Application of Google Inc. for Certification to Provide Spectrum Access System and Environmental Sensing Capability Services

GN Docket No. 15-319

TABLE OF CONTENTS

1 INTRODUCTION **1**
2 OVERVIEW OF SAS AND ESC PROPOSAL **3**
2.1 Description of Google's SAS and ESC Functionality 3
2.1.1 Information Gathering and Retention (47 C.F.R. § 96.55) 6
2.1.2 Registration, Authentication, and Initial Authorization of CBSDs (47 C.F.R. § 96.57) 8
2.1.3 Frequency Assignment Process (47 C.F.R. § 96.59) 9
2.1.4 Security (47 C.F.R. § 96.61) 13
2.1.5 SAS Administrator Requirements (47 C.F.R. § 96.63) 13
2.1.6 SAS Administrator Fees (47 C.F.R. § 96.65) 15
2.2 Google Technical Expertise 15
2.3 Google Financial Capability 16
2.4 Assuring Secure and Reliable SAS-to-ESC Communications 16
2.5 Google's SAS and ESC Architecture and Functional Interaction 17
2.5.1 SAS and ESC Integration 18
2.5.2 SAS Architecture 19
2.5.3 ESC Architecture 20
2.5.4 Interactions Between Functions 25
2.6 Propagation Model 26
2.7 SAS and ESC Software and Firmware Security Management 29
2.8 Affirmation of Compliance 30
3 SAS OPERATION **30**
3.1 Processing of CBSD, ESC, and SAS Information 30
3.1.1 Data Retention 30
3.1.2 Data Security 30
3.1.3 Location and Device Verification 31
3.1.4 Authority (Installer, PAL, SAS, ESC, and Federal User) Verification 31
3.2 Interference Mitigation and Resolution 32
3.3 Protection of FSS Earth Stations and Grandfathered 3650-3700 MHz Licensees 33
3.4 Coordination Among SAS Operators 33
3.5 Completeness of SAS Operations 34
3.6 SAS Communications Methods 34
3.6.1 CBSD-to-SAS and SAS-to-CBSD Interface 34

3.6.2 SAS-to-SAS Interface 34
3.6.3 Sensor-to-ESC and ESC-to-SAS Interface 34
3.6.4 CBSD-to-SAS Communications Verification 35
3.7 Non-Retention of Federal Emissions Records 36
3.8 SAS Security 36
3.9 Typical Interference Avoidance Use-Case Scenarios 38
3.9.1 Aspects of Interference Protection Common to All Use Cases 38
3.9.1.1 Characterizing the Transmitter 38
3.9.1.2 Applying Path Loss 44
3.9.1.3 Characterizing Impact at the Receiver 45
3.9.1.4 Incorporating the Effect of a Receive Filter 48
3.9.1.5 Calculating Passband and Blocking Interference Impact 50
3.9.1.6 Accounting for Aggregation 51
3.9.1.7 Admission Control 51
3.9.1.8 Coexistence Among GAA Users 52
3.9.2 Assignments Made By Multiple SASs 53
3.10 Commission Access to Information Retained by the SAS 53
4 ESC OPERATION 54
4.1 ESC-to-SAS Communications Methods 54
4.1.1 ESC-to-SAS Interface Design 54
4.1.2 ESC and ESC-to-SAS Interface Protection 54
4.2 Sensing Methodology 54
4.2.1 Description of Previous ESC Development and Testing Outcomes 54
4.2.2 ESC Architecture and Sensor Hardware Design 55
4.2.3 Signal Processing and Detection Algorithms 55
4.2.4 Sensor and SAS Data Retention Protections 55
4.3 Sensor-to-ESC Communications 55

LIST OF FIGURES

Figure 1: Combined SAS and ESC Ecosystem
Figure 2: Architecture of Google's SAS
Figure 3: Google ESC Block Diagram
Figure 4: Coverage of a Notional Deployment of 103 Dedicated ESC Sensors
Figure 5: ESC Sensor Block Diagram
Figure 6: Prototype ESC RF Front-End in Weather-Proof Enclosure
Figure 7: Comparison of Measured Propagation Loss to Propagation Loss Predicted by Longley-Rice in the Mountain View, California, Area
Figure 8: Comparison of Measured Propagation Loss to Propagation Loss Predicted by Longley-Rice in the Arlington, Virginia, Area
Figure 9: Flowchart Depiction of PSD Calculation
Figure 10: Graphical Representation of CBSD Emission Mask
Figure 11: Example Transmit Filter Response
Figure 12: Antenna Gain v. Frequency of Example CBSD Antenna
Figure 13: Net Power Spectral Density of CBSD after taking into Account Frequency-Dependent Conducted Emissions, Transmit Filter, and Antenna Gain
Figure 14: Free Space Path Loss over 1 km in the 3.5 GHz Band
Figure 15: Horizon Gain of FSS Dish with Low (5.1 degree) Elevation Angle
Figure 16: Polar Plot of Figure 15
Figure 17: Horizon Gain of an FSS Dish with a Higher Pointing Elevation
Figure 18: FSS Receive Filter Response for an Adjacent-Band FSS Receiver
Figure 19: Net Signal PSD at Receiver, Including All Transmitter, Receiver, and Propagation Effects
Figure 20: Passband RF Power Spectral Density in Units of dBm/MHz

LIST OF TABLES

Table 1: Key Personnel
Table 2: Key Functional Components
Table 3: ESC Key Functional Components
Table 4: Performance Expectations for Sensor Components
Table 5: CBSD, SAS, ESC, and Sensor Communications
Table 6: SAS and ESC Ecosystem Certificates
Table 7: Maximum Heartbeat Times
Table 8: Types of Masks Accepted by Google's SAS
Table 9: Part 96 OOBE Limits
Table 10: Treatment of Various Filter Types
Table 11: Treatment of Various Antenna Types
Table 12: Protection Criteria and Methodology of Google's SAS

Application of Google Inc. for Certification to Provide Spectrum Access System and Environmental Sensing Capability Services

GN Docket No. 15-319

1 INTRODUCTION

Google Inc. (Google) here provides information supporting its request for certification of both a Spectrum Access System (SAS) and an Environmental Sensing Capability (ESC) to enable commercial wireless access to the 3550-3700 MHz band (the 3.5 GHz band). Google's proposal is consistent with the Commission's rules, its *Order* authorizing the Citizens Broadband Radio Service (CBRS),[1] and its *Order on Reconsideration and Second Report and Order* clarifying certain aspects of the rules and adopting additional requirements.[2] The request is also informed by the Commission's *Public Notice* calling for SAS and ESC operator applications,[3] as well as guidance provided by Commission staff during its SAS/ESC certification workshop.[4]

Google has long supported intensive and dynamic spectrum sharing, including through active participation in both the President's Council of Advisors on Science and Technology (PCAST) and the 3.5 GHz proceeding. Continuing its support of Commission's initiatives to improve spectrum utilization, Google has developed SAS and ESC capabilities essential to enabling more extensive use of the 3.5 GHz band. Google's SAS meets the Commission's requirements for SAS capabilities, while embracing industry standards and operational transparency to promote competitive alternatives for all users and support innovation in the band. To these core features and principles, Google adds the technical capability to implement a band-specific, clutter-aware propagation model based on large volumes of measured data.[5]

---

[1] *See* 47 C.F.R. Part 96; *In the Matter of Amendment of the Commission's Rules with Regard to Commercial Operations in the 3550-3650 MHz Band*, Report and Order and Second Further Notice of Proposed Rulemaking, 30 FCC Rcd. 3959 (2015) (*Report and Order* or *Second FNPRM*).
[2] *In the Matter of Amendment of the Commission's Rules with Regard to Commercial Operations in the 3550-3650 MHz Band*, Order on Reconsideration and Second Report and Order, GN Docket No. 12-354, FCC 16-55 (rel. May 2, 2016) (*Second Report and Order*).
[3] *Wireless Telecommunications Bureau and Office of Engineering and Technology Establish Procedure and Deadline for Filing Spectrum Access System (SAS) Administrator(s) and Environmental Sensing Capability (ESC) Operator(s) Applications*, Public Notice, 30 FCC Rcd. 14170 (2015) (*SAS/ESC Applications Public Notice*).
[4] *See Wireless Telecommunications Bureau and Office of Engineering and Technology Announce Meeting for Prospective Spectrum Access System Administrators and Environmental Sensing Capability Operators To Take Place February 16, 2016*, Public Notice, 31 FCC Rcd. 248 (2016).
[5] Google recognizes that SAS operators will be required to use a common propagation model to be certified by the Commission. *See, e.g.*, *Second Report and Order* ¶¶ 138, 188, 190, 278. Nevertheless, as described in section 2.6, below, Google continues to believe that band-specific, clutter-aware models can unlock access to substantial additional spectrum in this band.

In particular, Google's SAS is being built to the applicable SAS and Citizens Broadband Radio Service Device (CBSD) specifications developed by the Spectrum Sharing Committee[6] (SSC) of the Wireless Innovation Forum[7] (WinnForum). These standards assure interoperability between CBSDs and SASs across SAS operators and device manufacturers. We also expect that they will create a framework for assuring only authorized devices, SAS operators, installers, and sensors can operate within the 3.5 GHz ecosystem. By relying on open standards, Google's SAS will allow all compliant devices access to the 3.5 GHz band, thereby fostering diversity and innovation in the products and services offered over this spectrum. Appendix A describes the open process leading to development and approval of these standards.[8]

Google has developed an end-to-end SAS capability based on the Commission's *Report and Order*, where applicable.[9] The SAS includes baseline propagation algorithms, a process for registering devices and granting spectrum requests, and a methodology for ensuring federal users, Fixed-Satellite Service (FSS) operators, and Priority Access License (PAL) users do not experience harmful interference. Google has deferred implementation of Part 90 protection awaiting further Commission guidance on this topic, but expects to build on existing protection algorithms in developing that protection. The protection algorithms address one-on-one interference limits, aggregate interference limits, and geographic exclusions. Consistent with ITU recommendations, the SAS represents and processes two- and three-dimensional antenna models. As noted below, Google's SAS does not accept leasing notifications at this time, but Google expects to provide this capability in the future.[10]

Google has been trialing a prototype SAS for nearly two years, with the algorithms evolving as rules are issued and standards are created. Over that period of time, Google has demonstrated its SAS prototype to industry and government (for example, to major wireless carriers, FCC staff, and National Telecommunications and Information Administration (NTIA) staff), and at public events (such as the 2015 International Symposium on Advanced Radio Technologies conference at the National Institute of Standards and Technology facility in Boulder, Colorado, and a 2015 meeting of the WinnForum SSC). Google will also be experimenting with early SAS operations during a trial of SAS and CBSD functionality in Kansas City, Kansas, beginning in June 2016.

Google will modify the processing and decision-making structures in its final SAS product and service to reflect future Commission orders, as well as additional industry consensus documents as appropriate. Because Google's SAS already performs processing for

---

[6] The SSC is a WinnForum committee that supports the development and advancement of spectrum sharing technologies based on the three-tier architecture proposed for the 3.5 GHz band. *See* Spectrum Sharing Committee, http://www.wirelessinnovation.org/ssc.
[7] WinnForum is an non-profit mutual benefit corporation dedicated to advocating for the innovative use of spectrum, and advancing radio technologies that support essential or critical communications worldwide. *See* About the Wireless Innovation Forum, http://www.wirelessinnovation.org/about_the_forum.
[8] As noted in Appendix D, all published WinnForum standards are available at http://groups.winnforum.org/Reports and http://groups.winnforum.org/Specifications.
[9] *See generally Report and Order*; *Second Report and Order*.
[10] *See Second Report and Order*, Appendix A § 96.66.

the types of protection generally contemplated, updating the decision algorithms to reflect further FCC decisions and industry standards will be straightforward.

The following sections of this application respond to the specific requests set forth in section IV of the Commission's *SAS/ESC Applications Public Notice* and conform to the structure of same.

2 OVERVIEW OF SAS AND ESC PROPOSAL

2.1 Description of Google's SAS and ESC Functionality

Immediately below, Google provides a high-level description of SAS and ESC functions. Subsections 2.1.1 through 2.1.6 specifically discuss the functional requirements set forth in 47 C.F.R. §§ 96.55, 96.57, 96.59, 96.61, 96.63, and 96.65. Google's ability to meet the requirements of 47 C.F.R. § 96.67, which specifies the functions of an ESC, is discussed in detail in sections 2.4, 2.5, 2.7, 3.1, 3.6.3, and 4.

Google's SAS:

1. Uses algorithms that implement the required protections provided by Part 96, using validated models for the estimation of radiofrequency impacts.
2. Determines permissible spectrum usage by each CBSD requesting a spectrum grant, and assures that all grants conform to permissible usage, both initially and over time.
3. Models the impact of each CBSD on higher tier operations, and determines permissibility of operation and the maximum power that that CBSD can emit, based on constraints from co- and adjacent-channel PALs, grandfathered Part 90 operations, FSS sites, and federal operations. The SAS also takes into account PAL protection areas, including validating operator-supplied areas against the default protection contours established in the *Second Report and Order*.[11]
4. Validates CBSD eligibility and registers CBSDs. This includes collecting location and identification information that will be validated using industry standard certificate management processes. To the extent location information cannot be provided automatically by the CBSD and is supplied by a professional installer, Google is prepared to provide validation using a similarly rigorous process.
5. Maintains federal exclusion and protection zones and ensures that all CBSD operations are consistent with rules that protect federal incumbents. Google is preparing its SAS to retain federal operations records consistent with the principles established by the WinnForum ESC Task Group, in which the Department of Defense (DoD) participates.
6. Communicates with Google's ESC network to:
    a. Receive ESC reports of federal shipborne and ground-based radar emissions in the 3550-3700 GHz range,
    b. Respond to the presence of protected federal systems, and

[11] *Second Report and Order*, Appendix A, §96.57(e).

   c. Ensure that CBSD operations that might impact those federal operations reduce power, are relocated to non-interfering channels, or have their operations terminated.
7. In addition to the functionality discussed in item 6, Google's SAS utilizes declared exclusion zones where no ESC is deployed, as well as other ad hoc exclusion or protection zones that may be defined by federal authorities in the future. Restricted areas where operation is not permitted due the presence of federal incumbent activity, protection zones, and exclusion zones are enforced by (1) requiring CBSDs to reduce transmissions to power levels that avoid harmful interference, (2) relocating CBSDs to other channels, or (3) terminating CBSD operation.[12]
8. Protects operations of existing non-federal FSS earth stations, including protection of grandfathered earth stations operating between 3600 and 3700 MHz and of earth stations used for telemetry, tracking, and control (TT&C) in the adjacent 3700-4200 MHz band. This capability includes importing the appropriate records from the FCC's records systems. Google's SAS can also implement site-by-site agreements that modify these protections.[13]
9. Protects PAL users from harmful interference from other PAL users, and from General Authorized Access (GAA) users. This protection includes cancelling any GAA grants in the PAL channel when authorized PAL access is requested, and limiting GAA devices to grants that do not violate the protection criteria. In addition, PAL spectrum grants are validated to assure that the requesting device has the appropriate certificate to establish its licensing status.
10. Offers a spectrum inquiry function that allows inquiring nodes to obtain information regarding channel assignments and use in a node's specific location. This functionality facilitates non-interfering operations by GAA users, giving them maximum flexibility and encouraging innovation while protecting PAL and incumbent operations.
11. Supports a coexistence mechanism between co-channel GAA users. Google's facilitation of these interactions will follow any specifications issued by the WinnForum.
12. Assures secure, confidential and reliable communications from devices and installers to and from Google's SAS through Transport Layer Security (TLS),[14] the widely adopted Internet standard for https traffic.
13. Protects grandfathered Part 90 users in the 3650-3700 MHz band. Google will implement specific protections for Part 90 users that are consistent with the Commission's disposition of pending questions on this subject.[15]

---

[12] Following the *Report and Order*, Google uses the term "exclusion zone" to refer to the predetermined areas where CBSDs must not operate in order to protect a federal operation. *Report and Order* ¶ 259. Once ESCs are deployed, these zones are called "protection zones." *Id.* ¶ 262. We refer to an area within a protection zone where use is not permitted because an ESC detects federal activity as a "restricted area."

[13] *Id.* ¶ 291.

[14] *See* The Transport Layer Security (TLS) Protocol, Version 1.2 (2008), https://tools.ietf.org/html/rfc5246.

[15] *See Wireless Telecommunications Bureau Seeks Comment on an Appropriate Method for Determining the Protected Contours for Grandfathered 3650-3700 MHz Band Licensees*, Public

14. Establishes zones along international borders where CBSD operation will be restricted, in accordance with guidance to be provided by the FCC. These border zones will honor existing agreements with respect to interference criteria at borders with Canada and Mexico, including, for example, "Arrangement R."[16]

The SAS will accept grants to lessees that have been duly registered with another SAS. Google expects to build a functionality to accept lease notifications and support leasing arrangements in the future.[17]

Google's ESC:

1. Will be constructed, operated, and maintained by Google without connectivity to any military or other sensitive federal database or system.
2. Includes a network of sensors, located within FCC-defined protection zones, that will detect the presence of federal shipborne and ground-based radar systems in the 3550-3700 MHz band and adjacent frequencies. The sensitivity of the sensors will meet requirements being developed within the WinnForum in conjunction with the DoD.[18]
3. Provides redundant coverage of all geographic areas that require monitoring.
4. Incorporates a decision system that will receive input from the sensors and formulate an appropriate message to the SAS in response to the information, allowing the SAS to reconfigure CBSDs under its control to avoid harmful interference to federal systems.
5. Includes a centralized controller that remotely manages software upgrades for the ESC components and can confirm proper functioning of those ESC components.
6. Provides secure, confidential, and reliable communications between all components of the ESC and between the ESC and the SAS, through TLS, the widely adopted Internet standard for https traffic.
7. Can be upgraded to detect newly deployed federal systems.
8. Retains information about detection of federal activity, and communications related to such detections. This capability will be guided by security requirements being developed by the WinnForum in consultation with DoD.[19]
9. Allows Commission personnel, through the SAS, to access any retained information regarding ESC activations.

Notice, 30 FCC Rcd. 11557 (2015) (asking questions about how to effectively protect these users).

