Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Wireless Telecommunications Bureau and	)	GN Docket No. 15-319
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	)	
	)	

PROPOSAL BY FEDERATED WIRELESS, INC. TO SERVE AS A SPECTRUM ACCESS SYSTEM ADMINISTRATOR AND ENVIRONMENTAL SENSING CAPABILITY OPERATOR IN THE 3550 – 3700 MHZ BAND

Kurt Schaubach
Chief Technology Officer
Federated Wireless, Inc.
4301 North Fairfax Drive
Suite 310
Arlington, VA 22203

May 16, 2016

TABLE OF CONTENTS

Page

PART I: OVERVIEW, EXPERTISE, AND FINANCIAL CAPABILITIES 5

A. OVERVIEW OF SAS AND ESC OPERATIONS 5

1. Scope of Functions Performed by the SAS and ESC 6

2. SAS and ESC Architecture 8

3. Models and Assumptions 15

4. Software and Firmware Updates and Addressing Security Vulnerabilities 18

B. ABOUT FEDERATED WIRELESS 19

1. Technical Expertise 21

2. Financial Capabilities, Business Structure, and Fees 24

C. COMPLIANCE 30

1. Designated Party Responsible for Compliance 30

2. Qualifications of Key Personnel 30

3. Cooperation with the Commission to Ensure Compliance with and Enforcement of Its Rules 31

4. Information Gathering and Retention 31

5. Response to Claim of Inaccuracies 32

6. Response to Claim of Interference 32

7. Commitment to SAS-SAS Coordination and Efficient Spectrum Use 32

8. Commitment to Secondary Markets and Spectrum Manager Lease Agreements 33

9. Affirmation of SAS Operations 33

10. No Anti-Competitive or Discriminatory Practices 33

11. Compliance with Statutory Obligations 34

12. Commitment to User Data Privacy 34

13. Conveyance of Service 35

PART II: SAS ADMINISTRATOR PROPOSAL 36

A. DIVISION OF FUNCTIONS 37

B. SAS DATA MANAGEMENT AND ACCESS POLICIES 37

1. General Data Retention Policies 38

2. Correcting Data 39
3. CBSD Data 39
4. PAL Data 42
5. SAS Data 42
6. ESC Data 43
7. FCC-Maintained Data 43
8. Exclusion Zone and Protection Zone 44
9. Federal Data and Transmissions 45
10. Commission Personnel Access 46
11. Public Data Availability 47

C. SAS INTERFACES 47
1. CBSD / CBSD-Proxy Interface 48
2. Verification of CBSD Communication 49
3. SAS-SAS Interface 50
4. ESC Interface 51
5. Government Database Interface 52
6. SAS Management Interface (Administrative) 52
7. Third Party Access Interface 53
8. Informing Incumbent Interface 53
9. Commission Enforcement Instructions 54
10. Connectivity to Military or Other Sensitive Federal Databases 54

D. SPECTRUM AVAILABILITY AND PROTECTIONS 55
1. Overview of Methods Employed 57
2. Determination of Nominal Maximum CBSD Power Levels 58
3. Protection of Federal Incumbent Users 59
4. Federated Wireless Solution 61
5. Protection of Existing FSS Earth Stations 64
6. Enforcing Current and Future International Agreements 66
7. Protection of Existing Operators in the 3650-3700 MHz Band 67
8. Protection of PAL Operations 67
9. Confirmation of Spectrum Availability 72
10. Channels in Use 74
11. PAL Channels 75

12. Management of GAA Spectrum 76
13. ESC-Determined Channel Availability 77
14. GAA Access to PAL Channels 79
15. Interference Resolution 81
16. Confirmation of Protection 82
17. Coordination Among GAA Users 83

E. SAS-SAS COORDINATION 88
1. WINNF SAS-SAS Protocol 91
2. Maintenance of and Public Access to CBSD Registration Data 94
3. Responding to ESC Events 94
4. Coordinating PAL Frequency Assignments 95
5. Aggregate Interference Calculations 96
6. Coordinating GAA Uses 97
7. Coordinating Informing Authority Events 98
8. Responding to Interference Reports and Requests for Additional Protection 98
9. Resolving Error Reports 99
10. Summary of Information Sharing in SAS-SAS Coordination 99

F. SAS SECURITY 101
1. Database Security and Preventing Unauthorized Access 103
2. SAS-CBSD Communications Security 105
3. SAS-SAS Communications Security 105
4. SAS-ESC Communications Security 106
5. FCC ID Verification 107
6. Additional Security Technologies and Procedures 108
7. Addressing Other Security Threats 109

G. DYNAMIC USE-CASE SCENARIOS 109
1. Aggregate Interference Calculation for Protecting Incumbent Users and PAL Protection Areas 109
2. Coordinated Protection of a PAL Protection Area When Allowing GAA Access to PAL Spectrum 113
3. Managing and Assigning Spectrum Resources to a GAA While Ensuring that Geographically and Spectrally Adjacent Operations Are Coordinated Consistent with the Commission's Rules 116

PART III: ESC OPERATOR PROPOSAL 120
A. MINIMUM PROPOSAL REQUIREMENTS AND STATEMENT OF COMPLIANCE 120
B. FEDERATED WIRELESS IS A NON-GOVERNMENTAL ENTITY 121
C. DETAILED ESC TECHNICAL PROPOSAL 121
D. ESC OVERVIEW 122
1. ESC Architecture 123
2. Detection and Protection of Federal Incumbent Users 125
3. SAS Connectivity 127
4. ESC, Sensor, and SAS Cybersecurity 127
5. Availability to Respond to Requests from Authorized Commission Personnel 129
6. Federal System Information Safeguards and Protection 129
7. Sensor Deployment Locations and Sensor Network Operations 130
E. ESC-SAS COMMUNICATIONS 131
1. ESC-SAS Message Protocol 131
2. Communications Security 131
F. SENSING METHODOLOGY 132
1. Sensor Types 132
2. Sensing Method 133
3. Sensor Sensitivity 134
4. Sensor Resiliency to Front-End Saturation and Burn-Out 134
G. SENSOR COMMUNICATIONS 134
1. Sensor Communication Methods 134
2. Verification of Sensor Operation and Communications 135
CONCLUSION 137
PROPOSAL COMPLIANCE 138

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Wireless Telecommunications Bureau and	)	GN Docket No. 15-319
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	)	
	)	

PROPOSAL BY FEDERATED WIRELESS, INC. TO SERVE AS A SPECTRUM ACCESS SYSTEM ADMINISTRATOR AND ENVIRONMENTAL SENSING CAPABILITY OPERATOR IN THE 3550 – 3700 MHZ BAND

Federated Wireless, Inc. ("Federated Wireless"), an innovator in the field of new spectrum management tools, such as spectrum sensing, cloud computing, dynamic spectrum database technologies, cognitive radio and small cell technology, hereby submits this application in response to the request made by the Federal Communications Commission ("Commission" or "FCC") for proposals from prospective Spectrum Access System ("SAS") Administrators and Environmental Sensing Capability ("ESC") operators in the above-captioned proceeding.[1]

INTRODUCTION

Federated Wireless is pleased to offer its proposal to serve as a SAS Administrator and ESC operator in the Citizens Broadband Radio Service ("CBRS"). Federated Wireless commends the Commission both for its leadership in adopting the innovative sharing framework governing the CBRS, and for moving expeditiously to enable consumer access to the services that will be offered in the band.

---

[1] *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*, GN Docket No. 15-319, Public Notice, DA 15-1426 (WTB/OET 2015) ("Application Procedures PN").

As demonstrated by the intense—and growing—industry interest in utilizing CBRS spectrum, the market for this band is already robust. Federated Wireless actively works with the many, varied stakeholders with an interest in 3.5 GHz spectrum, including the Commission, the Department of Defense ("DoD"), the National Telecommunications and Information Administration ("NTIA"), the National Institute of Standards and Technology ("NIST"), the National Advanced Spectrum and Communications Test Network ("NASCTN"), the Defense Advanced Research Projects Agency ("DARPA") in connection with its Shared Spectrum Access for Radar and Communications ("SSPARC") program, wireless operators, Fixed Satellite Service ("FSS") earth station operators, and Grandfathered Wireless Broadband Licensees ("GWBLs").

Through cross-industry stakeholder efforts such as those unfolding in the Wireless Innovation Forum ("WINNF"), in which Federated Wireless is an active participant and co-chairs the Spectrum Sharing Committee ("SSC"), industry requirements, standards and protocols for CBRS operations have developed and continue to rapidly develop. As launch of the CBRS nears and as uses in the band evolve, Federated Wireless will continue to work with all stakeholders, the government agencies referenced above, and the Commission to ensure the CBRS is a success.

In this proposal, Federated Wireless details its proposed implementation of SAS and ESC technology in accordance with the requirements of Part 96 of the Commission's rules. By offering both of these key technologies for the CBRS in a fully integrated manner, Federated Wireless can best guarantee the efficiency and security of its solutions, as well as seamless interoperability in the SAS-ESC ecosystem. The Federated Wireless SAS and ESC design will protect both federal and non-federal incumbents from interference while also providing access to much-needed, valuable spectrum for commercial services. The SAS and ESC design and implementation are described in detail in this proposal as well as the manner in which Federated Wireless will act as a SAS Administrator and ESC operator. To the extent this proposal contains commercially sensitive,

proprietary information, or information that implicates operations security concerns, such information has been redacted from the publicly filed version of this proposal and submitted to the Commission under confidential seal, in accordance with section 0.459 of the Commission's rules.[2]

Federated Wireless acknowledges that there are outstanding issues related to the CBRS, such as the implementation of the recently released Order on Reconsideration and Second Report and Order and final protections for Grandfathered Broadband Wireless Licensees, and that industry standards remain under development in the WINNF. Federated Wireless also believes it is vitally important for the CBRS community to collaborate to develop industry-standard protections to ensure the privacy of CBRS user data. CBRS users must be assured that their valuable information will be handled appropriately, competitively sensitive information will not be disclosed, and end user privacy will be maintained. SAS Administrators must also adopt protocols to ensure that the information they share with other Administrators is only used for the purposes of managing CBRS spectrum. How data is handled by SAS Administrators, and the effects of those policies on CBRS users' trust in providing their valuable data to the SAS, is as important as what information is shared.

As such, this application details Federated Wireless's current proposed implementation of SAS and ESC technology.[3] As the Commission noted in the Application Procedures PN, the SAS and ESC certification process is expected to be an iterative process, and Federated Wireless is committed to amending or supplementing this proposal as necessary, to reflect compliance with newly developed rules and standards or as a result of Commission requests. Federated Wireless looks forward to working with the Commission throughout the certification process, and affirms

---

[2] 47 C.F.R. § 0.459.

[3] This detailed application, notwithstanding evolving Part 96 rules and industry standards, demonstrates Federated Wireless' progress in SAS and ESC technologies and its readiness for the Commission to further assess and test its SAS and ESC.

that it will comply with all applicable rules, enforcement mechanisms, and procedures as they evolve in its capacity as a SAS Administrator and ESC operator.

PART I: OVERVIEW, EXPERTISE, AND FINANCIAL CAPABILITIES

As requested in the Application Procedures PN, Part I provides the following information related to the Federated Wireless SAS and ESC:

- A detailed description of the scope of the functions that the Federated Wireless SAS and ESC perform;
- A demonstration that Federated Wireless possesses sufficient technical expertise to operate an SAS and ESC, including the qualifications of key personnel who will be responsible for operating and maintaining the SAS and ESC;
- A demonstration that Federated Wireless is financially capable of operating an SAS and ESC for a five year term, including a description of the 'Federated Wireless' business structure, ownership information, and anticipated fee collection mechanisms;
- A description of how data will be securely communicated between the SAS and its associated ESC and how quickly and reliably these communications will be accomplished;
- Technical diagrams showing the architecture of the SAS and ESC, and a detailed description of how each function operates and how each function interacts with the other functions;
- A description of the propagation model and any other assumptions that Federated Wireless proposes to use to model operations and facilitate coordination in the 3.5 GHz Band;
- A description of the methods that Federated Wireless will use to update software and firmware and to expeditiously identify and address security vulnerabilities; and
- An affirmation that Federated Wireless will comply with all of the applicable rules, as well as applicable enforcement mechanisms and procedures, in its capacity as a SAS Administrator and ESC operator.

A. OVERVIEW OF SAS AND ESC OPERATIONS

This section provides an overview of the operation of the Federated Wireless SAS and ESC. Further details on the proposed SAS are provided in Part II, and on the proposed ESC in Part III.

1. Scope of Functions Performed by the SAS and ESC

(a) SAS Functions

The Federated Wireless SAS will provide nationwide service and implements all required functions of a SAS, including acting as a data repository and providing registration, channel availability calculations, and query services. The Federated Wireless SAS fully implements the SAS capabilities defined in Part 96, Subpart F, including:

- Enacting and enforcing all policies and procedures developed by the SAS Administrator pursuant to section 96.63;[4]
- Determining and providing to Citizens Broadband Radio Service Devices ("CBSDs") the permissible channels or frequencies at their location;
- Determining and providing to CBSDs the maximum permissible transmission power level at their location;
- Registering and authenticating the identification information and location of CBSDs;
- Retaining information on, and enforcing, Exclusion Zones and Protection Zones in accordance with sections 96.15 and 96.17;[5]
- Communicating with the Federated Wireless ESC to obtain information about federal Incumbent User transmissions and instructing CBSDs to move to another frequency range or cease transmissions when federal incumbent operations are detected;
- Ensuring that CBSDs operate in geographic areas and within the maximum power levels required to protect federal Incumbent Users from harmful interference, consistent with the requirements of sections 96.15 and 96.21;[6]
- Ensuring that CBSDs protect non-federal Incumbent Users from harmful interference, consistent with the requirements of sections 96.17 and 96.21[7]

---

[4] 47 C.F.R. § 96.63.

[5] *Id.* §§ 96.15, 96.17.

[6] *Id.* §§ 96.15, 96.21.

[7] *Id.* §§ 96.17, 96.21.

- Protecting Priority Access Licensees ("PALs") from interference caused by other PALs and from General Authorized Access ("GAA") users, including the calculation and enforcement of PAL Protection Areas, consistent with section 96.25;[8]

- Facilitating coordination between GAA users operating Category B CBSDs, consistent with section 96.35;[9]

- Resolving conflicting uses of the band while maintaining, to the extent feasible, a stable radio frequency environment;

- Ensuring secure and reliable transmission of information between the SAS and CBSDs;

- Protecting GWBLs consistent with sections 90.1307, 90.1338, and 96.21;[10]

- Implementing the terms of current and future international agreements as they relate to the CBRS; and

- Receiving reports of interference and requests for additional protection from Incumbent Access Users and promptly addressing interference issues.

(b) ESC Functions

The ESC proposed by Federated Wireless facilitates coexistence of CBRS users with federal Incumbent Users through signal sensing and does not rely on governmental agencies to affirmatively communicate information about the operations of incumbent radio systems. The Federated Wireless ESC fully implements the ESC capabilities defined in Part 96, Subpart G, including the following functions:

- Accurately detecting the presence of a signal from a federal system in the 3550-3650 MHz band using methodologies that have been developed in close coordination with the federal Incumbent Users to ensure that any CBSDs operating pursuant to ESC will not cause harmful interference to federal Incumbent Users;

- Communicating information about the presence of a signal from a federal Incumbent User system to the Federated Wireless SAS;[11]

---

[8] *Id.* § 96.25.

[9] *Id.* § 96.35.

[10] *Id.* §§ 90.1307, 90.1338, 96.21.

- Maintaining security of detected and communicated signal information;
- Complying with all Commission rules and guidelines governing the construction, operation, and approval of ESCs;
- Being available at all times to immediately respond to requests from authorized Commission personnel for any information collected or communicated by the ESC; and
- Operating without any connectivity to any military or other sensitive federal database or system and not storing, retaining, transmitting, or disclosing operational information on the movement or position of any federal system or any information that reveals other operational information of any federal system that is not required by Part 96 to effectively operate the ESC.

2. SAS and ESC Architecture

This section provides technical diagrams depicting the architecture of the Federated Wireless SAS and ESC and a detailed description of how each function operates and interacts with the other functions.

(a) System Architecture

The architecture of the Federated Wireless SAS and ESC is consistent with the WINNF SAS Notional CBRS Architecture, which contains the following components:

- ***CBSD***: *Citizens Broadband Radio Service Device*: Fixed or Portable Base stations or access points, or networks of such base stations or access points, that operate on a PAL or GAA basis in the CBRS consistent with Part 96. Does not include End User Devices ("EUDs"). For managed networks, it is likely that information exchanges between CBSDs and the SAS would be aggregated through a domain proxy such as a network access manager.
- ***SAS 1***: *Spectrum Access System 1:* Consistent with Part 96, Subpart F, a system that maintains records of all authorized PAL, GAA, and non-federal incumbent services and devices in the CBRS frequency bands, does not retain records of federal incumbent operations, is capable of determining the available channels at a specific geographic location, provides information on available channels to CBSDs that have been certified under the Commission's equipment authorization procedures, determines and enforces maximum power levels for CBSDs, and enforces protection

[11] Communication of such information from Federated Wireless ESC to a SAS operated by another entity is not supported at the time of this proposal, but may be provided later subject to market demand and approval.

criteria for Incumbent Users and PAL licensees, and performs other functions as set forth in the FCC rules.

- ***SAS 2****: Spectrum Access System 2:* Another SAS with which SAS 1 coordinates actions via the SAS-SAS Interface.

- ***ESC:*** *Environment Sensing Capability:* Consistent with Part 96, Subpart G, a radio environment sensing element that is responsible for detecting incumbent presence and operation.

- ***EMS:*** *Element Management System:* Consists of systems and applications for managing network elements on the network element-management layer of the Telecommunications Management Network model in a cellular or small cell wireless environment.

- ***Domain Proxy***: A Domain Proxy is a managing intermediary, its primary function is to perform bidirectional information processing and routing, including bulk CBSD registration and directive processing, optionally through the EMS if present.

- ***FCC Databases:*** Databases (*e.g.*, the Equipment Authorization System ("EAS") and the Universal Licensing System ("ULS")) that maintain information relevant to the management of CBRS spectrum.

- ***Informing Incumbents:*** Interfaces by which the SAS can handle exceptional (rare) inputs such as erroneous data, interference reports, enforcement actions, waivers, and instructions from federal government entities.

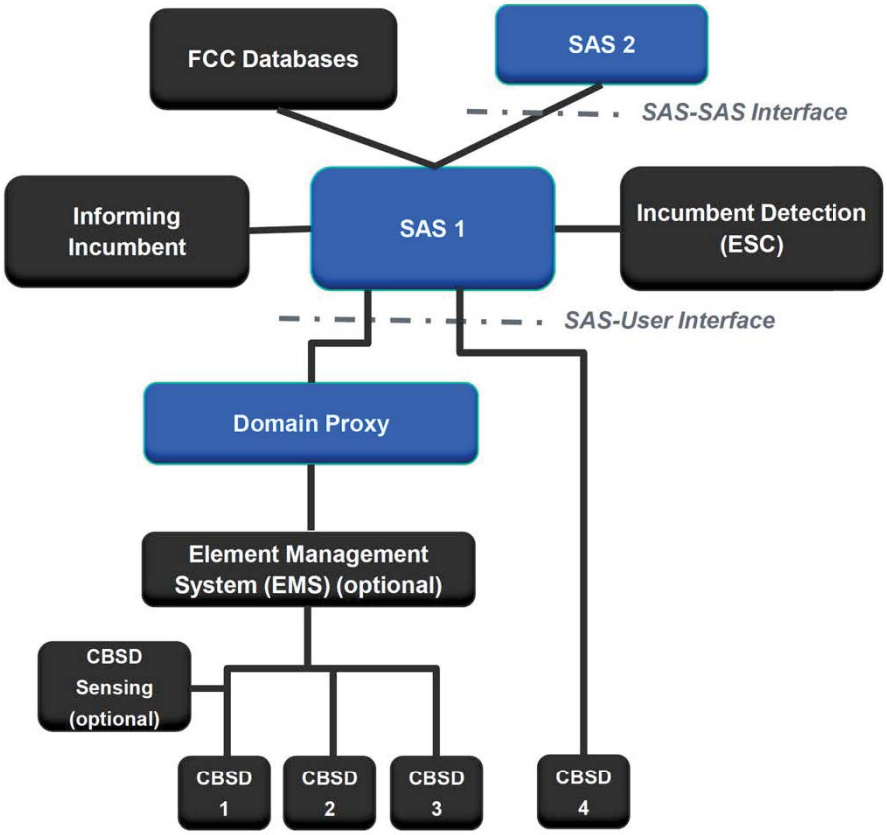

Figure 1: WINNF Notional CBRS System Architecture[12]

(b) SAS Architecture

This section provides a brief description of the Federated Wireless SAS Architecture, as depicted in Figure 2.

[12] Wireless Innovation Forum, *SAS Functional Architecture*, Document WINNF-15-P- 0047 (published Sep. 7, 2015) ("WINNF Notional CBRS System Architecture"), *available at* http://groups.winnforum.org/d/do/8512 (last accessed Apr. 5, 2016).

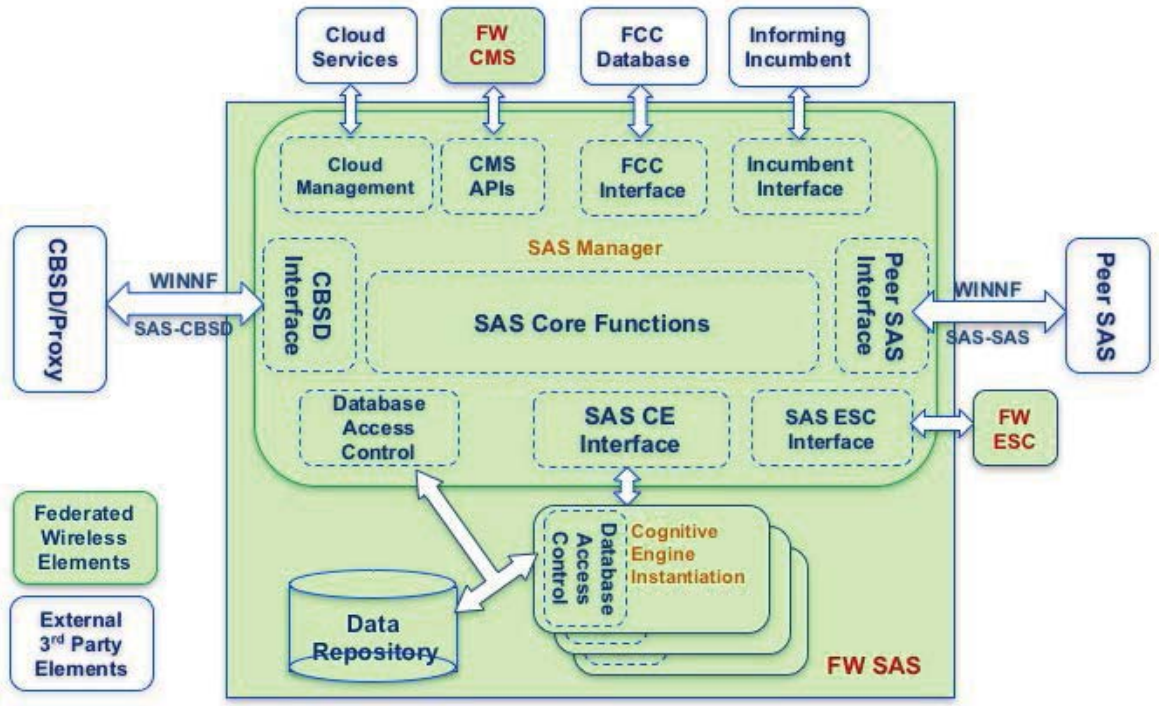

Figure 2: High Level Depiction of the Federated Wireless SAS Architecture

As can be seen in Figure 2, the Federated Wireless SAS Architecture implements each of the SAS interfaces of the CBRS System Architecture defined by the WINNF. The Federated Wireless SAS is modular and cloud-based, which allows the SAS to readily scale up and down as needed, to distribute and replicate calculation services to reduce computation and communications time, and to simplify the automation of data retention and backup subject to applicable policies and regulations.[13] Note that the Federated Wireless SAS operates without any connectivity to any military or other sensitive federal database or system, except as otherwise required by Part 96. The Federated

[13] The modular software architecture allows for functionality to be modified, implemented, and tested in a rapid and efficient manner.

Wireless SAS also does not store, retain, transmit, or disclose operational information on the movement or position of any federal system or any information that reveals other operational information of any federal system that is not required by Part 96 to effectively operate the SAS. The architecture is extensible to support the later addition of interfaces to other supporting databases, as may be needed to support the continuing evolution and innovation of the CBRS ecosystem.

The following are brief descriptions of the major components of the Federated Wireless SAS Architecture.

- ***CBSD/Proxy:*** A CBSD implementing the WINNF SAS-CBSD standard protocol[14] (for direct SAS-CBSD interactions) or a CBSD Proxy implementing the WINNF SAS-CBSD Proxy standard protocol[15] which is used when the SAS is interfacing with a network of CBSDs, typically managed through an Element Management System for LTE networks.

- ***SAS-CBSD Interface:*** Software to support the implementation of the SAS-CBSD and SAS-CBSD Proxy protocols. This includes the registration, authentication, and authorization functions defined in 96.57.[16]

- ***Web Services/Cloud Services/Cloud Management:*** Software to implement cloud management services, *e.g.*, cloud administration, logging, application monitoring, versioning, and software patches.[17]

- ***Content Management System ("CMS")/CMS APIs:*** A set of Representational State Transfer ("REST") and HTTP over Transport Layer Security ("TLS") ("HTTPS") Application Programming Interfaces ("APIs") for access to the SAS data and software to manage the publishing, editing, modifying of SAS content and support for querying services. The web-based Graphical User Interface ("GUI") for user access interfaces with and interacts with the CMS APIs. Different roles, *e.g.*,

---

[14] Wireless Innovation Forum, *SAS to CBSD Protocol Technical Report-B*, Document WINNF-15-P-0062 (published Mar. 30, 2016) ("WINNF SAS-CBSD Protocol"), *available at* http://groups.winnforum.org/Reports (last accessed Apr. 7, 2016).

[15] *Id.*

[16] Some of the services defined in section 96.57 depend on other components of the SAS, *e.g.*, the FCC interface for lists of valid FCC IDs and the Cognitive Engine for Protection Zone determinations.

[17] Web and cloud services are provided by a leading provider of cloud-based solutions, trusted by some of the largest enterprises because of the breadth and depth of their hosting infrastructure and robust control to maintain security and data protection.

CBSD owner, incumbent, administrator, FCC personnel, and the general public, permit different degrees of data access and obfuscation.[18]

- ***FCC Interface:*** Software for regularly acquiring and storing in the database necessary and appropriate information from the Commission's databases, including valid FCC ID lists, PAL auction results, and synchronizing the Federated Wireless SAS at least daily with the current Commission databases to include newly licensed facilities or any changes to licensed facilities.

- ***Incumbent Interface:***[19] Interfaces and software services by which the SAS handles exceptional (rare) inputs. These include reports of erroneous data, interference reports, inputs of alternate interference protection relationships, FCC enforcement actions, FCC waivers, and instructions from the President of the United States or another designated federal government entity, issued pursuant to 47 U.S.C. § 606.

- ***Peer SAS Interface:*** Interfaces and software necessary to coordinate with other SAS Administrators including, to the extent possible, sharing information, facilitating non-interfering use by CBSDs connected to other SASs, maximizing available GAA frequencies by assigning PALs to similar channels in the same geographic regions, coordinating actions in response to exceptional inputs and other functions necessary to ensure that the available CBRS spectrum is used efficiently consistent with Part 96. The protocol used over the Peer SAS Interface complies with the WINNF SAS-SAS Standard.[20]

- ***Data Repository:*** A regularly updated database that contains the information described in section 96.55.[21] Note that the Data Repository does not store or retain, transmit, or disclose operational information on the movement or position of any federal system or any information that reveals other operational information of any federal system that is not required by Part 96 to effectively operate the SAS. In fact, the interface separating the ESC from the SAS ensures that such information could never be communicated to the SAS.

