Broadcom
15191 Alton Parkway
Irvine, CA 92618
broadcom.com

BROADCOM®

November 17, 2021

Via Electronic Filing

Marlene H. Dortch
Secretary
Federal Communications Commission
45 L Street NE
Washington, DC 20554

Re: Broadcom, Inc. Proposal to be Approved as an Automated Frequency Coordination System Operator (ET Docket No. 21-352)

Dear Ms. Dortch:

Broadcom, Inc. here submits its proposal to become an Automated Frequency Coordination system operator. Should you have any questions or need additional information, please contact the undersigned.

Respectfully submitted,

Chris Szymanski

Chris Szymanski
Director
Product Marketing & Technology Strategy
Wireless Connectivity & Communications Division
Broadcom, Inc.

Broadcom, Inc. Automated Frequency Coordinator Operator Application

ET Docket No. 18-295

TABLE OF CONTENTS

LIST OF DIAGRAMS

I. Introduction and Summary of Proposal

In response to the Office of Engineering and Technology's ("OET") *AFC Public Notice,*[1] Broadcom, Inc. ("Broadcom") submits this application requesting certification as an Automated Frequency Coordination ("AFC") System operator. Broadcom's AFC System (the "Broadcom AFC") will fully comply with Commission rules.

The Commission's *6 GHz Report and Order* marks an important advance for wireless technology. Providing additional unlicensed spectrum for 6 GHz Wi-Fi (today Wi-Fi 6E, and in the near future, Wi-Fi 7) will benefit consumers and U.S. competitiveness by promoting technological innovation and investment in broadband delivery.

A critical part of the Commission's vision for the 6 GHz band is the use of AFC-governed access points operating at standard power. The Commission established clear rules and specifications for AFC operators in the *6 GHz Report and Order*.[2] Further, the *AFC Public Notice* establishes a careful process for accepting AFC operator applications, reviewing those applications, providing an opportunity for testing AFC Systems, and certifying operators. The Commission and OET have developed substantial experience with this process, through the administration of two previous, and more complicated, certification processes—the TV White Spaces ("TVWS") Database Administrator process and the Citizen Broadband Radio Service ("CBRS") Spectrum Access System ("SAS") process. The process of certifying AFC operators will be simpler and more streamlined than either the TVWS or CBRS processes both because of the experience the Commission developed from these prior processes and because AFC Systems are substantially less complicated.

AFC systems will enable standard power unlicensed devices with greater spectral efficiency, lower latency, higher throughput, and will lead to greater range, which will greatly improve wireless broadband for consumers.

Because of the criticality of AFC-enabled standard power Wi-Fi to the wireless broadband market, Broadcom believes there must be a robust AFC operator market that will meet the needs of its diverse customers. Broadcom is supporting the creation of this robust market through its participation in the Telecom Infra Project ("TIP") Open AFC Software Group, its leadership within the Wi-Fi Alliance on AFC matters, and in applying to be an AFC operator.

The Broadcom AFC will employ the Open AFC Software for its core functions. As described more fully below, the Open AFC Software is an open-source software mechanism designed and built collaboratively by leaders in the field of wireless innovation.

[1] *The Commission Begins the Process for Authorizing 6 GHz Band Automated Frequency Coordination Systems,* Public Notice, FCC No. 21-100, ET Docket No. 21-352 (rel. Sept. 28, 2021) ("*AFC Public Notice*").

[2] *Unlicensed Use of the 6 GHz Band*, Report and Order and Further Notice of Proposed Rulemaking, 35 FCC Rcd. 3852 (2020) ("*6 GHz Report and Order*").

Inquiries regarding the Broadcom AFC System should be addressed to:

Position	Name	Contact Information
Product Line Manager	Christopher Szymanski	Chris.Szymanski@broadcom.com; (949) 926-4265
AFC Service Software	Dr. Daniel Edelson	Daniel.Edelson@broadcom.com; (669) 298-8098
AFC Calculation Engine	Dr. Vinko Erceg	Vinko.Erceg@broadcom.com; (858) 521-5885
AFC Legal Matters	Simone Yew	Simone.Yew@broadcom.com; (408) 433-6342

II. Overview of Open AFC

The Broadcom AFC will employ the Open AFC Software for its core functions. The Open AFC project is a dedicated community committed to the design, development, testing, and certification of AFC Software for unlicensed services in the 6 GHz band. The Open AFC group is comprised of representatives from more than thirty companies, representing a broad cross-section of the wireless ecosystem, and is sponsored and supported by TIP.[3] Its mission is to develop standard open-source AFC Software that a wide range of different AFC operators can employ in countries around the world. By working together on an open-source framework, the Open AFC group will give implementing operators economies of scale, standardization, robust performance, transparency, and the security advantages of open-source software.