[16] *Arrangement R: Sharing Arrangement Between the Department of Industry of Canada and the Federal Communications Commission of the United States of America Concerning the Use of the Frequency Band 3650 to 3700 MHz By the Fixed and Mobile Services Along the Canada-United States Border*, https://transition.fcc.gov/ib/sand/agree/files/can-nb/Arrangement_R.pdf.

[17] See *Second Report and Order* ¶ 220 (noting that a SAS may choose whether to accept leasing notifications and support leasing arrangements).

[18] *See* Appendix D.4 (referring to specification for operational and functional commercial requirements for SAS and ESCs and SASs).

[19] A number of WinnForum standards are in process, including documents that cover operational security requirements.

The Commission's *SAS/ESC Applications Public Notice* asks entities seeking to provide both SAS and ESC services to "address any potential conflicts of interest between the two functions."[20] Google perceives no conflict of interest in operating both a SAS and an ESC. Google's ESC will meet performance objectives determined by external, multi-stakeholder processes and provide information that initiates action by Google's SAS. Both SAS and ESC operators must adhere to regulatory requirements that mandate the protection of higher tier users, while making spectrum as useful as possible. They are simply different systems designed to work together to accomplish the same goal.

2.1.1 Information Gathering and Retention (47 C.F.R. § 96.55)

Information Gathering

Google's SAS maintains a database of all information required to implement the Part 96 requirements. For registered CBSDs, the components of this database include the following content:

1. Location (latitude, longitude, and altitude above ground level).
2. Operating characteristics, including maximum conducted power and antenna characteristics as applicable: gain, pointing azimuth, beamwidth, downtilt, antenna pattern (if applicable), and height above average terrain (if applicable).
3. Professional installer identification and authentication ("certificate identification") (a topic currently being addressed by a WinnForum task group).[21]
4. Authorization status (i.e., PAL or GAA), and category of deployment (i.e., PAL, CBSD Category A, or CBSD Category B).
5. Contact information for the device operator.
6. Confirmation that the CBSD operator understands the potential interference and pre-emption risks associated with operation in the band.
7. Any call sign provided by the CBSD.
8. Individual device information, including FCC ID, unique manufacturer's serial number, authentication certificate, air interface technology, and channel sensing capability (if applicable).
9. The identity of the SAS managing a device and providing the registration or grant information via a SAS-to-SAS interface.
10. Grant status (date and time issued, expiration date and time, maximum power authorized, frequencies granted, and suspension status).
11. Heartbeat status,[22] expiration, and interval.

---

[20] *SAS/ESC Applications Public Notice* at 5.

[21] In addition to developing a certificate process, the WinnForum has also begun to consider requirements for a qualification program for professional installers.

[22] CBSDs use the heartbeat process to request continuing authorization from the SAS, at which time the SAS can instruct the CBSD about changes in its environment requiring any spectrum relocation due to incumbent or higher tier activity. If a CBSD cannot contact the SAS within the heartbeat expiration period, it must cease transmission. For example, expiration periods for CBSDs operating within protection zones where an ESC has not detected federal activity will be less than 240 seconds, in order to ensure that devices receive timely notifications from the ESC.

Items 1-9 are applicable to all CBSDs registered with Google's SAS. Items 10 and 11 are applicable only to CBSDs that have current spectrum grants. The SAS will also be capable of collecting signal measurement data as supported by CBSDs, according to section 96.39(d) of the Commission's rules and any applicable WinnForum standards.

Google's SAS maintains records of incumbent users of the band, including:

1. Federal protection and exclusion zones, and their current activity status if provided by the ESC network.
2. Location of in-band and adjacent band FSS sites, including the information required by 47 C.F.R. § 96.17.
3. Grandfathered Part 90 operations.

In order to ensure that information regarding federal and non-federal incumbents is current, Google's SAS will access relevant databases and other information from the FCC and the National Telecommunications and Information Administration (NTIA). Google will also accept direct incumbent registrations and updates consistent with FCC requirements. Finally, Google will accommodate any ad hoc protection or exclusion zones as defined by federal authorities.

After PAL auctions are conducted, Google's SAS will maintain a database of PAL holders. This database will include the name of the license holder, the license area (i.e., census tract), the license issuance and expiration dates, and licensee preferences such as default physical channel(s) and preferred contiguous channel assignments.

Information Retention and Disclosure

Google will maintain the data set forth in subsection 2.1.1 for a period of at least 60 months from initial or updated submission, with the exception of the ESC network detections and restricted area activations, which will be retained in accordance with information retention policies to be established as part of the ESC approval process.[23] To the extent that the FCC, in collaboration with NTIA, establishes a specific maximum (or minimum) retention time for information regarding federal operations, Google is prepared to implement such a requirement. Absent a specific requirement, data on federal emissions and restricted area activations will be retained as required to support immediate operations of Google's SAS. Consistent with 47 C.F.R. § 96.55(a)(3), Google's SAS will make CBSD registration information available to the general public. The identity of licensees will be withheld from the public in accordance with the Commission's rules. In addition, federal access to SAS database content will be provided by a Regulators' Console. This access will be provided online to authorized federal users.

SAS-to-SAS Information Exchange

Google's SAS fully supports the SAS-to-SAS exchange requirements established to date by the WinnForum SSC, including provisions that allow two SAS providers to tailor the exchange to the needs of each system through a bilaterally developed "Technical Protocol."[24] The requirements specify at a high level both the elements to be exchanged and an interface for

[23] *Report and Order* ¶ 326.
[24] *See* Appendix D.1.

exchanging that information. The standard, like all WinnForum standards for the 3.5 GHz band, was developed through an industry consensus process.

Under the Technical Protocol, information exchanged by SAS providers includes:

- Registration data provided to the SAS;
- All grants as they are issued by the SAS;
- All changes in registration and grant status; and
- Regulatory inputs received through the regulators' console.

This WinnForum-specified interface provides for near real time synchronization of all SAS transactions. Google intends to incorporate updates from external SAS operators within 10 seconds of receipt. It also intends to send out updates to other SAS operators within 10 seconds of an action taken by Google's SAS. The specific items of communications are set forth in section 3.6 of this application.

Upon receipt of a registration from an external SAS, Google's SAS will update its computation of aggregate interference to all of the appropriate protected nodes or areas, using the same methods as used for Google SAS grants. Grants from other SASs will be accepted as valid.

To effectuate data exchanges, Google is prepared to establish bilateral SAS data exchange and technical protocol agreements, consistent with the WinnForum specification, with other FCC-approved SAS Administrators.

2.1.2 Registration, Authentication, and Initial Authorization of CBSDs (47 C.F.R. § 96.57)

Google's SAS will support all types of CBSDs operating under the Commission's Part 96 rules. Registration, authentication, and authorization of CBSDs will follow WinnForum SSC standards, which are being developed collaboratively by over 50 stakeholder entities and organizations.[25]

Registration and authorization are predicated on successful authentication. To authenticate a device, the SAS will first validate that the device has an appropriate certificate indicating that the software used by the CBSD behaves as certified. Google plans to accept only manufacturer certificates deriving from a set of Certificate Authorities maintained by the WinnForum to issue Part 96 manufacturer certificates, in a process similar to the way browsers validate SSL certificates and manage certificate authorities.[26] It is Google's understanding that manufacturer certificates will be issued only to devices certified by the Commission. The presentation of the certificate with every request will validate on an ongoing basis that the CBSD is eligible to operate under Part 96, and that the information provided by the CBSD can be trusted. This mechanism also provides a way for innovative new CBSD technology to be introduced into the ecosystem quickly. If a new CBSD passes the FCC's certification tests and qualifies for WinnForum manufacturer certificates, that CBSD can be immediately brought into service using Google's SAS. Second, the SAS confirms that the device presents a valid FCC ID.

---

[25] Appendix D.2 sets standards for CBSD-SAS communications. A number of WinnForum standards are in process, including documents that cover certificate authority standards. *See also* section 3.1.4.
[26] *See* section 3.1.4.

FCC IDs will be obtained from the Commission's Equipment Authorization database and this information will be updated as needed—likely once per day.[27] Once these two steps are completed, and the information set forth in section 2.1.1 above is collected, the device is registered with Google's SAS.

Successful registration makes the device eligible to request from Google's SAS a grant of authorization to use spectrum. Operators, however, may decide to register devices without immediately requesting a grant. For example, a professional installer may deploy devices, but the network operator offering service over those devices may wait to activate them.

2.1.3 Frequency Assignment Process (47 C.F.R. § 96.59)

The SAS's process for authorizing CBSD operations validates initial grants and monitors grants for compliance with the Commission's rules over time. For example, grants are monitored and revised to accommodate changes in higher-tier usage. Some aspects of this process are common to all grants, and others are specific to the tier (GAA or PAL) for which the grant is requested. In particular, the WinnForum protocol allows the same CBSD to be registered as operating either as a PAL user or a GAA user.[28] This approach allows users to transition their devices as desired between tiers.

The following discussion describes the logic employed by the SAS for each tier of user. Specific interference criteria and methods of computation are provided in later sections of this application.

<u>Aspects Common to All Grants</u>

All requests are first examined for compliance with relevant Part 96 requirements. The following conditions are validated before a grant can be issued.

1. The device will not cause harmful interference to federal incumbents. This condition can be met two ways:
   a. The device is not located within an exclusion zone or protection zone; if the device is located in an exclusion zone not covered by a fully functional ESC, the device cannot operate.
   b. The device is located in a protection zone, but the SAS has determined that the device's requested spectrum grant will not cause harmful interference to any federal incumbent activity detected by the ESC in the vicinity of the device's operation.
2. Granting an authorization does not violate the rules implementing international agreements on the protection of borders with Mexico and Canada.
3. For devices located within 150 km of co-channel FSS earth stations, or within 40 km of in-band non-co-channel earth stations or adjacent band TT&C FSS earth stations, the SAS will confirm that allowing the device to operate will not increase aggregate emissions to a level that would exceed interference protection of FSS earth stations established in 47 C.F.R. § 96.17, unless the potentially affected FSS site has waived

[27] Google hopes to work with the Commission to make use of an application program interface (API) to extract this information.
[28] *See* Appendix D.2.

such protection. Potential interference is calculated using power spectral density (PSD) modeling. Google's SAS will use the minimal regulatory standards for emissions masks, unless the manufacturer provides actual performance of the CBSD.[29] The use of actual device performance will motivate industry to achieve performance levels beyond the minimal FCC standards by reflecting the improved performance in the SAS decision-making.

4. If the request includes spectrum above 3650 MHz and the request is made during the grandfathering period for Part 90 operations, the SAS confirms that operation will not violate the protection criteria for grandfathered Part 90 operations.

A common process for all categories of access (Category A or B) provides the option for devices to be transitioned between Category A or B after initial device registration, or even grant issuance. This approach avoids the need to re-register device based on a category change.

PAL Grants

The mapping of PAL auction results to physical channels will be determined after the auction results are available. PAL physical assignments will be made for all active PALs, and then subsequently updated after each PAL auction. The fixed assignment process will attempt to:

1. Maximize the degree of contiguous spectrum for holders of multiple PALs;
2. Maximize the consistency of PAL assignments throughout contiguous license areas; and
3. Maximize the consistency of PAL assignments throughout contiguous individual land masses of the United States and its possessions.

The WinnForum multi-stakeholder group has begun to balance these objectives where they cannot all be met, and Google expects to implement the specifics of channel frequency assignments as negotiated in that forum. In addition, Google expects that, consistent with the *Second Report and Order*, this same forum will develop additional standards to address the calculation of maximum PAL protection areas, including proposing appropriate propagation models to be used in such calculations.[30]

Google also anticipates that some license holders may hold more than one PAL in a given census tract. In such cases, we expect that the device will not only specify that it requests a grant to operate as a PAL CBSD, but also specify which particular licenses—and therefore, which frequencies—it wishes to utilize for the grant. That is, in a given census tract, selection of an individual PAL will imply selection of a particular physical frequency.

---

[29] Section 3.9.1 contains additional details and an example of how PSD is modeled. While the Commission decided in the *Second Report and Orde*r not to change its device certification rules to provide for reporting of out-of-band emissions (OOBE) characteristics, it did not preclude SAS Administrators from taking account of appropriately documented device characteristics. *Second Report and Order* ¶¶ 308-09. Google is prepared to incorporate OOBE information that is provided to the Commission by manufacturers, for instance in test reports from certified laboratories. This process is discussed in further detail in section 3.9.1 as well.

[30] *See Second Report and Order*, Appendix A, § 96.25.

The SAS processes requests for PAL spectrum in several ways.

- In all cases, if the SAS receives a request for PAL spectrum usage, it will validate that the request is made by a licensed owner or lessee authorized to use PAL spectrum, and that the request is associated with a PAL protection area that both conforms to the license terms and does not exceed the default protection contours established in the *Second Report and Order*.[31]
- A CBSD can declare itself part of a network by providing a network ID in its grant or registration request. If this field is provided, the entering device is not rejected even if it might cause co-channel interference to a node in the same network ID, regardless of census tract. This mechanism enables network operators to manage the interference between their devices, without intervention by the SAS.
- If no network ID is provided, then the device requesting entry into the PAL protection area must not cause interference to any existing PAL device, even one operated by the same PAL holder.
- In all cases, if the SAS predicts that a grant will result in harmful interference to devices operated by another network (presumably, an adjacent PAL holder), then the grant request will be rejected, unless the potentially affected PAL holder has waived protection.

The default channel assignments for PALs may be temporarily suspended to protect federal operations. In this case, the SAS will provide alternate channels (if available within the ten channels allocated for PAL operation) to PAL devices that were suspended due to federal activity. There may some cases where relocation is not possible; for example, federal activity may preclude operation across all PAL frequencies.

GAA Grants

Google's SAS uses the following logic to determine GAA frequencies:

When a GAA CBSD requests an authorization, it may either specify the frequencies it seeks or seek assistance from the SAS in selecting a particular set of frequencies. Google recognizes that devices may have the ability to sense the actual, rather than predicted, signal background in their vicinity, which is why it allows GAA users to designate a preference for particular frequencies.

In the first case, where the GAA user requests a specific set of frequencies, the SAS will authorize operation on those frequencies so long as operation will not cause interference to higher tier users. The process for evaluating potential interference to incumbents is set forth above under “aspects common to all grants.” Then, the SAS determines whether the GAA user is operating within a PAL license area that is in use, and if so, whether the GAA user seeks access to PAL frequencies in use. In determining PAL protection, the SAS calculates potential interference using PSD models that reflect the actual performance of CBSDs and interference requirements of PAL operations. If the requested grant will not cause harmful interference to spectrally or physically proximate PAL users, it is authorized and recorded with the SAS.

[31] *Id.* § 96.25(c)(2).

In the second case, where a GAA user does not request a particular set of frequencies, Google's SAS begins by considering the pool of all possible GAA frequencies. It then excludes any frequencies where operation would cause interference to incumbents, under the process described above under "aspects common to all grants." From that pool, the SAS eliminates any frequencies where operation would cause harmful interference to any deployed PAL CBSDs. The list of remaining frequencies is then provided to the requesting GAA CBSD. From these frequencies, a GAA user may choose a desired set of frequencies, and that choice is reported back to the SAS.

After Grants Are Issued

Certain events may require modification or termination of grants. These include the following:

1. *All tiers:*
   a. All grants will be re-examined when new FSS sites are registered, or registration data for FSS sites are changed, thereby ensuring that existing grants do not cause interference to a modified in-band FSS earth station or a newly-registered adjacent-band TT&C earth station.
   b. A declaration or activation of federal exclusion zone, protection zone, or restricted area within a protection zone will cause all grants to be re-evaluated.
2. *PAL tier:* If a PAL CBSD does not contact the SAS for seven days, the SAS will discontinue PAL protection for that CBSD.[32]
3. *GAA tier:* Grants made to PAL CBSDs will trigger examination of all GAA devices operating in frequencies overlapping the PAL channel to assure non-interference with the entering PAL device.

The WinnForum's SAS-CBSD protocol describes the mechanism by which the SAS communicates the outcome of these reevaluations to CBSDs.[33] All CBSDs receive ongoing authorization from the SAS using a heartbeat mechanism with a refresh period controlled by the SAS. Thus, in areas where transient incumbent activity may occur at any time (such as those within an NTIA protection zone), refresh periods are shorter. Elsewhere, refresh periods can be extended.[34] This heartbeat mechanism also protects non-federal incumbents from harmful interference due to CBSD emissions. If positive continuing authorization cannot be obtained from the SAS, a CBSD must cease transmission at the end of the heartbeat authorization interval. The protocol allows the SAS to dynamically adjust the refresh interval used by a CBSD. Thus, a CBSD within a protection zone can be provided with a refresh interval sufficiently short to achieve the Commission's requirements on spectrum-vacate intervals when the SAS enforces an ESC-based restricted area requirement.[35]

---

[32] *Id.* § 96.25(c)(1)(ii).
[33] *See* Appendix D.2.
[34] Additional detail regarding proposed heartbeat times is set forth in section 3.6.4, which how SAS operators will ensure that CBSDs can and are communicating properly with the SAS.
[35] *See infra*, section 3.6.4.

2.1.4 Security (47 C.F.R. § 96.61)

47.C.F.R. § 96.61 requires that: (1) a SAS must ensure its communications and interactions with CBSDs are accurate and secure; (2) unauthorized parties cannot access or alter the SAS; (3) its communications with an ESC are secure; (4) its communications with other SASs are secure; and (5) the FCC ID supplied by a CBSD corresponds to a certified device.[36]

Each of these requirements is discussed in other sections of this application. Communications and interactions between the SAS and CBSDs are discussed in section 3.6. The security of the SAS itself is discussed in sections 2.7, 3.1.2, and 3.8. Communications between the SAS and its associated ESC are discussed in section 2.4. Communications between SASs are discussed in section 3.4. Verification of CBSDs is discussed above in section 2.1.2.