- ***Cognitive Engine:*** Software that determines the available and appropriate channels/frequencies for CBSDs at any given location using the information supplied by CBSDs, including location, the authorization status and operating parameters of other CBSDs in the surrounding area, information communicated by the ESC, other SASs, and such other information necessary to ensure effective

---

[18] 47 C.F.R. § 96.55 (a)(3) "("SAS Administrators must make CBSD registration information available to the general public, but they must obfuscate the identities of the licensees providing the information for any public disclosures")."
[19] Labeled "Informing Incumbent" for consistency with WINNF Notional CBRS System Architecture. This provides services in compliance with sections 96.63(f), (k), (l), and (m).

[20] *See* Wireless Innovation Forum, *Interim SAS to SAS Protocol Technical Report-B*, Document WINNF-16-P-0003 ("WINNF Interim SAS-SAS Protocol"), *available at* http://groups.winnforum.org/Reports (last accessed Apr. 7, 2016).

[21] 47 C.F.R. § 96.55.

operations of CBSDs consistent with Part 96. All such determinations and assignments are made in a non-discriminatory manner. This includes calculations of allowable geographic areas, frequencies, and maximum power levels required to enforce Part 96 protections. Further details on the functions of the Cognitive Engine are provided in Section II D Spectrum Availability and Protections.

- ***ESC Interface:*** Software to communicate with the Federated Wireless ESC to obtain information about federal Incumbent User transmissions. Other components in the SAS are used to determine allowable spectrum parameters (Cognitive Engine) and to instruct CBSDs to move to another frequency range or cease transmissions (CBSD Interface).

Additional details on the Federated Wireless SAS design and implementation are provided in Part II of this proposal and in associated Appendices.

(c) ESC Architecture

The Federated Wireless ESC System depicted in Figure 3 consists of the following two types of components:

- ***Sensors:*** Federated Wireless designed devices that accurately detect the presence of transmissions from a federal system in the frequency range of 3550-3650 MHz. Sensors are deployed within or in the vicinity of Exclusion Zones and Protection Zones to facilitate accurate detection.

- ***Decision System:*** Cloud hosted software that performs the following functions:

  - Combines the sensor results to determine Protection Zone activation(s);

  - Communicates to the Federated Wireless SAS activated Protection Zones; and

  - Controls and monitors the sensors for security and operation, including maintaining software versioning.

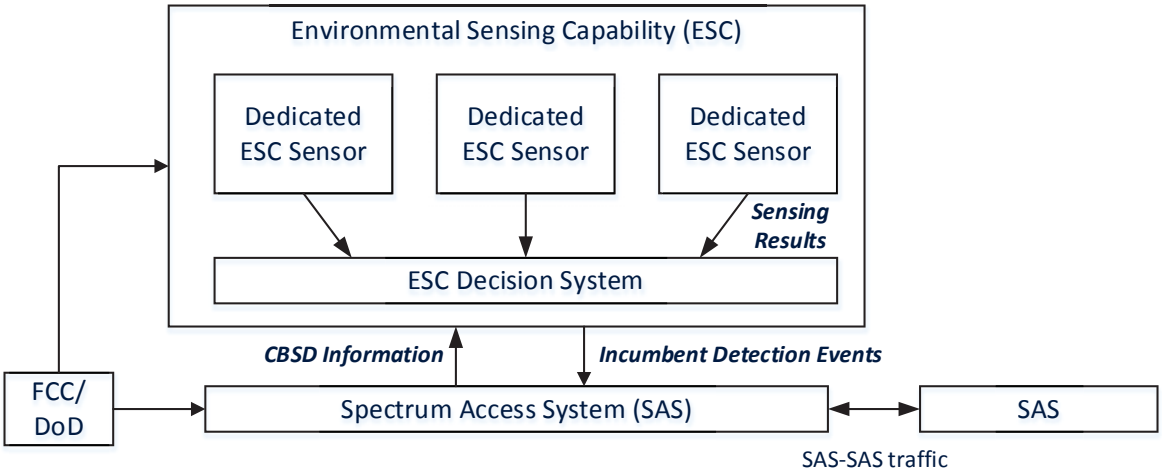

Figure 3: High Level Depiction of Federated Wireless ESC Architecture

A secure protocol that employs TLS is used for communication between the sensors and the decision system. The protocol supports the transmission of sensing results from sensors to the ESC Decision System, monitoring of the health and security of the sensors, and software versioning control of the sensors. For coastal Protection Zones, sensors are arrayed with approximately 40 km spacing on or near the coast at sites with advantaged views of the ocean.

Additional details on the Federated Wireless ESC design and implementation are provided in Part III of this proposal and in associated Appendices.

3. Models and Assumptions

The following briefly describes the propagation model and other assumptions that Federated Wireless proposes to use to model operations and facilitate coordination in the band.[22]

[22] The models and assumptions described in this section are those that will be activated, or applied, for the purpose of test and approval of SAS operations by the Commission. Consistent with the Commission's recommendations in the Second Order, Federated Wireless has opted to implement straightforward, well-known, readily implementable models. *See Amendment of the Commission's Rules with Regard to Commercial Operations in the 3550-3650 MHz Band*, GN Docket No. 12-354, Order on Reconsideration and Second Report and Order, FCC 16-55 (2016) ("Second Order").

(a) Propagation and Clutter Loss Model

Propagation and clutter loss are modeled using the same propagation and clutter loss models used in the NTIA analysis of the 3.5 GHz Exclusion Zones,[23] namely the Extended Hata Model ("EHATA") and the ITS Irregular Terrain Model ("ITM"). These models are applied in calculating protections for different incumbents as follows:

- For propagation calculations related to PAL protections, the NTIA model is used.
- For FSS and GWBL protections, ITM-only is used for consistency with the typical practices of those communities.
- For situations where both EHATA and ITM are applicable, the exact model used depends on antenna height and the land cover classification.

In general, assumptions and modeling parameters conform to the assumptions and modeling parameters of the NTIA analysis, such as building attenuation loss, clutter loss, and loss due to frequency dependent rejection.

To populate the EHATA and ITM models, the following data sources are used:

- Data from CBSD registration fields, *e.g.*, locations, terminal heights, antenna configurations, indoor vs. outdoor. Note that this permits the SAS to use these values rather than performing Monte Carlo simulations with varied parameters, *e.g.*, rather than assuming 80% of CBSDs and EUDs are indoors in an urban setting, the indoor/outdoor field determines whether a CBSD should be treated as indoors or outdoors.
- The National Land Cover Database ("NLCD") is used to categorize land into categories, *e.g.*, urban, suburban, and rural.
- A terrain database is used to inform the terrain profiles used in the models.

Further details on the specifics of the models used by Federated Wireless are provided in Appendix 19: Propagation Model Implementation.

---

[23] See E. Drocella Jr., J. Richards, R. Sole, F. Najmy, A. Lundy, P. McKenna, *NTIA Technical Report TR-15-517: 3.5 GHz Exclusion Zone Analyses and Methodology*, Appendix A (published June 2015) ("NTIA 3.5 GHz Report"), *available at* http://www.its.bldrdoc.gov/publications/2805.aspx (last accessed March 1, 2016).

(b) Statistical Models of End User Devices

The locations of EUDs are unknown to the SAS, but contribute to aggregate interference. For EUD modeling, the Federated Wireless SAS leverages the CSMAC Report[24] approach for determining the number of EUDs in the link budget calculated coverage area of each CBSD and the Cumulative Distribution Function ("CDF") curves characterizing the EUD effective isotropic radiated power ("EIRP"), which varies due to power control.

(c) Propagation Reciprocity for ESC Protections of Shipborne Radar Systems

The possibility of atmospheric ducting over the ocean complicates the application of propagation models to protect shipborne radar systems. Recently, NTIA published a technical report that proposes a method to address this propagation phenomenon by measuring received power at each ESC sensor and then estimating path loss from knowledge of the maximum radar transmit power.[25] As described in more detail in Section III: ESC and Appendix 16: Environmental Sensing Capability, the Federated Wireless ESC system utilizes this modeling technique and builds on the technical report's proposed approach to enhance protections and spectrum efficiency by utilizing more sensitive sensors and by interpolating receive signal strengths at points along the coast between sensor sites. SAS-ESC Communications

Communications between the Federated Wireless SAS and Federated Wireless ESC occurs through the SAS's ESC Interface and the ESC's SAS Interface. The secure communications protocol implements Hypertext Transfer Protocol within a connection encrypted by Transport

---

[24] Commerce Spectrum Management Advisory Committee, *Working Group 1 – 1695-1710 MHz Meteorological-Satellite*, Final Report (2013) ("CSMAC Report"), *available at* https://www.ntia.doc.gov/files/ntia/publications/wg1_report_07232013.pdf (last accessed Feb. 11, 2016).

[25] F. Sanders; E Drocella Jr.; R. Sole, *Using On-Shore Detected Radar Signal Power for Interference Protection of Off-Shore Radar Receivers*, NTIA Technical Report 16-521 (Mar. 2016) ("NTIA Radar Detection Report"), *available at* http://www.its.bldrdoc.gov/publications/2828.aspx (last accessed Apr. 9, 2016).

Layer Security ("HTTPS") to maintain secure communication and authenticate communication endpoints. Information is communicated via JavaScript Object Notation ("JSON") data objects utilizing REST APIs for reliable transfer. As both the SAS and ESC Decision System reside in the hosted cloud, communications between the two entities occurs in milliseconds or less. Additional details of the Federated Wireless SAS-ESC Communications protocol are provided in Section III.E: ESC-SAS Communications

4. Software and Firmware Updates and Addressing Security Vulnerabilities

The Federated Wireless SAS and ESC support secure updates of all software (SAS and ESC Decision System) and firmware (ESC sensors). Cloud management and related security processes will comply with Federal Risk and Authorization Management Program ("FedRAMP") guidelines[26] to protect customer and CBRS ecosystem data and as a protection against tampering that might impact incumbent operations. The cloud-based implementation of the Federated SAS and ESC Decision System allows the vast majority of software updates to these systems to occur during operation without service interruption.

Security will be continually monitored via industry best practices and vulnerabilities proactively identified through security testing. Security testing will leverage Approved Scanning Vendor ("ASV") tools in a Continuous Security Integration type environment with continuous evaluation of the following six phases of testing: Static Code Anti-Pattern Matching, Static Code Analysis, Project Dependency Security Scans of Code, Vulnerability Scanning Deployed Assets, Fuzzing Deployed Assets, and Manual Penetration Testing. Detected vulnerabilities will be

[26] *See* https://www.fedramp.gov/

prioritized for response via the NIST Common Vulnerability Scoring System ("CVSS").[27] NIST 800-53[28] security controls will be used to assess the effectiveness of our implementations.

Further details on the security policies and procedures for the Federated Wireless SAS and ESC are provided in Sections II.F: SAS Security, Section III: ESC, and Appendix 15: Security.

B. ABOUT FEDERATED WIRELESS

Federated Wireless, a leader in spectrum sharing technology, was founded in 2012 by globally recognized wireless and radio communication leaders to enable and commercialize technologies to unlock the enormous potential of dynamically sharing spectrum resources. Today, Federated Wireless is leading the industry in developing shared spectrum management systems, which include spectrum access systems, environmental sensing technologies, cognitive radios, and spectrum sensing that together dramatically improve spectrum utilization, increase the reach and reliability of wireless communication systems, and reduce the cost and complexity to deploy wireless networks. The innovative cloud-based wireless infrastructure solutions developed by Federated Wireless will break down traditional barriers to spectrum use that are found in both exclusive licensing regimes and unlicensed use regimes – alleviating the high costs of spectrum acquisition, and alleviating spectrum congestion in unlicensed bands. The result is more effective spectrum management for all users.

Since its inception, Federated Wireless has partnered with the Commission, federal and non-federal incumbents, carriers, innovators, unlicensed user groups, and industry working groups, such as the WINNF, to contribute to a flexible, innovative regulatory framework for the CBRS. For

---

[27] *See* NIST, *Common Vulnerability Scoring System Version 2 Calculator*, *available at* https://nvd.nist.gov/CVSS/v2-calculator (last accessed Mar. 2, 2016).

[28] NIST, "*Security Controls and Assessment Procedures for federal Systems and Organizations*," NIST Special Publication 800-53 (Rev. 4), *available at* https://web.nvd.nist.gov/view/800-53/Rev4/ (last accessed Apr. 5, 2016).

example, Federated Wireless co-founded the SSC of the WINNF, bringing together industry stakeholders to develop and advance spectrum sharing technologies based on the three-tiered architecture of the CBRS. In February 2016, Federated Wireless, together with five wireless industry leaders – including Google, Intel, Nokia, Qualcomm and Ruckus Wireless – announced their shared commitment to develop, market, and promote solutions utilizing the CBRS.[29]

Federated Wireless also was selected as an important partner to the federal government for developing new spectrum management tools. In September 2015, NASCTN announced its first test spectrum sharing project, focused on developing spectrum sensing technology for use in the Citizens Band. Federated Wireless was asked to join this effort in combination with DoD, NIST, and NTIA.

The broad stakeholder partnerships in which Federated Wireless is involved, with foundations in both industry and government, have allowed the spectrum sensing and sharing technologies that will be leveraged for the CBRS to develop at a remarkable rate. Federated Wireless' initial efforts focused on enabling spectrum sharing in the 3.5 GHz band. During the summer of 2014, Federated Wireless demonstrated the feasibility of using a dedicated sensor network to detect the presence of shipborne SPN-43 radar systems to allow commercial use of 3550-3650 MHz spectrum while protecting federal incumbent operations along the coastlines.[30] Federated Wireless also conducted and reported experiments that demonstrated that LTE systems

---

[29] *See* Ruckus Wireless, *Industry Leaders Collaborate to Expand Cellular Coverage and Capacity for Buildings and High-Density Areas*, News Release (published Feb. 18, 2016), *available at* http://investors.ruckuswireless.com/phoenix.zhtml?c=251538&p=irol-newsArticle_print&ID=2140687 (last accessed Apr. 7, 2016).

[30] *See* Letter from Iyad Tarazi, Chief Executive Officer, Federated Wireless, Inc., to Marlene H. Dortch, Secretary, FCC, GN Docket No. 12-354 (filed Oct. 2, 2014).

could operate close to land-based radar systems, demonstrating that protection of incumbents rather than protection of secondary systems was the principal concern in the band.[31]

Demonstration and testing of Federated Wireless SAS and ESC technologies has already begun. Federated Wireless was awarded a contract from Leidos to participate in the SSPARC research program. The SSPARC research program, run by DARPA, aims to expand spectrum sharing between radar and commercial wireless systems. The subcontract provides Federated Wireless with the opportunity to demonstrate its SAS with an integrated commercial LTE network to enable radar and commercial wireless spectrum sharing. Federated Wireless has further begun work to establish a test bed in the Norfolk, VA-Virginia Beach, VA, area, where it will validate its sensor and ESC technology through field testing.

Federated Wireless has entered into multiple partnership and pilot agreements with service providers, together with technology partners, to demonstrate and test an integrated end-to-end 3.5 GHz band spectrum sharing solution, including a SAS, ESC, and LTE technology. Later this year, Federated Wireless will seek Special Temporary Authority from the FCC to utilize spectrum in the band in support of these pilot programs.

1. Technical Expertise

Since its founding in 2012, Federated Wireless has placed a strong emphasis on assembling a diverse and experienced team from the Information and Communications Technologies sector. Federated Wireless stands today at the forefront of the wireless industry revolutionizing the way spectrum will be managed for the future.

Developing industry changing, innovative technologies is the heritage of Federated Wireless. Our innovation can be traced from our Founding Scientists and their work at the Hume Center,

[31] *See* Letter from Jeff Reed, Willis G. Worcester Professor in Electrical and Computer Engineering, Virginia Polytechnic Institute and State University, to Marlene H. Dortch, Secretary, FCC, GN Docket No. 12-354 (filed Sep. 3, 2014).

Wireless@VT at Virginia Tech, and government agencies such as DoD and DARPA. Dr. Charles Clancy was the co-author of Spectrum Sharing strategy for the DoD. Dr. Jeff Reed served as a member of The United States President's Council of Advisors on Science and Technology ("PCAST") and was influential in shaping the shared spectrum model adopted by the FCC. Dr. Robert McGwier is one of the foremost leading scientists in telecommunication systems engineering and, along with Dr. Joe Mitola, laid the foundation for spectrum sensing cognitive radio. Our parent company Allied Minds, partners with universities and federal research institutions to develop new technologies, bridging the commercial gap to create businesses based on these technologies.

Federated Wireless is led by Iyad Tarazi as CEO, and a team of industry veterans who continue to build on that heritage by pioneering new territory in the commercialization of licensed shared spectrum. Iyad Tarazi brings seasoned understanding of commercial wireless networks and technologies, having previously served as Sprint's Vice President of Network Development and Nextel's Vice President of Network Engineering and Technology Integration. Kurt Schaubach, the CTO for Federated Wireless, was previously the Vice President and Chief Technology Officer of the National Rural Telecommunications Cooperative and Senior Vice President of Engineering for NextWave Wireless, and has extensive experience in spectrum management and sharing applications. Sepehr Mehrabanzad, the Senior Vice President of Engineering for Federated Wireless, was previously the Vice President of Engineering for Airvana, a provider of consumer femtocell technology, and a co-founder of Sentient Wireless. He has strong experience researching and analyzing network function virtualization for spectrum sharing.

Federated Wireless has complemented its executive leadership team with a world class team of technologists, researchers, engineers, and software system architects, software security experts, and software developers. The Federated Wireless team is composed of software engineers with broad experience in database development and management, networking, security, cloud and

distributed computing, and web and Graphical User Interface ("GUI") implementation, as well as radio frequency engineers with experience in all aspects of the wireless ecosystem. Notable accomplishments and capabilities of the Federated Wireless Team include:

- The Federated Wireless Team averages 16 years of industry experience.
- 28 full-time members of the Federated Wireless Team hold advanced degrees – 12 Doctoral degrees and 16 Master degrees – in technical fields including Electrical Engineering, Computer Science, Information Technology and Applied Mathematics.
- Vast technical and operational expertise spanning:
    - dynamic spectrum access, software defined radio, cognitive radio, and machine learning;
    - game theory, stochastic modeling, information theory, and digital signal processing;
    - spectrum engineering, radio propagation measurement and modeling, radio planning and optimization tools, self-optimizing network technology;
    - software engineering, web programming, software security testing;
    - Java, JavaScript, C, C++, and Python programming languages in Android, iOS, Linux, Windows and Embedded Wireless, SQL and non-SQL database languages and geo-database applications;
    - network protocols, network security, network services orchestration, and network virtualization;
    - software, mobile device, and application security solutions, data center and network security implementation, test, and monitoring;
    - analog hardware and ASIC development;
    - wireless and wireline network engineering, network planning, and network development;
    - specification development, test and certification of hardware and software technologies;
    - virtualization, cloud services, and software-as-a-service deployment and support; and
    - financial data clearing, roaming, and interworking.
- The Federated Wireless Team holds more than 100 patents, has published nearly 250 technical papers, and have authored or co-authored at least three technical textbooks.

- Team members contributed to the development of wireless technology standards, including co-authoring IEEE 802.11 and provided major contributions to the development of IEEE 802.16.

- Members of the Federated Wireless Team contributed to the commercialization of wireless technologies including the initial deployments of TDMA, iDEN, CDMA, WiMAX, and services and systems to support international CDMA roaming.

- Executive team members pioneered small cell technology, including both the technology development and deployment of the industry's first major small cell network.

- Team members were co-founders of the WiFi Alliance and Mobile WiMAX Forum.

- Federated Wireless leaders currently serve on the Executive Committee of the National Spectrum Consortium, the Commerce Spectrum Management Advisory Committee ("CSMAC"), and the Board of Directors for the WINNF.

- Team members were founders, co-founders, or principal contributors to more than 12 technology startups.

Select biographies for the Federated Wireless Executive Leadership Team, Technology Leadership Team, Founders, and Advisors can be found in Appendix 1: Select Federated Wireless Biographies.

2. Financial Capabilities, Business Structure, and Fees

In this section, Federated Wireless describes its financial capability to act as a SAS Administrator and ESC operator, its business and ownership structure, and the fees it will charge for its services.

Federated Wireless is financially capable of operating a SAS and ESC for a five-year term in accordance with Part 96.63(e).[32] As detailed below, Federated Wireless is a well-capitalized enterprise fully supported by its parent company, Allied Minds, and its other investors. As a result, Federated Wireless possesses financial resources that are more than sufficient to support the engineering, development, testing, certification, customer pilot, and commercial launch of its SAS and ESC technologies, and to operate them over the long term. In addition, Federated Wireless will collect

[32] 47 C.F.R. § 96.63(e).

fees for its management and value added services – delivered via a "Spectrum-as-a-Service" model developed by Federated Wireless – that will aid both in funding Federated Wireless' ongoing operation and advancement of the SAS and ESC technologies and, given the reasonable levels of the fees and the value provided to customers by the services, drive commercial operator investment in and adoption of the CBRS.

(a) Financial Capabilities

As evidenced by its most recent funding round, Federated Wireless is fully funded to support the engineering, development, testing, certification, customer pilot, and commercial launch of its SAS and ESC technologies. On February 1, 2016, Allied Minds announced that Federated Wireless had raised $22 million of new equity in a Series A Preferred round from investors including Woodford Investment Management ($15 million) and Allied Minds ($5 million). The proceeds of the fundraising will enable Federated Wireless to complete its SAS and ESC certification, conclude development and accelerate commercialization of its cloud-hosted CINQ XP platform, and conduct field trials in the second half of 2016 with technology partners. Federated Wireless does not anticipate the need to raise additional funds prior to the launch of its commercial product for the CBRS.

As detailed elsewhere in this application, Federated Wireless has made important architectural and engineering design decisions to ensure that it can keep operational costs low while providing a spectrum management service that fully complies with the Commission's Part 96 rules. These architectural and engineering design decisions include:

- A fully cloud hosted SAS platform which provides scalability, high availability, and resiliency at very lost cost.
- Machine learning algorithms that incorporate the Signal Level Reporting data from CBSDs to continually enhance the accuracy of SAS propagation predictions and interference calculations so that additional R&D is not required as use of the band increases.

- Sensor technology, designed by Federated Wireless and manufactured by its contract manufacturer, for use in the ESC network. The sensor technology was developed and commercialized by Federated Wireless at a fraction of the cost of common-off-the-shelf spectrum analyzers and radiowave measurement devices.

(b) Business Structure

Federated Wireless' parent company, Allied Minds, is an innovation company that forms, funds, manages and builds startups based on early-stage technology originating from U.S. universities and federally funded research institutions. This unique approach overcomes the traditional early-stage gap between basic research and commercial development. Allied Minds – together with its investors – provides its subsidiaries with capital resources, from seed to self-sustainment. Its aim is to promote growth, generate jobs, foster innovation and create societal benefit.

Allied Minds is structured as a diversified holding company with a strong central management team active in the strategic development of its subsidiary businesses. This is a key distinguishing feature of the company when compared with investment funds. Allied Minds' core aim is to focus on early-stage disruptive technologies, often developed in an academic setting, that it believes have significant upside potential and to realize that potential through supporting commercial development.

With regard to corporate structure, Allied Minds PLC is the parent company, which is a publicly traded company in the UK (LSE: ALM). Allied Minds LLC is the U.S. subsidiary and Federated Wireless, Inc. is majority owned by Allied Minds Federal Innovations, Inc., (AMFI) which is 100% owned by Allied Minds LLC. A depiction of Federated Wireless' ownership structure is provided in Appendix 2: Ownership Structure.

(c) Spectrum Access System Administrator Fees

(i) Spectrum-as-a-Service Delivery Model

As commercial use of the CBRS builds, Federated Wireless will collect fees for the spectrum management and other value added services it offers to PAL and GAA users of the CBRS. Pursuant to section 96.65,[33] Federated Wireless will charge PAL and GAA users a reasonable fee for the provision of the services set forth in section 96.53,[34] and Federated Wireless agrees to comply with Commission requests to review such fees and modify such fees if they are found to be unreasonable.

By diversifying revenue through a broad range of optional, value added services, Federated Wireless firmly believes that the fees it will charge for the management services it will provide to comply with the Commission's Part 96 rules will be very economical, especially in light of the tremendous value that access to high-quality coordinated shared spectrum represents to its users.

Federated Wireless will implement a "Spectrum-as-a-Service" ("SaaS") delivery model, similar to the Software-as-a-Service delivery model that is now commonplace throughout industry. This delivery model has proven to be progressive, elastic, and scalable, and will provide the ideal economic flexibility to enable access to the CBRS spectrum on a subscription basis. Like its Software-as-a-Service counterpart, the Federated Wireless SaaS model offers on-demand delivery and reduces operational costs by providing services to customers on a hosted basis (*i.e.*, spectrum management services can be provided directly to CBSDs via a broadband Internet connection; thus, a user of the Federated Wireless SaaS service will not require additional IT infrastructure to support its operations in the CBRS). While Federated Wireless has not finalized its pricing plans, pricing models currently under consideration for the Federated Wireless service follow well-known

[33] *Id.* § 96.65.

[34] *Id.* § 96.53.

conventions established in the Software-as-a-Service industry, segmenting pricing tiers/bundles to be responsive to the services required by customers' varying business needs. Applying these methods and models, along with other industry benchmarks for managed IT and Telecom services, Federated Wireless is confident that it will arrive at a competitive price plan that will stimulate adoption and use of the CBRS.

(ii) CINQ XP™ Commercial Product Offering

Federated Wireless' commercial product offering is CINQ XP™, a cloud-based application platform that will enable next-generation networks on shared spectrum. The CINQ platform is built on a highly available, redundant and secure multi-tenant cloud architecture. This cloud model also allows dynamic scaling as needed to support the increasing number of endpoints needing spectrum services. Built on Federated Wireless's dynamic SAS and ESC, the CINQ XP platform complies with all aspects of Part 96 of the Commission's rules for commercial operations in the CBRS. Beyond the required functionality for spectrum management across the federal and non-federal Incumbent User, PAL, and GAA tiers, CINQ XP extends the services Federated Wireless offers its subscribers even further to provide additional spectrum capabilities. CINQ XP provides a range of enhanced shared spectrum services for users, including the following:

Network Visibility & Planning

CINQ XP provides network visibility and planning capabilities for CBRS users through a cloud-based interactive web interface. This interface offers users a view of how their wireless equipment can be deployed to optimize across metrics such as coverage and capacity. Through the web interface, users get a real-time snapshot of the shared spectrum environment showing a comprehensive view of shared assets managed by Federated Wireless's SAS and other SASs, which can be used to determine the availability of shared spectrum in a specific geographic region.

CINQ XP's Network Planning and Management design is optimized to consider the unique constraints and requirements for CBRS operation. Rapid planning tools allow radio network planners to efficiently evaluate candidate network layouts, each with different constraints, such as accounting for site acquisition adjustments. The application leverages GeoData (*e.g.*, building data, terrain, clutter, population, device density), device capability data, and network measurements (*e.g.*, sensing measurements) to provide very accurate coverage and capacity calculations. Rich and interactive analytics facilitate evaluation of candidate solutions for a user's network.

Spectrum Analytics

The CINQ XP platform's web-based user interface provides detailed network analytics through data visualization, reporting, and audit capabilities, allowing the user to understand how equipment is operating in a shared network environment and how it can be optimized for shared spectrum. Analyzed data includes spectrum usage, capacity, and coverage, and this data can be exposed for the user's billing purposes. Network analytics also include data obtained from other SASs through real-time SAS-SAS communication to enable the best understanding of the complete radio environment map across CBRS components.