In doing so, the Open AFC Software will also advance the Commission's goals of bringing the 6 GHz band into use for consumers more quickly and comprehensively than a single closed-source, proprietary AFC implementation could achieve.[4] The Open AFC's open-source, standards-based AFC Software will provide a high-quality, open-source AFC option, enable increased competition in the market, and reduce barriers to new market entrants. Open-source software encourages the contribution of multiple collaborators, each bringing unique expertise to the design of the software both during development stages and after deployment, ensuring optimal functionality in initial construction and future updates. By making the source code available to multiple entities validating operation, an open-source approach is more likely to be

[3] *Open AFC Charter,* Telecom Infra Project (Aug. 4, 2021), https://cdn.brandfolder.io/D8DI15S7/at/h7sz87qgprkcmwssvtgrw9n/TIP_Project_Group_Charter-Open_AFC-forSignature-FINAL.pdf.

[4] *Open AFC*, Telecom Infra Project (last visited Nov. 15, 2021), https://telecominfraproject.com/open-afc/.

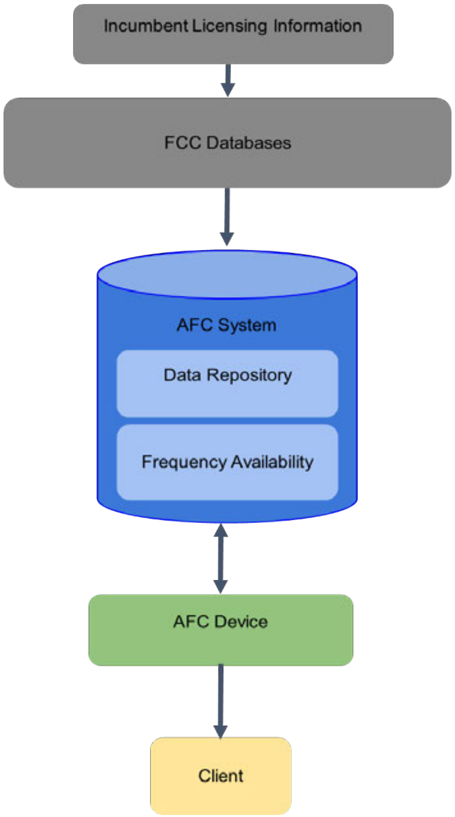
reliable. Open AFC Software is potentially available for use by any candidate AFC operator, which reduces the cost of production for a new entrant seeking certification as an AFC operator, thereby fostering diversity and competition in the marketplace. An open-source architecture also promotes interoperability and facilitates collaboration between separate entities, including new entrants, by standardizing and commodifying AFC functions.

III. Responses to AFC Public Notice Requirements.

a. Response 1: A technical diagram showing the architecture of the AFC system with a brief description of its operation.

Broadcom's AFC will employ the Open AFC Software for core AFC functions. The Open AFC Software is a modular reference software system for use by AFC operators. Diagram 1 illustrates the complete 6 GHz AFC architecture to contextualize the position and role of the Broadcom AFC System integrating the Open AFC Software.

Diagram 1: Overall 6 GHz AFC Architecture with Broadcom AFC System based on Open AFC Software

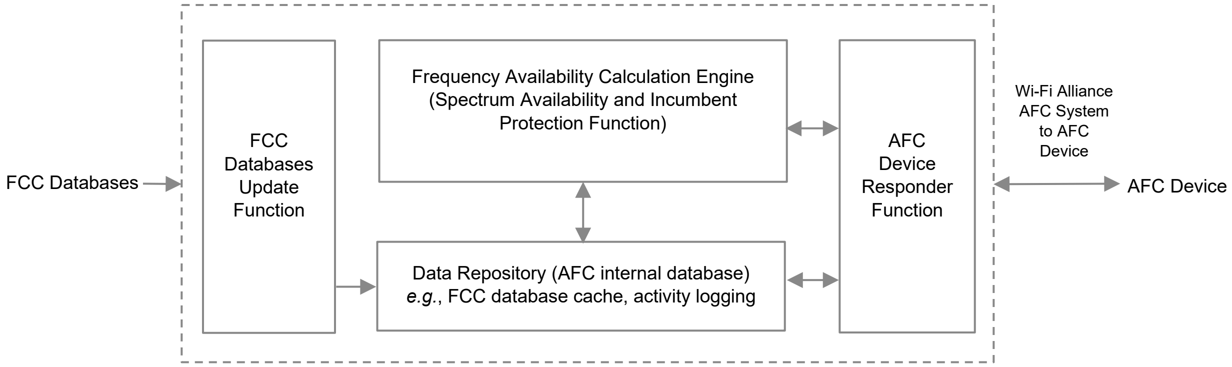


AFC Component	Description
Incumbent Licensing Information	Licensed incumbents' RF operational parameters for designated incumbent systems with superior spectrum rights. For example, if so designated, data about 6 GHz fixed

