemented in them. However before mesh networks can be implemented in the 5725-5850 MHz ISM band, technical analysis similar to those for the U-NII devices in the 5 GHz band would have to be performed assessing the potential impact to government radars that also operate in this band. The analysis should consider the appropriate technical and operational characteristics of the radar systems as well as those of the mesh network systems. Based on the results of the analysis, the maximum transmit power and any interference mitigation techniques (e.g., DFS and TPC) for the mesh network devices that are necessary to ensure compatible operation with the radars can be determined.

Since the length of communications paths for mesh network devices are short by design, it may be possible to implement this technology at higher frequency bands where propagation losses are greater. Radio signals at higher frequencies (e.g., above 10 GHz) are increasingly reflected and absorbed by rain and atmospheric gases. The maximum usable range of such signals is partly dependent on the tolerable degree of interruption by inclement weather. Further ranges are subject to greater chances of interruption by rainstorms. Still higher in frequency, radio signals are absorbed by gases in the atmosphere. For example, water vapor lightly absorbs radio signals near 20 GHz, and oxygen very strongly absorbs signals near 60 GHz.[7] Atmospheric absorption would be considered a disadvantage for many radio systems, however, mesh network systems may be able to use this phenomenon to limit the range of interfering signals within the mesh network and to substantially increase frequency reuse.

As discussed earlier, another aspect of mesh networks is that the capacity of the mesh increases as more nodes are added. This phenomenon is known as Cooperation Gain.[8] For example, rather than blast a message at high power so that a receiver at the edge of town can hear it, a message could be transmitted at a low power to a receiver that is nearby, and it could then in turn transmit that low power signal to the next receiver, and so on. Through their cooperation, these nodes operating in a mesh could reduce the power required by any particular transmission. If the power of any particular transmission is reduced, then the total capacity would increase. It may also be possible to use technologies for the mesh nodes such as ultrawideband, which has the potential to support data rates of 100 mega bits per second or more at short distances.

A mesh network allows nodes or access points to communicate with other nodes without being routed through a central switch point, eliminating centralized failure, and providing self-healing and self-organization. NTIA believes that the short-range characteristics of mesh networks lends itself to using higher frequencies. Higher

[7] National Telecommunications and Information Administration, NTIA Report 98-349, *A Technological Rationale to Use Higher Wireless Frequencies,* at 4 (April 1998).

[8] As computers get faster, this gain is referred to as processing gain. Radios can achieve a similar gain from cooperation.

frequencies will become continually more attractive as: RF devices become cheaper and better; denser device deployments such as mesh networks reduce the required path length; and demand for wide bandwidths and frequency reuse increases. Operating at higher frequencies will also reduce the potential for aggregate interference to other radio services. NTIA also believes mesh networks that have the capability to increase capacity as the number of nodes increases can deliver broadband data rates to support high-speed data, video and voice applications.

APPENDIX E
GEO-ENCRYPTION TECHNIQUES AS A METHOD TO PROTECT OVER-THE-AIR SOFTWARE DOWNLOADS

A guiding principle behind the development of cryptographic systems is that security should not depend on keeping the algorithms secret, only the keys. This does not mean that the algorithms must be made public, but that they be designed to withstand attack under the assumption that the adversary knows them. Security is then achieved by encoding the secrets in the keys, designing the algorithms so that the best attack requires an exhaustive search of the key space, and using sufficiently long keys that the exhaustive search is infeasible.

Broadly speaking, encryption algorithms or ciphers can be divided into two categories: symmetric algorithms and asymmetric algorithms. Symmetric algorithms use the same key (such as a specific digital code or bit pattern used with the algorithm) for encrypting (locking) plain text and decrypting (unlocking) cipher text.[1] Keeping the key private is essential to maintaining security. Asymmetrical algorithms have distinct keys for encryption and decryption. One major drawback to asymmetrical algorithm is that their computational speed is typically orders of magnitude slower than symmetrical algorithms. This has led to hybrid algorithms, where a random key sometimes called the session key, is generated by the originator and sent to the recipient using an asymmetric algorithm. The session key is then used by both parties to communicate securely using a much faster symmetric algorithm.

Location-based encryption or geo-encryption refers to any method of encryption in which ciphertext can be decrypted only at a specified location.[2] If someone attempts to decrypt the data at another location, the decryption process fails and reveals no details about the original plaintext information. The device performing the decryption determines its location using some sort of location sensor, such as a GPS receiver. Location-based encryption can be used to ensure that data cannot be decrypted outside of a particular facility (e.g., the headquarters of a government agency or corporation). Alternatively, it may be used to contain access to a broad geographic region. Time and space constraints can also be placed on the decryption location.

One implementation of the geo-encryption builds on established security algorithms and protocols, which modifies the previously discussed hybrid algorithm to include a "Geo-lock".[3] In this implementation, on the originating (encrypting) side, a Geo-lock is computed on the basis of the intended recipient's position, velocity, and time (PVT). The PVT defines where the recipient must be in terms of position, velocity and

[1] Numerous very fast symmetrical algorithms are in wide spread use, including the Data Encryption Standard (DES) and Triple DES and the newly released Advanced Encryption Standard (AES).

[2] Geo Intelligence, *GPS-Based Geo Encryption*, at 26 (Winter 2003).

[3] *Id.* at 28.

time for decryption to be successful. The Geo-lock is then added to the session key to form a Geo-locked session key. The result is then encrypted using an asymmetric algorithm and conveyed to the recipient, much like that in the hybrid algorithm. On the recipient's (decryption) side, Geo-locks are computed using a spoof-resistant GPS receiver for PVT input into the PVT-to-Geo-lock mapping function.[4] If the PVT values are correct, then the resultant Geo-lock will be used with a Geo-locked key to provide the correct session key. A point or a geographic area with an arbitrary shape could be used to define the Geo-lock. For example, the shape of the Disneyland theme park could map into a single Geo-lock value to permit successful decryption when the user is located in the theme park but not when outside.

Geo-encryption is an approach to location-based encryption that builds on established cryptographic algorithms and protocols. Geo-encryption techniques can allow information to be encrypted for a specific place or broad geographic area, and it supports constraints in time as well as in space. Geo-encryption can support both fixed and mobile applications and a variety of data-sharing and distribution policies. Depending on individual implementations, it can also provide strong protection against location spoofing. NTIA believes that geo-encryption techniques can be used in conjunction with existing encryption techniques to provide protection of over-the-air software downloads.

[4] Most civil or non-military GPS receivers are easy to spoof or fool into determining erroneous positions. However, civil GPS receivers can be made to be more resistant to spoofing through a series of hardening measures.