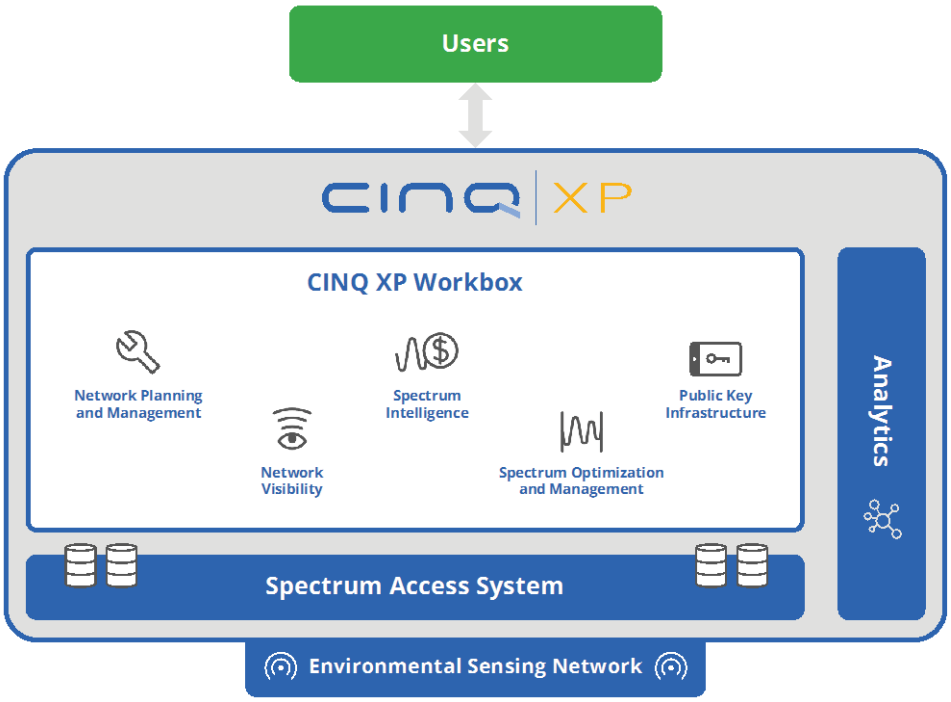

Figure 4. Federated Wireless CINQ XP™ Commercial Product Offering

C. COMPLIANCE

Federated Wireless affirms that it will comply with all of the applicable rules as well as applicable enforcement mechanisms and procedures for both SAS Administration and ESC operation.

1. Designated Party Responsible for Compliance

Federated Wireless designates Kurt Schaubach, Chief Technology Officer, as the responsible party who will ensure compliance with the rules and conditions set forth by the Commission.

2. Qualifications of Key Personnel

Qualifications of Federated Wireless personnel responsible for operating and maintaining the SAS and ESC are provided in Appendix 1: Selected Federated Wireless Biographies.

3. Cooperation with the Commission to Ensure Compliance with and Enforcement of Its Rules

Federated Wireless will comply with all of the Commission's applicable rules as well as applicable enforcement mechanisms and procedures.

Consistent with section 96.55(k),[35] and as described elsewhere in this proposal, Federated Wireless will provide any information contained in the database to the Commission and remove information from the database upon direction from the Commission. Federated Wireless will make APIs available to Commission personnel and will allow authenticated web-based access to the FCC for administrative purposes. Federated Wireless will provide the Commission access to information used to determine channel availability, log records, and bulk downloads of relevant data. Additionally, the portal will provide a capability for the Commission to submit, and for Federated Wireless to respond to, specific inquiries.

As indicated above, Federated Wireless is fully committed to supporting and readily adapting to any future changes to the Commission's rules, enforcement mechanisms, and enforcement procedures.

4. Information Gathering and Retention

Federated Wireless will comply with the information gathering and retention rules as set forth in section 96.55.[36] Specifically, Federated Wireless affirms that the Federated Wireless SAS will retain records and information or instructions received regarding federal transmissions from the ESC in accordance with the information retention policies established as part of the ESC approval process.[37] Further details can be found in Appendix 6: Information Retention.

---

[35] *Id.* § 96.55(k).

[36] *Id.* § 96.55.

[37] *Id.* § 96.55(c).

5. Response to Claim of Inaccuracies

Consistent with section 96.63(f),[38] Federated Wireless will respond in a timely manner to verify, correct or remove, as appropriate, data in the event the Commission or a party brings any inaccuracy in the Federated Wireless SAS database to its attention. Further details can be found in Appendix 7: Error Resolution and Interference Reporting Policy.

6. Response to Claim of Interference

Consistent with section 96.53(o),[39] Federated Wireless will respond in a timely manner to interference complaints from FSS earth station licensees. In conjunction with its interference coordination and mitigation efforts, Federated Wireless will work collaboratively with the affected FSS earth station licensee, other SAS Administrators, and the Commission, if necessary, to resolve any claims that may arise.

7. Commitment to SAS-SAS Coordination and Efficient Spectrum Use

As described in Sections II.C.3: SAS-SAS Interface and II.E: SAS-SAS Coordination, the WINNF has standardized an interface and protocol for SAS-SAS information exchange to foster a healthy, interoperable spectrum sharing ecosystem and to facilitate compliance with sections 96.63(h) and 96.63(i).[40]

Federated Wireless is committed to coordinating operations with other SASs to avoid conflicting spectrum assignments, to maximize shared use of available frequencies, to facilitate non-interfering use by CBSDs connected to other SASs, to maximize available GAA frequencies, to

---

[38] *Id.* § 96.63(f).

[39] *Id.* § 96.53(o).

[40] *Id.* §§ 96.63(h)-(i).

assign PALs to similar channels in the same geographic regions, to ensure continuity of service to all registered CBSDs, and to provide the data collected pursuant to section 96.55.[41]

8. Commitment to Secondary Markets and Spectrum Manager Lease Agreements

Federated Wireless fully supports the Commission's belief that there are significant benefits to a robust secondary market for PAL spectrum. Federated Wireless will accept PAL leasing notifications and support PAL Spectrum Manager Lease Agreements ("SMLAs") in compliance with sections 96.32 and 96.66.[42] Federated Wireless will also operate a spectrum exchange as it is ideally situated to facilitate the light-touch leasing process defined by the Commission.

9. Affirmation of SAS Operations

Consistent with section 96.63(n),[43] Federated Wireless will operate the Federated Wireless SAS without any connectivity to any military or other sensitive federal database or system, except as otherwise required by this part. The Federated Wireless SAS also will not store, retain, transmit, or disclose operational information on the movement or position of any federal system or any information that reveals other operational information of any federal system that is not required by Part 96 to effectively operate the SAS.

10. No Anti-Competitive or Discriminatory Practices

As part of its commitment to growing the spectrum sharing ecosystem, Federated Wireless agrees to make the database services proposed herein available to users on a non-discriminatory basis and agrees that it will not use its capacity as a SAS Administrator to engage in any

---

[41] *Id.* § 96.55.

[42] *Id.* §§ 96.32, 96.66.

[43] *Id.* § 96.63(n).

discriminatory or anti-competitive practices, or any practices that may compromise user privacy. Federated Wireless' proposed Terms of Use and Privacy Policy are provided in Appendix 17: Terms of Use and Appendix 18: Privacy Policy.

11. Compliance with Statutory Obligations

Consistent with the Commission's enforcement responsibilities and its statutory obligation to comply with Presidential orders, Federated Wireless has implemented protocols to respond to directions from the President of the United States or another designated federal entity to manually discontinue operations of its associated CBSDs in a given area pursuant to 47 U.S.C. § 606. Federated Wireless has also implemented protocols to manually discontinue operations of associated CBSDs in response to enforcement actions taken by the Commission. These protocols and procedures are described in Appendix 4: Access Protocols and Procedures.

12. Commitment to User Data Privacy

Federated Wireless is fully committed both to compliance with section 96.55 and to protecting the privacy of customer data. To comply with section 96.55(a)(3), the Federated Wireless SAS will make available to the public CBSD registration information, but will obfuscate the identities of the licensees providing that information. To preserve the privacy and security of customer data, Federated Wireless has implemented a number of security measures and adopted a Privacy Policy that provides robust protections for Federated Wireless customers. Federated Wireless only collects and uses information that is necessary to effectuate its duties as a SAS Administrator, including interference protection, spectrum management, and does not disclose such information unless required to do so by law. Any information collection, use, and retention is conducted strictly in accordance with Part 96 of the Commission's rules. More information on the

security of the SAS database is provided in Appendix 15: Security, and the Federated Wireless Privacy Policy is provided in Appendix 18: Privacy Policy.

13. Conveyance of Service

Pursuant to section 96.63(g),[44] in the event Federated Wireless does not continue as a SAS Administrator at the end of its term, and subject to the consent of its customers, Federated Wireless will securely transfer the information in the Federated Wireless SAS, along with the IP addresses and URLs, and a list of registered CBSDs, to another approved entity. Federated Wireless may charge a reasonable price to the approved entity for such conveyance.

[44] *Id.* § 96.63(g).

PART II: SAS ADMINISTRATOR PROPOSAL

This portion of the proposal provides the following information related to SAS Administration as requested in the Application Procedures PN.

- A detailed description of how the SAS will retain, secure, and verify information from CBSDs (including location data), licensees, associated ESCs, and other SASs.

- A demonstration that the SAS will be capable of resolving various sources of interference between and among CBRS users and/or Incumbent Users.

- A description of how the SAS will ensure that non-federal FSS earth stations and grandfathered 3650-3700 MHz licensees are protected from harmful interference consistent with the rules.

- A description of how coordination will be effectuated (*e.g.*, through data synchronization) between multiple SASs, if multiple SASs are authorized, and how quickly this synchronization of data will be accomplished.[45]

- If the prospective SAS Administrator will not be performing all SAS functions, it must provide information on the entities operating other functions and the relationship between itself and these other entities. In particular, it must address how the Commission can ensure that all of the requirements for SAS Administrators in Part 96, subpart F are satisfied when SAS functions are divided among multiple entities, including a description of how data will be transferred among these various related entities and SASs, if multiple SASs are authorized, and the expected schedule of such data transfers (*i.e.*, real-time, once an hour, etc.).

- A description of the methods (*e.g.*, interfaces, protocols) that will be used by: (1) CBSDs to communicate with the SAS; (2) the SAS to communicate with CBSDs; (3) the SAS to communicate with other SASs; and, if applicable, (4) the SAS to communicate with one or more ESCs. The prospective SAS Administrator must also describe the procedures, if any, which it plans to use to verify that a CBSD can properly communicate with the SAS.

- An affirmation that, consistent with section 96.55, the SAS will only retain records and information or instructions received regarding federal transmissions from the ESC in accordance with information retention policies established as part of the ESC approval process.

- A description of the security methods that the prospective SAS Administrator plans to use to ensure that unauthorized parties cannot access or alter the SAS or otherwise corrupt the operation of the SAS in performing its intended functions, consistent with the Commission's rules.

[45] We recognize that some details of the SAS-SAS coordination process may depend on the specific architecture and system design of the various conditionally approved SASs.

- Descriptions of dynamic use-case scenarios for how the SAS will manage and assign spectrum resources to ensure that geographically and spectrally adjacent operations are coordinated consistent with the Commission's rules. Use case scenarios should include the methodology and protection approach for cases of radio interference due to adjacent blocking, out-of-band emissions, and aggregate co-channel interference. Describe how multiple SASs will coordinate the calculation of aggregate interference for protecting Incumbent Users and PAL licensees.

- A description of the methods that the SAS will use to make information stored or retained by the SAS available in response to a request from authorized Commission personnel.

A. DIVISION OF FUNCTIONS

Federated Wireless will, as a single entity, provide all of the required SAS functionality itself. As described in Section I, the Federated Wireless SAS is cloud-based, which provides scalability and resiliency, allows the SAS to distribute and replicate calculation services to reduce computation and communications time, and allows the SAS to simplify the automation of data retention and backup, subject to applicable policies and regulations. Federated Wireless is currently using an industry-leading cloud infrastructure hosting and cloud services partner and Federated Wireless directly administers, manages, and monitors the hosting services provided by its cloud hosting partner. The cloud-based SAS architecture enables the creation and use of multiple SAS instances and partitioning of SAS functions, if required. The multiple SAS instances and partitioned SAS functions communicate, exchange, and synchronize their operations on a real-time basis.

B. SAS DATA MANAGEMENT AND ACCESS POLICIES

In compliance with sections 96.63(a) and 96.66(a)(2),[46] Federated Wireless maintains a regularly updated database that contains data from a number of sources required by the SAS to perform its functions. To manage this data, Federated Wireless has established and will follow a set

[46] 47 C.F.R. §§ 96.63(a), 96.66(a)(2).

of protocols and procedures relating to data acquisition and synchronization, information retention, error resolution, and access control.

Further information regarding Federated Wireless's data management and access policies can be found in the following appendices:

- Appendix 4: Access Protocols and Procedures
- Appendix 5: Database Information;
- Appendix 6: Information Retention; and
- Appendix 7: Error Resolution and Interference Reporting Policy.

1. General Data Retention Policies

Consistent with sections 96.53(e), 96.55(b), 96.55(c), and 96.55(e),[47] Federated Wireless has established an information retention policy in order to retain all required information necessary to operate as a SAS Administrator. This includes, but is not limited to, federal Incumbent User Exclusion Zones and Protection Zones, registration information for protected FSS earth stations, registration data for GWBLs, current information on registered CBSDs, PAL Protection Areas, interference reports, interference protection requests, and SMLAs. In addition to details of these registered endpoints, Federated Wireless also retains SAS transaction records not pertaining to federal Incumbent User transmissions for a period of 60 months.

Further information regarding Federated Wireless's information retention policy can be found in Appendix 6: Information Retention.

[47] *Id.* §§ 96.53(e), 96.55(b)-(c), (e).

2. Correcting Data

Consistent with 96.63(f),[48] Federated Wireless has established an error resolution policy that includes procedures to identify and resolve data inaccuracies contained in the SAS. Because the interference protections and services provided by the Federated Wireless SAS depend on the accuracy of the data stored in its database, Federated Wireless is keenly interested in quickly resolving any errors in its SAS database. The SAS takes steps to automatically and proactively detect errors during CBSD registration, data acquisition from FCC databases, and data acquired from measurement reports. In addition, external parties are also able to identify data errors and bring them to our attention. These external parties include the Commission, general public users, CBSD owners and Certified Professional Installers ("CPIs"), and non-federal Incumbent Users. Once a data inaccuracy has been identified, Federated Wireless will respond to and resolve the error within 12 hours.[49]

Further information regarding Federated Wireless's error resolution policy can be found in Appendix 7: Error Resolution.

3. CBSD Data

The SAS maintains records of all CBSD information. This information enters the SAS via a variety of methods, including through SAS-CBSD exchanges, data entered into the SAS by a CPI via an industry-standardized interface, and information obtained over the SAS-SAS interface.

Consistent with 96.55(e),[50] as part of Federated Wireless's Terms of Use policy that users must accept,[51] the SAS retains records of an acknowledgement by all entities registering CBSDs that

---

[48] *Id.* § 96.63(f).

[49] Or sooner, if so required by service level agreements with Federated Wireless customers or end users, or as may otherwise be required by the Commission.

[50] 47 C.F.R. § 96.55(e).

they understand the risk of possible interference from federal Incumbent User transmissions in the band.

(a) CBSD Data Retention

Consistent with sections 96.39, 96.45, and 96.57,[52] a CBSD must register with and be authorized by the SAS prior to its initial service transmission. During registration, the CBSD must provide the SAS with the following details, which the SAS retains for a period of 60 months.

<u>Category A & B CBSDs</u>

- Geographic location
- Antenna height above ground level
- CBSD class (Category A/B)
- Requested Authorization Status (PAL/GAA)
- FCC ID
- Call sign
- Air interface technology
- Manufacturer's serial number
- Sensing capabilities
- User contact information
- Deployment profile (indoor/outdoor)

<u>Category B CBSDs</u>

- Antenna gain
- Beamwidth

---

[51] *See infra* Appendix 17.

[52] 47 C.F.R. §§ 96.39, 96.45, 96.57.

- Azimuth
- Downtilt angle

Further information regarding Federated Wireless's database information and information retention policy, including the specific CBSD details stored and their retention policy, can be found in Appendix 5: Database Information and Appendix 6: Information Retention.

(b) CBSD Data Verification

Consistent with sections 96.57(c) and 96.57(d),[53] the SAS verifies that any CBSD seeking access to the SAS possesses a valid FCC ID and that the CBSD is operating within an approved geographic region prior to authorizing the CBSD to begin transmissions. The SAS obtains the FCC IDs of valid devices from the Commission's Equipment Authorization System database.

Consistent with sections 96.43(a), 96.43(b), and 96.43(c)[54], the SAS verifies the necessary information for Category A CBSDs, including the deployment profile and antenna height, to ensure that the device's classification as a Category A CBSD is correct.

Consistent with sections 96.45(a), 96.45(b), 96.45(c), and 96.45(d),[55] the SAS verifies the necessary information for Category B CBSDs, including professional installation, deployment profile, and specific Category B details such as antenna gain, beamwidth, azimuth, and downtilt angle, to ensure that the device's classification as a Category B CBSD is correct.

For CBSDs installed by a CPI, the SAS verifies location data to ensure that all CBSD input locations lie within the boundaries of the United States; eliminating entries of locations of 0,0 (off the coast of Africa) or entries that transpose latitude and longitude. Reported locations are also screened against IP address-location mappings, which is generally sufficient to ensure that a CBSD is

[53] *Id.* §§ 96.57(c)-(d).

[54] *Id.* §§ 96.43(a)-(c).

[55] *Id.* §§ 96.45(a)-(d).

within the correct metropolitan area. In each case, a location that fails either of these checks is flagged for the CPI to verify and correct during registration. Further information about data verification for CPI devices can be found in Appendix 14: Certified Professional Installers.

4. PAL Data

The Federated Wireless SAS maintains a database that maps each PAL, as defined in the WINNF SAS-CBSD Protocol,[56] to a census tract and 10 MHz channel. This database is initially populated based on the third-party defined PAL Channel Assignment Plan, as specified in Appendix 11: PAL Channel Assignment Plan. The PAL must be associated with one or more CBSDs before these CBSDs can request authorization from the SAS to operate on the PAL channels.

The Federated Wireless SAS will also store the geo-coordinates defining PAL Protection Areas, regardless of whether these areas are self-reported by the PAL licensee or computed by the SAS.

Further information regarding the specific data stored for a PAL and PAL Protection Areas can be found in Appendix 5: Database Information.

5. SAS Data

The Federated Wireless SAS maintains all SAS transactional records not pertaining to federal Incumbent User transmissions for 60 months from the transaction date. These records are available for analysis as needed. These records include:

- CBSD registration records, including updates;
- CBSD spectrum requests and responses as will be defined in the SAS-CBSD Protocol Technical Specification currently under development in the WINNF;
- Channel assignments by the SAS to CBSDs;

[56] *See* WINNF SAS-CBSD Protocol

- Interference reports received including report data, timestamp, SAS actions taken for resolution; and
- SMLAs.

Further information regarding Federated Wireless's SAS data can be found in Appendix 6: Information Retention.

6. ESC Data

For federal Incumbent User transactions, the ESC notifies the SAS of a federal Incumbent User detection event with the following information:

- A geographical description, which defines the extent of the federal incumbent activity to be protected;
- A frequency range, which defines the extent of federal incumbent activity to be protected;
- An activation time for this protection; and
- A deactivation time for this protection.

Once the ESC notifies the SAS that the federal Incumbent User detection event has expired, the SAS will retain the record for only 300 seconds. For auditing purposes, the SAS stores the total number of federal Incumbent User detection events in an area at each frequency, but does not retain the event record itself beyond the retention time.

Further information regarding Federated Wireless's ESC data can be found in Appendix 6: Information Retention.

7. FCC-Maintained Data

Consistent with sections 96.55(a), 96.55(d), and 96.63(b),[57] the SAS interfaces with all necessary FCC databases to acquire data, including PAL assignments, authorized devices and their

[57] 47 C.F.R. §§ 96.55(a), 96.55(d), 96.63(b).

FCC IDs, and protected FSS and GWBL locations. Once data is acquired from these various external data sources, this data is aggregated and stored in Federated Wireless's SAS databases so that it can be utilized by the SAS for its operations. The SAS synchronizes with the necessary FCC databases at least once every 24 hours by default to pull the latest updates and ensure the accuracy of the data in the SAS database. The FCC databases included in this daily synchronization are the EAS and ULS.[58] The synchronization rate is configurable to occur more frequently, if necessary.

Further, consistent with section 96.66(a)(2), the Federated Wireless SAS acquires and stores SMLA notification information and synchronizes this information, including information about the expiration, extension, or termination of leasing arrangements, with the Commission databases at least once per day.[59]

Beyond FCC sources, the Federated Wireless SAS interfaces with other sources to acquire data related to census tracts and the Canadian and Mexican borders for use in the SAS's administration of the CBRS.

Further information regarding Federated Wireless's database information and synchronization process can be found in Appendix 5: Database Information.

8. Exclusion Zone and Protection Zone

Consistent with sections 96.15(a)(3) and 96.53(e),[60] the boundaries of several Exclusions Zones are maintained for protection of federal Incumbent Users. In particular, Exclusion Zones are

[58] Not all Commission databases are subject to the requirement for daily synchronization. Additional databases the Federated SAS connects to, and the associated policies regarding synchronization, are listed in Appendix 5: Database Information.

[59] *See* 47 C.F.R. § 96.66(a)(2).

[60] 47 C.F.R. §§ 96.15(a)(3), 96.53(e).

maintained along the coastline,[61] around federal radiolocation sites,[62] and an 80 km radius around the federal radiolocation sites listed in 47 C.F.R §§ 90.1331, 2.106, US 109.

Consistent with section 96.15,[63] the Commission may temporarily extend or modify Exclusion Zones and Protection Zones to protect temporary operations by federal Incumbent Users. Such modifications will be communicated to the SAS, along with the expiration date and time of any modification. Given this requirement, the SAS will maintain:

- Original Exclusion Zones;
- Modified Exclusion Zones; and
- Expiration Date and Time of Modified Exclusion Zones.

Upon expiration of the modified Exclusion Zone, the SAS-enforced Exclusion Zone will revert back to the original Exclusion Zone. In accordance with section 96.15,[64] Exclusion Zones shall be converted to Protection Zones once ESCs are approved by the Commission.

Further information regarding Federated Wireless's database information related to Exclusion Zones and Protection Zones can be found in Appendix 5: Database Information.

9. Federal Data and Transmissions

Federated Wireless affirms that, consistent with section 96.55,[65] the SAS will only retain records and information or instructions received regarding federal incumbent transmissions from the ESC in accordance with information retention policies established as part of the ESC approval

---

[61] *See* National Telecommunications and Information Administration, *3550-3650 MHz*, *available at* ntia.doc.gov/category/3550-3650-mhz (last accessed Apr. 7, 2016).

[62] *Id.*; *see also* 47 C.F.R. § 96.15(a)(3).

[63] 47 C.F.R. § 96.15.

[64] *Id.*

[65] *Id.* § 96.55.

process. Moreover, consistent with section 96.63(n)(2),[66] the SAS does not store, retain, transmit, or disclose operational information on the movement or position of any federal system or any information that reveals other operational information of any federal system that is not required to effectively operate the SAS.

Further information regarding federal data and transmissions can be found in Appendix 6: Information Retention.

10. Commission Personnel Access

Consistent with section 96.63(k),[67] the SAS is available at all times to immediately respond to requests from authorized Commission personnel for any and all information stored or retained by the SAS. This is done through a web-based GUI that allows authorized Commission users to view the information retained by the SAS. Federated Wireless employs role-based control to govern access to the SAS data through the GUI and users must create user accounts and register to access this GUI.

Verified employees of the Commission have access to view any and all data in the SAS pursuant to the Commission's oversight of the ecosystem. Commission-initiated modifications or changes to the data in the database must be conveyed to Federated Wireless according to the SAS Error Resolution and Interference Reporting Policy.[68] Additionally, Commission users may view spectrum availability at particular locations via this interface. Further information regarding the how data is exposed to Commission personnel can be found in Appendix 4: Access Protocols and Procedures.

---

[66] *Id.* § 96.63(n)(2).

[67] *Id.* § 96.63(k).

[68] *See infra* Appendix 7.

Commission users will also be provided access to an operational dashboard for the SAS that will provide real-time information regarding the operational status of the SAS and SAS subsystems, as well as Federated Wireless-defined performance metrics related to the cloud hosting platform (*e.g.*, compute, data and storage, networking, identity and access management, etc.).

11. Public Data Availability

Consistent with sections 96.55(a)(3) and 96.63(j),[69] the SAS makes non-federal, non-proprietary CBSD registration information available to the general public, with the identities of the licensees obfuscated. This is accomplished through a web based GUI that allows users to view the information retained by the SAS, according to that user's role-based access privileges. Federated Wireless employs role-based control to govern access to the SAS data through the GUI, and all users must create user accounts with the SAS and register to access this GUI.

Further information regarding the how data is exposed to general public users can be found in Appendix 4: Access Protocols and Procedures.

C. SAS INTERFACES

Federated Wireless has established and will follow protocols and procedures sufficient to ensure that all communications and interactions between the SAS, ESC, and CBSDs are accurate and secure and that unauthorized parties cannot access or alter the SAS or the information transmitted from the SAS to CBSDs. The Federated Wireless SAS will have the following major external interfaces:

- CBSD / CBSD-Proxy Interface;
- SAS-SAS Interface;

[69] 47 C.F.R. §§ 96.55(a)(3), 96.63(j).

- SAS-ESC Interface;
- Government Database Interface;
- SAS Management Interface (Administrative);
- Third Party Interface (FCC, Public, Protected Incumbent); and
- Informing Incumbent Interface.

All interfaces will implement standard-specified or best industry practice security mechanisms for secured communications between the Federated Wireless SAS and external entities. In compliance with section 96.63 (n)(1),[70] there is no interface that will enable "connectivity to any military or other sensitive federal database or system, except as otherwise required by this part." The remainder of this Section describes the design of these interfaces in more detail.

1. CBSD / CBSD-Proxy Interface

This interface implements the open, public standard for SAS-CBSD communications and SAS-CBSD Proxy communications being defined in the WINNF, where the proxy is used to facilitate communications with collections of CBSDs.[71] These protocols encode data with JSON and communicate the encrypted data via HTTPS Public Key Infrastructure ("PKI") to mutually authenticate the SAS, CBSD, or proxy. This protocol enables device authentication and communications encryption to ensure unauthorized parties cannot alter the information transmitted between SAS and CBSD.

These protocols support the following features:

[70] *Id.* § 96.63.(n)(1).

[71] *See* WINNF SAS-CBSD Protocol.

- Device Registration including all fields required under sections 96.39, 96.43, and 96.45,[72] along with other industry-specified fields.

- Device Registration confirmation wherein the SAS informs the CBSD if registration was successful or failed for a specified reason, *e.g.*, use of an unapproved FCC ID.

- Spectrum Inquiry wherein the SAS can confirm to a CBSD whether frequencies are available at the CBSD's location.

- Frequency / Power Assignment wherein the SAS communicates to a CBSD the available and appropriate channels / frequencies consistent with the information provided by the CBSD and the rules of Part 96.

- Spectrum Usage Confirmation wherein the SAS communicates to the CBSD which frequencies will be utilized when the SAS grants a range of frequencies.

- Signal Level Reporting wherein the SAS receives information from a CBSD regarding received signal strength in its occupied frequencies and adjacent frequencies, received packet error rates or other common standard metrics of interference for itself and associated End User Devices as directed by an SAS.

- Rapid Channel Evacuation on ESC events wherein the SAS directs a CBSD to shut down or move to another available frequency in response to information received from the ESC and the CBSD confirms to the SAS that such actions have been taken. This is facilitated via a HeartBeat message wherein the CBSD must renew its spectrum grant with the SAS at intervals of less than one minute or relinquish the spectrum authorization and cease transmissions.[73]

2. Verification of CBSD Communication

In compliance with the WINNF SAS-CBSD protocol,[74] the SAS implements the following procedures to verify that a CBSD can properly communicate with the SAS and remains in contact with the SAS.