	microwave links would include licensing information such as transmitter and receiver locations, frequencies, bandwidths, polarizations, transmitter effective isotropic radiated power ("EIRP"), antenna height, and the type of equipment used from an FCC database (*e.g.*, Universal Licensing System ("ULS")). This also includes information about microwave operations in border areas or specific exclusion areas if provided by the FCC.
FCC Databases	Databases maintained by the FCC and that allow the information in the databases to be extracted for the purpose of administering AFC Systems. FCC Databases contain Incumbent Licensing Information and equipment authorization records.
AFC System	Broadcom's AFC System, which integrates the Open AFC Software, combined with Broadcom proprietary software (*e.g.*, security and administrative tools).
AFC System Data Repository	Broadcom AFC operations related to collecting, maintaining, and provisioning data based on Open AFC Software. See Diagram 2 for additional information.
AFC System Frequency Availability Calculation	Broadcom AFC operations, based on Open AFC Software, related to employing Incumbent Licensing Information acquired through FCC Databases, in combination with FCC approved propagation models, to calculate the maximum power at each frequency available for AFC Devices operating at a particular location. See Diagram 2 for additional information.
AFC Device	An AFC-governed 6 GHz license-exempt access point, proxy device, or network control device that is lawfully marketed in accordance with FCC regulations.
Client Devices	6 GHz license-exempt client devices under the control of an AFC Device.

Diagram 2 provides an overview of Broadcom's AFC functional architecture based on the Open AFC Software Project.

**Diagram 2: Broadcom AFC Functional Architecture
Based on Open AFC Software Project**


FCC Databases
FCC Databases Update Function
Frequency Availability Calculation Engine (Spectrum Availability and Incumbent Protection Function)
Data Repository (AFC internal database) *e.g.*, FCC database cache, activity logging
AFC Device Responder Function
Wi-Fi Alliance AFC System to AFC Device
AFC Device

AFC System Key Functions	**Description**
FCC Database Update Function	This function imports data from the relevant FCC Database to determine if there are any changes to Incumbent Licensing Information, additions of information related to temporary fixed microwave links, changes to information related to border operations, and changes to the list of devices authorized/certified by the FCC to operate as AFC Devices. The Broadcom AFC System will use this Open AFC function to populate, update, and maintain databases (1) and (2) in the Data Repository Function listed below.
Data Repository Function	This function houses three core datasets: (1) a database of incumbent services; (2) a database of access points that are authorized/certified to operate as AFC Devices, including specific AP identifiers and FCC identifiers; and (3) a database of activity logs pertaining to frequency calculations and AFC Device activity to comply with FCC recordkeeping regulations. The Broadcom AFC System will update and maintain databases (1) and (2) through the FCC Database Update Function.
AFC System Frequency Availability Calculation Function	This function performs calculations to identify frequencies and power levels that are permissible for AFC Device operation at specific geographic locations. AFC Devices provide geolocation information to the AFC

	System through the AFC Device Responder Function. FCC Databases provide relevant Incumbent Licensing Information through the FCC Database Update Function.
AFC Device Responder Function	This function handles queries from AFC Devices and communicates either an error message to unauthorized or denied AFC Devices or a list of permissible frequencies and transmit power levels to validated AFC Devices. The Broadcom AFC System will use the Open AFC Software Frequency Availability Calculation Function to populate responses to AFC Device queries.

Note that the Broadcom AFC will use the Wi-Fi Alliance AFC System-to-AFC Device Interface to communicate with AFC Devices.[5]

b. Response 2: A description of whether the AFC system is based on a proprietary implementation or open-source.

The Broadcom AFC is based on open-source software. Specifically, the Broadcom AFC will (1) base core AFC functions on the Open AFC Software; (2) execute the AFC System Frequency Availability Calculation Function using open-source libraries such as the Irregular Terrain Model ("ITM") and other publicly available databases; and (3) execute the AFC Device Responder Function using the industry standard Wi-Fi Alliance AFC System to AFC Device Interface. Broadcom may supplement the open-source software components of the AFC system with proprietary or local enhancements to adapt the open-source software for Broadcom's cloud deployment, including for example, in areas such as user interfaces, logging, audit capability, replication, database connectivity, authentication, and in other areas, or for otherwise enhancing the open-source solution.

c. Response 3: A demonstration that the prospective AFC system operator possesses sufficient technical expertise to operate an AFC system.