2.1.5 SAS Administrator Requirements (47 C.F.R. § 96.63)

47 C.F.R. § 96.63 sets forth a number of specific requirements for SAS Administrators. Below, Google highlights its capability to: (1) obtain information from the Commission's databases; (2) respond in a timely manner to verify, correct, or remove data, as appropriate; (3) ensure that the SAS is available to respond to Commission personnel; (4) establish protocols to respond to instructions from the President of the United States or another designated federal government entity; and (5) comply with enforcement instructions.[37]

The SAS Administrator will perform a number of the functions set forth above. These include:

1. Scheduling and performing synchronization with FCC and other databases essential to the operation of the SAS at least once daily;
2. Assuring reliable operation of the Graphic User Interfaces (GUI) supporting SAS services, such as device descriptions, the Regulators' Console,[38] and public distribution of SAS data; and
3. Assuring software is updated to reflect any changes in regulatory requirements, or to correct any discrepancies that are detected.

To comply with the requirements to respond in a timely manner to notifications of discrepancies, respond to instructions from the President and designated federal entities, and execute enforcement instructions, Google will provide a capability for receiving reports of exceptional circumstances requiring the attention of the SAS Administrator.

---

[36] *See generally* 47.C.F.R. § 96.61.
[37] *See* 47 C.F.R. § 96.63(b), (f), (k), (l), (m). Other subsections of this rule—for example, the requirement to establish protocols to ensure secure communications between the SAS, ESC, and CBSDs—are addressed in other sections of this application. Still others—for example, the requirement to "establish and follow protocols and procedures to ensure compliance with the rules set forth in this part"—are the subject of Google's response as a whole.
[38] Google will provide an online console with restricted access to authorized government users, which will allow regulators to query the SAS for information.

Such reports can be received from these entities and/or their designated agents:

1. Federal government entities;
2. Operators of incumbent FSS earth stations;[39]
3. Operators of grandfathered Part 90 stations operating in the 3650-3700 MHz band;
4. Operators of networks protected by PALs;
5. Operators of network equipment licensed by GAA rules;
6. Other SAS Administrators; and
7. ESC Administrators.

Reporting is supported for the following exceptional circumstances:

1. A report of erroneous data in the SAS database;
2. A report of harmful interference experienced by an incumbent station or Priority Access licensee which is prohibited by Part 96 rules;
3. A report of an alternative interference protection relationship between an incumbent station (or group of stations) and CBSDs operating under Part 96;
4. A report of an alternative interference protection relationship between a Priority Access network operator and other CBSDs operating under Part 96;
5. A request for additional protection made by an FSS operator;[40]
6. Any FCC enforcement action taken regarding a particular CBSD or group of CBSDs;
7. Any FCC waiver granted to provide an exception to Part 96 rules for CBSDs or other CBRS entities; and
8. Any FCC waiver granted to a non-CBRS entity which impacts CBRS operations.

When Google receives a report of exceptional circumstances, Google's SAS will provide the full details of such a report to all other SAS Administrators as set forth below:

1. Reports originated by the federal government will be provided to other SAS Administrators.
2. Reports of alternative interference protection relationships between incumbents and CBSDs or between Priority Access and GAA users will be provided to other SAS Administrators.
3. Reports leading to corrections in the SAS database will be communicated to other SAS Administrators to the extent that the correction impacts previously-communicated information the SAS Administrator has corrected as a result of the report.
4. Reports of harmful interference may be communicated to other SAS Administrators in the process of responding to such a report.
5. Alternative protection arrangements for FSS earth stations under 47 C.F.R. § 96.17(f) will be communicated to all other SAS Administrators.

[39] *See Second Report and Order*, Appendix A, § 96.17(f).
[40] *Id.*

The SAS expects to implement any standard reporting procedures requested by government users and included in future WinnForum requirements.[41] Such tools will also inform the submitter, and any impacted CBSD user, that reports may be acted upon by the FCC.

2.1.6 SAS Administrator Fees (47 C.F.R. § 96.65)

A discussion of Google's proposed business structure for SAS services is set forth in greater detail in section 2.3.

2.2 Google Technical Expertise

Google's Access group is focused on improving Internet access for everyone. As a part of these efforts, Google has long advocated for more intensive spectrum use and dynamic spectrum sharing. The SAS team brings deep background in wireless network architecture, radio frequency engineering, and spectrum access system development.

Key members of the SAS team and their subject matter expertise are shown below.

Key Personnel	SAS Role	Qualifications
Mr. Milo Medin	Vice President, Access Services, and project supervisor	Founder and CTO of M2Z Networks. Co-founder and CTO of Excite@home. Invited Expert, PCAST working group on spectrum sharing. Member of the FCC's Technological Advisory Council.
Dr. Preston Marshall	Technical lead for SAS engineering and development of industry standards	Program Manager for DARPA spectrum sharing research. Principal investigator for DARPA spectrum sensing program. Invited Expert, PCAST working group on spectrum sharing. Author of two books on cognitive radio and spectrum sharing. Co-chair of WinnForum's standards-setting process for CBSD and SAS products. Ph.D. in electrical engineering.
Dr. Andrew Clegg	Develop industry standards for SAS and ESC operations. Liaise with DoD and other incumbents regarding protection requirements. Architect for Google ESC. Propagation/clutter modeling lead.	Prior lead member of technical staff at major cellular carrier. Spectrum manager for the National Science Foundation and representative to NTIA's Interdepartment Radio Advisory Committee. U.S. delegate to WRC-2007 and WRC-2012. Current chair of WinnForum SSC Working Group 1, which derives functional and operational standards for SAS and ESC systems. Ph.D. in radio astronomy with a minor in electrical engineering.

[41] *See* Appendix D.4.

Mr. Greg Leon	Propagation algorithms, validation, and development of new algorithms for future submissions.	Nine years of technical and business experience at leading propagation modeling software firm, including experience supporting spectrum regulatory efforts. MS in telecommunications with a focus on spectrum and interference modeling.

Table 1: Key Personnel

The SAS team works with software development and system operations teams drawn from Google's technical staff, based on their skills in the development and operation of complex systems, such as software engineers responsible for the development and maintenance of applications and systems including Google Search, Adwords, Gmail, and Android. To assure the smooth development and operation of its SAS, Google utilizes the same programming and execution environment of these Google products in the deployment of its SAS, including relying on Google's data centers, interconnection fabric, user access networks, and programming resources.

Google's systems are easily capable of accommodating the provision of SAS services. Google Search alone handles around *three million searches of the entire Internet* (on average) every minute,[42] whereas the average rate of new CBSD registrations at the peak of deployment is only expected to reach around six registrations per minute. Google's development processes, computing and communications resources, and operational capability are sufficient to operate the SAS and ESC.

2.3 Google Financial Capability

Alphabet, Google's parent company, is a publicly traded Fortune 50 company with a market capitalization of over $500 billion. In 2015, Google had net income of approximately $16.3 billion on approximately $75 billion total revenue, and its assets as of December 31, 2015, included $73.1 billion in cash, cash equivalents, and marketable securities. Google has the financial resources to operate a SAS and an ESC for a minimum of five years. Google has not yet made a decision as to whether and how it may charge fees to CBSD users for the use of its SAS, but any fees will be reasonable and non-discriminatory. Fees may be individually negotiated.

2.4 Assuring Secure and Reliable SAS-to-ESC Communications

<u>Security</u>

The security of ESC communications is maintained through the use of a TLS-protected session protecting the contents of all information passed from ESC sensors to the cloud-based ESC decision system itself. In addition, the communications from this ESC decision system are encrypted and carried on in a secure network within Google's internal infrastructure.

[42] For actual search volume, see Google Searches in 1 Second, http://www.internetlivestats.com/one-second/#google-band.

Data traveling between Google's SAS and an ESC will be encrypted using HTTPS/TLS . As part of Google's ongoing commitment to security, Google upgraded its RSA certificates to 2048-bit keys and implemented perfect forward secrecy (PFS), which minimizes the impact of a compromised key, or a cryptographic breakthrough. It protects network data by using a short-term key that lasts a few days and is only held in memory, rather than a key that is used for years and kept on durable storage. Google was one of the first major web service providers to enable perfect forward secrecy by default. In addition, Google encrypts data as it moves between our data centers on our private network, in order to prevent attacks based on intercepting unencrypted inter-datacenter transmissions.

Reliability

Google intends to implement a number of reliability mechanisms to ensure seamless communications between its ESC and its SAS, including:

- Overlapping coverage of ESC sensors, so that a single sensor failure or a single instance of lost connectivity does not require CBSDs to shut down.
- Multiple backhaul paths to and from ESC devices to provide multiple, independent channels of communications between the ESC and the SAS. Homing will be site specific, and will consist of one or more cellular, point-to-point, or wired/fiber connections, depending on site availability.
- Replicated sensors in the same location to provide redundancy. Multiple sensors provide reliability to the detection process, and enable the SAS to minimize reliability caused disruptions.

Google's communications and processing network is itself highly redundant and capable of switching traffic and communications loads in response to local outages. Although these redundancies are designed to ensure uninterrupted operation, if the SAS does not receive positive confirmation that naval operations are not occurring within a CBSD's field of view, devices in the area of uncertainty will be required to vacate all of the channels used by the Navy. Thus, naval operations are under no risk of harmful interference due to any communications failure between the SAS and the ESC.

2.5 Google's SAS and ESC Architecture and Functional Interaction

Google has designed its SAS and ESC according to the industry consensus architecture developed by the WinnForum.[43]

The logic of our SAS is centrally implemented, but the SAS is physically implemented across Google's distributed computing fabric, with processing present in multiple data centers in order to assure reliability and adequate computing resources, even in the unlikely event of a failure of an entire data center or communications network.

Our ESC function consists of two logical components, a distributed physical sensor component that is deployed in the field within coverage areas of potential naval operations, and an ESC decision component. The ESC decision component is centrally implemented both logically and physically. The sensors report the presence or absence of federal activity to the ESC decision engine, which then provides the "YES/NO" determination for an area of coverage

[43] *See* Appendix D.3.

to the SAS. This architecture provides the reliability of multi-sensor coverage, but minimizes the amount of information that is actually provided to the SAS.

A high-level view of Google's SAS ecosystem is shown below.

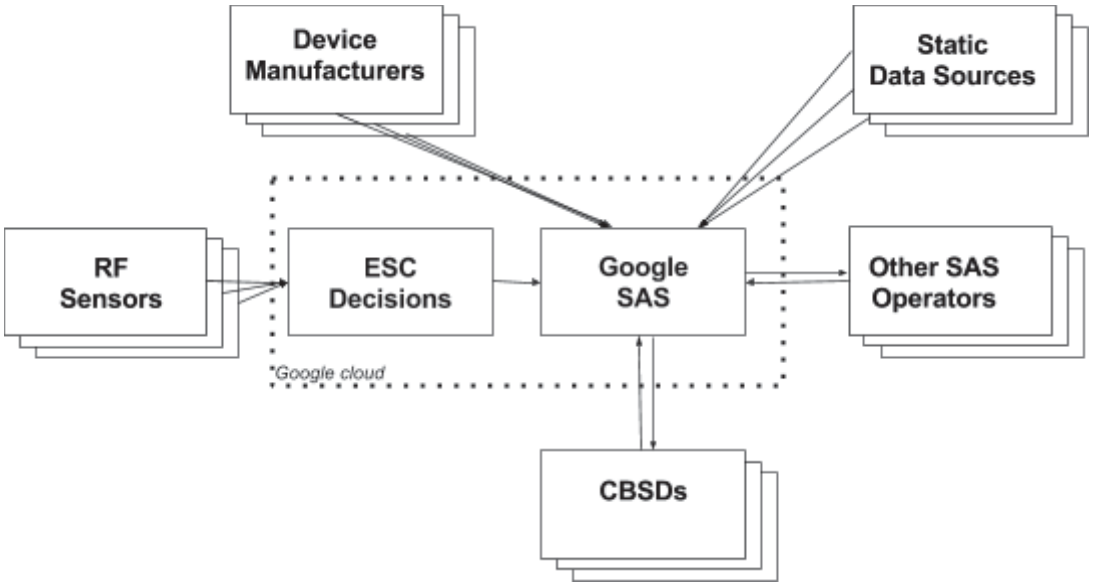

Figure 1: Combined SAS and ESC Ecosystem

The following paragraphs discuss this structure in greater detail.

2.5.1 SAS and ESC Integration

The ESC informs the SAS of a specific restricted area and channel(s) requiring protection. This process does not provide any additional information regarding the basis of that decision.[44] An area is designated for protection whenever the following conditions are met:

- The area is not covered by a functioning ESC sensor. In this case, the entire uncovered area constitutes an exclusion zone under the Commission's rules, and all channels on which naval operations may occur are marked for protection.
- A sensor detection is reported, and meets the threshold criteria for reporting. In such cases:
  - A total bandwidth of the center frequency ±5 MHz is reported as protected.
  - The entire geographic area within the coverage of the sensor is reported for protection, unless sub-areas are reported as clear by another overlapping sensor.

Upon receipt of an occupancy report, the SAS marks all CBSD nodes within the frequency range and perimeter of the restricted area for heartbeat termination. They will have

[44] For example, the ESC will not provide information regarding the specific sensor(s) that detected a federal signal, the amplitude of the signal, either initially or over time, or any other information that could be used to determine any details of naval operation that could compromise operational security.

their operation on these channels terminated upon their next heartbeat request. If they fail to ask for a heartbeat in a timely fashion, software on the CBSD itself will automatically terminate operation.

The commercial operating standards for ESCs currently under development within the WinnForum intend to accommodate the requirement that ESCs must adapt to future radar systems that require protection.[45] DoD has participated actively in these discussions. Google anticipates that the WinnForum SSC will be the appropriate venue for periodic reviews with DoD of new or refined protection requirements. Google expects to follow any WinnForum standards developed to address future radar systems.

2.5.2 SAS Architecture

The functional relationship of the major SAS components is shown in the figure below. For clarity, other functions that are not related to interference protection, such as spectrum availability inquiries, are not shown in the depiction of the interference protection functionality.

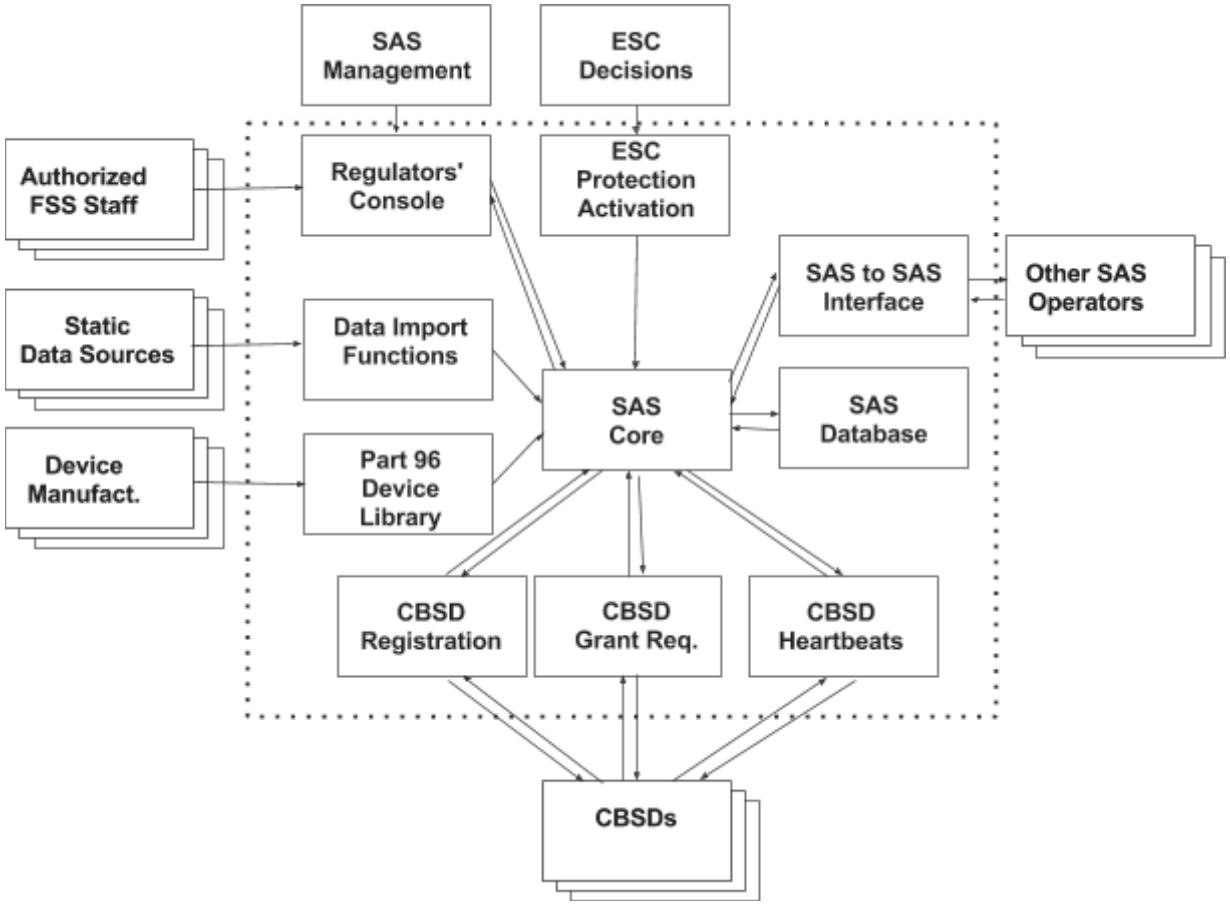

Figure 2: Architecture of Google's SAS

[45] *See* Appendix D.4 (discussing standard operational and functional commercial requirements for ESC and SAS operators).