- Protocol Version Verification - The SAS informs the CBSD via an error code that the protocol version is not supported by the SAS.

[72] 47 C.F.R. §§ 96.39, 96.43, 96.45.

[73] The HeartBeat Message is specifically designed to enable the SAS to confirm suspension of a CBSD's operation or location to another frequency consistent with section 96.15(b)(4).

[74] WINNF SAS-CBSD Protocol.

- Data Field Error Trapping - Via various error codes defined in the protocol, the SAS informs the CBSD that required data is missing or otherwise in error.

- HeartBeat Timeout Detection - The SAS detects that the timing of regular communication between CBSD and SAS is outside of acceptable bounds. When communications persists, the SAS informs the CBSD of this issue via an error code and corrective action is taken.[75]

3. SAS-SAS Interface

The SAS-SAS Interface implements the protocol for SAS to SAS Exchange being defined by the WINNF.[76] The protocol enables the SAS to exchange information as required by Part 96 to facilitate access to the band by CBSDs connected to other SASs, coordinate operations between and among such CBSDs, provide a stable radio frequency environment for PAL licensees, and other functions required for orderly spectrum administration and the fulfillment by the SAS of its responsibilities under Part 96.

The interface exchanges JSON data objects communicated via HTTPS with PKI used for mutual authentication. This protocol enables device authentication and communications encryption to ensure unauthorized parties cannot alter the information transmitted between SASs while also facilitating broad applications and easy adoption.

Several message classes are supported by the protocol and include all exchange data required to implement Part 96 requirements, including the following:

- SAS Administrator - SAS Administrator contact and FCC certification information.

- SAS Implementation - Public Key, FCC certification information and associated ESC Implementation information of a SAS implementation instance.

- ESC Operator - ESC Operator contact and FCC certification information.

---

[75] If communication does not persist, whereupon the CBSD cannot receive an affirmative response from the SAS regarding spectrum management, it is to cease transmission, but this is a CBSD function.

[76] *See* WINNF Interim SAS-SAS Protocol.

- ESC Implementation - Public Key and FCC certification information of an ESC implementation instance.

- CBSD Domain Proxy - contact information, FCC certification information, and Public Key of CBSD Domain Proxy implementation instance.

- CBSD Device Type - device manufacturer, contact information, FCC certification information, and device characteristics (*e.g.*, air interface and antenna data) of a specific type of CBSD devices.

- CBSD Record - Public Key, installation parameters, and operational parameters (*e.g.*, spectrum grants) of a CBSD registration record.

- CBSD Operator - contact information of a CBSD operator and a copy of a retained acknowledgement by the operator that it understands the risk of possible interference from federal Incumbent User radar operations in the band in compliance with section 96.55(e).[77]

- Incumbent - data relevant to federal and non-federal Incumbent User protection, *e.g.*, protection contours or operational parameters.

- Zones - data that conveys relevant geographic area description data (*e.g.*, service area, Exclusion Zone, Protection Zone) described in GeoJSON.[78]

- Professional Installer - contact and FCC certification information of a CBSD professional installer.

- Coordination Event - a specified area with associated creation and expiration times, description, geographic boundaries, and other relevant data used to facilitate coordinated SAS action for exceptional events (*e.g.*, interference events, FCC or Presidential directives).

4. ESC Interface

The ESC Interface enables the SAS to communicate with the Federated Wireless ESC to obtain information about federal Incumbent User transmissions. Other components in the SAS are used to determine allowable spectrum parameters (Cognitive Engine) and to instruct CBSDs to

[77] 47 C.F.R. § 96.55(e).

[78] GeoJSON is an open standard format used to represent simple geographical features, along with their non-spatial attributes, and is based on JSON.

move to another frequency range or cease transmissions (CBSD / CBSD Proxy Interface) when federal Incumbent User operations are detected.

The interface exchanges JSON data objects communicated via HTTPS with PKI used for mutual secure authentication. This protocol enables mutual authentication and communications encryption to assure unauthorized parties cannot alter the information transmitted between SASs

Further details of the Federated Wireless ESC Interface are included in Appendix 16: Environmental Sensing Capability.

5. Government Database Interface

This interface is used to regularly acquire and store in the SAS the necessary and appropriate information from the Commission's databases, including valid FCC ID lists, PAL assignments. The interface is also used to synchronize the Federated Wireless SAS at least every 24 hours with the Commission databases to ensure the SAS database reflects any newly licensed facilities or any changes to currently licensed facilities. Accessed FCC databases include ULS, EAS, IBFS, and other FCC-hosted data relevant to Part 96 (*e.g.*, PAL auction results).

Data that may be hosted on other relevant government systems or websites are also processed via this interface including:

- The U.S. Census Bureau for census tract data;
- The National Oceanographic and Atmospheric Administration ("NOAA") for maritime boundaries; and
- NTIA for Exclusion Zone boundaries.

6. SAS Management Interface (Administrative)

This interface allows authorized Federated Wireless users to perform management and maintenance tasks of the SAS, *e.g.*, cloud administration, logging, application monitoring, versioning, and software patches.

7. Third Party Access Interface

This interface provides access for authenticated third parties to query the SAS about data in the database, perform spectrum inquiries, and report errors in the database. This is provided via REST APIs presented via web-based GUIs. As described in Appendix 4: Access Protocols and Procedures, the following different classes of users are given different degrees of access to the database:

- General Public;
- Authorized Commission Personnel;
- Owners of CBSDs or CPIs; and
- Non-federal incumbent System Operators.

8. Informing Incumbent Interface

Federated Wireless can be contacted by federal government entities, including the President of the United States or a designee, on a 24/7 basis. Both a phone number and email address that reach the relevant Federated Wireless employees are provided on the Federated Wireless webpage.[79] For immediate response, government entities should contact Federated Wireless via the provided phone number. Calls to this phone number are broadcasted to the Network Operations Center ("NOC") manager and a designated support engineer to ensure there is always someone available to respond to these requests. Further information on the access procedures related to this interface are provided in Appendix 4: Access Protocols and Procedures.

Upon request, Federated Wireless will also develop a dedicated GUI as an Informing Incumbent Interface. Information entered via the GUI will be immediately transmitted to the NOC

[79] Contact information for Federated Wireless' headquarters location is found at http://www.federatedwireless.com/contact/.

for response. Consistent with the access procedures provided in Appendix 4: Access Protocols and Procedures, the GUI would be accessible by authenticated users only.

9. Commission Enforcement Instructions

While the Third Party Interface with Commission login supports Commission review of the Federated Wireless SAS database information and spectrum availability, the Commission should use either the phone number or email address provided on the Federated Wireless webpage to issue an enforcement instruction directly to the Federated Wireless SAS. Calls to this phone number are broadcasted 24/7 to key personnel responsible for the operation of the SAS and ESC, including the NOC manager and a designated support engineer, assuring there is always someone available to respond to these requests. This will allow the Commission to reach the relevant Federated Wireless employees on a 24/7 basis.

Upon request, Federated Wireless will also develop a dedicated GUI for receiving Commission enforcement instructions. Information entered via the GUI will be immediately transmitted to the NOC for response. Consistent with the access procedures provided in Appendix 4: Access Protocols and Procedures, the GUI would be accessible by authenticated users only.

10. Connectivity to Military or Other Sensitive Federal Databases

In compliance with section 96.63(n)(1), there is no interface that will enable "connectivity to any military or other sensitive federal database or system, except as otherwise required by this part."[80]

[80] 47 C.F.R. § 96.63(n)(1).

D. SPECTRUM AVAILABILITY AND PROTECTIONS

Required functions of the SAS to determine spectrum availability and to provide incumbent protections are provided in Part 96, Subpart F of the Commission's rules. Specifically, sections 96.53(a) through 96.53(k), section 96.53(m), and section 96.66 address the SAS's responsibility with regard to spectrum management, incumbent protection, PAL protection, and PAL SMLAs. Moreover, section 96.59 provides additional detail on the SAS's obligations in making frequency assignment .

According to section 96.53, the purpose and the required functionality of the SAS includes:

(a) To enact and enforce all policies and procedures developed by the SAS Administrator pursuant to section 96.63.

(b) To determine and provide to CBSDs the permissible channels or frequencies at their location.

(c) To determine and provide to CBSDs the maximum permissible transmission power level at their location.

(d) To register and authenticate the identification information and location of CBSDs.

(e) To retain information on, and enforce, Exclusion Zones and Protection Zones in accordance with sections 96.15 and 96.17.

(f) To communicate with the ESC to obtain information about federal Incumbent User transmissions and instruct CBSDs to move to another frequency range or cease transmissions.

(g) To ensure that CBSDs operate in geographic areas and within the maximum power levels required to protect federal Incumbent Users from harmful interference, consistent with the requirements of sections 96.15 and 96.21.

(h) To ensure that CBSDs protect non-federal Incumbent Users from harmful interference, consistent with the requirements of section 96.17 and 96.21.

(i) To protect PAL users from interference caused by other PALs and from GAA users, including the calculation and enforcement of PAL Protection Areas, consistent with section 96.25.

(j) To facilitate coordination between GAA users operating Category B CBSDs, consistent with section 96.35.

(k) To resolve conflicting uses of the band while maintaining, as much as possible, a stable radio frequency environment.

(l) To ensure secure and reliable transmission of information between the SAS and CBSDs.

(m) To protect GWBLs consistent with section 90.1307, 90.1338, and 96.21.

(n) To implement the terms of current and future international agreements as they relate to the Citizens Broadband Radio Service.[81]

(o) To receive reports of interference and requests for additional protection from Incumbent Access users and promptly address interference issues.

According to section 96.59, a SAS must support or perform the following functions related to frequency assignment:

(a) An SAS must determine the available and appropriate channels/frequencies for CBSDs at any given location using the information supplied by CBSDs, including location, the authorization status and operating parameters of other CBSDs in the surrounding area, information communicated by the ESC, other SASs, and such other information necessary to ensure effective operations of CBSDs consistent with this part. All such determinations and assignments shall be made in a non-discriminatory manner, consistent with this part.

(1) Upon request from the Commission or a CBSD, an SAS must confirm whether frequencies are available in a given geographic area.

(2) Upon request from the Commission, an SAS must confirm that CBSDs in a given geographic area and frequency band have been shut down or moved to another available frequency range in response to information received from the ESC.

(3) If an SAS provides a range of available frequencies or channels to a CBSD, it may require that CBSD to confirm which channel or range of frequencies it will utilize.

(b) Consistent with the requirements of section 96.25, an SAS shall assign geographically contiguous PALs held by the same Priority Access Licensee to the same channels in each geographic area, where feasible. The SAS shall also assign multiple channels held by the same Priority Access Licensee to contiguous frequencies within the same License Area, where feasible.

(c) An SAS may temporarily assign PALs to different channels (within the frequency range authorized for Priority Access use) to protect Incumbent Access Users or if necessary to perform its required functions.[82]

---

[81] *Id.* § 96.53.

[82] *Id.* § 96.55.

Federated Wireless has implemented and will further implement protocols and procedures sufficient to ensure efficient spectrum management that protects all federal and non-federal Incumbent Users and PAL users, while also making efficient allocations of the spectrum for GAA users.

1. Overview of Methods Employed

The Federated Wireless SAS exploits different methodologies to meet the requirements of sections 96.15 and 96.59.[83] These methodologies are described in different subsections of this proposal, and start from verification of CBSD registration parameters, including CBSD category, and matching that with maximum power supported, CBSD antenna height, and other physical antenna characteristics such as antenna gain, downtilt, azimuth, etc.

The SAS will enforce Exclusion Zones and Protection Zones as transmitted to the SAS by the Federated Wireless ESC network, and will use information from the FCC's ULS database, as well as the location of FSS earth stations and GWBL sites registered to the SAS, to provide the required protection from aggregate interference from CBSDs operating in the 3550-3700 MHz band.

Further information related to the processes and methods applied to determine spectrum availability and provide protections to designated users are provided in Appendix 13: Registration, Appendix 12: CBRS Measurement Report, Appendix 16: Environmental Sensing Capability, Appendix 11: PAL Channel Assignment Plan, Appendix 10: Commercial FSS Incumbent and Grandfathered Wireless Service Protections, Appendix 9: Engineering Definition of Use, and Appendix 8: SAS Channel Availability.

---

[83] *Id.* §§ 96.15, 96.59.

2. Determination of Nominal Maximum CBSD Power Levels

Section 96.41 specifies the maximum power levels for EUDs and different CBSD categories and usage models.[84] Table 1 summarizes the FCC's prescribed maximum power levels.

Table 1. CBRS Power limits

Device	Max EIRP (dBm/10 MHz)	Max PSD (dBm/MHz)
End User Device	23	N/A
Category A CBSD	30	20
Category B CBSD	47	37

As Table 1 illustrates, the maximum EIRP for EUDs, regardless of their channel bandwidth, is 23 dBm. For Category A CBSDs, the maximum EIRP is 30 dBm for a 10 MHz channel bandwidth. If another channel bandwidth is used, the maximum power spectral density of 20 dBm/MHz is used to determine the maximum EIRP. For example, if the transmission channel bandwidth is 5 MHz, the corresponding maximum EIRP is 27 dBm. For Category B devices, which are limited to only outdoor operation, the same treatment described above is applied to determine the nominal maximum EIRP.

(a) Federated Wireless Solution

To satisfy the requirement of section 96.53(g) that the SAS ensure that CBSDs operate within the appropriate power limits, Federated Wireless will determine a CBSD's maximum power limits according to the CBSD category reported and verified during the CBSD registration process.[85] The CBSD reports its peak power upon requesting a spectrum grant from the SAS, and the

[84] *Id.* § 96.41.

[85] *See infra* Appendix 13.

Federated Wireless SAS then validates this reported peak power against the permitted power levels for the CBSD's category and accepts or rejects the request accordingly.

The Federated Wireless SAS uses maximum power levels in its interference calculation methodologies, which utilize an efficient and appropriate propagation model to perform PAL and GAA management. The Federated Wireless SAS also will use techniques to ensure that this aggregate interference complies with the requirements to protect federal and non-federal Incumbent Users, as described in sections 96.15 and 96.21, respectively.[86]

According to the Commission's requirements and WINNF protocols, as long as the CBSD power is below the prescribed peak power for the category, the SAS does not control the transmit power. The SAS only uses the measurement reports to evaluate the interference levels in the environment. However, Federated Wireless has proposed a potential solution for more active management of transmit power, as found in Appendix 12: CBRS Measurement Report, to assist CBSDs in using more efficient power levels.

3. Protection of Federal Incumbent Users

Section 96.15 prescribes the requirements for protecting federal Incumbent Users from harmful interference generated by CBRS operations as follows:

(a) This subsection applies only to CBSDs operating in the 3550-3650 MHz band.

> (1) CBSDs and End User Devices must not cause harmful interference to and must accept interference from federal Incumbent Users authorized to operate in the 3550-3700 MHz band and below 3550 MHz.
>
> (2) The SAS shall only authorize the use of CBSDs consistent with information on federal frequency use obtained from an approved ESC, except as provided in this section.

[86] Further treatment of protection methodologies and the aggregate interference protection thresholds currently implemented in the Federated Wireless SAS is provided in Appendix 10: Commercial FSS Incumbent and Grandfathered Wireless Service Protections.

(3) For Category A CBSDs, Exclusion Zones shall be maintained along the Coastline, as shown at ntia.doc.gov/category/3550-3650-mhz. Exclusion Zones shall also be maintained around federal radiolocation sites as set forth at ntia.doc.gov/category/3550-3650-mhz . NTIA shall notify the Commission in writing if and when the list of protected federal radiolocation sites is updated. Exclusion Zones shall be maintained and enforced until one or more ESCs are approved and used by at least one SAS, in accordance with section 96.67. Thereafter, Exclusion Zones shall be converted to Protection Zones.

(i) Category A CBSDs may be authorized by an approved SAS in geographic areas outside of Exclusion Zones before an ESC is approved.

(ii) Once an ESC is approved and used by at least one SAS, Category A CBSDs may only be authorized consistent with information on federal frequency use provided to the SAS by an approved ESC.

(iii) Category B CBSDs may only be authorized consistent with information on the presence of a signal from a federal system provided to the SAS by an approved ESC.

(4) Within 300 seconds after the ESC communicates that it has detected a signal from a federal system in a given area, the SAS must either confirm suspension of the CBSD's operation or its relocation to another unoccupied frequency, if available.

(5) The Commission will, as necessary, add or modify Exclusion Zones or Protection Zones to protect current and future federal Incumbent Users.

(6) The Commission may temporarily extend or modify Exclusion Zones and Protection Zones to protect temporary operations by federal Incumbent Users. federal Incumbent Users will coordinate with the Commission prior to the beginning of any non-emergency operation requiring additional protection. Such modifications will be communicated to the SAS along with the expiration date and time of any modification.

(b) This subsection applies to CBSDs operating in the 3650-3700 MHz band.

(1) CBSDs and End User Devices must not cause harmful interference to and must accept interference from federal Incumbent Users authorized to operate in the 3500-3700 MHz band.

(2) Exclusion Zones shall be maintained for an 80 km radius around the federal radiolocation sites listed in 47 CFR 90.1331 and 47 CFR 2.106, US 109. These Exclusion Zones shall be maintained and enforced until one or more ESCs are approved and used by at least one SAS, in accordance with section 96.67. Thereafter, Exclusion Zones shall be converted to Protection Zones.

(3) CBSDs may only be authorized within these Protection Zones consistent with information on the presence of a signal from a federal system provided to the SAS by an approved ESC, in accordance with section 96.67.

(4) Within 300 seconds after the ESC communicates that it has detected a signal from a federal system in a given area, the SAS must either confirm suspension of the CBSD's operation or its relocation to another unoccupied frequency.

4. Federated Wireless Solution

The Federated Wireless SAS will use a two-phase process to satisfy the requirements of sections 96.15(a)(1)-(3) and 96.15(b)(1)-(3).

The first phase is applied if the Federated Wireless ESC is not in operation to enable dynamic Protection Zones. Such a condition may occur if the ESC network is not yet approved for operation by the Commission or it is not operational along the coastline area to be managed by the SAS.[87] In this instance, in accordance with section 96.15(a)(3)(iii), the SAS will not authorize operation of a 3550-3650 MHz Category A CBSD within the NTIA-defined Exclusion Zones or a 3550-3650 MHz Category B CBSD operation anywhere. In accordance with sections 96.15(a)(3) and 96.15(a)(3)(i)-(ii), the SAS maintains the Exclusion Zones shown at ntia.doc.gov/category/3550-3650-mhz and those maintained around federal radiolocation sites as set forth at ntia.doc.gov/category/3550-3650-mhz. Similarly, in accordance with section 96.15(b)(2), the SAS will not authorize operation of a 3650-3700 MHz CBSD within Exclusion Zones around federal radiolocation sites listed in 47 C.F.R. § 90.1331 and 47 C.F.R. § 2.106, US109.

When a CBSD requests a spectrum grant, the Federated Wireless SAS compares the location and category of the CBSD provided through the registration procedure and, if the request complies with the requirements for Exclusion Zone protection, the spectrum request will be granted by the SAS; otherwise, the request is rejected.

The second phase exploits the Federated Wireless ESC network deployed along the coast within or near exclusion zones to detect the presence of federal Incumbent User transmissions. The

[87] The SAS will not authorize operation of CBSDs within the frequency ranges and exclusion zones established by the NTIA if those areas are not monitored by an ESC network.

details of ESC design and thresholds used to detect federal Incumbent User transmissions are explained in Sections III.D and III.F. The Federated Wireless SAS protects federal Incumbent Users in two different ways:[88]

- By controlling frequency assignment to CBSDs, described in Appendix 8: SAS Channel Availability.
- When the ESC decision system determines a federal radar is present, the SAS first requests the CBSDs to change their operation parameters using the HeartBeat Procedure.[89] The operation parameters include peak powers (to control aggregate interference to the Incumbent User), and the operation frequency bandwidth. If any other channel is available in the area, the SAS directs CBSDs in the Protection Zone to move to those channels, otherwise it expires the transmission of all CBSDs in the Protection Zone using the HeartBeat Procedure.

To meet the requirement of section 96.15(a)(4), and as illustrated in Figure 5, the HeartBeat Durations (HBD1 and HBD2) are determined such that:

$$HBD_1 > t_{SAS}$$

$$HBD_1 + t_{http} + MAX\,(HBD2,\ t_{CBSD}) < 60\ seconds$$

[88] Compliance with the requirement in section 96.15(a)(1) to protect federal Incumbent Users below 3550 MHz is presumed to be an obligation for CBSDs and EUDs. Federated Wireless will comply with SAS-related functions to protect federal Incumbent Users below 3550 MHz should they be further delineated by the Commission.

[89] *See* WINNF SAS-CBSD Protocol.

In Figure 5, HBD1 is the default value for HeartBeat Duration requested by the SAS, and HBD2 is the new HeartBeat Duration requested by the SAS after the spectrum switch or transmit expire request is reported to the CBSD. In this Figure, t_{http} is the time required for HTTP message transmission, t_{SAS} is the time required for the SAS to calculate the interference and determine the CBSDs that are required to change their operational parameter, and t_{CBSD} is the time required for the CBSD to either hand over all its associated EUDs, switch its radio to another channel, or cease operation on the ongoing channel.

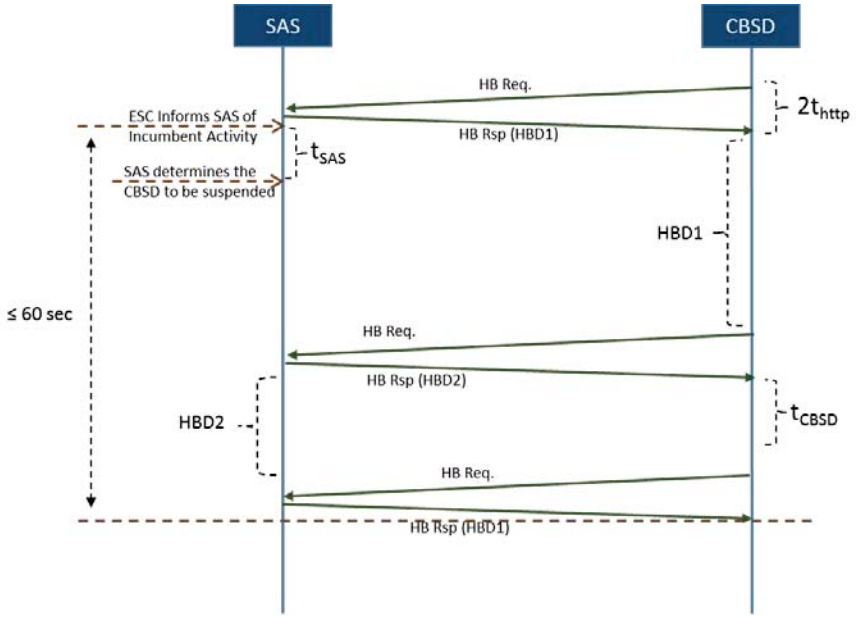

Figure 5. CBSD Suspension Time[90]

To meet the requirements of sections 96.15(a)(5)-(6),[91] the Federated Wireless SAS follows the process of Protection Zone and Exclusion Zone updates, including activation drills, as described

[90] *Id.*

[91] 47 C.F.R. §§ 96.15(a)(5)-(6).

in Appendix 5: Database Information, Appendix 6: Information Retention, and Appendix 8: SAS Channel Availability.

5. Protection of Existing FSS Earth Stations

Sections 96.17, 96.21, and 96.53(h) of the Commission's rules require the Federated Wireless SAS to protect FSS earth stations authorized to operate in the 3600-3700 MHz band and FSS earth stations responsible for critical telemetry, tracking, and control ("TT&C") operations in the 3700-4200 MHz band. FSS earth stations authorized for protection in accordance with the Commission's rules are listed at fcc.gov/cbrs-protected-fss-sites. To provide FSS protection and satisfy section 96.55, the Federated Wireless SAS maintains in its database the geographic locations and configuration of protected FSS earth stations.[92]

In accordance with section 96.21(c), the Federated Wireless SAS shall protect grandfathered 3650-3700 MHz FSS earth stations according to existing protection criteria in Part 90, subpart Z of the Commission's rules until the last GWBL's license expires within the protection area defined for a particular grandfathered FSS earth station. Specifically, the SAS will create a protection area of 150 km surrounding the grandfathered 3650-3700 MHz FSS earth station. While there are unexpired GWBL licenses in this protection area, the SAS will prohibit 3650-3700 MHz CBSD transmissions in this protection area and ensure the section 96.17(a)(3) blocking requirement is satisfied for any 3550-3650 MHz CBSD assignments within 40 km of the grandfathered 3650-3700 MHz FSS earth station.

In accordance with the requirements of section 96.17(a), the SAS will also protect other registered FSS earth stations licensed to operate in the 3600-3700 MHz and requiring SAS protection by ensuring the section 96.17(a)(2) co-channel and section 96.17(a)(3) blocking

[92] *See infra* Appendix 5.

requirements are satisfied. Further, the SAS will protect registered 3700-4200 MHz FSS earth stations used for satellite TT&C operations by ensuring the section 96.17(b)(1) out-of-band emissions ("OOBE") and section 96.17(b)(2) blocking requirements are satisfied.

The SAS uses aggregate interference calculations to satisfy the co-channel, blocking, and OOBE limits provided in section 96.17 for each protected FSS earth station. Co-channel calculations, applied to 3600-3700 MHz FSS earth stations, are performed over all co-channel CBSDs within 150 km of the FSS earth station and ensure that the aggregate passband RF power spectral density at the output of a reference RF filter at the FSS earth station does not exceed a median root mean square ("RMS") value of -129 dBm/MHz. Co-channel calculations will be performed across the bandwidth listed at fcc.gov/cbrs-protected-fss-sites for a specific 3600-3700 MHz FSS earth station.

The blocking calculations, applied to 3600-4200 MHz FSS earth stations, are performed over all CBSDs within 40 km of the FSS earth station. The SAS ensures that the aggregate RF power at the output of the reference RF filter at the FSS earth station does not exceed a median RMS value of -60 dBm. Blocking calculations are performed by integrating the CBSD interference over the bandwidth extending from the reference RF filter passband lower edge minus 150 MHz to the passband upper edge plus 150 MHz.

OOBE calculations are performed for each 3700-4200 MHz FSS earth station requiring SAS protection. The OOBE from all CBSDs within 40 km of the 3700-4200 MHz FSS earth station are SAS controlled such that the aggregate passband RF power spectral density at the output of a reference RF filter at the FSS earth station does not exceed a median RMS value of -129 dBm/MHz. OOBE calculations will be performed across the bandwidth listed at fcc.gov/cbrs-protected-fss-sites for the specific 3700-4200 MHz FSS earth station.

The Federated Wireless SAS uses the ITM for propagation modeling in FSS protection calculations. The ITM is used to generate the statistics of the path loss between each CBSD device and FSS earth station. In addition, the Federated Wireless SAS calculates the antenna gain of the FSS earth station in the direction of each CBSD using the antenna patterns described in sections 25.2091(a)(1) and 25.209(a)(4). In scenarios where multiple SASs control CBSDs that interfere with an FSS earth station, these SASs use a WINNF-defined procedure over the SAS-SAS interface to negotiate individual aggregate interference power spectral densities and blocking levels such that, across SASs, the co-channel, blocking, and OOBE requirements are satisfied.

6. Enforcing Current and Future International Agreements

Section 96.19 requires that CBRS operations in the 3550-3700 MHz band are subject to existing and future international agreements with Mexico and Canada.[93] At present, there are no agreements between the U.S. and Mexico or Canada with regard to operations in the 3550-3650 MHz band. However, there are agreements regarding operations in the 3650-3700 MHz band. As a result, the current Federated Wireless implementation of the SAS extends the provisions of the existing 3650-3700 MHz agreements to the entire CBRS spectrum band. In keeping with this approach, the Federated Wireless SAS will ensure that all CBSDs are located at least 8 kilometers from the U.S.-Canada or U.S.-Mexico border if the antenna of that CBSD looks within the 160° sector away from the border. CBSDs must be located at least 56 kilometers from each border if the CBSD antenna looks within the 200° sector towards the border. The Federated Wireless SAS will ensure that all CBSDs will comply with the requirements of any future agreements with Canada and Mexico regarding operation in U.S.-Canada and U.S.-Mexico border areas.