Broadcom is an American technology company with deep roots in communications innovation, based on the technical heritage of AT&T/Bell Labs, Lucent, and Hewlett-Packard/Agilent. It occupies a leading position in a diverse set of markets, including, but not limited to, semiconductors, software, components for consumer wireless and wireline technologies, broadband modems, enterprise infrastructure, switching, sensing, filtering, and security. Its workforce of approximately 21,000 personnel delivers sector-leading solutions in each of these areas, serving the world's most successful companies as well as key government partners. Broadcom is well positioned to provision AFC operator services because of its

[5] *See* Wi-Fi Alliance, *AFC Specification and Test Plans*, https://www.wi-fi.org/downloads-registered-guest/AFC_Specifications_and_Test_Plans.zip/38132.

technical expertise in wireless technologies, databases, and software, and because it combines global scale, engineering depth, broad product portfolio diversity, superior execution, and operational focus to deliver products that enable its customers to meet the technological needs of a constantly changing environment.

Broadcom is an active participant of the TIP's Open AFC Software Project. It is a core technical contributor to the Open AFC Software Project, with engineers advancing the rapid deployment of AFC technologies to facilitate the intensive use of the 6 GHz band that the Commission has set as its goal. Broadcom's technical capabilities and cross-industry expertise contributed to the Open AFC group's ability to design a fully functioning AFC System complete with technical specifications, documentation, and testing protocols.

Broadcom has expertise in every aspect of the wireless ecosystem, making it optimally suited to provide AFC operator services. Its semiconductor-focused hardware portfolios include data center switches and routers, set-top/CMTS, cable modems, and PON/DSL, Ethernet NICs, filters and amplifiers, ASIC, wireless connectivity solutions, embedded processors, HDD/SSD controllers, enterprise SAS/SATA/Fibre Channel connectivity, optical isolation/motion encoders/LEDs, and fiber optic solutions. Its infrastructure software portfolio includes enterprise solutions for building, connecting, managing, and securing complex digital environments. In addition to its hardware portfolio, its infrastructure software portfolio includes data center networking and storage, enterprise and mainframe software focused on automation, monitoring and security, smartphone components, telecoms and factory automation. In each of these areas, Broadcom provides end-to-end service, from the design, production, testing, and deployment to the continued maintenance of its product offerings. Accordingly, its business requires a commitment to and expertise in the implementation of advanced security features, systems capable of scaling, and networks built on redundancies, all of which are critical to the provisioning of the database functions required of AFC operators.

Broadcom's hardware expertise adds to its capacity to serve as an AFC operator. The ability to deliver such substantial hardware offerings requires deep experience with security, quality, and contingency planning. Moreover, Broadcom's worldwide leadership role in Wi-Fi chip manufacturing means that it is designing the chips present in 6 GHz capable Wi-Fi access points, providing it with a unique understanding of the operation of the devices that will be governed by the Broadcom AFC System. Further, Broadcom has world-class expertise with access points equipped with cryptographically signed chips, or other trust protocols, that will augment the security features implemented in the AFC System, further ensuring the secure transmission of information.

Broadcom's proven capabilities in complex, high volume data transmission provides an additional layer of technical expertise in database operation. For example, Broadcom's world-class global navigation satellite systems ("GNSS") products require the development, provisioning, and maintenance of secure databases. Given the nature of these systems and the highly sensitive information they collect, the databases Broadcom designed, built, and operate must be secure, capable of scaling, and resilient to network disruptions and adversarial attacks. Broadcom's advanced databases collect information from numerous stations from around the world about GNSS satellite orbits and parameters. The system includes software designed to process the data collected and then transmit that data to every device containing a Broadcom GNSS chip. To manage a system of such magnitude requires the most advanced solutions addressing secure transmission of data, recordkeeping of large volumes of data, centralized processing and calculations of information, and validation of devices permitted to send and receive data. This specialized experience deepens Broadcom technical qualifications to serve as an AFC operator.

Beyond its GNSS services, Broadcom also provides substantial and complex internal database services, both to run its diverse businesses, as well as externally through its Wireless Communications and Connectivity Division. These technical teams have extensive experience operating cloud services, data centers, public and private databases, and public and private websites. For example, Broadcom's storage connectivity solutions help maximize server speed and uptime, providing the foundational technologies that are required to provide centralized AFC services at scale. Additionally, given the importance of its internal and external-facing databases, Broadcom's security solutions are designed to protect its digital infrastructure from multifaceted security threats, both for data in transit and data at rest. One core component of its security solutions is its use of endpoint protection such as Symantec Endpoint Protection ("SEP"), an endpoint detection software used to detect and quarantine malicious software.