The dotted line indicates the scope of Google's SAS, and its components are summarized below:

Component	Description
CBSD Interfaces	Includes interfaces for registration, authorization (including requests for grants and grant issuances), and heartbeat requests. A common Google Front End (GFE) is shared with other Google services. The GFE authenticates transactions into the SAS from all sources, including authenticating message signing and identifying the certificate authority issuing the required certificate(s).
SAS Core	Performs the basic SAS operations and executes all SAS interactions with the SAS database.
Data Import Functions	Import relevant information from specific static databases used by Google's SAS. These databases are specified and in some cases provisioned by the FCC, and include the International Bureau Filing System (IBFS) for FSS sites and usage, census tract designations, protected Part 90 deployments, as well as Part 96 equipment authorizations and license information as it become available for retrieval.
Part 96 Device Library	Accepts additional, optionally-provided Part 96 device information that is not collected through Part 96 device certification. Such information could include actual OOBE characteristics and other information that further characterizes the interference potential of authorized Part 96 devices.
ESC Protection Activation	Accepts activation and inactivation messages from the ESC decision functionality, activates protection in specific restricted areas, and restores operation within protection zones. Ad hoc protection zones are implemented at the SAS, not within the ESC.
SAS-to-SAS Interface	Synchronizes Google's SAS with other SAS Administrators. This function includes providing all relevant SAS persistent store changes to other SAS Administrators, and receiving and processing changes from other SAS Administrators.
Regulators' Console	Provides regulators with web-based access to CBSD registration, frequency usage, and interference information. Allows regulators to change the status of one or more CBSDs.
SAS Database	Holds all SAS-related information that is needed beyond the time scope of a single registration, grant request, or heartbeat. As noted above, data will be stored for 60 months.[46]

Table 2: Key Functional Components

2.5.3 ESC Architecture

The general ESC architecture is shown in figure 3.

[46] *See* 47 C.F.R. § 96.55(b).

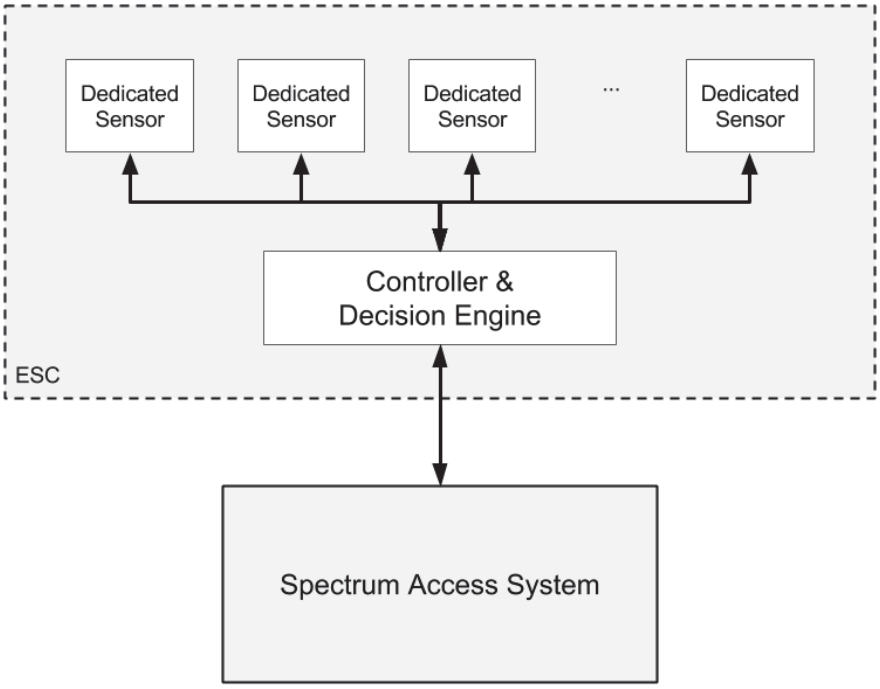

Figure 3: Google ESC Block Diagram

Key characteristics and operating algorithms of Google's ESC are shown below.

Component	**Description**
Reporting Threshold	Google has demonstrated successful detection of the current incumbent radar using Google-developed algorithms, deployed in an actual military operating environment in the Norfolk/Virginia Beach, Virginia, area. WinnForum is developing a specific threshold for radar detection in a joint working group with DoD and the Navy.[47] Google expects that its commercial ESC network will utilize the WinnForum SSC working group-established methodology with regard to the distance and speed with which radar operations must be detected.
Coverage Area Definition	Refers to the ocean areas that could have a radar signal detected at a level that will achieve the reporting threshold. The determination of this area uses the SAS propagation algorithm, as expected to be certified by the FCC, and applied with consideration of the appropriate ground conductivity, sensor placement, antenna pattern and orientation. Each sensor will have a coverage area determined by the ESC decision tool, based on its coverage analysis.
Restricted Area Determination	Restricted areas are activated as follows: • An ambiguity region is determined based on the entire area covered by the

[47] *See* Appendix D.4 (discussing standard operational and functional commercial requirements for ESC and SAS operators).

	sensor(s) reporting a detection, minus any areas covered by operational sensors in which no detections were reported. This ambiguity region is entirely in the ocean. • An active restricted area is determined by identifying all points that are within a restriction distance from any point in the ambiguity region. Restriction distances will account for the differences between Category A and B CBSD signal propagation. By limiting CBSD transmissions within a restriction distance of all points within the ambiguity region, the entire ambiguity region is protected from harmful interference. The process for determining restriction distances is a subject of active discussion in the WinnForum SSC ESC task group, and Google expects to implement restriction distances consistent with the outcome of that process. • Heartbeats are terminated for the impacted frequency range throughout the resulting restricted area, and all transmissions will cease within one heartbeat interval (<240 seconds), plus the allowed device shutdown interval (<60 seconds).[48]
Operational Capability	ESC sensors will include a capability to ensure that the sensors are performing as designed. By way of illustration, each sensor system may periodically insert low level reference signals of known amplitude and antenna response in front of the sensor's aperture to assure end-to-end detection and processing of all naval emissions. The signal-to-noise ratio of this inserted signal establishes the functionality and noise floor of the sensor. This self-test will be performed at intervals no longer than the minimum required channel clearing time. Self test results will be communicated rapidly to the ESC decision component.
Communications Connectivity Assurance	The sensor will respond to status requests from the ESC decision component and return its current condition to the ESC. As noted immediately above, this connectivity assurance polling will occur at a frequency sufficient to assure that a sensor or connectivity failure will not result in lack of monitoring or reporting for an interval greater than the required channel clearing time.
Sensor Placement	Sensors will be placed to ensure that there are at least two sensors covering all required naval operating areas, as close to shore as siting constraints will allow. An illustrative set of sites is depicted below, though precise siting is subject to change.

Table 3: ESC Key Functional Components

An illustrative sensor deployment scenario on the Atlantic, Pacific, and Gulf coasts, as well as associated sensor coverage patterns, is shown below. The diagram shows that under reasonable assumptions a network of 103 sensors placed on existing towers registered with the

[48] This approach complies with today's Part 96 rules, but several parties have proposed reconsideration of these time frames. *See, e.g.,* WinnForum Petition for Reconsideration, GN Docket No. 12-354, at 3-5 (filed July 22, 2015). Google will modify its SAS and ESC to reflect any further FCC actions in this area.

FCC's Antenna Structure Registration database could establish redundant coverage across all coastlines on the continental United States.[49]

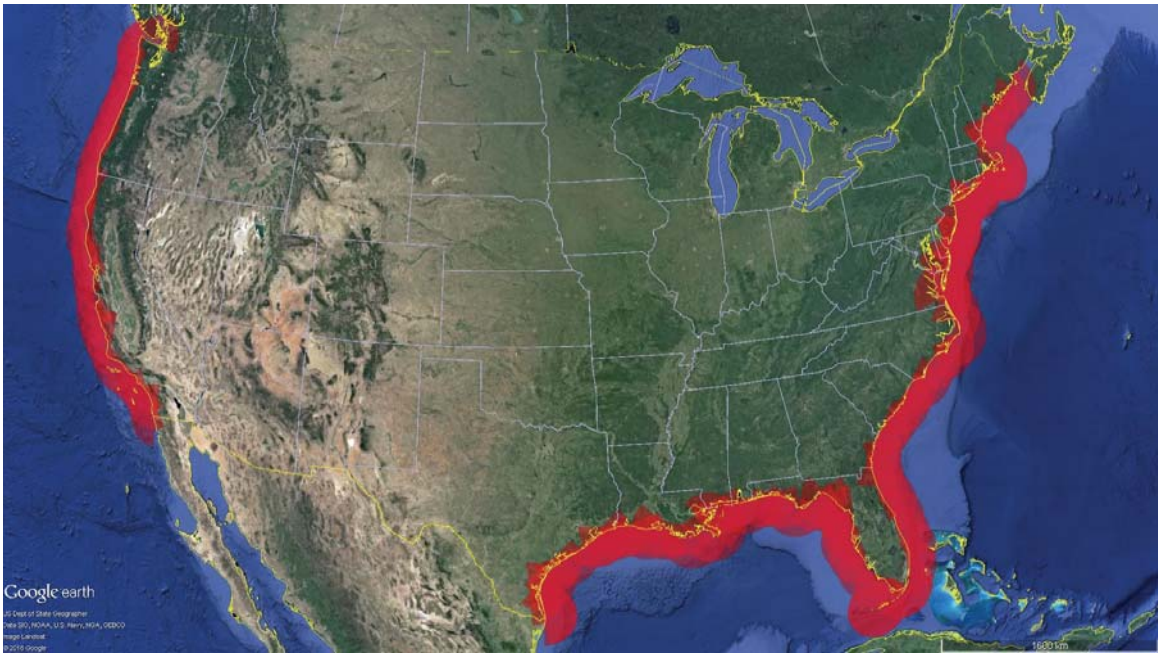

Figure 4: Coverage of a Notional Deployment of 103 Dedicated ESC Sensors
Deployment reflects sensors placed along the Atlantic, Pacific, and Gulf coasts, utilizing constructed towers as registered in the FCC's Antenna Structure Registration database. Each node is assumed to have a detection range of 150 km—a range well within the capability of Google's sensors, and a horizontal angular coverage of 180, 270, or 360 degrees, depending on local coastal geometry. The locations, angular coverages, and pointing azimuths for each node are established to ensure that almost every point within approximately 70 km of the coastline is covered by at least two sensor nodes.

Locations for sensor siting are currently under consideration. Coverage redundancy, backhaul reliability, cost, and visibility to the ocean will all drive siting decisions. At the same time, minimum sensor system performance levels are being developed with DoD through the WinnForum ESC task group.[50] Both these requirements and the considerations in Appendix B, which address coverage redundancy, will be critical in determining sensor site locations. Google expects to implement sensor performance requirements as developed in collaboration with DoD.

A schematic of the nominal ESC sensor design is shown below.

---

[49] The figure assumes sensors are placed on towers that have already been constructed and registered in the FCC's Antenna Structure Registration database. Antenna Structure Registration, http://wireless.fcc.gov/antenna/index.htm?job=home.
[50] *See* Appendix D.4 (discussing standard operational and functional commercial requirements for ESC and SAS operators).

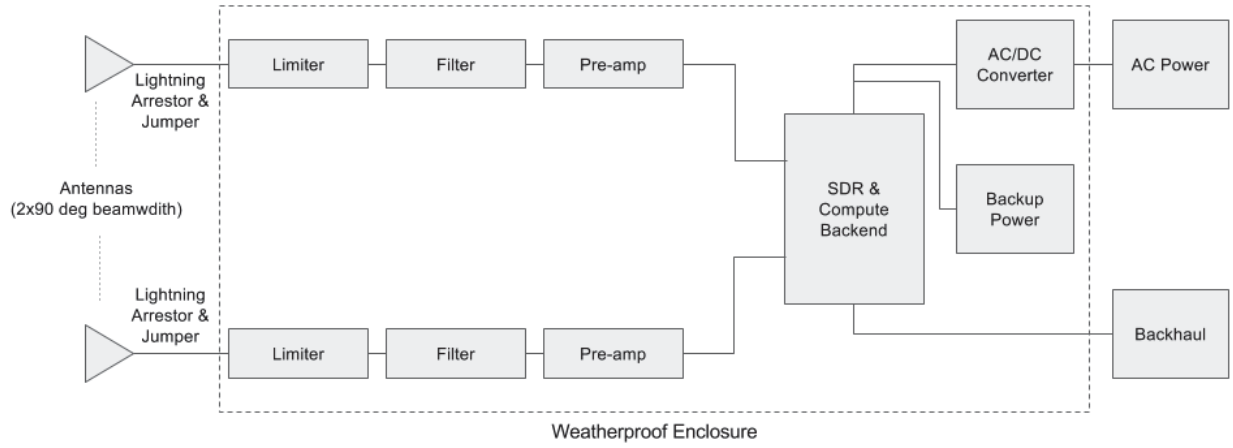

Figure 5: ESC Sensor Block Diagram

Major components of the sensor and representative performance specifications for each component are set forth in the table below.

Component	**Representative Performance Level**
Antenna	17 dBi gain, 90 deg horizontal beamwidth, 7 deg vertical beamwidth, dual (H/V) polarization
Bandpass Filter	3000-4300 MHz passband, <1 dB insertion loss across 3.5 GHz band
Low Noise Amplifier	23dB gain, <1 dB noise figure
SDR Platform	Instantaneous sampling bandwidth equal to the radar bandwidth or greater, across the CBRS and adjacent bands
Compute Backend	Small form-factor, low-power, general-purpose compute platform with bus interface capabilities matched to SDR platform

Table 4: Performance Expectations for Sensor Components

A picture of a prototype sensor front end is set forth below. Packaging design will be informed by initial experience with the deployment of sensor prototypes in Norfolk, Virginia, and San Francisco, California.

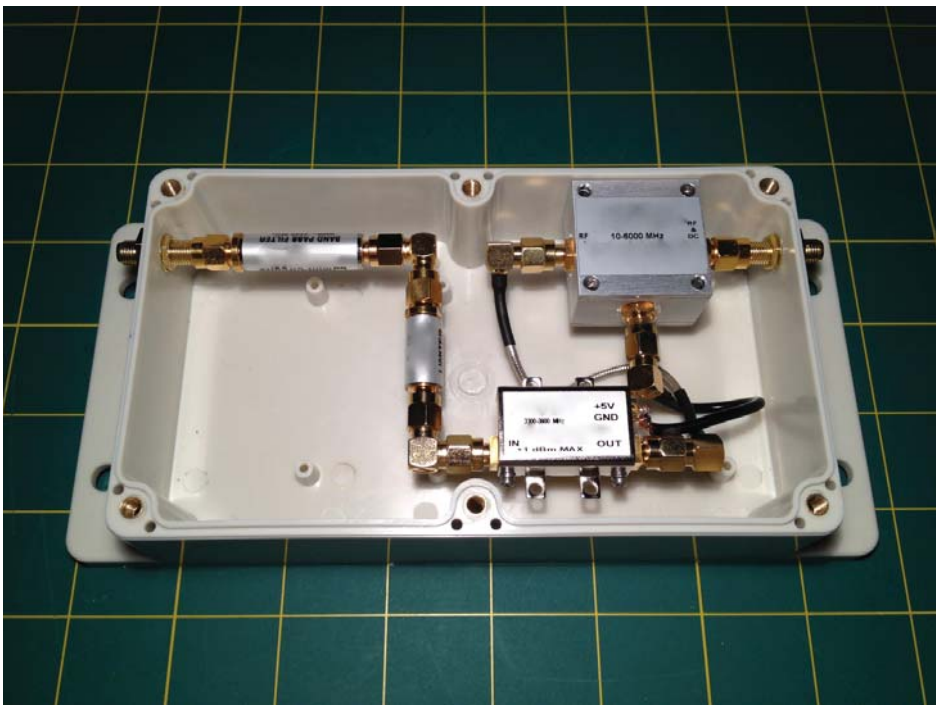

Figure 6: Prototype ESC RF Front-End in Weather-Proof Enclosure

As designed, the RF system provides strong immunity to front-end overload and device burnout. The proprietary design of our detection algorithms continues to provide excellent pulse detection even if the low noise amplifier (LNA) is driven into compression, in part because the sensor only needs to detect pulsed power, rather than the complex phase/amplitude/frequency modulation factors in a typical communications signal. To avoid device burn-out, Google's sensors employ a limiter before the LNA, which limits power into the LNA below the LNA's damage point. Both overload performance and damage immunity have been demonstrated through two years of deployment in close vicinity to operating incumbent radars in the Virginia Beach, Virginia, area. No sensor has been damaged during this period.

2.5.4 Interactions Between Functions

A summary of the types of interactions among and between SAS and ESC functions is shown below, as well as the methods used to implement each. Each interface is bidirectional. Additional details regarding message and information flow are provided later in this application.

From	To	Interface	Standards/Design
Sensor	ESC	IP Message	Internal Google message, specific to Google sensors and ESC design
ESC	SAS	API	Internal Google message compliant with WinnForum requirements[51]

[51] *See* Appendix D.4 (discussing functional and operational requirements).

CBSD	SAS	IP Message	WinnForum standard message being adopted by industry[52]
SAS	SAS	IP Message	WinnForum standard message being adopted by industry[53]
Regulator	SAS	HTML	Google developed regulators' console functionality
Device Manufacturers	SAS	HTML	Google developed device description functionality accepting additional information regarding CBSDs
Sources of static data	SAS	File Transfer	File imports from applicable FCC and other governmental databases, such as the IBFS and ULS, and specialized lists, such as census tract boundaries and urban area definitions

Table 5: CBSD, SAS, ESC, and Sensor Communications

2.6 Propagation Model

Consistent with the *Second Report and Order*, Google is prepared to implement a common propagation model, as approved by the Wireless Telecommunications Bureau and the Office of Engineering and Technology.[54] Below, Google sets forth its recommended approach to propagation modeling, as well its plan to incorporate improved propagation modeling if permitted to do so by the Commission. We also provide background on the propagation research Google has conducted in connection with this proceeding.

Google understands that a transition to an automated propagation model that takes into account detailed information regarding the local environment would be a significant innovation. Therefore, Google proposes to evolve its SAS propagation model through three phases. If such evolution is permitted, Google expects to submit all models for Commission testing and public review before implementing them.