[93] *Id.* § 96.19.

7. Protection of Existing Operators in the 3650-3700 MHz Band

As specified by sections 96.21 and 96.53(m), the Federated Wireless SAS is required to protect GWBL devices in the 3650-3700 MHz band.[94] To provide this protection and satisfy Section 96.55, the SAS maintains in its database GWBL device information as described in Appendix 5: Database Information.

The SAS methodology for GWBL device protection is similar to that described above for FSS earth station protection. In particular, the Federated Wireless SAS will ensure that the aggregate interference from CBSD transmissions is less than a specified threshold at each GWBL device in the SAS's database.

Final rules to optimize protections for GWBL device protection are still under consideration. Federated Wireless will implement and comply with the Commission's final rules, as well as any further requirements or standards developed through the WINNF. The GWBL device protection methodology described here reflects the current implementation in the Federated Wireless SAS.

8. Protection of PAL Operations

To facilitate development of the CBRS, the WINNF developed a baseline common and simple band plan, WINNF-15-I-0137, that complies with Part 96.[95] This band plan can be summarized as follows:

- Ten contiguous 10 MHz channels, numbered 1-10, are defined as available for PAL assignment from 3550 MHz to 3650 MHz.
- Of these ten channels, up to seven can be allocated for PAL use by the auction.

---

[94] *Id.* §§ 96.21, 96.53(m).

[95] WINNF-15-I-0137 is a working document in the WINNF and has not yet been released publicly.

As described in more detail in Appendix 11: PAL Channel Assignment Plan, Federated Wireless recommends that post-auction, a third party will use a program to translate these PAL auction results into Owner Areas ("OAs") such that PALs held by the same PAL licensee are contiguous geographically (section 96.25(b)(1)(i)) and contiguous in channels (section 96.25(b)(2)(i)). This plan may be updated, may also define contingency allocations, and may consider additional objectives.[96]

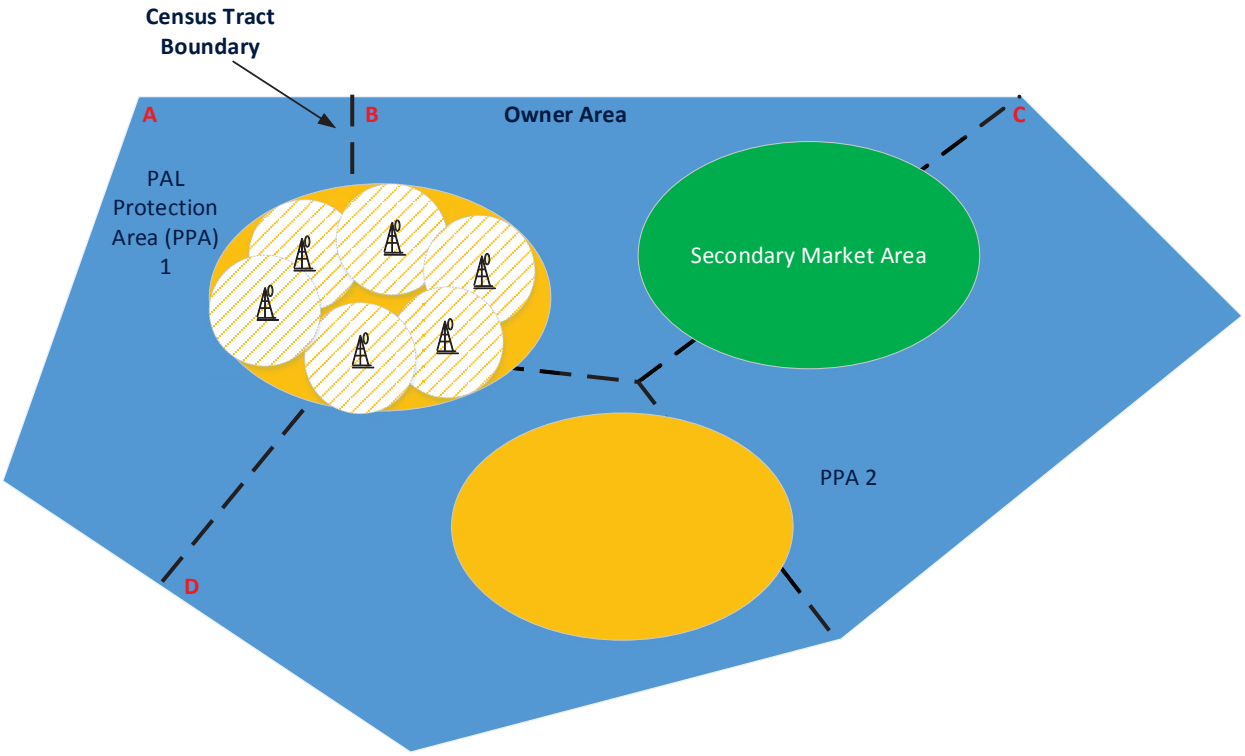

Figure 6. Owner Area, Operating Area, and Secondary Market Area ("SMA") Definition

Consistent with section 96.25(c), channels not in use by a PAL operator are available for GAA use and are thus not protected. As described in more detail in Appendix 9: Definition of Use and Secondary Markets, Federated Wireless currently envisions that a PAL operator will indicate a

[96] *See infra* Appendix 8.

desire to use a channel when a PAL CBSD makes a Spectrum Grant Request to the Controlling SAS for that OA.

The PAL owner can establish SMLAs with other entities ("Lessees") for all or a portion of the owner's assigned bandwidth and all or a portion of the OA. The leased geographic areas are denoted Secondary Market Areas ("SMAs"). In accordance with section 96.66, the SAS will verify that the Lessee is certified, that the lease will not result in the Lessee holding more than 40 MHz of Priority Access spectrum in the SMA, and that the SMA is within the OA and outside all PAL Protection Areas ("PPAs"). After this verification, the SAS will confirm notification and verification with the owner and Lessee. The Controlling SAS will then use the SAS-SAS interface to communicate the SMAs with other SASs. The Controlling SAS will also send the Commission a daily report of all leasing notifications.

The SAS will estimate PPAs based on the Engineering Definition of Use criteria detailed below, subject to revision pending further guidance from the Commission or Wireless Innovation Forum ("WINNF"). Use will be defined similarly in SMAs, establishing SMA-PPAs.

When a CBSD begins the registration process, the Controlling SAS determines the CBSD parameters needed for channel assignment and the CBSD PAL credentials via the WINNF-defined SAS-CBSD Protocol[97]. Then, upon a Spectrum Inquiry or Grant Request, the Controlling SAS will calculate the area over which the grant-candidate CBSD's transmissions would provide a signal of -96 dBm or larger following the propagation modeling methodology in the NTIA 3.5 GHz Report or any possible propagation model prescribed by WINNF or the FCC. The Controlling SAS will use the calculated coverage area and the grant-candidate CBSD's PAL credentials to determine the outer limit of the potential PPA change due to transmissions from the grant-candidate CBSD.

---

[97] *See* WINNF SAS-CBSD Protocol

Specifically, the Controlling SAS will update its outer limit PPA calculations by taking the intersection of the individual -96 dBm CBSD coverage areas and applying an algorithm to rationalize the PPA by including areas associated with model-predicted coverage holes. A PAL CBSD can then be assigned a frequency if the resulting PPA is inside the OA and does not violate any SMA boundary and overall PAL and incumbent protection is maintained. PAL licensees may choose to self-report protection contours smaller than the SAS-computed outer-limit. If so, the SAS will protect the smaller, self-reported area as a PPA.

Any CBSD that does not make contact with the SAS for seven days shall not be considered in use and will be excluded from the calculation of the PPA until such time as contact with the SAS is reestablished. The PPA will also be adjusted if the PAL licensee informs the SAS that a previously activated CBSD is no longer in use.

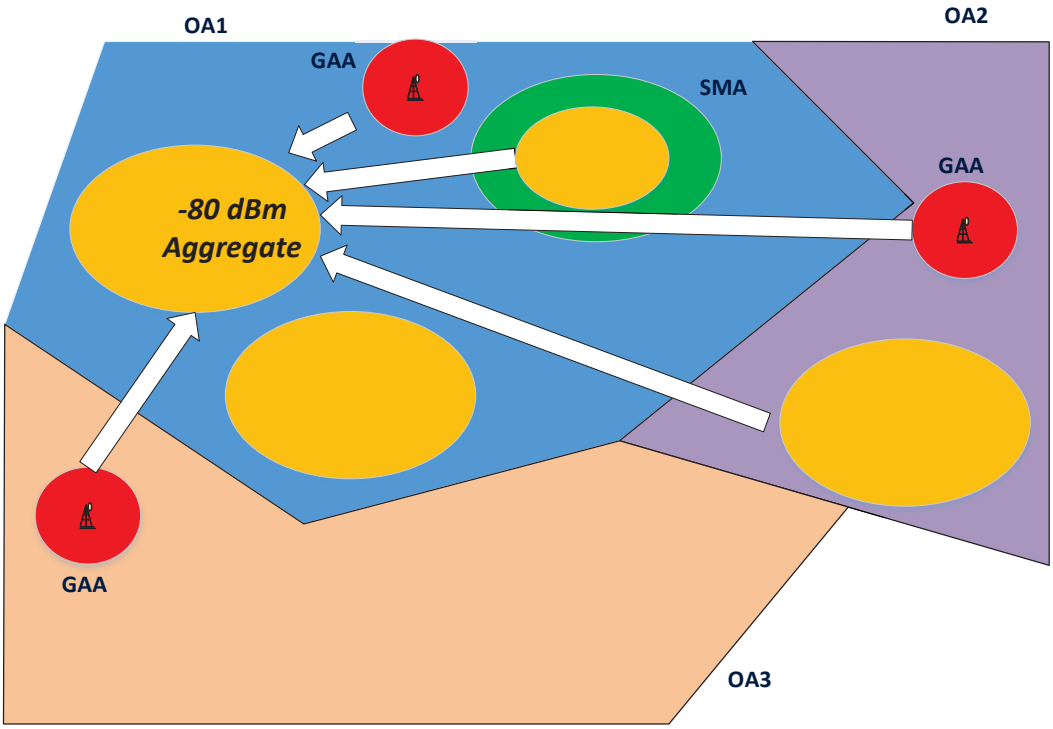

Figure 7. PPA Protection/Allowance of GAAs

Consistent with section 96.41(d)(1) and as shown in Figure 7, the SAS manages CBSDs such that the aggregate received signal strength, measured at any location within any co-channel PPA or SMA-PPA, will not exceed an average (RMS) power level of -80 dBm in any direction when integrated over a 10 MHz reference bandwidth, with the measurement antenna placed at a height of 1.5 meters above ground level, unless the affected PAL licensee agrees to an alternative limit and communicates that alternative limit to the Controlling SAS.[98] Note that because the PAL Channel Assignment Plan ensures that geographically adjacent PALs held by the same PAL licensee are

[98] *See* 47 C.F.R. § 96.41(d)(1).

grouped into the same OA, and because PPAs are allowed to cross census tract boundaries (while remaining within a single OA), this approach also assures satisfaction of section 96.41(d)(2).[99]

As described in more detail in Appendix 9: Definition of Use and Secondary Markets, a possible method to allocate interference contribution from CBSDs under control of multiple SASs is to fractionally apportion the interference margin among the SAS Administrators managing CBSDs within interfering range of the PPA or SMA-PPA (called the PPA Interference Region). This apportionment strategy ensures that each SAS can independently manage their CBSDs to individually identifiable thresholds while the PAL operations are protected to the desired aggregate interference level. For instance, with two SAS Administrators managing devices in a PPA's Interference Region, each Administrator could manage its own CBSDs to ensure that the aggregate interference from its own CBSDs does not exceed -83 dBm within the PPA or SMA-PPA. As a result, the combined aggregated interference from the total population of CBSDs, under the control of the two SASs, will not exceed -80 dBm.

9. Confirmation of Spectrum Availability

To meet the requirements of section 96.59(a)(1) stated above, the Federated Wireless SAS will provide the list of available channels in any geographical area to the FCC and a requesting CBSD.[100]

The Federated Wireless SAS maintains several databases created by accessing FCC, NTIA and other government records. These databases include details on non-federal Incumbent Users, boundaries (*e.g.*, census tracts, international), owners, PALs, CBSDs, and secondary markets. To

[99] *Id.* § 96.41(d)(2); *see also infra* Appendix 11.

[100] *Id.* § 96.59(a)(1).

meet the section 96.59(a)(1) requirement, the Federated Wireless SAS principally uses the following six sources of information:

- FCC PAL database, providing the list of auctioned PAL channels in each area;
- The PPA according to the FCC's "Engineering Definition of Use" listing channels being used by PAL licensees in areas smaller than census tracts;
- The database of CBSDs, and their granted channels, registered with the Federated Wireless SAS and their granted channels;
- A database including the GAA channels assigned in each area;
- The list of CBSDs and allocated channels provided through SAS-SAS exchange; and
- SMLAs provided by PAL licensees or through SAS-SAS exchange.

Using these sources, the Federated Wireless SAS will respond to any request from the FCC about the available channels.

To respond to CBSD spectrum requests, the Federated Wireless SAS will implement the Spectrum Inquiry Procedure defined in the WINNF SAS-CBSD Protocol.[101] After successful registration of the CBSD, it can request the SAS to provide the information about available spectrum. The CBSD can later decide operational parameters for a grant request. Because a CBSD might have multiple simultaneous grants, it can send this Spectrum Inquiry Request even when it is in Granted or Transmission state and has an ongoing grant.

The SAS performs an assessment of channel availability for the frequency ranges indicated in the Spectrum Inquiry Request. If the request succeeds, the Federated Wireless SAS sends a spectrum Inquiry Response, including the list of available channels and their types (PAL or GAA).

[101] *See* WINNF SAS-CBSD Protocol.

10. Channels in Use

To meet the requirements of section 96.59(a)(3), the Federated Wireless SAS will implement the Spectrum Inquiry Procedure and Grant Request Procedure defined in the WINNF SAS-CBSD Protocol.[102] After the CBSD is registered with the Federated Wireless SAS, it can optionally send the Spectrum Inquiry Request to obtain the available channels in a frequency range it desires. The Federated Wireless SAS will provide a Spectrum Inquiry Response.

Upon learning the available channels, the CBSD must request a grant from the SAS and the grant must be approved before the CBSD can start transmission in any frequency range within the 3550-3700 MHz band. The grant request message from the CBSD includes a contiguous frequency range requested by the CBSD, and optionally a list of credentials if the CBSD is operated in the Priority Access tier. The SAS will check the the availability of the requested frequency range, verify the PAL credentials, and determine whether the requested channels match with the PAL channel assignment procedure described in Appendix 8: SAS Channel Availability. For all or a portion of the requested channels, or frequency range(s), the SAS will respond with a grant response message granting either all or a segment of the requested frequency range. If all or a portion of the requested channels, or frequency range(s), requested cannot be allocated as a PAL channel corresponding to the list of PAL credentials, or if no PAL credentials are provided, the SAS may grant the available channel as a GAA channel or frequency range. If no segment of the requested frequency range is available, the grant request is rejected.

The CBSD cannot start transmission corresponding to a particular grant before the grant is approved and it receives at least one successful HeartBeat Response corresponding to that grant.

[102] *Id.*

11. PAL Channels

In accordance with sections 96.59(b)-(c) and 96.25, if a PAL licensee can operate in multiple census tracts that are geographically contiguous to each other, the SAS will attempt to allocate the same channel to the licensee across those census tracts.[103] Moreover, if a licensee holds more than one PAL in the same census tract, the SAS is required to allocate contiguous frequency channels to that PAL licensee in that census tract.

PAL channels must also meet the requirements of section 96.13:[104]

> (a) Each PAL shall be authorized to use a 10 megahertz channel in the 3550-3650 MHz band.
>
> > (1) No more than seven PALs shall be assigned in any given License Area at any given time.
> >
> > ***
>
> (b) The 3650-3700 MHz band shall be reserved for GWBLs and GAA Users.

The Commission has not formally defined a specific CBRS band plan, but to meet requirements of section 96.13 and to facilitate development of the CBRS, the WINNF has developed a baseline common and simple band plan, as depicted in Figure 8.

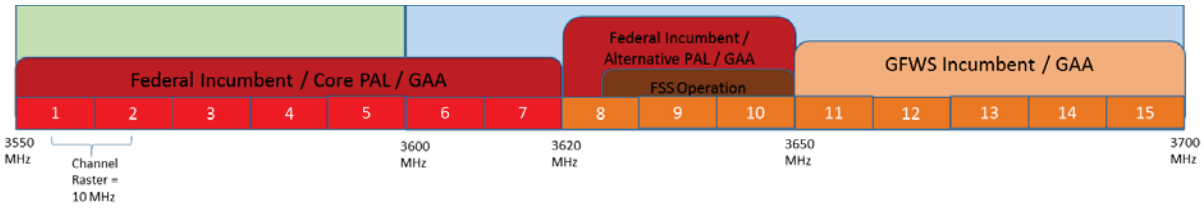

Figure 8. Proposed WINNF Band Plan

In order to meet the contiguity requirements of sections 96.59(b)-(c) and 96.25, channel assignments to PAL licensees by the SAS represent a complex integer programming problem, albeit

[103] 47 C.F.R. §§ 96.25, 96.59(b)-(c).

[104] *Id.* § 96.13.

one that nominally must be solved once every three years or after out-of-cycle Commission auctions as announced via public notice. SAS-SAS coordination to solve this problem could be complicated.

The assignment of PAL channels is performed at the conclusion of the auction and prior to the commencement of PAL use by an independent party with appropriate expertise, which is contracted by the community to solve the integer programming problem of assigning "steady-state" frequencies subject to the rules of Part 96. This entity could be selected by the FCC or a multi-stakeholder industry group such as the WINNF. The cost could be borne as an auction administrative cost or through a cost-sharing mechanism among auction winners and is expected to be nominal. PAL licensees will be given the opportunity to define additional constraints and objectives that should be considered by the third party. The details are described in Appendix 11: PAL Channel Assignment Plan.

12. Management of GAA Spectrum

Section 96.35 defines GAA requirements as follows:

(a) General Authorized Access Users shall be permitted to use frequencies assigned to PALs when such frequencies are not in use, as determined by the SAS.

(b) Frequencies that are available for General Authorized Access Use shall be made available on a shared basis.

(c) General Authorized Access Users shall have no expectation of interference protection from other General Authorized Access Users operating in accordance with this part.

(d) General Authorized Access Users must not cause harmful interference to and must accept interference from Priority Access Licensees and Incumbent Users in accordance with this part.

(e) General Authorized Access Users operating Category B CBSDs must make every effort to cooperate in the selection and use of available frequencies provided by an SAS to minimize the potential for interference and make the most effective use of the authorized facilities. Such users shall coordinate with an SAS before seeking station authorization, and make every effort to ensure that their CBSDs operate at a location, and with technical parameters, that will minimize the potential to cause and receive interference among CBSDs. Operators of CBSDs suffering from or causing harmful interference are expected to

cooperate and resolve interference problems through technological solutions or by other mutually satisfactory arrangements.[105]

The Federated Wireless SAS management of GAA spectrum includes the following components:

- SAS access to PAL database in a geographical area, and knowledge of PAL-assigned channels in the area;
- SAS access to ESC information regarding the operation of federal Incumbent Users in the frequency range of 3550-3650 MHz;
- SAS access to the location, frequency of use, and protection criteria of FSS earth stations and GWBLs;
- Registration or calculation of PPA, smaller than the census tract, according to the "Engineering Definition of Use," or SMA-PPA;
- SAS-SAS information about CBSDs registered at other SASs and their assigned channel;
- Measurement Reports received from CBSDs; and
- A GAA channel assignment mechanism in order to maximize public use of available channels in the CBRS in a fair and efficient manner, and to allow co-existence of GAA users in the same area.

13. ESC-Determined Channel Availability

To meet the requirements of section 96.53(f), the SAS communicates with the ESC through an interface to the ESC Decision System as depicted in Figure 9.[106]

[105] *Id.* § 96.35.

[106] 47 C.F.R. § 96.53(f).

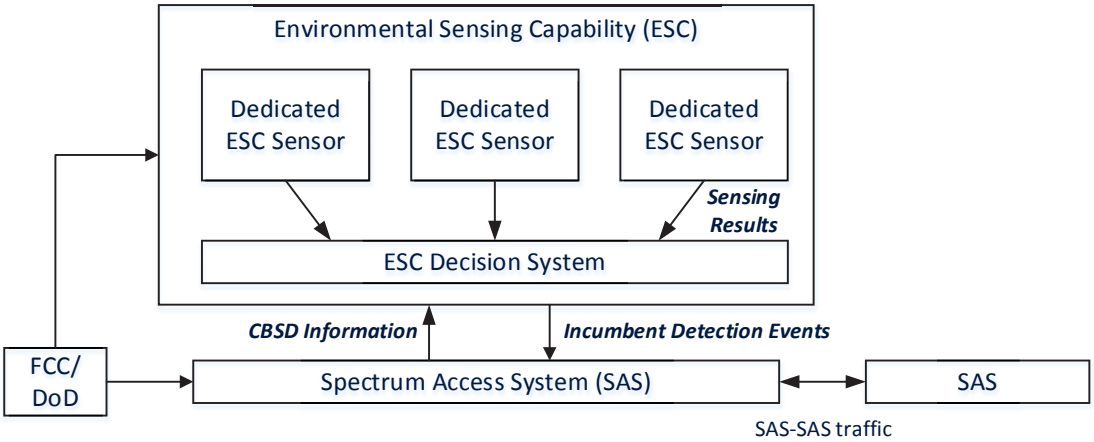

Figure 9. Federated Wireless ESC Architecture

The dedicated sensors that securely communicate with the ESC Decision System provide quantized signal strength measurements to the ESC Decision System, which uses the procedure defined in Appendix 16: Environmental Sensing Capability to detect the presence of federal Incumbent Users and activate Protection Zones as needed. It then communicates federal Incumbent User detection events to the Federated Wireless SAS, allowing the SAS to suspend CBSD operation or relocate CBSDs to frequencies unoccupied by federal Incumbent Users as necessary to prevent harmful interference to such users.

Upon receiving notification from the ESC of a federal Incumbent User detection event, the Federated Wireless SAS identifies the CBSDs located in the Protection Zone, using the corresponding frequency range(s) or channel(s), and contributing to the aggregate interference to the federal Incumbent User based on the location information received during CBSD registration procedure.[107] Using the HeartBeat Response message defined in the WINNF SAS-CBSD Protocol, the SAS will require the CBSDs to either move to another channel, by instructing a new operation parameter object in the response, or request the CBSD to suspend its transmission by expiring the

[107] *See infra* Appendix 13.

TransmitExpireTime parameter in the HeartBeat Response, or completely expiring the grant by expiring the grantExpireTime parameter in the in the HeartBeat Response.

14. GAA Access to PAL Channels

To satisfy section 96.35(a), the Federated Wireless SAS has implemented the "Engineering Definition of Use" methodology.[108] According to this requirement, if a PAL channel is not in use by the PAL licensee, the SAS may assign the channel to GAA users. This procedure entails two components. The first step is to determine the area used by the PAL licensee (or used by the Secondary Market Lessee) according to the methods detailed in Appendix 9: Definition of Use and Secondary Markets. The second step is the assignment of channels or a range of frequencies to GAA users to make sure the aggregate interference within PPAs and SMA-PPAs does not exceed -80 dBm/10 MHz.

(a) Determination of Use

Section 96.35 permits the use of PAL channels by GAA users if the channel is not used by the PAL licensee or the SMA owner in any area within the OA or SMA, as determined by the SAS.[109]

Each PAL owner will be assigned an OA, consisting of geographically contiguous census tracts, for PAL operation. The OA is equivalent to the PAL service area as defined in section 96.3.[110] The PAL owner can also establish secondary SMAs within the OA – these SMAs will be shared with all SASs, and cannot overlap with PPAs or other SMAs. The Federated Wireless SAS will determine use within the OA, or the PPA, by calculating CBSD downlink coverage. Use will be defined

[108] *Id.* § 96.35(a).

[109] *Id.*

[110] 47 C.F.R. § 96.3.

similarly in SMAs, establishing SMA-PPAs. The Federated Wireless SAS will protect PPAs and SMA-PPAs from excess interference from other PAL and GAA users. GAA authorizations can be granted outside of a PPA and SMA-PPA, as long as PPA and SMA-PPA protection is maintained.

The Federated Wireless SAS determines the CBSD parameters needed for channel assignment and the CBSD PAL credentials via the WINNF-defined procedure.[111] The SAS will first calculate the area over which the CBSD transmissions will provide a signal of -96 dBm or larger following the propagation modeling methodology in the NTIA 3.5 GHz Report or another propagation model as may be prescribed by WINNF or the FCC.[112] The SAS will use the calculated coverage area to ensure that the CBSD has appropriate PAL credentials.

If the CBSD PAL credentials are acceptable, the Federated Wireless SAS will update the outer limit of the PPAs (or, if applicable, SMA-PPAs) by taking the integration of the individual -96 dBm CBSD coverage areas and considering the contour of these areas as the outer limit of the PPA. PAL licensees may choose to self-report protection contours smaller than the outer limit. If so, SAS will protect the smaller PAL licensee self-reported area as the PPA.

(b) Assignment to GAA

In order to assign unused PAL channels outside PPAs and SMA-PPAs to GAA users, the SAS will ensure that the aggregate interference does not exceed -80 dBm within each PPA and SMA-PPA. This interference will be calculated over co-channel GAAs as well as co-channel PALs not owned by the Owner and not in the OA. Secondary Market CBSDs will be included in the interference calculation. Figure 7 depicts this concept.

---

[111] *See* WINNF SAS-CBSD Protocol.

[112] *See* NTIA 3.5 GHz Report.

15. Interference Resolution

Outside of egregiously incorrect information (*e.g.*, an attempt to register a CBSD outside U.S. borders), the first chance that a SAS will have to detect errors will be when a system experiences unexpected levels of interference. The Federated Wireless SAS can become aware of interference via the following methods:

- Error Reports specifying interference to a protected system;
- SAS-CBSD protocol Measurement Reports (for CBSDs), which can be used to autonomously infer unexpected levels of interference; and
- Interference Event Coordination Messages from other SAS Administrators via the SAS-SAS protocol.

When interference to a protected system (*i.e.*, federal Incumbent User, FSS, GWBL, PAL) has been detected or reported, the following steps are taken.

- All SAS Administrators subscribed to the interference region around the location given in the Interference Report are immediately informed of the Interference Event via the SAS-SAS protocol using a Coordination Event message. Each of these SAS Administrators will adjust their spectrum allocations for CBSDs within the interference region so that spectrum allocations return to the last known safe allocation to ensure elimination of the interference condition. This impacts CBSD co-channel and adjacent channel spectrum allocations
- The source of the interference will then be determined via a variety of offline and online methods including examining transaction and Measurement Report logs, coordinating with other SAS Administrators, performing field measurements, and other diagnostic techniques as needed. The choice of techniques will depend on the type of error encountered (*e.g.*, a malfunctioning CBSD may only be confirmable from field tests or from diagnostic spectrum allocation routines).
- When the source of the interference is determined, appropriate steps to address the interference will be taken (*e.g.*, alerting the owner of a malfunctioning CBSD, adjusting interference protection margins, updating terrain databases). The determined interference cause and corrective actions are reported back to the originator of the Interference Report (removing identifying information from any CBSDs if the originator is not granted such information access) and are logged in the Federated Wireless database. Following this resolution, the SAS's subscribed to the interference region can resume normal spectrum management operations.

The interference coordination region for FSS earth station is contained within either a 40 km or 150 km radius from the site location consistent with section 96.17 and the specific interference protection scenario considered.[113] The interference region for GWBL stations is also described in Appendix 10: Commercial FSS Incumbent and Grandfathered Wireless Service Protections.