Finally, Broadcom has extensive experience maintaining worldwide unlicensed spectrum regulatory compliance for billions of devices. Not only does Broadcom diligently track and comply with the Commission's unlicensed spectrum rules, but it also tracks and complies with all applicable requirements from relevant international regulatory authorities that impact the operation of Broadcom's client and access point devices operating in 2.4, 5, and 6 GHz bands. Broadcom works with its customers to ensure that every stock keeping unit ("SKU") provides excellent performance while always fully complying with the complex network of applicable international regulations. It implements both silicon-level features as well as extensive software engineering infrastructure to comply with regulations in areas including specific absorption rates ("SAR"), band edge emissions, spectral masks, radar detection, restricted channels, and maximum power spectral density ("PSD") or EIRP transmit powers.

Name	**Expertise**	**Description**
Christopher Szymanski	Marketing program line manager for AFC System programs	Mr. Szymanski is responsible for product marketing, regulatory affairs and technology strategy for the wireless communications and connectivity division. He is Broadcom's board representative for the Wi-Fi Alliance and Dynamic Spectrum Alliance. He also is Co-Chair of the Open AFC Software Project.

Dr. Vinko Erceg	IEEE standardization, WFA, regulatory, propagation, system engineering	Dr. Erceg has 31 years of experience in communication systems, propagation, cellular, and Wi-Fi products. He is an IEEE and Broadcom Fellow.
Dr. Thomas Derham	Wireless systems and standards design, regulatory and propagation engineering	Dr. Derham is Sr. Principal Scientist in Broadcom's Wi-Fi standards team. He is Technical Editor of the Wi-Fi Alliance AFC System to AFC Device Specification, and a lead contributor to the 6 GHz design in Wi-Fi Alliance and IEEE standards. He has over 20 years of experience in RF propagation and wireless systems design.
Dr. Daniel Edelson	AFC System and Wi-Fi Client software engineering senior management	Dr. Edelson has 30 years of experience in systems software development and management, with approximately 15 years deploying Wi-Fi products. He currently is responsible for Wi-Fi software engineering for Broadcom's wireless communications and connectivity client devices as well as AFC System development.
Shankar Shettar	AFC System, and Wi-Fi Client and WFA software engineering management	Mr. Shettar has two decades of experience with design, development and productization of systems software, 802.11 protocols, and product security. He currently is responsible for managing firmware development, software optimizations, security architecture for Broadcom's mobility WLAN chipsets, WFA Software engineering, and AFC service development.
Dima Rozenfeld	Software engineering management and Open-Source liaison	Mr. Rozenfeld has 20 years of experience in embedded software development. Currently he is responsible for managing software development and security aspects of Broadcom's WLAN client chips and AFC service development.
Scott Wilkinson	Wi-Fi Router/AP software engineering	Mr. Wilkinson has 24 years of experience in the networking industry,

	senior management	and 22 years of experience with 802.11 Wireless LAN. He is currently responsible for Wi-Fi software engineering for Broadcom's wireless communications and connectivity access point devices.
Rajesh Sundaram	Wi-Fi Router/AP software engineering management	Mr. Sundaram has two decades of experience in wireless (Wi-Fi/LTE) embedded software architecture and implementation. At Broadcom, he is responsible for protocol and security aspects of wireless router software stack (L2-L7) and firmware with a current focus on Wi-Fi 6, 6E & 7/IEEE 802.11be.
Tamar Wainshal	AFC System development program management	Ms. Wainshal has extensive industry experience in many aspects of communications and systems solutions program management. Her current roles include providing senior program management oversight for Broadcom's AFC system development.

d. Response 4: A description of the prospective AFC system operator's recordkeeping policies, including registration record retention as well as retention of historical frequency availability data.

The Broadcom AFC will retain AFC Device information and permissible-frequency query results in compliance with Commission rules. Specifically, the AFC will store registered information in a secure database until a standard power access point or fixed client device ceases operation at a location, which, under the Commission's rules, is presumed to have occurred when a device has not contacted the AFC System for more than three months to verify frequency availability.[6] Additionally, the AFC will maintain and update records from incumbent databases, standard power access point and fixed client device registrations, and Commission deny lists for as long as necessary to comply with the Commission's rules and carry out AFC functions.[7]

The Broadcom AFC will use the Wi-Fi Alliance AFC System to AFC Device Interface for device-to-system and system-to-device communications. The Broadcom AFC will retain, for example, information such as the following that is provided in valid requests from AFC Devices: Serial Number, FCC ID, Geographic Location, Request Data/Time, and IP Address. In addition,

[6] 47 CFR 15.407(k)(5).
[7] 47 CFR 15.407(k)(15)(iii).

all regulatory data from the response will be retained including, for example, Allowed Channels, Allowed Transmit Powers, and Restrictions/Deny Lists (if applicable).