- **Initial SAS Operation**. Consistent with the *Second Report and Order*, Google proposes to use a standard propagation model when it first deploys its SAS.[55] We expect the WinnForum to develop a proposed propagation model and appropriate input parameters by industry consensus, and that these will be submitted for FCC approval.[56]
- **Site-Specific Clutter Model**. Some propagation models include a rudimentary (and typically highly conservative) clutter loss model that takes into account general characteristics of the sites where emitters and protected receivers are in operation. Google favors use of clutter models, as the impact of clutter on propagation loss has been shown to be substantial.
- **Path-Specific Model**. Subject to industry consensus and FCC approval, Google intends ultimately to refine path loss predictions by calculating the least expected path loss for each specific path considered by the SAS. This analysis may be based,

[52] *See* Appendix D.2.
[53] *See* Appendix D.1.
[54] *See Second Report and Order* ¶¶ 138, 188, 190, 278.
[55] *Id.*
[56] *See id.* ¶ 278.

for example, on a regressed database of path loss measurements described in more detail below.

Transitioning to a path-specific model has the potential to dramatically increase spectrum availability. To date, Google has collected more than 1.5 million data points of propagation loss measurements in the 3.5 GHz band. These measurements have been acquired in a variety of environments in which CBSD deployments are contemplated. Substantial data have been collected the in vicinity of Arlington, Virginia, and Mountain View, California, with additional collection activities planned for Kansas City, Kansas; San Francisco, California; and other areas.[57]

Google collects these measurements to compare them with predictions made by standard propagation models, and to better characterize how clutter along transmission paths affect the measured losses. When examined together with high resolution geographic information from Google Earth, Street View, satellite imagery, and other Google resources, these measurements enable high-confidence estimates of each of the contributors to path loss beyond the model predictions.

The data collected by Google demonstrate that clutter adds tremendous additional path loss beyond the losses predicted by standard models. The average difference is typically 20-30 dB for many environments (a factor of 100-1000). The average difference can be even higher (50 dB, or a factor of 100,000) in some environments, especially when both the transmitter and receiver are located well below the typical clutter height, and/or are located indoors—scenarios that we expect to be common for small-cell deployments.

Two examples of the impact of clutter on propagation loss are shown below. The first example (figure 7) shows data collected in the Mountain View, California, area. In this case, the transmitter and receiver were both located at heights consistent with first-floor deployments, and tested in both indoor and outdoor environments. Indoor deployments constitute roughly one-third of the measurements, and outdoor deployments constitute the remaining two-thirds. Although Mountain View is a light-to-moderate clutter environment, featuring mostly one- and two-story industrial and residential buildings, with some trees and relatively little terrain variation, embedding the receiver and transmitter in clutter contributed to a sizable departure from predicted propagation loss. The average difference between measured loss and loss predicted by Longley-Rice was 46.1 dB over distances of only 1 km or less.

A similar comparison is shown in figure 8 for the Arlington, Virginia, area, with the transmitter located indoors and outdoors at the second-floor level. As in Mountain View, about one-third of the Arlington data points represent indoor deployments, and two-thirds represent outdoor deployments. The average difference between measured losses and Longley-Rice predictions is 43.9 dB.

[57] Google has presented the results of this testing to the DoD Spectrum Sharing Test & Demonstration Program Propagation Working Group. The presentation shared with DoD appears as Appendix E.

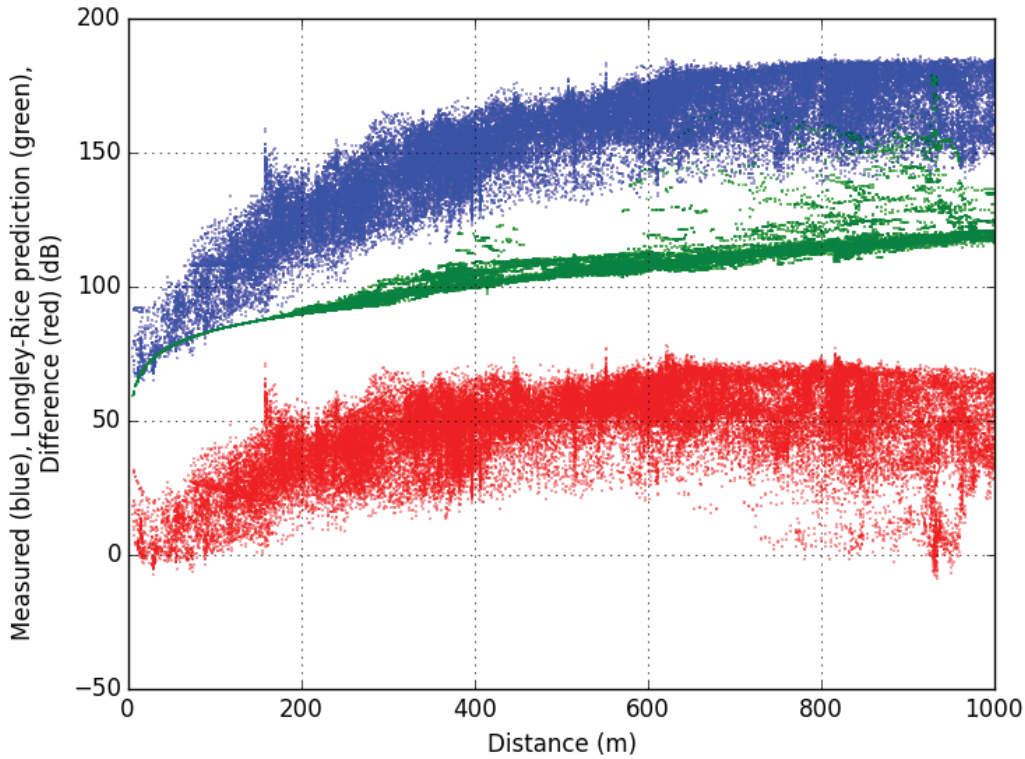

Figure 7: Comparison of Measured Propagation Loss (Blue Points) to Propagation Loss Predicted by Longley-Rice (Green Points) in the Mountain View, California, Area

The difference between measured and predicted is shown in red, where positive red values show that Longley-Rice under-predicted the loss, by an average of 46.1 dB for the data shown. These data were obtained for a mix of indoor and outdoor placement of the transmitter (approximately one-third and two-thirds of the data points, respectively), with both the transmitter and receiver at the first-floor level.

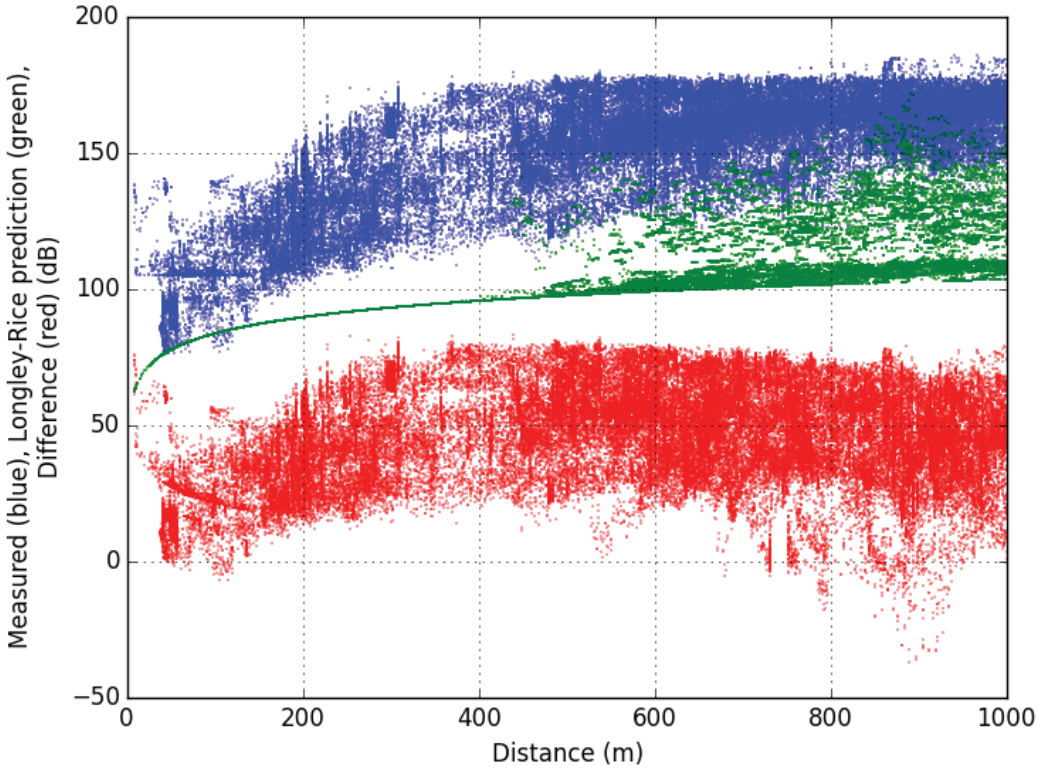

Figure 8: Comparison of Measured Propagation Loss (Blue Points) to Propagation Loss Predicted by Longley-Rice (Green Points) in the Arlington, Virginia, Area

The difference between measured and predicted is shown in red, where positive red values show that Longley-Rice under-predicted the loss, by an average of 43.9 dB for the data shown. These data were obtained for a mix of indoor and outdoor placement of the transmitter (approximately one-third and two-thirds of the data points, respectively), with the transmitter at the second-floor level and the receiver at the first-floor level.

In both cases, the conclusion is clear: measured loss is substantially greater than predicted loss for the vast majority of test points. We attribute most of the difference to the impact of clutter.

2.7 SAS and ESC Software and Firmware Security Management

Across Google, over 500 staff ensure that its global production infrastructure, which is the infrastructure used to provide Google's SAS, remains secure from attacks, can assure privacy, and preserves data integrity.[58] Google makes frequent security enhancements, which automatically protect the SAS and ESC functionalities, to its infrastructure.

Google has extensive internal software test and release management processes that currently manage software for applications such as Google Search, GMail, YouTube, Calendar, and Google Play, as well Android and Nest devices, driverless cars, Project Loon balloons, and the network and computing infrastructure necessary to host its services. Google software

[58] *See* Security Team, https://privacy.google.com/google-security.html.

handles over forty thousand searches alone every second,[59] whereas the anticipated rate of Part 96 registrations is estimated to be on the order of one registration every ten seconds.

Additional information regarding the security and resiliency of Google's systems is provided in section 3.8.

2.8 Affirmation of Compliance

Google affirms that it will comply with all applicable rules regarding SAS and ESC operation, as well as applicable enforcement mechanisms and procedures.

3 SAS OPERATION

3.1 Processing of CBSD, ESC, and SAS Information

3.1.1 Data Retention

As described in section 2.1.1, Google's SAS will comply with the data retention requirements of 47 C.F.R. § 96.55. Data received from other SASs will be retained in the same way that data of a similar type received directly from CBSDs, FSS operators, the Commission, or other federal entities are retained.

3.1.2 Data Security

This section addresses the security of data in transit. Security measures protecting the SAS as a whole are addressed in sections 2.7 and 3.8.

Google's SAS will provide an integrated data security and authority verification framework. In finalizing this framework, Google expects to follow the interface design set forth in the WinnForum's communications security requirements.[60] The design uses TLS (a follow on to Secure Sockets Layer (SSL)), an industry standard for securing remote communications,[61] for two purposes:

- Assuring secure, confidential, and tamper-proof communications between the SAS, CBSDs, ESC sensors, the ESC itself, and other SAS operations; and
- Assuring that CBSD devices are valid users of the SAS, that only inputs from Google's ESC sensors are recognized, and that SAS-to-SAS synchronization is performed only with certified SAS operators.

TLS provides a security feature that immediately detects attempts at a "man in the middle" attack, which could allow unauthorized parties to access or alter information sent to or from the SAS. TLS creates a unique key for each SAS communications session—whether with a CBSD, ESC, or another SAS—and either end of the session can detect any changes, or errors in the information it receives. This key is not known to any entity other than the two parties, so communications cannot be decrypted by a third party. Google will employ TLS on its ESC

[59] Google Search Statistics, http://www.internetlivestats.com/google-search-statistics/.
[60] A number of WinnForum standards are in process, including documents that cover communications security requirements.
[61] More detail on the specifics of the TLS mechanism can be found at Transport Layer Security, https://en.wikipedia.org/wiki/Transport_Layer_Security.

sensors and ESC, and SAS-to-SAS links are similarly protected in accordance with the WinnForum standards.[62] In order to provide secure services, TLS should be used on the device side as well.[63]

3.1.3 Location and Device Verification

As set forth in section 2.1.2, Google expects to rely on certificates issued to device manufacturers to authenticate devices. As part of initial device registration, the FCC ID provided by the authenticated registration message will be verified against the list of approved Part 96 devices provided by the FCC.

Location information will be accepted only from FCC-certified Part 96 devices that provide a certificate obtained by the manufacturer. Location information for professionally installed CBSDs can be provided by an installer consistent with Commission requirements.[64] Google's SAS will retain information regarding the source of CBSD location data—i.e., whether it was provided automatically or by a professional installer. If location information was reported by a professional installer, Google will also retain the identity of that installer. As described in section 2.1.5, Google will also maintain a capability to respond promptly to any reports of errors in its SAS database, including location information, and correct such errors.

3.1.4 Authority (Installer, PAL, SAS, ESC, and Federal User) Verification

The WinnForum is establishing a process to approve Certificate Authority (CA) organizations granting certificates that will be recognized by the SAS and by CBSDs.[65] The WinnForum has obtained a unique SSL code from the Internet Assigned Numbers Authority (IANA) for the types of certificate extensions necessary to authenticate SAS ecosystem entities and will maintain the list of approved CA entities. Certificates for internal interfaces (e.g., between Google's SAS and its ESC) will be issued internally, as these authorizations will not be used by any external party.

Certificates will be validated for the following entities or devices that communicate with Google's SAS or its ESC. Google's SAS expects to rely on the certificate issuance process to provide assurance that a counterparty holds any necessary authorizations (e.g., Part 96 device authorization, professional installer certification).

Entity or Device	Criteria for Certificate Issuance	Role in SAS/ESC operation
Part 96 Device	Issued to entities that manufacture at least one FCC-certified Part 96 device.	Required for most CBSD interactions with Google's SAS, including registration and grant request.

[62] *See* Appendix D.1.
[63] Indeed, WinnForum requirements make use of TLS on the device side. A number of WinnForum standards are in process, including documents that cover communications security requirements.
[64] *See* section 3.1.4 *infra*.
[65] A number of WinnForum standards are in process, including documents that cover certificate authority requirements.

SAS Operator	Issued to organizations operating an FCC-certified SAS system.	Required to provide or receive SAS registrations and grants, as well as other SAS-to-SAS exchanged information.
PAL Owner	Issued to organizations holding at least one active PAL license from the FCC.	Required to validate operator identity for any grant requesting PAL protection status. Further validated against specific PAL holdings at the CBSD location.
Certified Professional Installer	Google expects that certificates will be issued only to individuals who have successfully completed a certified installer program. Certified installer qualification is currently being developed within the WinnForum.	Mandatory for Category B devices and all device registrations where location is not determined through automated mechanisms.
Google Sensor Device	Issued internally by Google to the Google-owned and deployed ESC systems. These certificates will be authorized on a whitelisted per-device basis.	Required for all sensor-to-ESC interactions to prevent spoofing of ESC detections or non-detections.
ESC	No certificate required for communications from Google's ESC to its SAS, as activation is performed via an internal API protected by equivalent machine-to-machine interface security, as well as access controls on the internal Google network.	Internal interfaces are protected by broader Google security measures, and can only be accessed by the internal processes authorized to utilize the interface. Authorization restricted to the ESC application.

Table 6: SAS and ESC Ecosystem Certificates

Federal users of Google's SAS will be provided a Google account to authorize their secure access to SAS information and direction. Two-factor user authentication (for example, password and YubiKey token) will be used to secure this interface.

Finally, the WinnForum is considering standards for proxy management of multiple CBSDs. Google expects to support these interfaces once established, if they are supported by FCC action to certify proxy level Part 96 devices.

3.2 Interference Mitigation and Resolution

Policies and processes to resolve claims of harmful interference are described in greater detail in section 2.1.5. Initially, Google will provide the functions set forth in section 2.1.5 through human support. Claims of harmful interference can be submitted to a Help Desk by either phone or e-mail, and Google will respond promptly to such inquiries.

3.3 Protection of FSS Earth Stations and Grandfathered 3650-3700 MHz Licensees

Google's SAS currently provides protection for FSS sites consistent with the Commission's rules and with prior filings by Google addressing this issue.[66] Google plans to protect incumbent FSS earth stations using the following general method:

- **Step 1:** Calculate FSS antenna gain in the direction of the CBSD requesting authorization to operate, in accordance with antenna patterns referenced in Appendix A of the *Second Report and Order*.[67]
- **Step 2:** Calculate the CBSD's power spectral density in the direction of the FSS antenna.
- **Step 3:** Calculate path loss between the CBSD and the FSS antenna using an appropriate propagation model.
- **Step 4:** Account for receiver filtering as specified in the *Second Report and Order*.[68]
- **Step 5:** Calculate the received interference power at the FSS antenna from the CBSD using the results of Steps 1-4.
- **Step 6:** Aggregate the received interference power from all CBSDs within 150 km of co-channel FSS earth stations, or within 40 km of in-band non-co-channel earth stations and adjacent-band TT&C earth stations, including the emissions from CBSDs seeking authorization.
- **Step 7:** Compare the aggregate power calculated in Step 6 to the interference thresholds established in the *Second Report and Order* (including the effects of both noise floor degradation and receiver blocking) and allow operation if the aggregate power falls below the required interference thresholds.[69]

This method is further described in Google's Reply Comments,[70] and an example is provided in section 3.9.

Absent further Commission action, Google's SAS will protect grandfathered Part 90 operations consistent with the WinnForum filing on this subject,[71] but Google is prepared to implement methods specified by any subsequent Commission action addressing this issue.

3.4 Coordination Among SAS Operators

As noted in section 2.1.1, Google's SAS implements the WinnForum standard for SAS-to-SAS synchronization.[72] Further details regarding this process are set forth in that section.

---

[66] Reply Comments of Google Inc., GN Docket No. 12-354, at 6-13 (filed Aug. 14, 2015) (Google's Reply Comments).
[67] *Second Report and Order*, Appendix A, § 96.17.
[68] *Id.*
[69] *Id.*
[70] Google's Reply Comments at 6-18.
[71] Comments of the WinnForum on the FCC Public Notice on an Appropriate Method for Determining the Protected Contours for Grandfathered 3650-3700 MHz Band Licensees, GN Docket No. 12-354 (filed Dec. 24, 2015).
[72] *See* Appendix D.1.