16. Confirmation of Protection

To meet the requirements of section 96.59(a)(2), the SAS will use the WINNF-defined Heartbeat and Spectrum Relinquishment procedures[114] to confirm that CBSDs in a given geographic area and frequency band have been shut down or moved to another available frequency range in response to information received from the ESC. Following these procedures, the SAS notifies the CBSD that the assigned spectrum is no longer available for CBSD use by either suspending or terminating the CBSD grant. This notification is contained in the response sent by the SAS as part of the CBSD Heartbeat procedure.

The SAS performs this action by setting the errorCode parameter in the Heartbeat Response as SUSPENDED_GRANT or TERMINATED_GRANT. If the errorCode is set to TERMINATED_GRANT, or it is set to SUSPENDED_GRANT with a new recommended operation parameter (through the parameter OperationParam), the CBSD shall immediate cease transmitting and send a Spectrum Relinquishment for the current grant within 60s of the CBSD receipt of the Heartbeat Response. Upon the SAS reception of the Relinquish Request message, the SAS relinquishes the spectrum assigned to the CBSD and confirms that the CBSD is not interfering with the federal incumbent User.

---

[113] Specifically, section 96.17(a)(2) requires coordination for co-channel CBSDs within 150 km of an FSS earth station operating in 3600 – 3700 MHz; section 96.17(a)(3) requires coordination for all CBSDs within 40 km of an FSS earth station operating in 3600 – 3700 MHz; and section 96.17(b)(1) requires coordination for all CBSDs within 40 km of a TT&C FSS earth station operating in 3700 – 4200 MHz.

[114] *See* WINNF Interim SAS-CBSD Protocol.

If the errorCode is set to SUSPENDED_GRANT and no recommended operation parameter is included, the SAS would set the OperationStatusReq to TRUE with a small heartbeatDuration so as to receive a new Heartbeat Request from the CBSD, which confirms it has ceased transmissions using the operationState parameter.

17. Coordination Among GAA Users

The matter of GAA coordination and co-existence is complex, considering the neutrality of CBRS toward air interface technologies. As described below, Federated Wireless has implemented some elementary methods, which fully satisfy the requirements of section 96.53(j).[115] Further, Federated Wireless intends to implement additional, more advanced methods for user-optional GAA interference management.[116]

Federated Wireless uses a straightforward channel assignment methodology, in which channels are explicitly assigned to GAA users based on the availability of the channels and the aggregate interference the channel assignment may cause to the Incumbent Users, PPAs, or SMA-PPAs. The channels are assigned in consideration of the band plan depicted in Figure 8 and assuming the maximum EIRP for the category of use according to Table 2. If aggregate interference conditions cannot be satisfied, the SAS might prescribe a lower EIRP to GAA users to manage the interference to protected users.

Federated Wireless intends to implement additional, user-optional methods following LTE Self Organizing Network ("SON") management principles, to facilitate coexistence for Category B

---

[115] *Id.* § 96.53(j).

[116] GAA coordination and co-existence mechanism(s) may be developed in the WINNF, and Federated Wireless will implement such mechanisms as they are standardized.

GAA CBSDs and GAA CBSDs generally.[117] Unlike conventional SON servers, however, the Federated Wireless SAS leverages the knowledge of all CBSDs outside an operator network, and would thereby be able to consider the interference contribution of those CBSDs in configuring the operator's CBSDs. The Federated Wireless SAS can provide services comparable to those expected from SON servers, but a user can leverage the SAS's knowledge to coordinate interference management with other service providers.

(a) Facilitating Coordination between GAA Users Operating Category B CBSDs

To comply with sections 96.35(e) and 96.53(j), Federated Wireless will provide the following interference management capabilities for Category B CBSDs operating in the GAA tier through features of the CINQ XP platform.[118] Through CINQ XP's network visualization functionality, GAA CBSD operators will be provided with a real-time depiction of the shared spectrum environment, displaying a comprehensive view of CBSDs managed by the Federated Wireless SAS and other SASs. This data, in conjunction with the network planning features of CINQ XP, can be used to determine the availability of shared spectrum in a given geographic region and to see what type of interference needs to be managed outside of the SAS. The following steps can be followed to determine and manage interference:

- CINQ XP's graphical web-based user interface will expose a visual representation of assets managed by the SAS, and other SASs, showing a comprehensive view of shared assets on a map across GAAs, PALs, and incumbents. Users can select a specific geographic region to see the CBSDs being managed within the region.
- CINQ XP's network planning functionality will produce a network plan with optimal CBSD placements considering the unique constraints and requirements for CBRS operation. The user may also specify a desired network plan based on desired CBSD locations and configurations.

---

[117] *See* H. Hu, J. Zhang, et al., Self-Configuration and Self-Optimization for LTE Networks, IEEE Communications Magazine (February 2010).

[118] 47 C.F.R. §§ 96.35(e), 96.53(j).

- Using the network plan and visualization tools, users will be able to determine any interference that may be encountered between the CBSDs being deployed and the existing assets managed by the SAS based on detailed CBSD characteristics and can use this data to plan accordingly.

(b) Co-existence Among GAA Users

While GAA users have no expectation of interference protection, the CBRS will be a commercial success only if various GAA users are able to co-exist. While the SAS is not specifically authorized to manage interference among GAA users, the Commission did nonetheless recognize the role of the SAS in resolving conflicting uses and creating a stable radio environment.[119]

GAA co-existence can be categorized in two main classes of operation, managed and unmanaged GAA operation. These two operating scenarios are described further below. For unmanaged operation, sharing of the available GAA spectrum is enabled through use of a contention-based protocol (such as "listen before talk") in the CBSDs themselves and the SAS does not play a significant role in managing the interference environment among GAA users. It is the view of Federated Wireless, however, that certain GAA users will desire to engage the SAS for GAA interference management services. Federated Wireless plans to develop its SAS to support managed GAA operation as an optional, differentiated service.

(i) Managed GAA Use

In this mode of operation, the GAA user is assigned particular frequency channels by the SAS based on the SAS's knowledge of the local interference environment and in keeping with its obligations to protect incumbent and PAL users. Contention-based operation is not required by GAA CBSDs. Rather, the SAS indicates the channels available in a given location and allows the respective GAA user requesting access to select from among the available channels. In all cases, GAA users must report the selected channel(s) to the SAS.

[119] 47 C.F.R. § 96.53(k)

Another element of centrally managed GAA operation is the management of GAA transmission EIRP for each CBSD separately, so that the aggregate interference to a particular victim target, such as a PPA or an Incumbent User, is constrained. An EIRP range (both minimum and maximum) can be established so CBSDs can be operated predictably and in compliance with the FCC-defined EIRP limits. Dynamic EIRP assignment can result in variable and unpredictable coverage for each GAA user, potentially causing coverage gaps and other performance issues, which in turn negatively impacts GAA user business objectives.

The LTE mode of operation used for fully managed GAA operation is TD-LTE.

(ii) Unmanaged GAA Use

In this mode of operation, the SAS indicates a range or collection of channels to more than one GAA user. The GAA CBSDs employ contention-based protocols to obtain the operational channel. These contention-based solutions require sensing and contention among GAA users. The channel set provided by the SAS could optionally include all GAA channels (all channels not in use by incumbents or PAL licensees), or a subset of available channels, according to SAS calculations. In all cases, GAA users are mandated to report the channel used to the SAS so that interference protections to Incumbent and PAL users are maintained. In unmanaged GAA operation, the SAS assumes GAA users are using maximum allowed EIRP in transmission, and allows distributed management of the channels and self-regulation by the users. The interference management in this mode can be achieved by contention-based solutions or by using distributed management, such as a SON infrastructure used by each GAA operator.

A variety of contention-based solutions in the LTE family of technologies, including LTE Licensed Assisted Access, e-LAA, and MuLTEFire, could be used for the unmanaged GAA mode of operation. Conventional TD-LTE with SON can also be used for unmanaged GAA operation, where distributed management and distributed channel assignment is used.

Despite the lower complexity of SAS implementation, the main disadvantage of unmanaged GAA is potential degradation of the efficiency of CBRS spectrum utilization, with an increased level of interference.

(c) GAA Fairness

GAA management involves GAA fairness, channel allocation management, and power level assignment by the SAS. The Commission has consistently emphasized the importance of a "congestion metric" or other advanced planning methods to help ensure GAA fairness. The fairness criterion defines how the SAS fairly allocates resources, such as frequency ranges or channels, transmit powers, and associated geographical coverages to GAA users, while maintaining adequate aggregate performance in the band.

As Federated Wireless has described previously, the SAS could employ different fairness criteria, each aiming to achieve a particular objective.[120] The definition of fairness is, however, subjective. Some may define fairness as providing equal opportunity to use shared resources, some might define it as greedy and opportunistic utilization of shared resources such that the individual performance of CBSDs or EUDs are optimized, and some might employ a criterion to improve the aggregate performance of all users. Several other criteria might be defined that represent a balancing of these approaches. The methodology depends on the Commission's request and potential industry agreements. The Federated Wireless SAS is capable of supporting different fairness criteria, including the following:

- Round-robin: In this method, the shared resources are assigned to all requested users equally with equal time limits in a round-robin fashion. The assignment pattern is repeated frequently.
- First-In-First-Out ("FIFO"): Where the first GAA users requesting spectrum grants have priority over late-comers. With this criteria, the investments of operators requesting GAA access could be protected; however, the shared resources are not necessarily available for the

[120] *See* Comments of Federated Wireless, Inc., GN Docket No. 12-354 (filed Jul. 15, 2015).

use of all GAA users. One way to soften this limitation is for the SAS to assign resources with time limits.

- Greedy Performance Maximization: Where the resources (channels and power levels) are assigned so that an aggregate performance metric is achieved. An example of such an aggregate performance metric is overall throughput, which in turn depends on the congestion of users and the distribution of CBSD-user channel qualities.
- Proportionally fair: In this mode two functions are defined, one is a performance objective, and the second is a cost function per GAA user. The performance function could be the aggregate throughput according to a congestion metric, and the cost per GAA user could be the amount of interference each user causes to the victim receiver(s), e.g., Incumbent or PAL users, or other GAA users.

A key consideration to define GAA fairness is to properly characterize the parameters of each approach, such as the time limits for each assignment, the performance objectives, and the cost functions. For example, a longer time limit for a FIFO management approach would encourage operators to rapidly invest in GAA deployment, but may also result in unfavorable race conditions.

One major concern of any GAA fairness criteria is how the different SASs operating in the same geographical area can synchronize their GAA fairness approaches. One potential approach is to share information (such as all CBSD registration information, assigned channels, and their assigned EIRPs) among SASs in a the geographical area where real-time coordination of a common pool of channels is needed. Another approach is to allocate channels for individual SAS management, based on pre-defined agreements among the SASs or through more dynamic coordination via the SAS-SAS protocol, such that each SAS is managing orthogonal channels.

E. SAS-SAS COORDINATION

Effective implementation of Part 96 of the Commission's rules necessitates the exchange of information among authorized SASs and coordination of certain SAS functions, both to ensure an accurate and consistent view of the radio environment, and to ensure the full protection of Incumbent Users. Recognizing the need for SASs to share information and for fair and efficient spectrum allocation to CBSDs managed by different SASs, the Commission directed SAS Administrators "to cooperate with one another to develop a standardized process for coordinating

their operations, avoiding any conflicting assignments, maximizing shared use of available frequencies, ensuring continuity of service to all registered CBSDs, and sharing the data collected from registered CBSDs."[121] Federated Wireless recognizes the spectrum sharing benefits that will accrue from the synchronization of SASs and is fully committed to achieve SAS-SAS information sharing and coordination consistent with the vision the Commission has reflected in sections 96.63(h) and 96.63(i) of its rules.[122]

The counterbalance is that information on spectrum use may be commercially sensitive and end user privacy and confidentiality must always be maintained. There is also a need to minimize the collection and distribution of information related to federal incumbent activity so as to ensure continued operational security. This is reflected in requirements to obfuscate identifying information from registered CBSDs[123] and in the handling and disclosure of federal incumbent activity.[124]

It is expected that initial SAS-SAS coordination will require limited data exchanges reflecting data privacy considerations and the reality that the CBSD deployments will initially be sparse. Federated Wireless believes it is crucial to assure the users of the CBRS band that their valuable information will be handled appropriately, competitively sensitive information will not be disclosed, and end user privacy will be maintained. SAS Administrators must ensure that the information they share with other Administrators is used only for the purposes managing CBRS spectrum. In addition, it is vital that SAS Administrators limit access to user network operations information to

---

[121] *See Amendment of the Commission's Rules with Regard to Commercial Operations in the 3550-3650 MHz Band*, GN Docket No. 12-354, Report and Order and Second Further Notice of Proposed Rulemaking, FCC 15-47, at para. 360 (2015) ("3.5 GHz Order").

[122] 47 C.F.R. §§ 96.63(h)-(i).

[123] *Id.* § 96.55(a)(3).

[124] *Id.* § 96.55(c).

only those personnel with a legitimate, spectrum-management-related need and to restrict access from personnel whose roles do not carry such a responsibility.

Federated Wireless is committed to working with stakeholders, either through the WINNF, the Commission, or the CBRS user community directly to develop the requirements and standards for information sharing that strike the right balance between user privacy and effective spectrum management.

The genesis of SAS-SAS coordination is the communication interface and protocol to support information exchange. Federated Wireless is leading the SAS-SAS protocol development in the WINNF. A key design goal is to ensure that the protocol is flexible and extensible to support both current and potential future needs for information sharing (*i.e.*, the protocol development process addresses how information elements are exchanged yet does not address whether these information elements should be exchanged).

Broadly the WINNF SAS-SAS protocol development addresses the potential to exchange the following information elements or events:

- Maintenance of and Public Access to CBSD Registration Data
- Facilitating Non-Interfering Use by CBSDs Connected to Another SAS
- Responding to ESC Events
- Coordinating PAL Frequency Assignments
- Aggregate Interference Calculation
- Coordinating GAA Uses
- Informing Authority Events
- Responding to Interference Reports and Requests for Additional Protection
- Resolving Error Reports

1. WINNF SAS-SAS Protocol

Federated Wireless has collaborated on the development of a SAS-SAS protocol in Working Group 3 of the WINNF[125] that will have to balance the competing interests of data privacy and spectrum efficiency. The SAS-SAS protocol is a foundational element by which the WINNF will later establish standards on information sharing and event coordination among authorized SASs.

Important issues that the WINNF standards will address include: (a) the type and content of information records and coordination events to be exchanged; (b) the reasons for which information may be exchanged; (c) the recurrence or frequency of synchronization; and (d) the method of communication. In considering each of these issues, Federated Wireless believes it is crucial to remain mindful of the importance and commercial sensitivity of CBRS users' data and the need to affirm to them that the privacy of such information is a paramount concern of SAS Administrators.

The WINNF has developed a flexible and extensible message encoding and method based on JSON. JSON is a widely accepted network data representation and exchange protocol that will readily support the needs of SAS-SAS information exchange as information records requirements are finalized.

Some information that Federated Wireless intends to share to ensure SASs can best perform their required functions include:

- SAS Administrator and Implementation records
- ESC Administrator and Implementation records
- Domain Proxy record
- CBSD Device Type record
- CBSD record: All registration parameters and detailed grant information, including fine-grained location, will be exchanged. Owner information will be exchanged as

[125] *See* WINNF Interim SAS-SAS Protocol.

needed, and measurement information may be exchanged after WINNF finalizes its requirements.

- Non-federal Incumbent User record: Information regarding FSS operations will not be exchanged. Treatment of information regarding GWBL operations will be decided after the Commission clarifies protection requirements of these entities.
- Zone record: Consistent with applicable WINNF standards, any Protection or Exclusion Zones manually defined by a regulator will be shared. To be consistent with the FCC and DoD's obfuscation requirements, ESC zones defining an area of active federal Incumbent use are not shared as they are unique to the ESC.
- CBSD Operator record
- Professional Installer record
- Coordination Event record: These records are designed to support coordination for exception events such as Interference Reports and responding to directions from an Informing Authority.

As described in other sections, the WINNF has adopted TLS to ensure security requirements are satisfied at the SAS-SAS communication transport layer. HTTP was selected by the WINNF for the data communication protocol because of its broad applications and easy adaption. HTTP supports both push (information transmission is initiated by a SAS) and pull (information transmission is requested by a SAS) communication methods to provide flexibility in its application to each of the information records to be exchanged.[126] Some of Federated Wireless' insights on communication methods are provided in the following sections.

Finally, the WINNF will develop recommendations on the recurrence or frequency of synchronization. Even though continuous and real-time synchronization of SASs may appear desirable, it introduces complexities – such as an overreliance on synchronization for basic SAS functions – which may obviate potential benefits. As described in the sections below, Federated Wireless believes that it is possible to simplify certain aspects of SAS-SAS coordination such that

[126] HTTP over TLS is more commonly known as HTTPS.

multiple SASs can perform their required functions without the need for continuous and real-time synchronization.

If the Commission approves multiple SAS Administrators, clear and mutual principles of information sharing and coordination among SASs are essential for the viability of the CBRS system. SAS-SAS synchronization should be implemented to benefit SASs and their users without introducing additional complexities. To this end, Federated Wireless believes the Commission should carefully consider the following as it relates to SAS functionality and SAS-SAS synchronization.

- A SAS should be individually responsible to obtain the information it needs to operate, and to perform its functions to comply with Part 96 of the Commission's rules. A SAS's basic operation shall not be contingent on information or functions exchanged by other SASs beyond the information required for exchange in Part 96.

- A SAS should retain the ability to autonomously determine the frequency ranges and technical parameters for the Devices it manages; make decisions about potential interference, and enact measures necessary to protect Incumbent Users, grandfathered services, or PAL licensees; and conduct its operation in compliance with Part 96.

- A SAS should use the information it receives from other SASs only to improve the performance of spectrum and interference management or to resolve critical problems in the CBRS ecosystem, e.g., an Interference Report .

- Information obtained by a SAS through a SAS-SAS exchange, such as related to CBSD registrations, should not be publicly disclosed by the receiving SAS. SASs should be separately responsible to satisfy the public information disclosure requirements for the CBSDs it manages.

- Information exchanges should be based on actual need. SASs should not necessarily synchronize entire databases of CBSD registration records, but rather obtain information only for geographical areas where it is actively managing spectrum.

- Information exchanges should be transactional. SASs should not store and retain information received from other SASs beyond its utility for spectrum and interference management.

Striking the right balance between the independent and coordinated operation of SASs is crucial, and Federated Wireless encourages the Commission to provide further guidance on SAS-SAS coordination as part of the approval process.

2. Maintenance of and Public Access to CBSD Registration Data

Federated Wireless will make the information regarding all of its registered CBSDs and licensees it manages available to other SASs, as required by Part 96 of the Commission's rules, or as agreed by other SAS Administrators, subject to any privacy and confidentiality agreements with other entities. Further detail regarding CBSD registration records can be found in Appendix 5: Database Information and Appendix 13: Registration.

Providing required public access to obfuscated registration data can be achieved via a variety of methods, each of which requires a different degree of data sharing, including the following:

- Complete sharing of CBSD registration data, where each SAS is individually responsible for providing the requisite identity obfuscation;
- Sharing of CBSD registration data with identifying information removed; or
- Sharing of only the CBSD identifier field and location. In this case, publication of additional CBSD information would redirect the inquirer to the managing SAS.

As described in Appendix 4: Access Protocols and Procedures, Federated Wireless will apply role-based access procedures so that any information disclosure is proportional to need of the entity seeking access to the information (*e.g.*, more detailed information is available to Commission personnel versus the general public).

3. Responding to ESC Events

Due to operations security ("OPSEC") threats, WINNF Working Group 2 ("WG2") recommends that federal Incumbent User detection event information can be shared only between SASs that receive input from the same ESC. At this time, Federated Wireless does not intend to

allow other SASs to have access to its ESC. As a result, the Federated Wireless SAS will not coordinate federal Incumbent User detection events with other SASs. Federated Wireless will implement coordination of federal Incumbent User detection events if WG2 revises its recommendations or if it is directed by the Commission.

4. Coordinating PAL Frequency Assignments

Section 96.25 requires that, to the extent feasible, a SAS must assign geographically contiguous PALs held by the same PAL licensee to the same channel(s) in each geographic area; and must assign multiple channels held by the same PAL licensee to contiguous channels in the same license area.[127] Compliance with these rules, and those in section 96.63(i), necessitates that SASs coordinate on PAL channel assignments.[128] Efficient and coordinated channel assignment to PAL users will further ensure that the frequencies available for GAA use are maximized.

Federated Wireless observes that compliance with section 96.25 by a single SAS is nontrivial, and the complexity increases when multiple SASs are responsible for managing the array of PALs awarded through auction. Unfavorable race conditions may result, whereby one SAS may maximize its compliance with contiguous PAL assignments at the expense of others. Dynamic reassignment of PAL channels, as may be periodically required for Incumbent User protection, will require some degree of real-time SAS-SAS interaction to deconflict channel re-assignments. Some pre-coordination and/or pre-planning of PAL channel assignments would be advantageous to ensure that contiguous PAL assignments are maximized for all PAL licensees and to increase the autonomy and reduce real-time coordination of SASs in protecting federal incumbents. Appendix 11: Priority Access License Channel Assignment Plan presents a possible approach for coordinating PAL

---

[127] 47 C.F.R. § 96.25.

[128] *Id.* § 96.63(i).

frequency assignments. This approach proposes that, at the conclusion of an auction and prior to PAL licensees commencing use, a "steady-state" PAL frequency assignment plan be developed for use by all approved SASs. This is one example of how PAL frequency assignments could be pre-planned with the objective of maximizing contiguous PAL assignments and reducing the degree to which SASs are required to coordinate in real time to facilitate a stable and predictable radio environment for PAL licensees.

This is just one example of many possible solutions to SAS-SAS coordination for PAL channel assignments. Federated Wireless will continue to collaborate within the WINNF to build consensus on an industry standard approach.

5. Aggregate Interference Calculations

The Federated Wireless SAS will coordinate with peer SASs on necessary information sharing to effect the calculation of accurate aggregate interference in the managed area. Specific methods for aggregate interference coordination are still under consideration in the WINNF. However, as described previously, a possible method to address CBSDs under control of multiple SASs is to fractionally apportion the total interference margin among the affected SAS Administrators. This apportionment approach ensures that each SAS can autonomously manage their CBSDs to individually identifiable thresholds while Incumbent and/or PAL operations are protected to the desired aggregate interference level. For instance, with two SAS Administrators managing devices near a PPA, each Administrator could manage its own CBSDs to ensure that the aggregate interference from its own CBSDs does not exceed -83 dBm within the PPA. As a result, the combined aggregated interference from the total population of CBSDs under the control of the two SASs will not exceed -80 dBm. The method may be further generalized to accommodate for multiple SASs; adjusted to further apportion interference margin to multiple SASs based on additional criteria, such as the ratio of CBSDs it manages to the total population of CBSDs; and

expanded to include specific agreements between and among SAS Administrators. In this case, no CBSD information would need to be regularly exchanged to perform these calculations, though the number of devices in different interference regions would have to be disclosed as part of the negotiation of Interference Partitions.

Another approach to coordinating interference calculations is the sharing and synchronization of interference environment maps, where each SAS shares its calculated estimate of aggregate interference at locations or bins in the local environment, but no CBSD data is shared. In this case, each SAS's allocations are dependent on the calculations of the other SASs, but CBSD privacy can be maximized.

While it is possible that the industry may evolve to greater sharing of CBSD data relevant to spectrum management (*e.g.*, locations, antenna configurations, spectrum assignments but not identifying information), Federated Wireless is of the view that such information is not necessarily required for effective spectrum management and may not be prudent to share in view of the need to maintain the privacy and security of user data.

6. Coordinating GAA Uses

As described in Section II.D.17, frequencies are made available for GAA use on a shared basis and GAA users have no expectation of interference protection. A SAS is obligated to permit a GAA device to operate so long as such operation is in compliance with Part 96 of the Commission's rules. However, in section 96.35(e), the Commission requires that GAA users must "make every effort to cooperate in the selection and use of available frequencies…to minimize the potential for interference and make the most effective use of the authorized facilities."[129] Federated Wireless' approach to facilitate coordination among GAA CBSDs is described in Section II.D.17. The

[129] *Id.* § 96.35(e).

exchange of CBSD registration data, as described in Section II.D.1, is needed to facilitate this coordination methodology.

Federated Wireless further recognizes that the SAS can play a significant role in coordinating frequency assignments and CBSD power levels to reduce the harmful interference caused to other PAL or GAA users. Federated Wireless is exploring standards and technology-based solutions for the SAS to implement GAA co-existence, generally. Once the technology and standards are developed for such co-existence, Federated Wireless, in collaboration with CBSD developers, will implement these capabilities. A variety of sharing approaches to implementing this function could be adopted, including: (a) the data sharing arrangements described for aggregate interference calculations; and (b) disclosing, on an opt-in basis, GAA operator contact information to other GAA operators in the area so they can identify other operators in their area and adopt independent technological solutions for GAA coordination as appropriate.

7. Coordinating Informing Authority Events

The Federated Wireless SAS interfaces with informing authorities to respond to requests or instructions from the President of the United States, authorized Commission personnel, or other designated federal government entities. The Federated Wireless SAS will share information related to these requests or instructions to other SASs based on appropriate sharing policies, all in compliance with its privacy and confidentiality agreements.

8. Responding to Interference Reports and Requests for Additional Protection

Consistent with interference management best practices and as required by section 96.53(o), the Federated Wireless SAS accepts reports of interference and requests for additional protection from protected users, including incumbent system operators. As resolving reports of interference will frequently require a coordinated response from SAS Administrators, our proposed approach to

resolving interference reports, described in Appendix 7: Error Resolution and Interference Reporting Policy, depends on coordination with other SAS Administrators. Similarly, requests for additional protection will be coordinated with other SAS Administrators to ensure consistent application.

9. Resolving Error Reports

Depending on the specific protection coordination mechanisms adopted by the CBRS community, an error in one database could propagate throughout the ecosystem. As described in Appendix 7: Error Resolution and Interference Reporting Policy, the Federated Wireless SAS will use the SAS-SAS interface and other coordination mechanisms to quickly alert other affected SAS Administrators of database errors brought to our attention.

10. Summary of Information Sharing in SAS-SAS Coordination

If the Commission approves multiple SAS Administrators, clear and mutual principles of information sharing and coordination among SASs are essential for the viability of the CBRS system. SAS-SAS synchronization should be implemented to benefit SASs and their users without introducing additional complexities. While spectrum efficiencies will have to be balanced against the need to implement robust protections to ensure the privacy of CBRS user data, there are fortunately many different ways in which different degrees of CBSD information can be shared to realize the CBRS ecosystem, as summarized in Table 2. In Table 3, Federated Wireless' proposed approach to coordinated SAS functions is provided.