The Broadcom AFC's Data Repository Function will maintain three core datasets: (1) a database of incumbent services; (2) a database of APs that are authorized/certified to operate as AFC Devices, including specific AP identifiers and FCC IDs; and (3) a database of activity logs pertaining to frequency calculations and AFC Device activity to comply with Commission recordkeeping requirements. Records will be kept in cloud-class data center storage, service-provider cloud-provisioned network attached storage ("NAS"), or storage area networks ("SAN"). All activity logs that pertain to mandatory record keeping activity will be redundantly stored until (no sooner than) the expiration of record-keeping requirements. Such records will be securely stored as per practices described later in this application.

e. Response 5: A description of how the prospective AFC system operator will handle unanticipated situations that may disrupt performance of the system's required functions—ranging from exceptional cases that affect the system's ability to perform its required functions in isolated instances to cases involving the type of widespread disruption that an event like a system failure might cause.

Broadcom has prepared for unanticipated situations that may impact the AFC System by designing a resilient system and by establishing protocols to respond to and mitigate disruptions of service. Broadcom's system architecture and security practices, discussed in greater detail in Response 6, are designed and implemented to prevent service disruptions. Dynamic software and firmware updates will ensure vulnerabilities are rapidly patched, and improvements are seamlessly rolled out. Rigorous user authentication and activity monitoring practices will reduce the risk of unauthorized access. Furthermore, the use of open-source AFC software will facilitate more robust feedback from stakeholders than is possible with proprietary software, expediting the process of identifying vulnerabilities and addressing them before disruptions occur.

Broadcom will utilize cloud technology to execute its AFC System's operations, allowing it to increase its system's uptime and resiliency and leverage state-of-the-art facilities and best practices for cloud security. For example, Broadcom's cloud solutions will employ elastic load balancing, which will make applications scalable to the requisite number of transactions per second. The physical implementation of Broadcom's AFC calculations will be distributed across cloud data centers. In the case of a system failure, automated processes will shift traffic away from the affected area. Moreover, the electric infrastructure of Broadcom's cloud providers is designed to be fully redundant, and each center is equipped with back-up power to enable continued service even in the circumstance of a grid outage. The data centers will also maintain physical security barriers, intrusion detection, and access monitoring to prevent and identify intruders. Broadcom itself has engineering centers in multiple time zones, including for example, North America and Asia/Pacific, allowing us to implement a "follow the sun" support and monitoring model.

f. Response 6: A description of the methods (*e.g.*, interfaces, protocols) that will be used for secure communication between the AFC system and its associated standard power devices.

Physical Security

As discussed above, Broadcom's AFC System equipment will be housed in cloud data centers, each of which comply with rigorous security standards. Access to physical data centers will only be provided to approved employees, who must first apply for access and provide a valid business justification. Access is layer-specific, limited to when the business justification is provided. Third-party access is similarly limited. Access logs will be analyzed regularly to review physical access to data centers to identify anomalous or unauthorized behavior. Real-time surveillance of server rooms will be recorded by Closed Circuit Television Camera ("CCTV"). The physical sites will include crash barriers and alarms to initiate incident response if access measures are not complied with (*e.g.*, a door is forced or held open).

Although Broadcom's AFC System operations will be conducted on a separate network and housed in cloud data centers, these networks are connected to Broadcom's internal networks through firewalls. Broadcom's internal sites and networks will also implement similar site security to the cloud service provider best practices listed above. These measures include 24/7 authorized user card access controls and tightly controlled access to networks and infrastructure.

Secure Access

Broadcom's AFC System will ensure secure access to its servers, limiting the potential for unauthorized access or unauthorized activities. All AFC networks will be protected by firewalls, denying access to administrative users from non-approved network locations. Even within approved network locations, only a specific list of pre-authorized personnel will be granted administrative access, minimizing the number of administrators capable of interacting with AFC data or configurations. These administrators will be required to comply with industry-set best practices for authorization, such as two-factor authentication for administrative log-ins. To the degree passwords are used for authentication, adequate minimum complexity and rotation will be mandated. Administrator behavior on AFC networks, including log-ons/log-offs and configuration changes, will be monitored with an independently securitized activity log for offline analysis.