3.5 Completeness of SAS Operations

Google's SAS provides all of the functional requirements outlined in Part 96, subpart F. It does not depend on any other SAS or external function, other than information gathered from Commission sources or voluntarily provided by entities with the 3.5 GHz ecosystem. There are no government-supplied inputs that augment or determine the capabilities of the ESC in detecting federal incumbent activity.

3.6 SAS Communications Methods

3.6.1 CBSD-to-SAS and SAS-to-CBSD Interface

Google's SAS applies the industry consensus WinnForum protocol for SAS-to-CBSD interfaces.[73] This standard addresses all communications between these two systems in a manner that prioritizes protection of higher tier users.[74] The critical functional capabilities of this interface are:

- Communicating device registration information (including, for example, type, vendor, locations, pointing, and antenna type) provided directly from the device or through a certified installer;
- Communicating and responding to spectrum grant requests to obtain authorization to operate and clearance using the heartbeat process;
- Communicating and responding to heartbeat requests for continued operation on a granted channel; and
- Communicating heartbeat authorizations for continued operation, or negative heartbeat responses and rationale.

Google's SAS ensures protection of higher-tier devices by terminating the periodic heartbeats, in accordance with WinnForum standards.[75]

3.6.2 SAS-to-SAS Interface

As set forth in section 2.1.1, Google's SAS has also adopted the industry consensus WinnForum protocol for SAS-to-SAS interface standard.[76] As noted in that section, the functional capabilities of this interface are as follows:

- Exchange registration data as it enters the SAS;
- Exchange all grants as they are issued by the SAS;
- Exchange all changes in registration and grant status; and
- Exchange regulatory inputs received by the regulators' console.

3.6.3 Sensor-to-ESC and ESC-to-SAS Interface

Google's sensor-to-ESC and ESC-to-SAS interfaces are proprietary. Sensors will report the minimum detection information required to the ESC decision module. Minimum detection information includes (1) which sensor performed a detection, (2) the time of detection using

[73] *See* Appendix D.2.
[74] For additional details regarding this specification, see *id*.
[75] *See id*.
[76] Appendix D.1.

precision that does not permit geolocation of detected radars (e.g., to the nearest second), and (3) the frequency range of sensed activity. Detection information also may include a power level at which activity was detected (e.g., -80 dBm or -90 dBm). The ESC module utilizes the detection history, and the specific sensors that are activated, to identify the appropriate restricted areas and channels for SAS protection.

The information passed from the ESC to the SAS in response to the detection of an incumbent activity event is limited to a geographical description (or reference) that defines the extent of that activity, a range of frequencies to be protected, activation and de-activation times for the protection to be applied (if known), specifiers indicating the type of protection to be applied for the notified geography, and a retention time governing maintenance of the activation record within the SAS.

3.6.4 CBSD-to-SAS Communications Verification

CBSD-to-SAS communications verification and authentication are discussed in greater detail in sections 3.1.2 through 3.1.4.

As noted in 2.1.3, the use of heartbeat intervals requires CBSDs to discontinue transmissions if they do not receive a positive authorization to continue operation on an ongoing basis. If this authorization cannot be obtained, the device must terminate operation. This "*pull mode*" interface is the basis of the WinnForum SAS-to-CBSD interface specification.[77] It protects higher tier users from any failure in the communications between the SAS and the device, as well as any failure of the SAS itself, because if the SAS fails, the devices will not receive reauthorization and must terminate operations.

The SAS will establish time intervals for reauthorization requests based on the location of the device, whether the channel occupied by the device can accommodate PALs, and the worst-case Part 96 shutdown requirements. For devices in a protection zone for naval radars, this interval will be less than the current 240 second maximum,[78] allowing devices to request reauthorization sufficiently early to assure uninterrupted operation. For devices outside of these protection zones, the interval will be set based on the most constraining exit time, driven by PAL deployment (if in a GAA in a PAL channel) or by notice of an FSS site deployment or antenna repositioning.

Based on the requirements of Part 96 and industry consensus standards for protection of newly deployed PALs and FSS actions, Google expects to follow maximum heartbeat times, which may be adjusted or clarified by subsequent Commission action. The SAS can dynamically adjust heartbeat times.

---

[77] *See* Appendix D.2.
[78] *See* 47 C.F.R. § 96.15(a)(4).

Spectrum	Outside of Protection Zone	Inside of Protection Zone
GAA device operating in either GAA spectrum or PAL spectrum that has not been auctioned	< FSS-requested clearance time[79]	< 240 Seconds[80]
GAA device operating in PAL spectrum that has been auctioned but is not in use	< Lesser of PAL-requested clearance time[81] and FSS-requested clearance time	< 240 Seconds
PAL device operating in PAL spectrum	< FSS-requested clearance time[82]	< 240 Seconds

Table 7: Maximum Heartbeat Times

3.7 Non-Retention of Federal Emissions Records

Consistent with section 96.55 of the Commission's rules, Google's SAS will retain records and information or instructions received from an ESC regarding federal transmissions in accordance with information retention policies established as part of the ESC approval process. This retention time limit is conveyed to Google's SAS by its ESC (see section 3.6.3).

3.8 SAS Security

As set forth above, Google's SAS will rely on Google's multipurpose infrastructure, which is protected by rigorous measures to maintain security and resiliency. Below, we highlight measures protecting several discrete elements of our system.

Data Centers

Google data centers use a layered security model for physical security, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, and biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24 hours a day, seven days a week by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training.

All of Google's data centers feature redundant power systems and environmental controls. Every critical component has a primary and alternate power source, each with equal power. Diesel engine backup generators can provide enough emergency electrical power to run each data center at full capacity. Cooling systems maintain a constant operating temperature

[79] Google anticipates that this clearance time will be specified through further Commission action.
[80] *See* 47 C.F.R. § 96.15(a)(4).
[81] Google anticipates that this clearance time will be specified through further Commission action.
[82] This time will not exceed 7 days. *See Second Report and Order*, Appendix A, § 96.25(c)(1)(ii).

for servers and other hardware, reducing the risk of service outages. Fire detection and suppression equipment helps prevent damage to hardware.

Server Equipment

Google uses purpose-built servers and network equipment designed and manufactured in-house, utilizing a custom-designed operating system (OS) based on a stripped-down and hardened version of Linux. Google's servers and their OS are designed for the sole purpose of providing Google services. Server resources are dynamically allocated, allowing for flexibility in growth and the ability to adapt quickly and efficiently, adding or reallocating resources based on demand. This homogeneous environment is maintained by proprietary software that continually monitors systems for binary modifications.

The location and status of all equipment within Google's data centers is tracked from acquisition to installation to retirement to destruction, via bar codes and asset tags. Google hard drives leverage technologies like full disk encryption (FDE) and drive locking, to protect data at rest. When a hard drive is retired, authorized individuals verify that the disk is erased by writing zeros to the drive and performing a multiple-step verification process to ensure the drive contains no data. If the drive cannot be erased for any reason, it is stored securely until it can be physically destroyed. Physical destruction of disks is a multistage process beginning with a crusher that deforms the drive, followed by a shredder that breaks the drive into small pieces, which are then recycled at a secure facility.

Google's Network

Google's IP data network consists of Google-owned fiber, public fiber, and undersea cables. This allows us to deliver highly available and low latency services. Industry-standard firewalls and access control lists (ACLs) are used to enforce network segregation. All traffic is routed through custom Google Front End (GFE) servers to detect and stop malicious requests and Distributed Denial of Service (DDoS) attacks. Additionally, GFE servers are only allowed to communicate with a controlled list of servers internally; this "default deny" configuration prevents GFE servers from accessing unintended resources. Logs are routinely examined to reveal any exploitation of programming errors, and access to networked devices is restricted to authorized personnel.

Efforts to Limit Latency and Maximize Availability

Google's network as a whole, as well its individual components, is highly redundant: server design, data storage, network and Internet connectivity, and software services are all built for redundancy. This "redundancy of everything" includes the handling of errors by design and creates a solution that is not dependent on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions on global products such as natural disasters and local outages. In the event of hardware, software, or network failure, platform services and control planes are automatically and instantly shifted from one facility to another so that platform services can continue without interruption. Google's highly redundant infrastructure also helps customers protect themselves from data loss. By way of example, Google's highly redundant design allows Google to achieve a Gmail uptime of approximately 99.99%, with no scheduled downtime.

3.9 Typical Interference Avoidance Use-Case Scenarios

The following discussion provides examples of how Google's SAS processes requests for authorization. It includes a detailed discussion of the SAS's method for computing interference potential. Should the Commission further clarify specific protection criteria for certain kinds of services (e.g., Part 90 users), Google will update its submission to account for any additional guidance. We first discuss aspects of the processing methodology common to all cases and then address how the methodology accommodates communications to and from other SASs.

3.9.1 Aspects of Interference Protection Common to All Use Cases

Google's SAS predicts potential interference by calculating the aggregate power spectral density of all emissions in the 3.5 GHz band at the location of a protected receiver. It also considers the propagation of emissions in the 50 MHz above and below the band to determine the effect of any adjacent channel blocking. PSD is measured in terms of power per "spectrum bin,"[83] or as the ratio of gain or loss through one of the components or paths.

In order to characterize PSD at the receiver, Google's SAS follows these steps:

1. Characterizes the energy being emitted by the transmitter.
2. Applies a path loss model to those transmissions, thereby calculating the strength and pattern of the emission at the receiver.
3. Uses information about the receiver to calculate the impact on the receiver, assuming there is no filter on the receiver.
4. Takes into account the impact of receiver filtering.

This results in a value representing received PSD at the receiver's low-noise amplifier. The flowchart provides a graphical depiction of these steps.

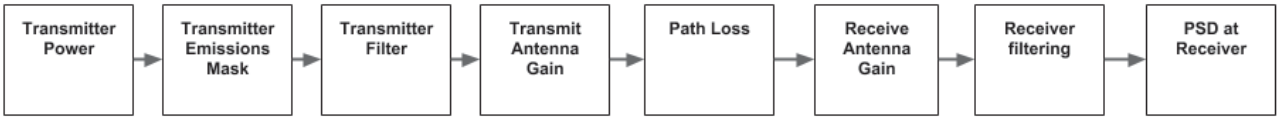

Figure 9: Flowchart Depiction of PSD Calculation

Below, Google provides an example highlighting these steps in detail. In this example, we use a 10 MHz bandwidth LTE transmitter as the potential interferor and an FSS earth station as the potentially affected receiver.

3.9.1.1 Characterizing the Transmitter

In the first step, Google relies on a number of inputs to characterize CBSD transmissions.

[83] The term "spectrum bin" refers to a set of frequencies (e.g., the 10 MHz between 3550 and 3560 MHz).

Mask characteristics

In calculating aggregate interference, Google's SAS characterizes emitters by their in-channel and OOBE masks. A mask consists of a range of frequencies, measured from the signal center, and the maximum power density levels at specified deviations from the center frequency.

Google's SAS can accommodate two types of masks—measured and regulatory threshold. Google's SAS will use the measured mask if available; this option of using actual performance levels will incentivize the industry to achieve performance levels beyond the minimum. If no measured mask is available, it will use the minimum performance standards adopted in Commission regulations, with which all Part 96 equipment must comply. Manufacturers can choose to provide information regarding measured device emissions or compliance with industry standards directly to Google, via the Part 96 Device Library interface.[84] If manufacturers provide measured emissions, such measurements should be substantiated by a test report submitted to the Commission by an FCC-approved test laboratory. The manufacturer should retain copies of relevant test reports and be able to furnish them on request.

Mask Type	Description
Measured	Because the manufactured device must equal or exceed regulatory requirements and is likely to meet or exceed industry specifications, measured data typically should reflect higher levels of performance.
Regulatory Thresholds	These standards are used as a default value used in the absence of vendor or certification data on the device.

Table 8: Types of Masks Accepted by Google's SAS

For all examples in this section, we use the CBRS OOBE limits established in 47 C.F.R. § 96.41(e):

Frequency Offset from CBRS Channel Edge (MHz)	OOBE Limits (dBm/MHz)
0 - 10	-13
> 10	-25
Below 3530 or above 3720	-40

Table 9: Part 96 OOBE Limits

The following plot shows the conducted emission levels for a CBSD transmitting with a center frequency of 3650 MHz using a 10 MHz emission bandwidth, transmitting with 30 dBm EIRP using a 6 dBi gain antenna. The measurement bandwidth is 1 kHz (a value chosen to improve the computational accuracy of the subsequent analysis). In this case, the values in table 9 are reduced by 30 dB to account for the difference in measurement bandwidth—i.e., 1

[84] *See* section 2.5.2, *supra*.

kHz rather than 1 MHz. The in-channel conducted emission is limited to 24 dBm/10 MHz (=30 dBm/10 MHz radiated PSD), reduced by 40 dB (=10log[10 MHz/1 kHz])to account for the 1 kHz measurement bandwidth, therefore the in-channel power spectral density is 24 dBm/10 MHz - 40 dB = -16 dBm/kHz.

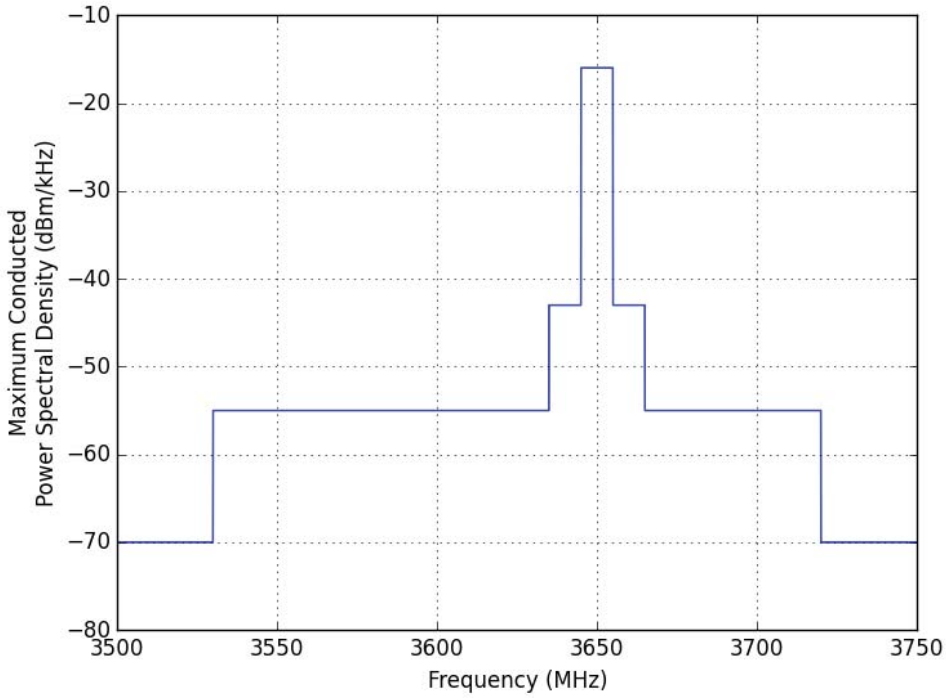

Figure 10: Graphical Representation of CBSD Emission Mask

Filter Characteristics

Google's SAS applies the effect of any applicable transmit filters to the OOBE mask. Transmit filters, however, may not be present in all CBSDs, or vendors may not break out their performance individually. Google's SAS thus considers four general cases:

Filter Type	**Treatment**
No Separate Filter Identified	No adjustment is made to the PSD implied by mask.
Fixed Filter	The filter PSD is independent of f_c (i.e., the center frequency). A single PSD will be used regardless of the frequency.
Selectable Filter	A number of individual filters are provided, each with a unique PSD. Google's SAS assumes that the lowest-loss filter is used.
Tunable Filter	A tunable filter will have its PSD passband centered on f_c. If separately provided, Google's SAS takes shaping information provided by the filter bandpass specification into account.

Table 10: Treatment of Various Filter Types

In sum, when a selectable filter or a tunable filter is used, Google's SAS takes the effect of those filters into account when calculating the PSD of the transmitting signal. An example of a transmit filter is shown in figure 11.

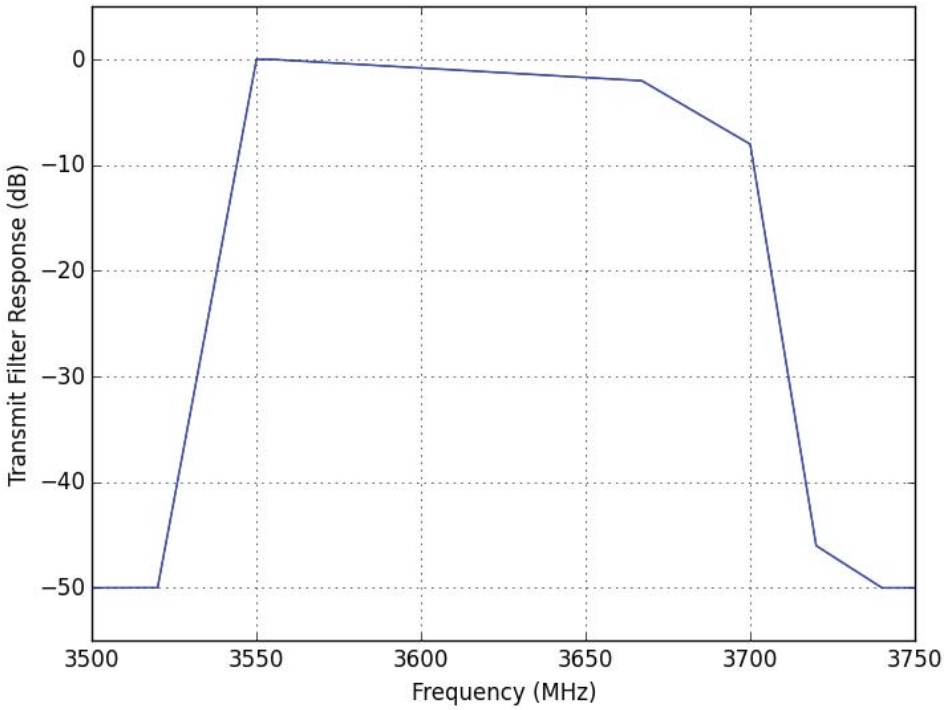

Figure 11: Example Transmit Filter Response

Transmit antenna characteristics

Transmit antenna gain or loss varies in both frequency and angle to the boresight (or other reference point) of the antenna. Google's SAS addresses pattern and frequency separately. A spatial model shows the azimuthal pattern, and a frequency PSD model, or spectral model, shows the impact across the operating band.