Table 2: Exemplary CBSD Data Sharing Approaches for Selected Coordinated SAS Functions

Function	Approach	CBSD Information to Share	Duration of Sharing
Aggregate Interference Protection	• Interference Partitioning	• None	• N/A

Aggregate Interference Protection	• Interference map distribution	• None. Only derived interference data	• Update as spectrum grants change
Aggregate Interference Protection	• Independent fully-informed calculation	• All CBSD registration information except for identifying information • Spectrum Assignments	• Duration of registration
Automatic partitioning of interference	• Fraction of CBSDs in regions	• Numbers of CBSDs • Managing SAS	• At time of negotiation
CBSD Online Public Lookup	• Partitioned (point to managed CBSD for additional info)	• Location • Who Manages	• Could be only at time of request or for the duration of CBSD registration
CBSD Online Public Lookup	• Shared obfuscated CBSD information	• All CBSD registration information but identifying information	• Duration of registration
Interference Report Resolution	• Verify other SAS calculations • Compare against measurement reports	• CBSD records • Spectrum assignments records	• Until interference is resolved
GAA Coordination	• Enable GAA operators to identify other operators to coordinate spectrum with	• Location • Managing SAS	• At time of request or permanent depending on opt-in arrangement

Table 3: Federated Wireless Proposed Approach for Selected Coordinated SAS Functions

Function	Approach	CBSD Information to Share	Duration of Information Sharing
Standard Aggregate Interference Protection	• Interference Partitioning	• None	• N/A
Automated (variable) Partitioning of Aggregate Interference Protection	• Fraction of CBSDs in coordination region	• Numbers of CBSDs • Managing SAS	• At time of negotiation
CBSD Online Public Lookup	• Partitioned (point to managed CBSD for additional info)	• CBSD Location • Who Manages	• At time of request (or for longer duration based on opt-in agreements)
Interference Report Resolution	• Compare against Signal Level Measurement reports	• Full CBSD registration records in affected region	• Until interference is resolved
Basic Category B GAA Coordination	• Matchmaker	• Location • Who manages	• At time of request (or for longer duration based on opt-in agreements)

Federated Wireless is committed to sharing necessary information with other SAS Administrators to maximize the spectrum efficiency of the CBRS ecosystem while preserving the privacy and security of our customers. The WINNF standardization of data exchanges between SAS Administrators to coordinate CBRS management is ongoing and Federated Wireless will support and fully implement the SAS-SAS coordination standards and recommendations that emerge from that process.

F. SAS SECURITY

Federated Wireless is committed to ensuring that its SAS and ESC employ industry leading security measures to ensure that its functions and communications, with CBSDs and other SASs, are conducted accurately and securely. Securing communications and data from unauthorized access

and modification are critical functions for any information system, but are especially important for a SAS that is entrusted to: (1) reliably enforce interference protections for federal systems with national security implications; (2) enforce protections for non-federal Incumbent Users and for PAL licensees where those protections are dependent upon secure maintenance and transmission of the data and coordination between SAS and CBSDs; and (3) store and maintain private and potentially sensitive data.

Federated Wireless founder and advisor T. Charles Clancy, Ph.D. is a leading expert and researcher in security technology and the Federated Wireless team has deep experience in architecting, implementing, and maintaining cloud security systems. Since early 2015, Federated Wireless has worked collaboratively with industry participants in the WINNF SSC to define the communication security and cybersecurity requirements for the SAS ecosystem to ensure that SAS transactions are trusted and that the overall system is secure. Charles Clancy is the WINNF SSC WG2 Chair, and Federated Wireless has provided key contributions in developing the cryptographic protocol and key management requirements, as well as the cybersecurity threat model.

Federated Wireless has implemented and will continue to implement the interim and final security standards developed by the WINNF SSC Security Working Group. The WINNF industry standards are the underpinning of Federated Wireless's SAS security architecture. More broadly, to ensure security is enforced in a consistent and continuous manner, Federated Wireless has chosen to leverage numerous principles of PCI, SOC2 Type II, and FedRAMP. FedRAMP provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services that enables cloud computing vendors to certify their services for federal use. The FedRAMP program provides an excellent template to ensure that Federated Wireless's commercial service offerings meet its commitment to the highest level of security.

Further information regarding Federated Wireless's security solutions, specifically details on compliance with sections 96.39(f), and 96.61(a)-(c),[130] can be found in, Appendix 15: Security.

1. Database Security and Preventing Unauthorized Access

Consistent with sections 96.61(a)-(b), Federated Wireless will ensure unauthorized parties cannot access or alter the SAS and that the SAS is protected from unauthorized data input or alteration of stored data.[131]

Federated Wireless has implemented its SAS in a hosted cloud environment. Some key benefits of a hosted cloud platform that contribute to accurate and secure operation of the Federated Wireless SAS, include:

- **Self-healing –** automatic recovery from hardware failures
- **Flexible capacity** – computing resources can be turned on or off depending on circumstances
- **Diversity –** multiple SAS instances can be distributed over servers in different physical locations
- **Resource pooling –** load balancing features allow the SAS to deal with rapid spikes in traffic, providing resiliency against security attacks that attempt to crash or flood services (*e.g.*, Distributed Denial of Service attacks)
- **Enhanced software deployment –** new software, security patches, bug fixes etc. can be rapidly deployed.

Federated Wireless has selected an industry-leading cloud services provider to host its SAS and ESC software platforms. This cloud services provider offers a broad set of global computing, storage, database, analytics, application, and deployment services. The services provided by Federated Wireless' chosen cloud service provider are trusted by many of the largest commercial and

---

[130] *Id.* §§ 96.39(f), 96.61(a)-(c).

[131] *Id.* §§ 96.61(a)-(b).

federal enterprises in part because of the robust controls established to maintain security and data protection in the cloud. The Federated Wireless cloud solution is fully PCI- and SOC-compliant.

The cloud-hosted environment enables Federated Wireless to deploy multiple instances of the SAS, leveraging virtual private clouds spanning numerous, geographically diverse locations within the United States. This capability not only provides for added scalability but also enhances security.

As described in Appendix 4: Access Protocols and Procedures, access to the Federated Wireless SAS will be managed through individual user accounts. For each user account category – including the general public, commercial users of the Federated Wireless SAS, the Commission, and other government entities – access to the SAS will be password-controlled. Federated Wireless will implement the NIST SP 800-53 Identity and Authentication family of controls to ensure authorized party access.[132] This will ensure that unauthorized parties cannot access or alter the SAS or otherwise corrupt the operation of the SAS in performing its intended functions, consistent with the Commission's rules. The family of NIST SP 800-53 controls ensures high integrity of user passwords and user authentication processes.

Federated Wireless will continually monitor all access attempts and address attacks intended to grant unauthorized access. Identification and resolution of attacks will leverage an ELK stack for log collection, event correlation, and alerting. An ELK stack is a technical implementation to realize effective log monitoring, security incident, and event management and comprises:

- (E)lastic Search: search and analysis of data collected from system logs in real-time;
- (L)ogStash: collecting, enriching, and transport of log data; and
- (K)ibana: exploring, correlating events, visualizing, and acting upon data.

[132] NIST, *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST Special Publication 800-53, Revision 4, (Apr. 2013), *available at* http://dx.doi.org/10.6028/NIST.SP.800-53r4 (last accessed Apr. 11, 2016).

2. SAS-CBSD Communications Security

Consistent with section 96.61(a), Federated Wireless will ensure all communications and interactions between the SAS and CBSDs are accurate and secure and that unauthorized parties cannot access or the information the SAS sends to a CBSD.[133]

Protocols and procedures to ensure accurate and secure SAS-CBSD communications have been established though WG2 of the WINNF. Federated Wireless contributed substantially to developing the SAS-CBSD communication security protocols because it believes that a common security standard is essential to ensure the overall security of the CBRS system. Federated Wireless has implemented the interim WINNF security recommendations and will implement all future interim and final WINNF recommendations to ensure a secure and interoperable ecosystem.

Per current WINNF requirements, secure communications between the SAS and CBSDs will be satisfied using an industry-recognized PKI, which is comprised of a hierarchical set of roles, policies, and procedures needed to mutually authenticate, create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption. The purpose of this PKI structure is to facilitate legitimate electronic communications of CBSD-SAS and SAS-SAS in a secure manner.

To protect the exchange of authorization information and communications between the SAS and CBSDs, TLS—a protocol created to provide authentication, confidentiality, and data integrity between two communicating applications—will be used with the PKI structure.

3. SAS-SAS Communications Security

Consistent with section 96.61(b), Federated Wireless will ensure all communications and interactions between the Federated Wireless SAS and other SASs are accurate and secure.[134]

---

[133] 47 C.F.R. § 96.61(a).

[134] *Id.* § 96.61(b).

Protocols and procedures to ensure accurate and secure SAS-SAS communications have been established though WG2 of the WINNF. As with other security standards, Federated Wireless contributed substantially to developing the SAS-SAS communication security protocols because it believes that a common security standard is essential to ensure the overall security of the CBRS system. Federated Wireless has implemented the interim WINNF security recommendations and will implement all future interim and final WINNF recommendations to ensure a secure and interoperable ecosystem.

Per current WINNF requirements, secure communications between and among SASs will be satisfied using an industry-recognized PKI, which is comprised of a hierarchical set of roles, policies, and procedures needed to mutually authenticate, create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption. The purpose of this PKI structure is to facilitate legitimate electronic communications of CBSD-SAS and SAS-SAS in a secure manner.

To protect the exchange of authorization information and communications between SASs, TLS—a protocol created to provide authentication, confidentiality, and data integrity between two communicating applications—will be used with the PKI structure.

4. SAS-ESC Communications Security

Consistent with section 96.61(b), Federated Wireless will ensure all communications and interactions between the Federated Wireless SAS and the Federated Wireless ESC is accurate and secure to prevent corruption or unauthorized interception of data.[135]

While the WINNF has not at this time elected to develop a SAS-ESC communications security implementation standard, the security requirements and standards established for SAS-CBSD communications are directly applicable.

---

[135] *Id.*

Secure communications between the Federated Wireless SAS and Federated Wireless ESC will be satisfied using TLS with mutual certificate authentication.

5. FCC ID Verification

Consistent with section 96.61(c),[136] the Federated Wireless SAS will verify that the FCC identification number supplied by a CBSD is for a certified device and it will not provide service to an uncertified device.

Protocols and procedures to perform FCC ID verification communications have been established though WG2 of the WINNF. Specifically, in the case of direct CBSD-SAS communication, Federated Wireless will extract and verify the FCC ID that is embedded in the PKI certificate of the CBSD. Prior to issuing a CBSD's PKI certificate, proper documentation of a CBSD's FCC certification will be provided to a device manufacturer Certificate Authority ("CA") by the device manufacturer.

The device manufacturer CA may have processes for direct signing of per-device certificates on behalf of a device manufacturer. Federated Wireless envisions the following:

- All CBSD manufacturers must obtain FCC IDs for the devices they manufacture;
- During the manufacturing process, the FCC ID provided to the manufacturer by the FCC is embedded into the CBSD certificate as a certificate attribute;
- CBSD devices are transported to retailers/wholesalers/etc.;
- Customer purchases a CBSD; and
- Following a purchase, a CBSD-SAS registration process occurs in which the CBSD's certificate provides FCC ID information to the SAS and add the FCC ID to the backend data store. This occurs only after successful mutual authentication of CBSD and SAS certificates within the ecosystem.

[136] *Id.* § 96.61(c).

For each subsequent mutual authentication of CBSD and SAS certificates, the FCC ID is compared to the known FCC ID within the backend data store.

In the case of Domain Proxy to SAS communication, the Federated Wireless SAS will verify FCC IDs that it receives via each Domain Proxy. Federated Wireless has implemented this interim WINNF specification and will implement all future interim and final WINNF recommendations related to FCC ID verification.

6. Additional Security Technologies and Procedures

Additional measures and technologies that Federated Wireless will implement to ensure accurate and secure functions and communications include:

- In addition to the PKI structure in which both the CBSD and SAS authenticate each other's certificates (mutual authentication) and leverage the capability of whitelisting/blacklisting of certificates (*e.g.*, certificate validation/revocation), end-user authentication into Federated Wireless APIs will be done against our identity store within a Web PKI. End user authentication and authorization requirements adhere to the authentication section above.

- Web application and network-based firewalls will be used to filter out malicious requests made to SAS.

- Continuous security integration ("CSI") testing efforts that span the software development life cycle are key to our success. CSI includes a deep and continuous analysis of weak source code patterns, insecure library dependency detections, and vulnerability detections in deployed environments leveraging a collection of industry-accepted security scanning tools as the ecosystem evolves.

- Regular (manual) penetration testing throughout the ecosystem to ensure our security technologies leveraged within CSI are sufficient in reducing the risk of our ecosystem to an acceptable level that meets requirements.

- Daily backups leveraging the cloud partner backup & recovery service to ensure all backups are centrally managed and any data lost can be recovered in a timely manner. Cloud-based backups ensure that no single facility loss will lead to the loss of any data backed up.

- Federated Wireless will continuously monitor for suspicious behavior through log collection, event correlation, and alerting.

7. Addressing Other Security Threats

Additional security threats to the CBRS system include availability, privacy, confidentiality, auditability, authentication, authorization, non-repudiation, and data integrity related threats. Further information regarding Federated Wireless's security solutions to these additional threats can be found in Appendix 15: Security.

G. DYNAMIC USE-CASE SCENARIOS

This section presents dynamic use-case scenarios to illustrate how the Federated Wireless SAS will manage and assign spectrum resources to ensure that geographically and spectrally adjacent operations are coordinated consistent with the Commission's rules. These use case scenarios include the methodology and protection approach for cases of radio interference due to blocking, out-of-band emissions, and aggregate co-channel interference. The section also describes how multiple SASs will coordinate the calculation of aggregate interference for protecting Incumbent Users and PAL licensees over the following three use cases:

- Coordination of the calculation of aggregate interference for Protecting Incumbent Users and PPAs;
- Coordinated protection of a PAL licensee when allowing GAA devices access to PAL spectrum; and
- Managing and assigning spectrum resources to ensure that geographically and spectrally adjacent operations are coordinated consistent with the Commission's rules.

1. Aggregate Interference Calculation for Protecting Incumbent Users and PAL Protection Areas

This use case illustrates the coordination among SASs used to protect an Incumbent User or a PAL Protection Area as part of their aggregate interference calculations. While the specific use case focuses on the protection of a single FSS earth station, the same basic approach is applied to PAL protections and to situations where multiple overlapping coordinated protections need to be

implemented (*e.g.*, an area where a PAL network lies within the 40 km zone around an FSS earth station, with both already separated in frequency).

(a) Overview

The Coordinated Aggregate Interference calculation is built on the following concepts:

- Each SAS performs its spectrum allocations and aggregate interference calculations independently of the spectrum allocations of the other SASs.
- Each SAS uses an interference protection threshold that is more conservative than if there was only one SAS. These different thresholds are designed such that their sum adds up to the protected system's protection threshold. For instance, two SASs allocating spectrum to CBSDs in the vicinity of a 3600-3700 MHz FSS earth station might each be working with co-channel RMS interference thresholds of -132 dBm / MHz so that the combination sums to -129 dBm / MHz, the desired aggregate interference protection threshold. Likewise, blocking interference could be partitioned between the two systems with each SAS managing aggregate interference such that, for instance, each SAS manages its CBSDs within 40 km of the FSS earth station so that its CBSDs produce no more aggregate RF power at the output of a reference RF filter than a median RMS value of -63 dBm.[137]
- The partitioning of aggregate interference thresholds for each protected user is negotiated among the relevant SASs with changes in partitioning made over a long period of time (weeks to months) to promote spectrum stability.

The processes used to coordinate the calculation of aggregate interference for protecting Incumbent Users and PAL Protection Areas are described more fully in Appendix 11: PAL Channel Assignment Plan and in Section II.D: Spectrum Availability and Protections.

(b) Use Case

To illustrate the processes associated with this coordination, consider the following scenario, where for purposes of clarity, no other incumbents or protected users are assumed to be in the area.

Two different SAS Administrators, labeled as SAS A and SAS B, are each managing CBSDs within 150 km of an 3600-3700 MHz FSS earth station (called the FSS earth station's 150 km Interference Region) and a smaller number of devices within 40 km of an FSS (earth station). It is

[137] *Id.* § 96.17(a)(3).

critical that the combined interference of the allocations made by the two SAS Administrators do not violate the co-channel protection requirement of section 96.17(a)(2) or the blocking protection requirement of section 96.17(a)(3).

The scenario considers the process by which SAS A registers and grants spectrum to five new CBSDs managed through a CBSD proxy where we assume three (3) of the new CBSDs are within the Interference Region and two (2) are outside of the Interference Region. Previously, SAS A and SAS B have negotiated to partition the allowable interference to the FSS earth station evenly, with each ensuring that the aggregate co-channel interference from the CBSDs with 150 km of the FSS earth station and that they manage does not exceed -132 dBm/MHz at the FSS earth station. In this case, the FSS earth station experiences no more than -129 dBm/MHz from the sum of interference contributions from the two sets of aggregated CBSD interference contributions. Similarly, SAS A and SAS B partition the allowable interference to ensure the sum of aggregate RF power from all CBSDs within 40 km at the output of a reference RF filter assumed inline with the FSS antenna does not exceed -60 dBm.

This scenario can be visualized as shown in Figure 10, where SAS B is managing the three CBSDs to the left of the FSS earth station and SAS A is managing the seven CBSDs to the right of the FSS earth station where the bottom five CBSDs are new entrants seeking spectrum via a Spectrum Grant Request, with two of the CBSDs outside of the 150 km radius coordination zone for the FSS earth station. Note that both SAS A and SAS B are also each managing one CBSD within the 40 km radius coordination zone of the earth station. Prior Registration and possible Spectrum Inquiry steps are ignored in this use case.

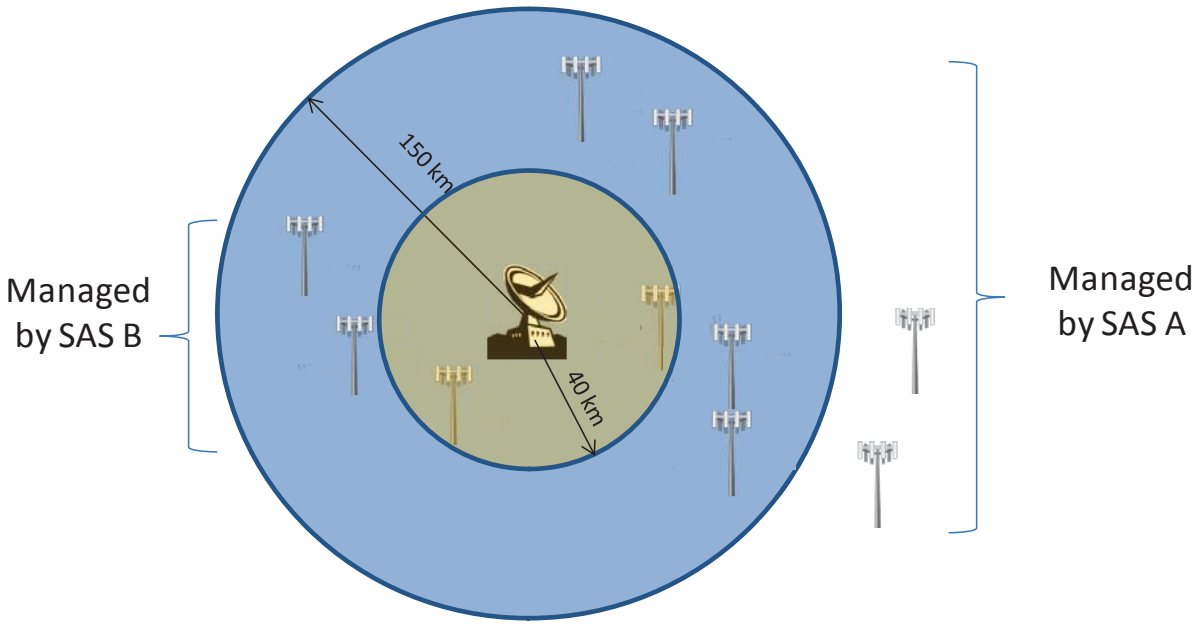

Figure 10: A scenario wherein SAS A will have to coordinate with SAS B to ensure that the combined contributions of their independently managed co-channel CBSDs within 150 km do not cause the interference as measured at the FSS site to exceed -129 dBm / MHz and aggregate RF power from CBSDs within 40 km and at the output of a reference RF filter assumed inline with the FSS antenna does not exceed -60 dBm.

For all five CBSDs requesting new spectrum, SAS A performs spectrum calculations to determine if the requested Spectrum Grants are allowable. For the two CBSDs located outside of the 150 km coordination zone, calculations are performed without consideration of their contribution of co-channel or blocking interference to the FSS earth station. For the remaining three CBSDs, SAS A determines the allowable frequencies and power levels for those three CBSDs, accounting for:

- co-channel interference using the Commission-defined CBSD spectral mask;[138] and
- contributions from the two other CBSDs that have current Spectrum Grants from SAS A.
- Additionally, spectrum allocations to the one new entrant within the 40 km radius (which is also one of the three within 150 km) will also have to satisfy the blocking protection criteria.

[138] *Id.* § 96.41(e).

However, the contributions from the three CBSDs managed by SAS B are not considered by SAS A. As a final step in the Spectrum Availability Algorithm, SAS A then applies obfuscation, if appropriate, and returns the results of this calculation of spectrum availability to the CBSD proxy for the five new CBSDs.

2. Coordinated Protection of a PAL Protection Area When Allowing GAA Access to PAL Spectrum

This use case illustrates the coordination among SASs used to protect a PAL licensee's devices. Further details are available in Appendix 9: Engineering Definition of Use and Appendix 11: PAL Channel Assignment Plan.

(a) Overview

As described in more detail in Appendix 11: PAL Channel Assignment Plan, post-auction, a third party will use a program to generate OAs from the auction results such that PALs held by the same PAL licensee are contiguous geographically and contiguous in channels.[139] This plan may be updated, may also define contingency allocations, and may consider additional objectives.

Within each OA, PPAs are defined by the PAL's Controlling SAS as part of the Spectrum Inquiry and Spectrum Grant process and communicated to other SASs. Each SAS can then independently implement the appropriate protections for that PPA based on interference thresholds previously determined through negotiation with other SASs.

(b) Use Case

Consider the PAL OA shown in Figure 12, with an existing PPA (yellow) based on Spectrum Grants to PAL-owned CBSDs (white). Also present are a number of GAA devices operating within the OA, managed by a red SAS and a green SAS, respectively, where the Green SAS is also the Controlling SAS for the OA. The Green SAS and Red SAS had previously and

[139] *Id.* §§ 96.25(b)(1)(i), 96.25(b)(2)(i).

independently made their Spectrum Grants to these GAAs to ensure that the existing PPA are protected consistent with the negotiated interference partition.

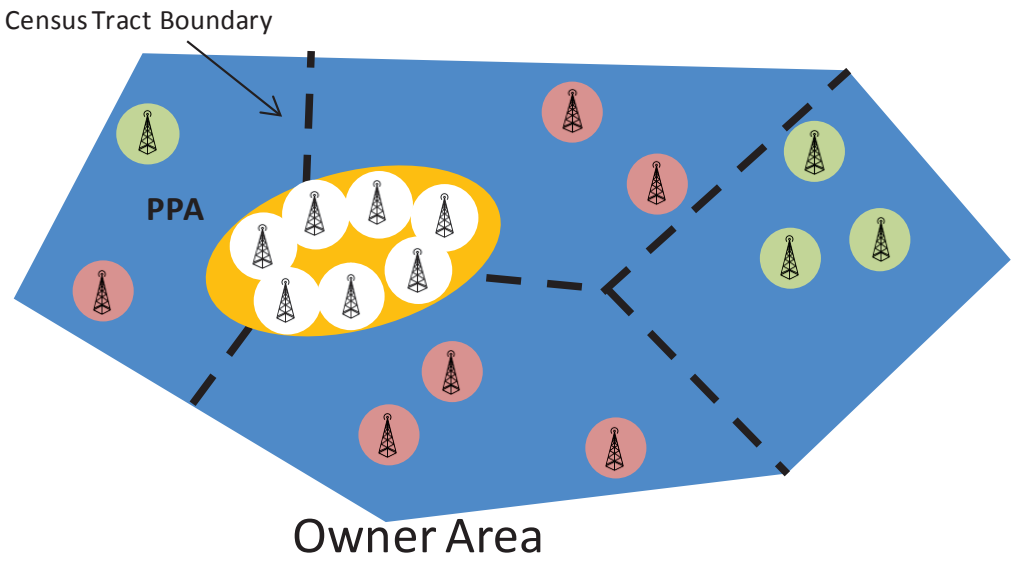

Figure 11: A PAL OA with GAAs granted spectrum in areas not in use by the PAL licensee by two different SASs (green and red)

From this initial state, the PAL licensee would like to add a number of CBSDs with PAL protections. The PAL licensee begins this process by registering these new CBSDs with the Controlling (green) SAS.

Later, the PAL licensee performs a Spectrum Inquiry request for its devices, presenting a proper PAL credential to the Controlling SAS. Using an assumption of maximum allowable transmit power, the Controlling SAS performs the calculations described in Appendix 9: Definition of Use and Secondary Markets to determine the adjusted boundaries of the PPA, ensuring that it does not infringe upon neighboring PAL OAs, with different owners, or upon an SMA that was previously designated by the PAL licensee. Based on the result of the allowable boundaries calculated by the Controlling SAS and other protection calculations, the Controlling SAS replies to the Spectrum Inquiry with the set of channels for the CBSDs.

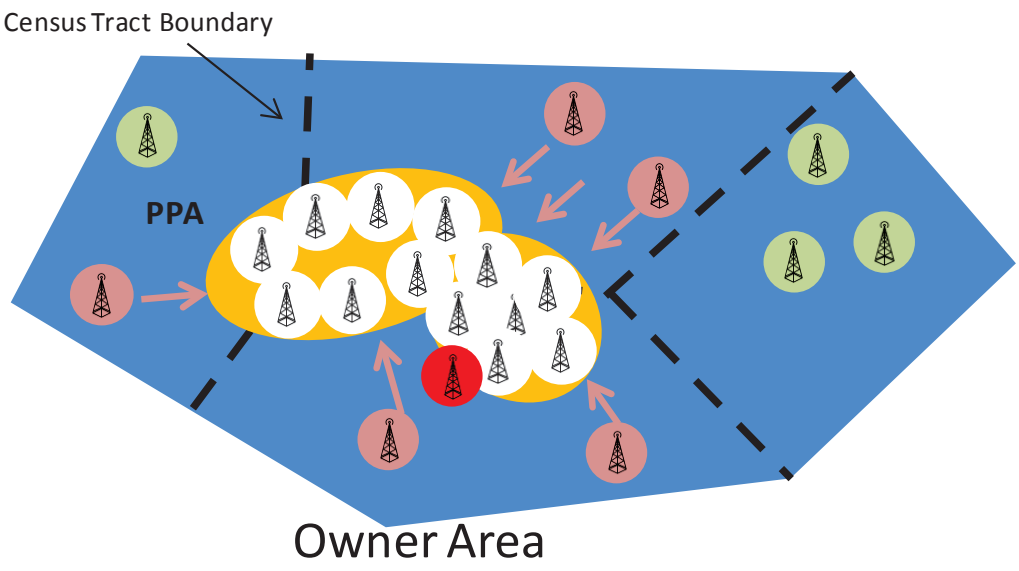

Figure 12: With the updated PPA (yellow), the CBSDs managed by SASs (green and red)

The PAL licensee then makes a Grant Request to the Controlling SAS using the information contained in the Spectrum Inquiry Response. The Controlling SAS repeats the PPA boundary calculation using the specifics of the Grant Request, and the Controlling (green) SAS then informs the red SAS of the new PPA boundaries.

Both the green and red SASs then independently adjust the Spectrum Grants to their managed CBSDs to reflect the new PPA boundary and the previously negotiated Interference Partition, which remains in force.

For instance, the bright red GAA site will need to be moved to a different channel that is likely not an adjacent channel to the PAL due to geographic proximity to the new PPA boundary. Note that even though each SAS (red and green) performs its calculations independently and without reference to the interference contributions of the other SAS's CBSDs, the Interference Partitioning Algorithm and independent Aggregate Interference Calculations ensure that the interference power level as measured at all points within the PPA as referenced to a modeled antenna placed at a height of 1.5 meters above ground level remains below the FCC-specified

protection level as aggregated from the red and green GAA devices, as well as from GAA and PAL devices in adjoining areas or adjacent channels.