In addition to Broadcom's internal secure access protocols, cloud service providers offer their own cloud security. For example, they provide a virtual private cloud ("VPC") secured with its own security groups and its own network access control lists ("ACLs"), which Broadcom will use to manage inbound and outbound traffic to the overall AFC network. This will grant Broadcom granular control and insight into network traffic, helping it ensure secure routing, or the ability to specify the permissible origins and destinations of network traffic. Broadcom will take advantage of cloud provider services that will permit it to manage both authorization and authentication of user access to the cloud servers to maximize data security. For example, Broadcom will implement tiered access and user- or role-specific access policies. Broadcom will also use network access control lists to manage inbound and outbound traffic and will use highly secure virtual private network ("VPN") tunnels to the cloud, which allow for highly secure administrative access.

Broadcom's access control practices ensure security down to the AFC Device level. Broadcom will not only produce the AFC System, but it will also produce the chips and firmware for AFC Devices, making it uniquely positioned to add an extra layer of security to the communication between the two. Original Equipment Manufacturers ("OEMs") may have the option to use custom integrated and/or firmware-based trust modules to store the common AFC root trust certificate (*i.e.*, a public key) and unique device identification credentials during manufacturing. Although the exact approach for unique device identification credentials is still under development, options under consideration include cryptographic key infrastructure with a trust chain of certificates originating from OEMs, hardware-backed secure-hashes, and user ID/passwords. AFC devices will be sufficiently identifiable such that the AFC service is able to implement the FCC requirement of being able to deny service to a device upon demand by regulatory authorities. A secure session-identifier established with bi-directional authentication will be used for all transactions between an AFC Device and the AFC System to ensure available frequencies and power levels are only transmitted to authorized AFC Devices.

Data Security

Security protocols will ensure data at rest and in transit is protected. Data at rest will be maintained in servers in an encrypted format, and as discussed above, subject to strict access control policies. Data in transit between an AFC System and AFC Device will be encrypted and integrity protected using transport-layer security ("TLS"). This ensures that no third party, or "man in the middle" can decrypt or alter the communication. Additionally, as with the root-of-trust certificate, the TLS "man-in-the-middle" functionality permits either party to detect whether any changes or errors were made in the information sent and received on the off chance a third party was able to replay or modify the message.

Software Security

All AFC System servers will be supported by the most up-to-date software and will be configured to allow for automatic updates to be pushed to relevant servers and devices.

All AFC System servers will run instances of a supported enterprise-class Linux operating system, with an active support agreement. Broadcom will automatically implement all critical-level operating system security updates to all its instances of the CentOS distribution within the time period recommended by the vendor. All AFC System servers will also run endpoint protection such as Symantec Endpoint Protection ("SEP"), an endpoint detection software that adds an additional layer of security protection that monitors all software running on the AFC System to further guard against malicious threat software and ensure the integrity of AFC System data and configurations. The endpoint protection software will auto-update as per vendor recommendations.

The underlying AFC System software itself is based on an open-source project, which gains the benefit of the broader community, a robust collection of developers, engineers, and security researchers who are incentivized to raise the quality of the software. This can allow for more expeditious resolution of security or other issues than with proprietary software, which is reliant on a small team of internal engineers for network security.

Audits

In addition to robust physical, cloud, access, and software security measures, Broadcom regularly conducts, and will continue to conduct, security audits, including with third-party security consultants, to test virtual platforms for vulnerabilities, identify any evidence of intrusions, and ensure the business is complying with industry best practices.

g. Response 7: If the prospective AFC system operator will not be performing all AFC functions, information on (1) the entities that will be responsible for operating other functions of the AFC system; and (2) how the Commission can ensure that all of the requirements for AFC systems in the rules are satisfied when AFC functions are divided among multiple entities.

Broadcom intends to provide an end-to-end AFC service, including all functions required by the Commission's rules in the *6 GHz Report and Order.*[8] Broadcom remains open to the possibility of collaborating with a third party should another entity with the relevant expertise demonstrate the capacity to collaborate on an aspect of AFC operations. Broadcom has established no partnerships to provide AFC services at this time.

h. Response 8: A description of how the prospective AFC system operator will provide access to their AFC system for a public trial period which will include thorough testing.

As required by the Commission's rules,[9] Broadcom commits to making its AFC accessible to the public for testing during the public trial period. Broadcom will enable interested parties to register and will make its AFC available to registered users for both lab testing in a controlled environment and field testing by permitting access to AFC functions by devices operating in different locations. Broadcom will provide a web interface to enable public trial access to its AFC.

i. Response 9: An affirmation that the prospective AFC system operator, and any entities responsible for operating other functions of the AFC system under the control of the AFC system operator, will comply with all of the applicable rules as well as applicable enforcement mechanisms and procedures.