Spatial Model

An antenna's spatial model may be described using an equation or as a set of piecewise points. However, unless the antenna is either fixed, or has a limited range of pointing angles, the SAS assumes that the antenna will be pointed at a potential victim of interference with its maximum gain. In such simple cases, no spatial pattern is relevant. The CBSD antenna used in this example is assumed to be omnidirectional.

A sample of antenna types and how they are treated by the SAS is shown below. For completeness, this table includes antenna types that may be present only in receivers, as the analysis of antenna gain for transmitters and receivers is very similar.

Antenna Type	Model	Gain Assumption
Generally Omnidirectional	Assume constant gain in all directions, in the absence of any fixed pointing information.	= max($G_{spatial}(\Theta)$)
Rotating or Agile	Assume antenna will sweep to any possible angle, therefore, assume maximum gain in any direction.	= max($G_{spatial}(\Theta)$)
Fixed Directional	Displace the axis to reflect the actual physical direction, if known. If not known, treat as rotating.	= $G_{spatial}(\Theta)$, or max($G_{spatial}(\Theta)$)

Limited Field of View	The antenna can only slew through a set of angles β from reference angle. Assume the pattern is symmetric around the boresight direction. The antenna is treated as having two regions, with the gain used being the highest in each region.	*if* $\Theta \leq \beta$, then
		= max($G_{spatial}(0...\beta)$)
		else
		= max($G_{spatial}(\beta...\pi)$)

Elevated Directional	Reinterpret the antenna gain equation to reflect off axis operation, and then process according to this table. The term ($sum_{3D}(\Theta + \alpha)$) reflects the 3D angular sum of the pointing angle (Θ) and the elevation angle (α).	= $G_{spatial}(sum_{3D}(\Theta + \alpha))$

Table 11: Treatment of Various Antenna Types

Transmit Antenna Spectral Model

An antenna's spectral model exhibits the antenna's gain across a range of frequencies. This information will generally be available as piecewise points across the limited range of frequencies for which it was originally intended for operation. If no such information is available, Google's SAS assumes the antenna has a 0 dB impact across all frequencies. The SAS will compute the energy loss from the transmitter to each receiver across the entire set of frequencies being managed by the SAS, or adjacent to those frequencies. The gain of an example CBSD antenna as a function of frequency is shown below.

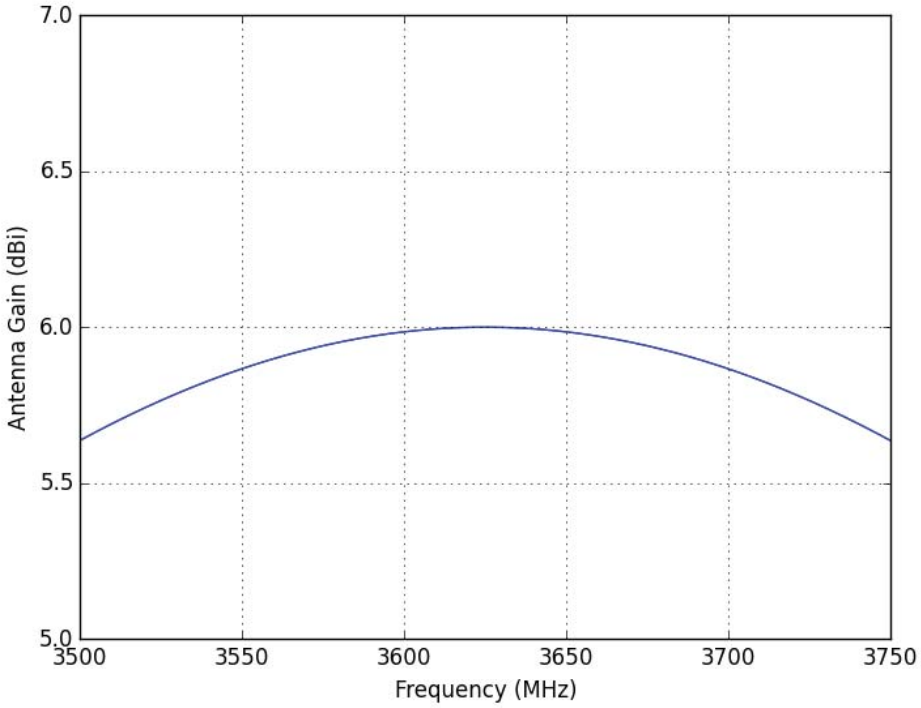

Figure 12: Antenna Gain v. Frequency of Example CBSD Antenna

The combined impact of all of these features of the transmitting device—mask characteristics, filter characteristics, and antenna characteristics—is shown below for the preceding illustrative values.

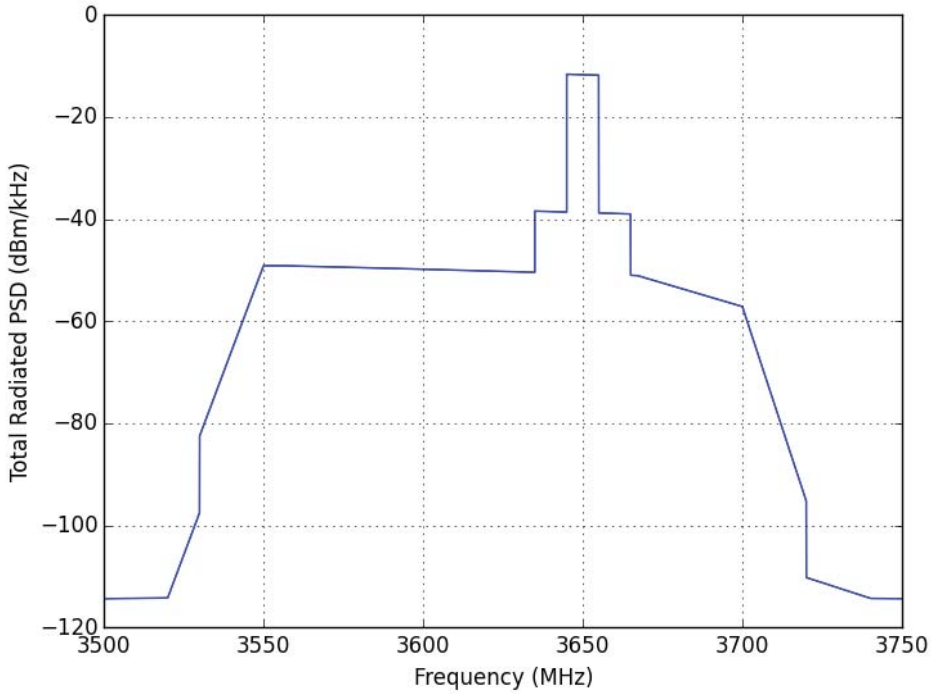

Figure 13: Net Power Spectral Density of CBSD after taking into Account Frequency-Dependent Conducted Emissions, Transmit Filter, and Antenna Gain

3.9.1.2 Applying Path Loss

In the second step of determining PSD at the receiver, the SAS applies a path loss model to the transmissions, thereby calculating the strength and pattern of the emission at the receiver. The approach taken to propagation modeling is set forth above in section 2.6. Applying path loss generates a PSD in the vicinity of the receiver. A simple case using free space path loss is shown below; Google's SAS will employ a more accurate and refined model, subject to industry consensus and regulatory approval. Actual propagation loss is generally observed to be much greater than free space loss, even over short distances.

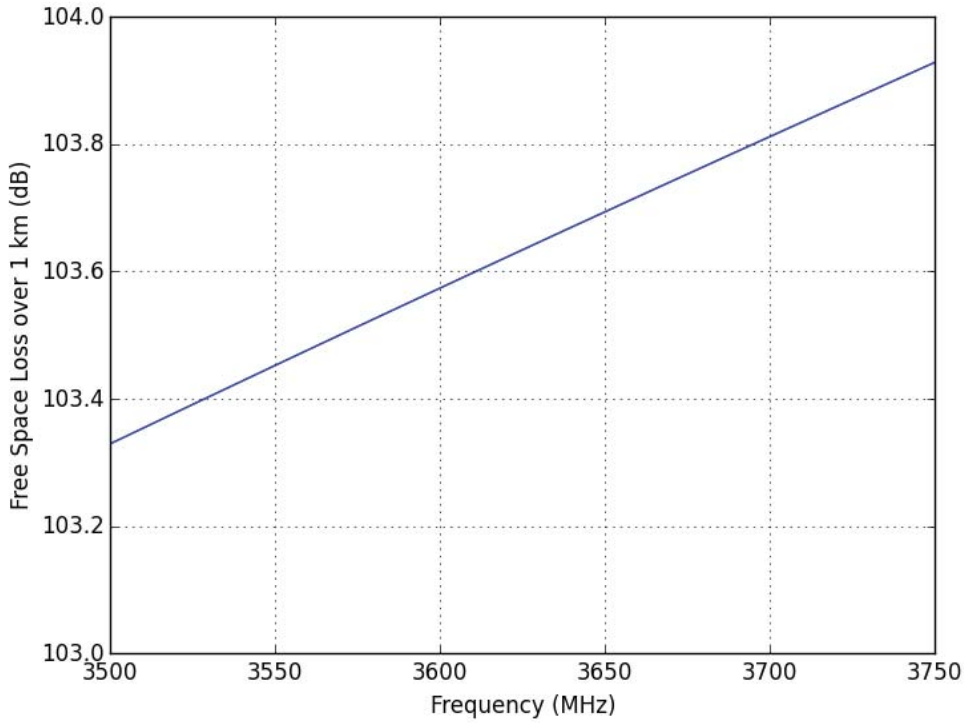

Figure 14: Free Space Path Loss over 1 km in the 3.5 GHz Band

3.9.1.3 Characterizing Impact at the Receiver

In the third step of characterizing PSD at the receiver, the SAS uses information about the receiving antenna gain pattern to calculate the received power at the antenna output.

Antenna Gain

The SAS first takes into account the impact of the receive antenna. Here, again, impacts are separated into spatial gain effects and frequency effects. Types of gain include those shown in connection with transmit antenna characteristics. Below, we illustrate the treatment of a C-Band FSS dish.

Receive Spatial Gain

In the example below, we depict a worst case of a C-band dish that is pointed at the lowest elevation angle found in the United States, 5.1 degrees above the horizon. Even this low elevation keeps the secondary users somewhat out of the main beam, which itself is much smaller than 5 degrees. We assume for the purpose of this example that the dish is in the far northeast (Maine, near 46°N 69°W) and looking at the AMC-8 satellite, which is at 139 degrees west longitude. The SAS uses this information to compute the azimuth of the antenna 255.3 degrees true. For the purpose of this example, we will use the off-axis gain of the antenna in the direction of the horizon as specified in Appendix A of the *Second Report and Order*.[85] However, 47 C.F.R § 96.17(d)(1)(iii) requires satellite operators to register their actual azimuth and

[85] *See Second Report and Order*, Appendix A, § 96.17 (referring to 47 C.F.R. § 25.209(a)(4)).

elevation gain patterns, and Google's SAS will use these actual patterns for its calculations, provided they conform to (or improve upon) Commission' default pattern.[86] Note that the maximum gain of the FSS dish (over 30 dB) is never achieved toward a terrestrial emitter, as even an emitter directly along the antenna's pointing azimuth is still more than 5 degrees off of the main lobe due to the antenna's upward-pointing elevation.

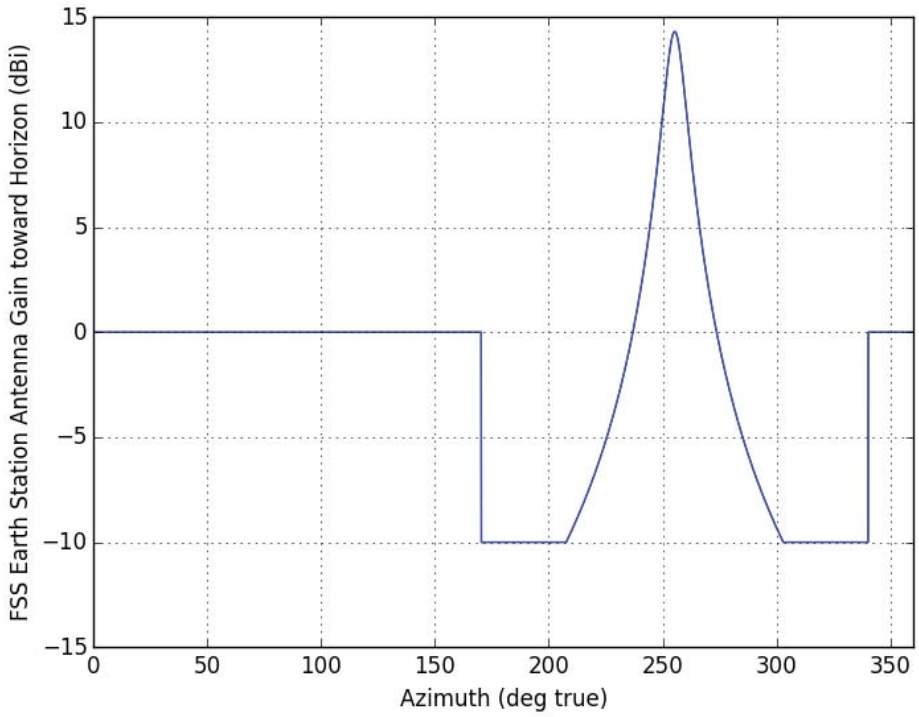

Figure 15: Horizon Gain of FSS Dish with Low (5.1 degree) Elevation Angle
Pattern is based on antenna pattern formula specified in the Commission's Second Report and Order.

The same information is depicted in a polar plot format below.

[86] *See id*.

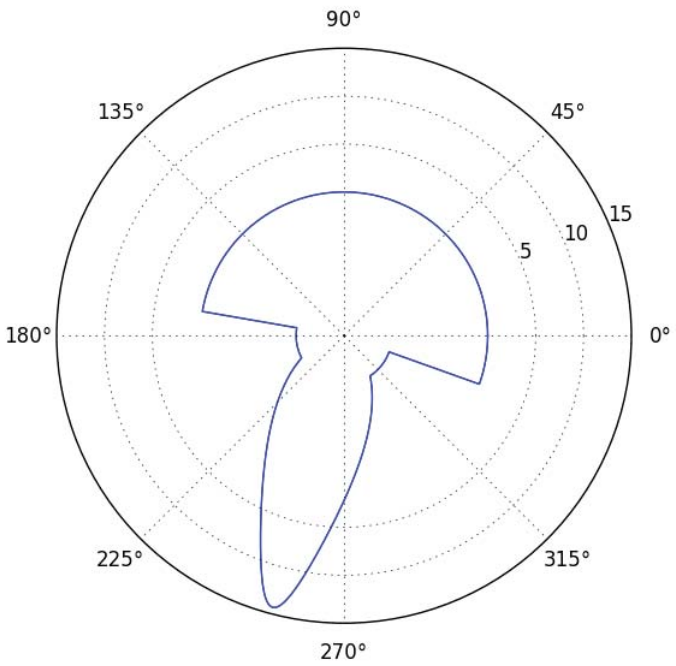

Figure 16: Polar Plot of Figure 15

The low-elevation antenna pointing conditions in the figures immediately above are rare in the United States. A more typical pattern, looking at the same AMC-8 satellite from a central location (in Tennessee, near 35°N 90°N) is shown below. The higher elevation angle of approximately 25 degrees results in almost 20 dB less signal received, limiting CBSD/C-band coexistence concerns.

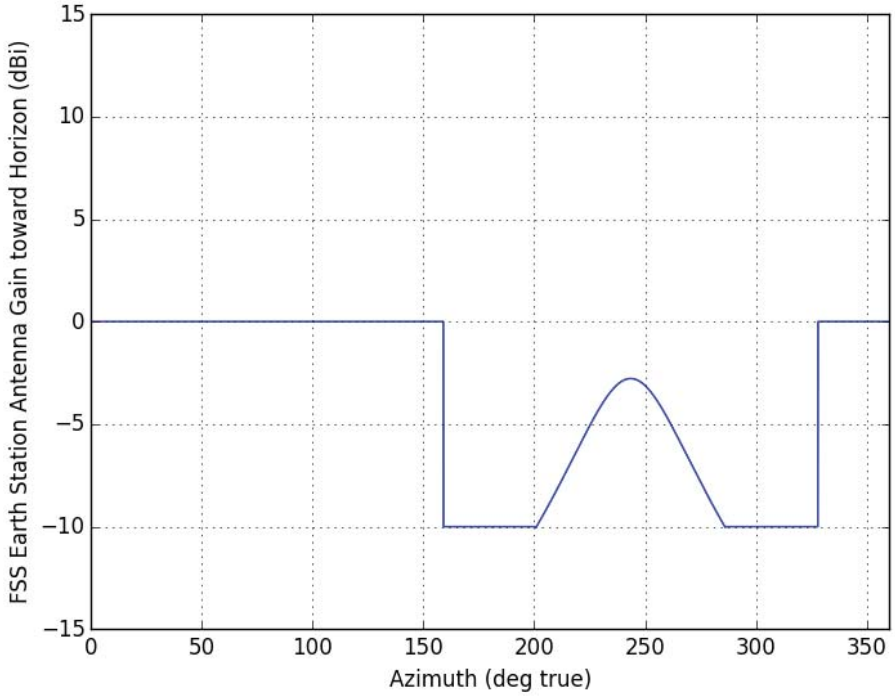

Figure 17: Horizon Gain of an FSS Dish with a Higher Pointing Elevation
This pattern is more typical of dishes within the central United States, as compared with Figures 15 and 16.