Broadcom will comply with all applicable rules as well as applicable enforcement mechanisms and procedures. For example, the Broadcom AFC will:

[8] *6 GHz Report and Order* ¶¶ 23–89.

[9] *6 GHz Report and Order* ¶ 49; *AFC Public Notice* ¶¶ 8, 9.

- Implement a centralized model where each standard power access point will remotely access the AFC to obtain available frequency ranges on which they are permitted to operate and the maximum permissible power in each frequency range;[10]

- Query ULS at least daily to protect pending as well as granted microwave links and temporary fixed microwave links;[11]

- Incorporate information once it is obtained by the Commission regarding microwave operations near the Canadian and Mexican borders to protect these operations;[12]

- Make use of data concerning the location and antenna height of standard power access points when calculating the availability of frequencies and channels of operations;[13]

- Apply interference protection parameters as specified in the Commission's rules to protect fixed microwave operations from harmful interference, using several propagation models consistent with Part 15 rules;[14]

- In addition to protecting co-channel Fixed Service operations, also protect adjacent-channel Fixed Service operations based on the out-of-band emission mask the Commission adopted for co-channel exclusion zones, which is -6 dB I/N or less;[15]

- Have the capability to determine frequency availability at the maximum permissible power of 36 dBm for standard power access points down to at least 21 dBm,[16] providing this maximum allowable power to requesting APs in increments of 3 dB or less;[17]

- Use the location uncertainty reported by an AP to calculate minimum required separation distances from fixed service receivers;[18] and have the capability to use the antenna height as provided by the AP in its calculations of available channels;[19]

- Employ security protocols and procedures to ensure that all communications and interactions between the AFC and standard power APs are accurate and secure and

[10] *6 GHz Report and Order* ¶¶ 27-29.
[11] *Id.* ¶ 32.
[12] *Id.* ¶ 33.
[13] *Id.* ¶ 34.
[14] *Id.* ¶ 35.
[15] *Id.* ¶ 77.
[16] *Id.* ¶¶ 36-37.
[17] *Id.*
[18] *Id.* ¶ 41.
[19] *Id.* ¶ 44.

that unauthorized parties cannot access or alter the database or list of available frequencies and power levels sent to an access point;[20]

- Register every AP requesting available operating frequencies and power levels[21] and obtain the geographic coordinates (latitude and longitude referenced to North American Datum 1983 (NAD 83)), antenna height above ground level, FCC identification number, and unique identifier (e.g., manufacturer's serial number)[22] either directly from the AP or from a proxy device or network control device;[23]

- At registration, authenticate every requesting AP, verifying the device's FCC ID by accessing the Commission's Equipment Authorization System,[24] and storing and referencing the device's serial number to ensure that rogue or prohibited devices are not operating in the band;[25]

- Have the ability to deny spectrum access to a particular registered standard power AP upon request by the Commission;[26] respond to Commission requests to deny access to all APs in a particular geographic region;[27] disable prohibited devices from obtaining standard power access from Broadcom's AFC when their FCC ID cannot be authenticated against the FCC Database; ensure frequencies are not authorized when a standard power AP's location falls within a Commission sanctioned geographic region for those frequencies; maintain prohibited device registration information, such as location, antenna height, FCC ID, and serial number on a deny list, and reference the deny list to ensure prohibited devices do not gain access to a list of available frequencies and power levels;

- Respond to requests from Commission personnel for information stored or maintained by the AFC[28] and employ organizational policies and procedures by which it would respond to government requests for information and enforcement instructions such as discontinuance of access point operations in designated areas;[29]

- Store registered information until an AP ceases operation at a location, meaning that it has not contacted the AFC to verify frequency availability information for more

[20] *Id.* ¶ 79-80.
[21] *Id.* ¶ 82.
[22] 47 C.F.R. § 15.407(k)(8)(ii).
[23] *6 GHz Report and Order* ¶ 85.
[24] *Id.* ¶ 83.
[25] *Id.*
[26] *Id.*
[27] *Id.*
[28] *Id.*
[29] *Id.*

than three months, and use information retained in the AFC database only to protect incumbents and mitigate potential harmful interference;[30]

- Protect radio astronomy observatories by prohibiting standard power APs from utilizing the 25.2 MHz of spectrum in the areas around these observatories, determining the size of the exclusion zone by the radio line-of-sight distance between the radio astronomy antenna and the unlicensed access point.[31]

Broadcom also commits either to serve as an AFC operator for the mandated five-year term or to provide 30-days' notice to the Commission before securely transferring its registration data to another AFC System.[32]

[30] *Id.* ¶ 86.

[31] *Id.* ¶ 88.

[32] *Id.* ¶¶ 53-54.