Receive Frequency Model

The SAS handles receive frequency response in the same way it handles transmit frequency response.[87]

3.9.1.4 Incorporating the Effect of a Receive Filter

In the final step of determining PSD at the receiver, the SAS takes into account the impact of any receiver filtering. Going forward, Google will assume the receive filter characteristics specified in FCC Rule 96.17 as the default. This filter is plotted below for an FSS earth station operating in the adjacent band (3700 MHz and above). For in-band earth stations, the filter fall-off from the passband is the same, but the passband will be below 3700 MHz and must be registered with the FCC by the FSS earth station operator.

[87] *See* section 3.9.1.1, supra.

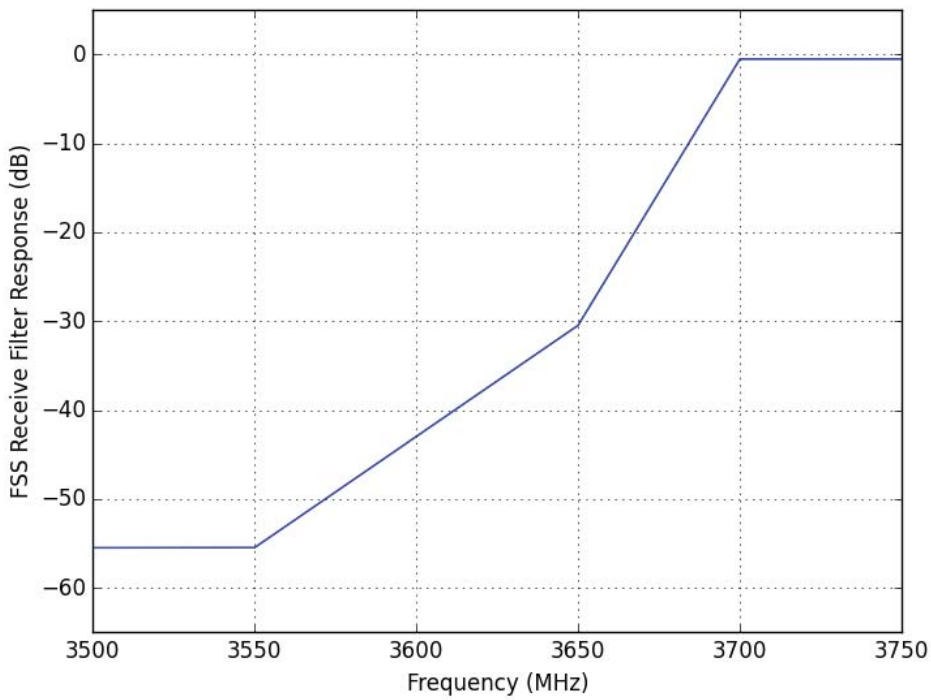

Figure 18: FSS Receive Filter Response for an Adjacent-Band FSS Receiver

Finally, to calculate the impact of single CBSD on an FSS earth station, the SAS combines all of the frequency-dependent and geometrical terms described above to compute the net CBSD power spectral density as received by the FSS system:

Total Received Signal PSD(f) = Tx PSD(f) - Tx Filter(f) + Tx Ant Gain(f,θ) - Path Loss(f,d) + Rx Ant Gain(ø) - Rx Filter(f)

where f is frequency, θ is the angle off the transmitter antenna boresight toward the FSS earth station from the CBSD, d is the distance from the CBSD to the earth station, and ø is the angle off the FSS dish boresight toward the CBSD. This net PSD is shown in the figure below for the example of the CBSD being located within the 0 dBi backlobe of the FSS dish:

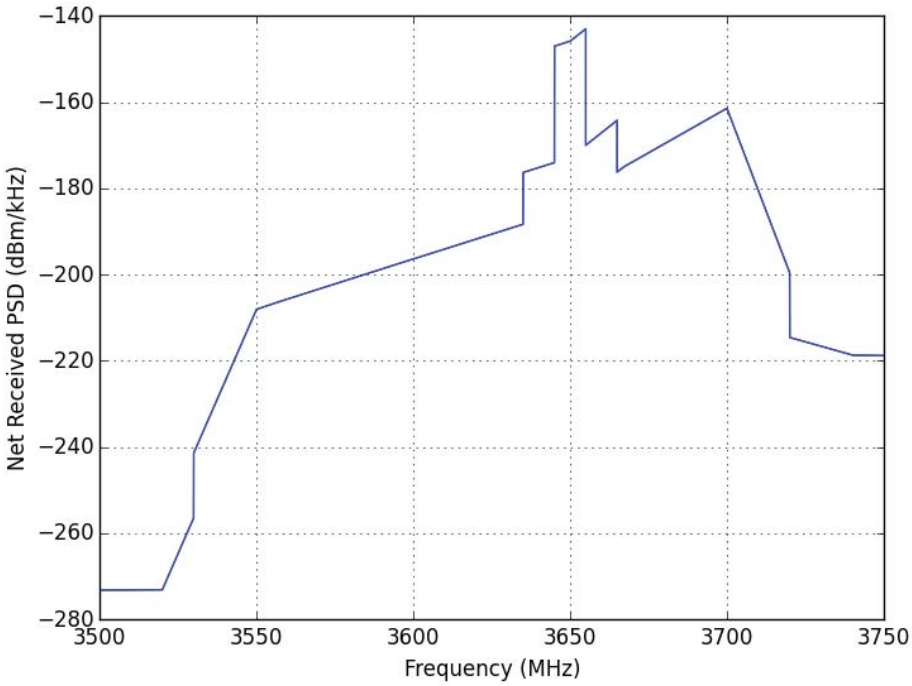

Figure 19: Net Signal PSD at Receiver, Including All Transmitter, Receiver, and Propagation Effects

3.9.1.5 Calculating Passband and Blocking Interference Impact

Passband Interference

The passband RF PSD is the PSD as received within the passband of the FSS system. In the example of figure 19, that corresponds to the PSD above 3700 MHz, because this FSS system is an adjacent-band system that utilizes frequencies above 3700 MHz. The FCC rules (47 C.F.R. § 96.17) limit the passband emissions to -129 dBm when measured in a 1 MHz bandwidth. By integration of the PSD in figure 19 over the range 3700-3701 MHz (where the passband interference is a maximum), we find that the worst-case passband interference level is -132 dBm/MHz. Therefore a single CBSD located within direct line-of-sight of the satellite dish, at a distance of 1 km, meets the FSS interference objective for passband interference at the very edge of the band, by more than 3 dB. Moving farther away in frequency from the band edge, the integrated passband power spectral density, integrated on a per MHz basis, decreases rapidly, as shown in figure 20.

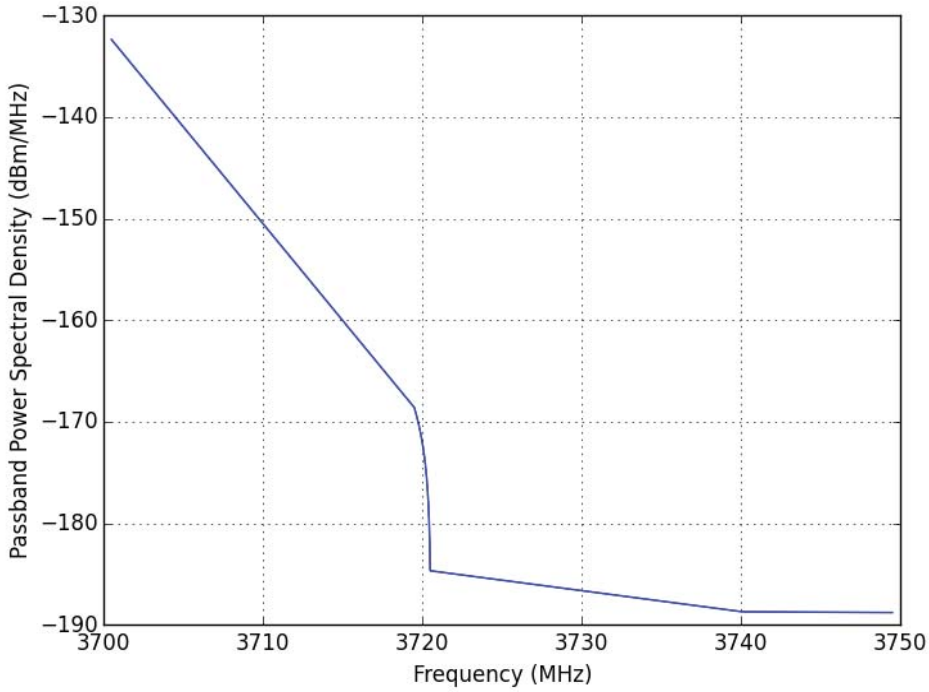

Figure 20: Passband RF Power Spectral Density in Units of dBm/MHz for the Example Presented in this Section

Blocking Interference

The blocking interference level is the total RF energy as received by the FSS dish, after filtering. It is, essentially, the integral over all frequencies of the power spectral density shown in figure 19. In reality, the integral can be taken over the range 3500-3750 MHz that is shown here, because outside this range, the signal is extremely weak (near or below -220 dBm/kHz, which is some 76 dB or more below ambient thermal noise). Google's SAS integrates the PSD shown in figure 19 to calculate a blocking signal level of -105.1 dBm, which is more than 45 dB below the maximum blocking level of -60 dBm allowed under FCC Rule 96.17.

3.9.1.6 Accounting for Aggregation

The four-step process set forth above is repeated for all CBSDs that could impact a victim receiver, and those calculations are adjusted as CBSD nodes are granted authorization or as authorizations are cancelled.

3.9.1.7 Admission Control

At the completion of this process, the SAS has the information needed to determine if entry of a device will interfere with any protected entity. The table lists the types of protected users, how aggregation is treated, and the criteria used to determine whether harmful interference is predicted to occur.

Protected User	Treatment of Aggregation	Protection Criteria
In-Band FSS	Protection criteria applied after aggregation is calculated	Aggregate passband RF power and blocking power are determined using the methodology set forth in section 3.3.
Out-of-Band TT&C FSS (impact of CBSD emissions above 3.7 GHz)	Protection criteria applied after aggregation is calculated	Aggregate passband RF power and blocking power are determined using the methodology set forth in section 3.3.
Part 90 Operations	Protection criteria applied after aggregation is calculated	TBD based on further Commission action.
Exclusion Zone	N/A	SAS asks whether a node is within an exclusion zone. If yes, the node is not granted an authorization.
Protection Zone	N/A	SAS asks whether a node is within a restricted area activated due to the presence of federal activity. If yes, the node is not granted an authorization.
GAA entering on a channel that may have PAL activity	Aggregation is taken into account only in the second step of the process	Step 1: SAS asks whether node seeks to operate on a PAL channel within the service area of an active PAL grant. If so, the node is not granted authorization. Step 2: Authorization is permitted only if the average power level does not exceed an average (rms) power level of -80 dBm in any direction when integrated over a 10 megahertz reference bandwidth, with the measurement antenna placed at a height of 1.5 meters above ground level, unless the affected PAL licensee(s) agree to an alternative limit and communicate that to the SAS.[88]

Table 12: Protection Criteria and Methodology of Google's SAS

3.9.1.8 Coexistence Among GAA Users

The WinnForum is developing a community-accepted standard for maximizing coexistence among GAA users. In the interim, Google's SAS will provide optional coexistence support through an inquiry function that provides worst-case estimates of coexistence challenges between GAA users. Devices can use the data to select frequencies, or can supplement the SAS-provided data with local sensing in selecting a channel for use. This hybrid

[88] 47 C.F.R. § 96.41(d).

approach combines the flexibility and density optimization associated with sensing with the global awareness of the database approach.

Google's SAS will not mandate coexistence for GAA users. Many GAA deployments will be indoors, and traditional propagation models do not effectively address interior losses because detailed interior plan information is not widely available, and because scattering loss data is rarely incorporated into propagation models. Absent a more defined standard for coexistence, and better data to calculate interference potential, SAS-mandated coexistence is unlikely to be useful to GAA users.

3.9.2 Assignments Made By Multiple SASs

The WinnForum has established a SAS-to-SAS interface that enables near-real-time coordination among SAS operators.[89] Google will use that interface to communicate with other SASs. Near-real-time communication should be sufficient to ensure protection against harmful interference. Assume for the purposes of this example that one device is registered every 10 seconds. This rate corresponds to a nationwide deployment of 10 million devices over 3 years—making expanded use of the 3.5 GHz band a resounding success. The land mass of the United States is approximately 9.1 million square kilometers. Assuming a typical device has an impact area of 1 km^2, the probability of any one device impacting any other specific device is extremely low. The probability that two interfering devices will register within seconds of each other is vastly lower still. Thus, asynchronous coordination is extremely unlikely to cause interference events. At the same time, asynchronous coordination has significant benefits: it allows the the SAS ecosystem to support multiple competitors and withstand the failure of one or more of the operators, and thus reduces the need for government oversight.

Effective SAS-SAS coordination not only must be timely, but also must take into account all relevant information. As such, success of the SAS ecosystem depends on agreement between SAS operators to disclose all information elements affecting aggregation and interference protection, including all emission-related information, such as location coordinates and other critical operating characteristics.

Google's SAS treats registrations by other SAS operators identically to registrations made via direct request to Google's SAS. The records are imported and the analysis described previously is executed in order to update the aggregate emissions for protected nodes that might be impacted. That is, once a new node has been accepted from another SAS, it may impact future decisions by Google's SAS through elevation of the aggregate interference level.

3.10 Commission Access to Information Retained by the SAS

Google's SAS provides a Regulators' Console that enables authorized government personnel to inquire into content available within the SAS, define zones of interest for initiating query actions or protection exclusions (on a frequency or band basis), and view the status of any device registered with the SAS. Queries can be based on registration data, grant data, or physical location. In addition, suspension policies can be created for specific zones or for specific CBSDs. The Regulators' Console also provides multiple user privilege levels: for

[89] *See* Appendix D.1.

example, it can limit some users to read-only access while permitting other users more advanced functionality.

This graphical user interface provides the minimum functionality required by Part 96, as well as additional functionality to increase regulators' visibility into SAS content and maximize the effectiveness of government interactions.

4 ESC OPERATION

Google plans to construct and operate an ESC system as a component of its SAS. The primary purpose of the ESC is to facilitate coexistence of CBSDs with federal incumbent users.[90] The ESC system will achieve this objective by sensing the presence of an incumbent radar and alerting the SAS that a detection has been made.

4.1 ESC-to-SAS Communications Methods

4.1.1 ESC-to-SAS Interface Design

In the absence of an industry-standard ESC-to-SAS interface, Google will employ a proprietary interface to connect its ESC system to its SAS. However, Google expects that the interface will follow requirements to be agreed in the joint WinnForum ESC working group.[91] This functionality is described in more detail in section 3.6.3.

4.1.2 ESC and ESC-to-SAS Interface Protection

As set forth in section 3.1.2, the communication from ESC sensors to the cloud-based ESC decision system is secured by use of TLS, the standard form of securing such Internet-based communications. The closed nature of the ESC sensor network allows the cloud-based component to rely on a fixed set of known certificates identifying all valid ESC sensors. These certificates are checked for each communication to ensure that all communications are authenticated and secured bidirectionally.

For the communications from the ESC to the SAS, the Google system will use proprietary and secured communications protocols on internal networks. Not only are such communications secured from other groups and individuals making use of these internal private networks, but a wide array of countermeasures are deployed to protect the private network itself from intrusion from any third parties. Additional information regarding methods used to secure Google infrastructure, including both the SAS and the ESC, is set forth in section 3.8.

4.2 Sensing Methodology

4.2.1 Description of Previous ESC Development and Testing Outcomes

As noted in section 2.5.3, Google has been monitoring incumbent federal activity in the 3.5 GHz band for the last two years in the Norfolk/Virginia Beach, Virginia, area. This area has the highest concentration of U.S. Navy ships with incumbent radars of any location in the

---

[90] 47 CFR § 96.67(a).

[91] A number of WinnForum standards are in process, including documents that cover communications security requirements.

country, with nine of 19 ships with incumbent radars homeported in Norfolk. This monitoring has allowed Google to test and refine various hardware configurations and software algorithms for detecting radar activity, all within a busy operations area. Our radar detection system in Norfolk is a custom software implementation on a software-defined radio board with commercial off-the-shelf RF hardware. Our detection algorithms were trained using off-the-air recordings of incumbent radar activity obtained at the Navy's St. Inigoes, Maryland, research and development site. Long-term monitoring underway at the Norfolk ESC site has employed simultaneous ESC and spectrum analyzer data collection for consistency checks.

4.2.2 ESC Architecture and Sensor Hardware Design

A discussion of ESC architecture and sensor hardware design is provided in section 2.5.3. Reporting thresholds, sensor sensitivity, and sensor resiliency are also discussed in that section.

4.2.3 Signal Processing and Detection Algorithms

Google uses proprietary signal processing algorithms to detect federal incumbent activity, and is prepared to submit a redacted description of these algorithms to the FCC upon request.

All of our algorithms are implemented in software and can be upgraded at any time through the ESC controller, either to improve performance or to adapt to changes in incumbent systems.

4.2.4 Sensor and SAS Data Retention Protections

The ESC sensors are stateless; they do not retain session information across multiple requests. They merely inform the ESC decision element when a signal is detected. Data retention is implemented in the decision element. Google expects that its ESC and SAS will comply with all data retention protection requirements that are currently being derived within the WinnForum, in consultation with DoD. Moreover, as specified in 3.6.3, sensors provide only minimal information to the ESC decision engine, and therefore to the SAS. Section 3.8 describes methods to ensure the security of stored data.

4.3 Sensor-to-ESC Communications

Individual sensors will communicate with the ESC using TLS. The sensors will communicate data elements consistent with operational security standards being developed in the WinnForum, in conjunction with the DoD. The sensors will maintain regular heartbeat communications with the ESC decision engine to confirm their ability to inform the decision engine of incumbent activity in a timely manner. The heartbeat rate can be varied to match any maximum notification timescale adopted now or in the future. To maximize physical security, sensors and antennas will be mounted in areas not readily accessible by the general public, using siting considerations similar to those employed by cellular carriers and other commercial wireless operators. The core sensor components (SDR board, microprocessor, and backhaul hardware) will be mounted inside locked weatherproof enclosures.