3. Managing and Assigning Spectrum Resources to a GAA While Ensuring that Geographically and Spectrally Adjacent Operations Are Coordinated Consistent with the Commission's Rules

(a) Overview

As described in more detail in Appendix 8: SAS Channel Availability and Appendix 9: Definition of Use and Secondary Markets, each SAS will manage its CBSDs to ensure that the aggregate interference from its own CBSDs does not exceed an interference threshold determined by the Aggregate Interference Threshold for each protected system. This use case focuses on the Aggregate Interference Calculation, which is principally a function of ascertaining which systems need to be protected, which of the CBSD sites contribute to aggregate interference at each protected location, and performing aggregate interference calculations for each of these systems to determine which Spectrum Grants are allowable. Prior to the steps described in this use case, all necessary PPA boundaries have been exchanged and all Interference Partitioning negotiations have been performed for all relevant protected users.

(b) Use Case

Consider the scenario shown in

Figure 13, where a GAA is inquiring about spectrum availability prior to requesting a Spectrum Grant. In the area, there is a PAL OA on one set of channels, a PAL OA on a different set of channels, and an FSS earth station operating in the band 3600-3700 MHz. The GAA (shown in yellow) has inquired about the availability of spectrum on Channel 8. Channel 8 is co-channel with spectrum assigned to PAL OA 2 by the post-auction PAL Spectrum Plan and is an adjacent channel to spectrum assigned to PAL OA 1. An assignment of the GAA in Channel 8 may produce interference to an FSS earth station as the GAA lies within 150 km of the earth station. However,

the GAA lies beyond the 40 km radius of the FSS earth station site. Additionally, the SAS is managing the CBSDs sites shown in red and is the Controlling SAS for both PPAs and the SMA-PPA.

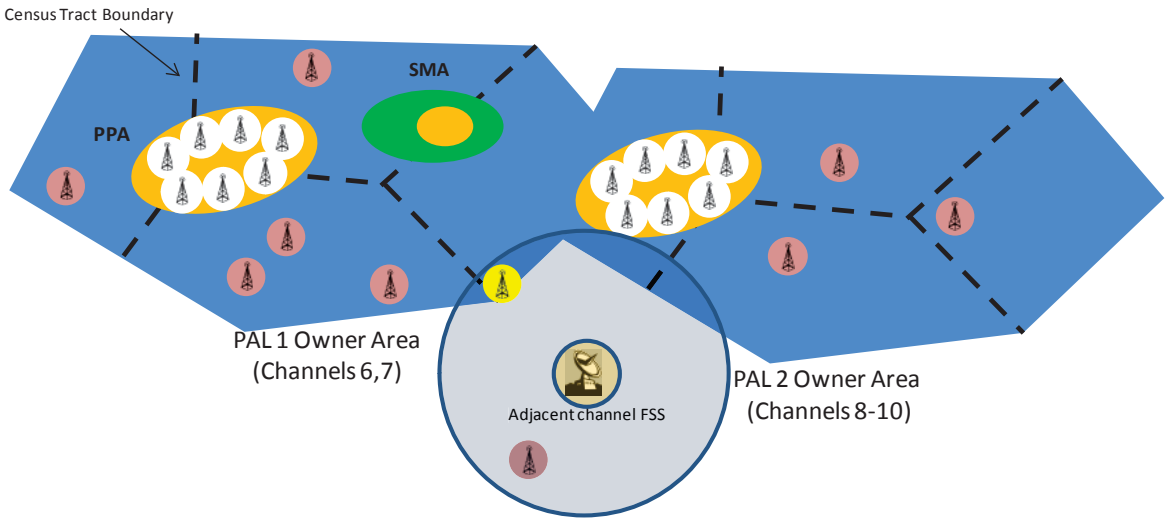

Figure 13: A scenario where a GAA (yellow) inquiring about spectrum availability on Channel 8 is within interfering range of two PAL OAs and an FSS earth station.

Note that there are other CBSDs being managed by other SASs in the area but because of the Interference Partitioning Algorithm, those other SASs are able to independently assign frequencies and power levels to those CBSDs such that their aggregate interference remain below those SASs target interference thresholds for those protected systems.

On receiving the Spectrum Inquiry from the yellow GAA, the SAS first ensures that the GAA use would not violate an Exclusion Zone[140] or the terms of International Agreements[141]. Then the SAS determines if the GAA lies within a 150 km or 40 km Interference Region for an FSS earth station. If it does (as it does in this case for the 150 km radius), the SAS performs the associated

[140] *See supra* Section II.D.3.

[141] *See supra* Section II.D.4.

calculations in Appendix 10: Commercial FSS Incumbent and Grandfathered Wireless Service Protections to determine if the frequency is allowable given the co-channel aggregate interference threshold available to the SAS for that earth station. Similar determinations and calculations are performed for other protected systems in the area (in this case, two PPAs with two different PAL licensees and a SMA-PPA).

At this point the SAS returns the result of the Spectrum Inquiry to the yellow GAA. To illustrate the breadth of devices factored into the aggregate interference calculation, consider the diagram shown in Figure 14, which depicts some of the major components in the calculation of the Aggregate Interference Protections for one of the PPAs in PAL 1's OA. As a result of Interference Partitioning negotiations with other SAS Administrators, this SAS has to protect the area within the PPA with a -85 dBm threshold (5 dB below the PPA protection of -80 dBm / 10 MHz). The Aggregate Interference Calculation considers the interference contributions from the following sources because the SAS is managing all of these:

- The GAA making the Spectrum Inquiry (yellow, adjacent channel);
- The SAS's other GAAs in the area (red), some of which are co-channel;
- Another PPA in an SMA within the PAL OA; and
- A PPA in a different OA (adjacent channel).

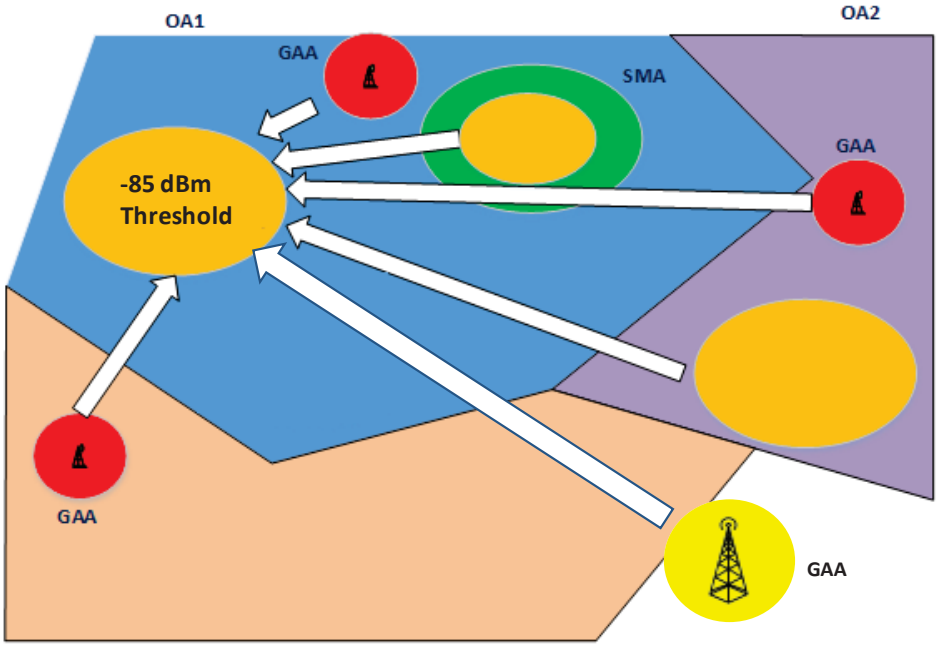

Figure 14: Factors in the calculation of Aggregate Interference to the Border of the PAL PPA (simplified).

The interference calculation considers the predicted interference contribution from each CBSD in the preceding list based on registered parameters (*e.g.*, location and antenna configuration) and Spectrum Grants (e.g., frequencies and maximum transmit powers).

After performing all of these calculations and applying spectrum obfuscation policies as needed, the SAS can return the results to the yellow CBSD of the availability of spectrum on Channel 8.

PART III: ESC OPERATOR PROPOSAL

Federated Wireless is pleased to provide the following proposal to serve as an ESC operator. The ESC operator proposal provided in this section details how Federated Wireless will comply with the requirements and core functions described in Part 96, subpart G of the Commission's rules. Specifically, this proposal details how the Federated Wireless ESC solution will accomplish the following:

- accurately detect the presence of a federal Incumbent User system in the 3550-3650 MHz band and adjacent frequencies;
- communicate information about the presence of a signal from a federal Incumbent User system to one or more approved SASs;
- maintain security of detected and communicated federal signal information;
- be available at all times to immediately respond to requests from authorized Commission personnel for any information collected or communicated by the ESC;
- ensure that the ESC operates without any connectivity to any military or other sensitive federal database or system; and
- ensure that the ESC does not store, retain, transmit, or disclose operational information on the movement or position of any federal system or any information that reveals other operational information of any federal system that is not required to effectively operate the ESC by Part 96.[142]

A. MINIMUM PROPOSAL REQUIREMENTS AND STATEMENT OF COMPLIANCE

Consistent with instructions provided in the Application Procedures PN, Federated Wireless is providing one proposal for certification as both a SAS Administrator and an ESC operator. The minimum required information for the ESC proposal is provided in Section I.A of this document. Federated Wireless' technical expertise, financial capabilities, business structure, and fees are described in Section I.B. The following additional information is provided to aid in the Commission's review of this proposal:

[142] *See* 3.5 GHz Order at para. 386; *see also* 47 C.F.R. § 96.67.

- Federated Wireless possesses sufficient technical expertise to operate an ESC. As described in Section I.B.1, Federated Wireless has contributed significantly to ESC development, starting with the work done by Federated Wireless' founders who first proposed the sensing as a mechanism to convert coastal Exclusion Zones into dynamic Protection Zones, and more recently in its efforts working with key DoD constituents at the WINNF to establish ESC requirements. Federated Wireless has developed a prototype of the sensor technology it will use as part of its ESC and has begun lab and field validation of this sensor technology.

- Federated Wireless is financially capable of operating an ESC for a five year term. Fees associated with the SaaS delivery model described in Section I.B.2(c)(i) of this proposal will include the costs to deploy, manage, and maintain both the SAS and ESC. Pricing models will follow well-known conventions established in the Software as a Service industry, segmenting pricing tiers/bundles to respond to the services required by customers' varying business needs. PAL and GAA users – *i.e.*, the entities that deploy and operate CBSDs – will be responsible for the SaaS fees and these fees will be collected through a variety of flexible methods including direct billing, credit card payment, etc. Federated Wireless will not have a commercial relationship with the user or users connected to EUDs.

Federated Wireless's statement of compliance is found in Section I.C of this document. Federated Wireless affirms that it will comply with all Commission rules governing the operation of an ESC, as well as any other rules that may apply to the manufacture, deployment, and operation of the RF sensors incorporated in the ESC. Federated Wireless does not perceive any conflict of interest in operating both a SAS and ESC. However, should the Commission identify specific conflicts, Federated Wireless will act swiftly to resolve such conflicts.

B. FEDERATED WIRELESS IS A NON-GOVERNMENTAL ENTITY

Federated Wireless affirms that it is a private, for-profit company, and that it will manage and maintain the ESC proposed herein.

C. DETAILED ESC TECHNICAL PROPOSAL

A detailed technical proposal for the Federated Wireless ESC is provided for Commission review in Appendix 16: Environmental Sensing Capability. The proposal contains company confidential and proprietary information and is therefore redacted from the public proposal in

accordance with Commission rules.[143] The following sections of this proposal, however, provide the information necessary to publicly demonstrate compliance with Part 96, Subpart G of the Commission's rules.

D. ESC OVERVIEW

As described in section 96.67(a),[144] the primary purpose of the ESC is to facilitate coexistence of CBRS users with federal Incumbent Users through signal sensing. An ESC is to be operated by a nongovernmental entity and is not to rely on governmental agencies to affirmatively communicate information about the operations of incumbent radio systems.

The Federated Wireless ESC consists of dedicated sensors deployed in coastal Exclusion Zones (*e.g.*, continental U.S. ("CONUS") Exclusion Zone regions as currently defined by the NTIA and CONUS or outside CONUS ("OCONUS") regions that may be defined in the future) interfacing with an ESC Decision System. Federated Wireless's ESC consists of dedicated sensors deployed along U.S. coastlines, which interface with an ESC Decision System. The sensors are designed, manufactured, and programmed in the U.S. to detect 3550-3650 MHz SPN-43 naval radar operations. The Federated Wireless ESC uses a fixed RF bandpass filter and field programmable gate array ("FPGA") with anti-tamper and secure boot functionality, which restricts sensor reconfigurability and mitigates cybersecurity risk. Upon detection of federal Incumbent User operations, the sensors report over a secure link to the ESC Decision System a quantized received signal strength indication ("RSSI") in each 10 MHz channel in the 3550-3650 MHz band. The ESC Decision System uses the RSSIs to interpolate the signal level of the federal transmission at each

---

[143] *See* 47 C.F.R. §§ 0.457, 0.459. Federated Wireless further observes that information contained in the Appendix may also be sensitive from an operations security and cybersecurity standpoint. Detailed, public disclosure of certain ESC system specifications, such as the sensor hardware design and sensor security methods, may inadvertently inform an adversary on potential vulnerabilities and increase security risks.

[144] 47 C.F.R. § 96.67(a).

point along the coastline. This signal strength estimate, together with known locations and configurations of CBSDs as provided through a secure interface to the SAS, are then used to determine a Protection Zone for each 10 MHz channel. The ESC Decision System accurately and securely reports the Protection Zones to the SAS, and the SAS suspends or reassigns all CBSDs within the Protection Zone to ensure protection of federal transmissions.

1. ESC Architecture

Figure 15 illustrates the Federated Wireless ESC architecture, consisting of a set of dedicated ESC sensors that provide sensing results to an ESC Decision System. The ESC Decision System then provides federal Incumbent User detection events to the SAS, allowing the SAS to suspend CBSD operation or relocate CBSDs to frequencies unoccupied by federal Incumbent Users as necessary to prevent harmful interference to such Users. ESC sensors and the overall ESC solution comply fully with Commission rules and, as described in the following subsections, with requirements and standards established by a multi-stakeholder group within the WINNF.

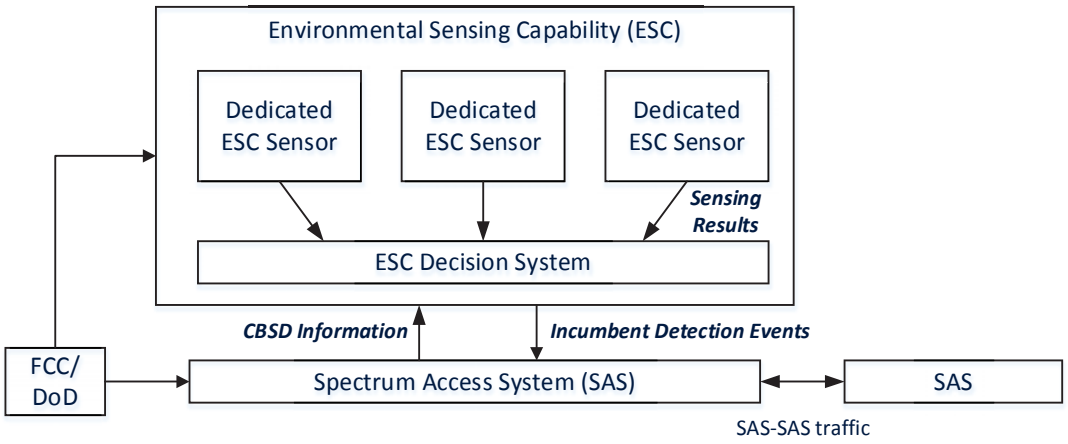

Figure 15. Federated Wireless ESC Architecture

To comply with section 96.67(c)(6), a secure GUI makes the ESC available to respond to requests (*e.g.*, evacuation drills, response to instructions from the President of the United States) from authorized Commission and DoD personnel.[145]

The Federated Wireless ESC includes sensors situated along the coastline and, to the extent possible, positioned at a location above average terrain, allowing for an unobstructed view of the ocean. ESC sensors will be spaced, on average, 30 to 40 kilometers apart along the coastline, and the precise sensor deployment locations will be determined to ensure that at least three sensors are capable of sensing each at-sea location within 50 km of the coast. The use of multiple sensors results in a resilient, high-availability system and ensures that the ESC can reliably detect federal transmissions.

ESC sensors are connected to a secure, low-latency wireless or wired interface to an ESC Decision System and will provide coarse time-stamped RSSIs in 10 MHz channels where the RSSI exceeds a detection threshold. The total time for an ESC detection event – including the sensor measurement, information transmission, decision, and reporting to the SAS – is expected to take less than three seconds.

[145] *Id.* § 96.67(c)(6).

The ESC Decision System will have access to the SAS's CBSD database, allowing it to dynamically determine detection thresholds at each location and 10 MHz channel on the coastline. This dynamism is needed to ensure that the federal Incumbent User is protected from the aggregate interference of CBRS transmissions. At frequencies and locations where the threshold is exceeded, the ESC Decision System will activate a Protection Zone and report the Protection Zone to SAS.

2. Detection and Protection of Federal Incumbent Users

The Federated Wireless ESC utilizes recommendations and methodologies developed through WG2 of the WINNF SSC to accurately detect the presence of a signal from a federal system in the 3550-3650 MHz band. Through collaboration with DoD stakeholders, WG2 has developed recommendations for detection of federal transmission and protection of federal Incumbent Users. These recommendations are based on OPSEC principles that preserve mission success of federal Incumbent Users by preventing inadvertent compromise of sensitive or classified activities, capabilities, or intentions at tactical, operational, and strategic levels. Federated Wireless founder Charles Clancy is the WG2 chair, Federated Wireless was the lead author of the OPSEC document, and, together with Google, Federated Wireless also co-led a task group focused on developing additional ESC requirements.

The overall detection and protection concept of ESC operation is shown in Figure 16.

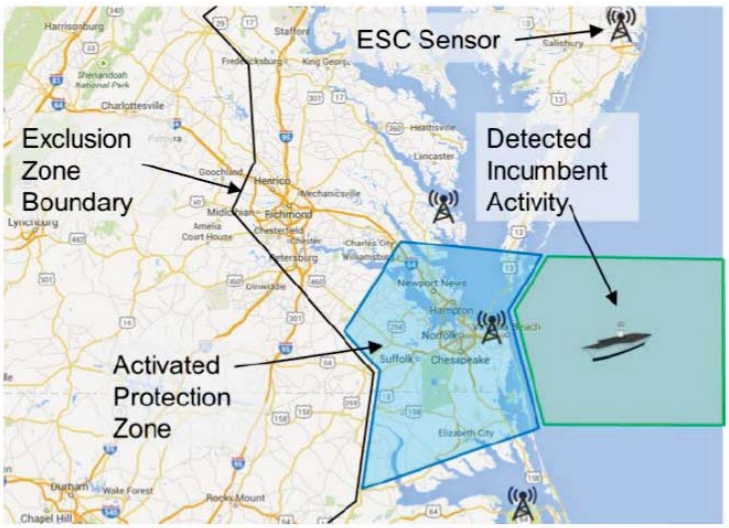

Figure 16. Relationship between federal transmission detection, ESC-activated Protection Zone, and NTIA-defined Exclusion Zone.

The ESC detects a federal transmission originating from a defined detection zone (at sea), based on coarsely time-stamped, quantized RSSI measurements provided by sensors that securely communicate with the ESC Decision System, and the ESC activates a Protection Zone defined as a subset of the NTIA-defined Exclusion Zone to provide federal incumbent protection. Aggregate interference to the federal incumbent is reduced by instructing CBSDs within the Protection Zone to move from a channel or frequency range that would cause interference to a channel or frequency range that would not cause interference. If necessary, the ESC may also instruct CBSDs to cease transmissions. The SAS instructs CBSDs to change channels, frequency ranges, or to cease transmissions over the SAS-CBSD protocol defined by the WINNF. Following a detection event, the Federated Wireless SAS will, within 300 seconds after the ESC communicates the event in a given area, confirm suspension of the CBSD's operation or its relocation to another unoccupied frequency.

With respect to federal Incumbent User detection and protection, WG2 recommends that:

- An ESC shall be capable of detecting an in-band signal associated with the SPN-43 air marshaling radar over a maximum propagation loss from the radar of 184 dB.

- Within the Protection Zone, CBRS activity authorized by the SAS will be managed such that the aggregate I/N ratio in the radar receiver does not exceed -6 dB.[146]
- An ESC shall be capable of detecting in-band federal Incumbent User radar activity within 60 seconds with 99% probability.[147]

The Federated Wireless ESC meets or exceeds these recommendations established by WG2.

3. SAS Connectivity

As illustrated in Figure 15 the Federated Wireless ESC connects to the Federated Wireless SAS for the purpose of: (a) communicating the presence of a signal from a federal Incumbent User system in the form of an Incumbent User detection event; and (b) obtaining CBSD location and configuration data from the Federated Wireless SAS database to enable the ESC Detection System to compute the detection threshold and Protection Zone. Apart from the information exchange between the SAS and the ESC, through a defined interface and message protocol, and over a secure communication link, each system operates independently of the other.

The Federated Wireless ESC communicates only with the Federated Wireless SAS. At this time, Federated Wireless does not anticipate connecting its ESC to other SASs. Due to "system-of-system" security risks identified by WG2, the Federated Wireless SAS will not share ESC information with other approved SASs.[148]

4. ESC, Sensor, and SAS Cybersecurity

Federated Wireless will ensure that unauthorized parties cannot access or alter the ESC or individual sensors or otherwise corrupt the operation of the ESC in performing its intended

---

[146] *See* NTIA 3.5 GHz Report at 10-11.

[147] The current WINNF WG2 requirement, developed in collaboration with the DoD, was established prior to the release of the Second Order. Federated Wireless will comply with any future revisions to this requirement.

[148] WG2 recommendations currently prohibit sharing of ESC information between SASs that receive input from different ESCs due to security risks. Of course, Federated Wireless will comply with any ESC information sharing requirements adopted by the Commission or if WG2 revises its recommendation.

functions. Threats to the ESC include unauthorized access, alteration, or corruption of ESC software functions; unauthorized use of sensors; and intrusion and tampering with sensor hardware, software, or functions. Additional OPSEC security threats, which have been carefully analyzed by WG2, include Internet-connected devices that probe the SAS through spectrum access queries and, as a result, learn information about federal Incumbent Users (*e.g.*, location, movement, spectrum use, etc.) at a higher level of fidelity than can be discovered through other publicly available information sources (*e.g.*, news reports about naval activity).

Federated Wireless will apply the following measures to ensure that ESC, sensor, and SAS operations are not compromised by attack, damage, or unauthorized access:

- As with the Federated Wireless SAS, software functions for the ESC (*i.e.*, the ESC Decision System) are hosted in a secure cloud environment provided by Federated Wireless' cloud partner. The cloud partner's services are trusted by many of the largest federal and commercial enterprises in part because of the robust controls established to maintain security and data protection in the cloud. The Federated Wireless cloud security procedures and protocols described in Appendix 15: Security will be applied to ESC operation.

- Access to interact with the ESC software platform will be restricted to authorized Federated Wireless personnel, Commission personnel, and other government personnel. The general public will not have access to, or the ability to interact with, any ESC software functions.

- As described in Appendix 16: Environmental Sensing Capability, Federated Wireless is coordinating closely with its contract manufacturer to mitigate cybersecurity risks in the supply chain.

- To prevent unauthorized use, the Federated Wireless sensor employs a secure boot function to ensure that the sensor can only be operated when authenticated by, and communicating with, the Federated Wireless ESC Decision System.

- Federated Wireless will implement physical security controls at sensor site locations, including restricting access to authorized personnel, installation of tamper-proof equipment enclosures, etc.

- The locations of sensor sites will be maintained by Federated Wireless and shared only with authorized personnel of approved SAS Administrators, ESC operators, Commission personnel, and government personnel.

- As described in Appendix 16: Environmental Sensing Capability, the Federated Wireless sensor has limited reconfigurability to address risks associated with intrusion and tampering of fielded sensor hardware.[149]

- Federated Wireless will implement interim and final recommendations of WG2 related to CBSD authorization limiting, obfuscation of federal Incumbent User detection events, public release of CBSD registration information, and federal incumbent frequency obfuscation in channel availability lists to assure that OPSEC is fully maintained.

5. Availability to Respond to Requests from Authorized Commission Personnel

Consistent with Section 96.67(c)(6), Federated Wireless will ensure that the ESC is available at all times to immediately respond to requests from authorized Commission personnel for any information collected or communicated by the ESC.[150] Access may be needed for the Commission to, for example, update or modify Protection Zones, or conduct evacuation drills. Additional information is found in Appendix 4: Access Protocols and Procedures, Appendix 5: Database Information, and Appendix 6: Information Retention.

Federated Wireless will also provide authorized Commission or government personnel access to a dashboard (as utilized by the NOC) indicating the general status, availability, and operational integrity of the ESC and sensor network.

6. Federal System Information Safeguards and Protection

Consistent with section 96.67(c)(7), the Federated Wireless ESC operates without any connectivity to any military or other sensitive federal database or system.[151] The Federated Wireless ESC also does not store, retain, transmit, or disclose operational information on the movement or

---

[149] *See infra* Appendix 16.

[150] 47 C.F.R. § 96.67(c)(6).

[151] *Id.*. § 96.67(c)(7).

position of any federal system or any information that reveals other operational information of any federal system that is not required by this part to effectively operate the ESC.[152]

To maintain OPSEC, the Federated Wireless ESC will report only coarse time-stamped, quantized RSSI measurements. These RSSI measurements will not be stored or retained by the ESC. Processing of RSSI measurements will be limited to comparison of the measured RSSI against a pre-defined detection threshold. Further, the ESC will not store or transmit any time-series data for detected federal Incumbent User signals; store or transmit radar signal waveform characteristics; time-stamp measurements with precision sufficient to enable Time Difference of Arrival geolocation techniques; or employ sensors with receivers or antennas capable of precise angle or arrival estimation.

Additionally, to prevent unintended disclosure of operational information on the movement or position of any federal system, the Federated Wireless ESC will maintain a federal Incumbent User position estimate uncertainty in the range of 25 – 65 nautical miles.

7. Sensor Deployment Locations and Sensor Network Operations

As authorized under section 96.67(d), ESC equipment may be deployed in the vicinity of the Exclusion Zones and Protection Zones to accurately detect federal Incumbent User transmissions.[153]

Federated Wireless will install its sensors along CONUS and OCONUS coastal areas. The sensors will be installed on commercially available communications towers, building rooftops, or other structures that are sufficiently elevated with respect to local clutter and provide an unobstructed line-of-sight measurement path to the horizon. Each sensor deployment location will

---

[152] *Id.*

[153] *Id.* § 96.67(d).

be selected to ensure it meets access and physical security requirements necessary to ensure the sensor is operated in a safe and secure manner, and that the general public and unauthorized persons cannot gain access to the sensor. Federated Wireless does not intend or require that its sensors be deployed on federal government facilities.

Each sensor will be handled and installed by Federated Wireless professional installers. The installation team will follow industry standard processes to ensure that sensors are securely handled and installed on sites. Access to site facilities will be limited to Federated Wireless personnel, Federated Wireless contractors or subcontractors, and persons authorized to access the site by the facility owner or authorized manager. All sensor installations will comply with the Commission's rules governing wireless facility siting.

E. ESC-SAS COMMUNICATIONS

1. ESC-SAS Message Protocol

A proprietary interface between the Federated Wireless ESC and the Federated Wireless SAS will convey a geographical description of the Protection Zone for any 10 MHz channels where the ESC Decision System detects federal Incumbent User activity.[154]

2. Communications Security

The SAS-ESC communications link security is described in Section II.F.4 and Appendix 15: Security. Secure communications between the Federated Wireless SAS and Federated Wireless ESC will be satisfied using an industry-recognized PKI, which is comprised of a hierarchical set of roles, policies, and procedures needed to mutually authenticate, create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption. The purpose of this PKI structure is to

[154] The WINNF has not yet initiated an effort to standardize the ESC-SAS interface. If the WINNF opts to develop a standard interface and protocol, Federated Wireless will implement the ESC-SAS interface according to WINNF requirements.

facilitate legitimate electronic communications between the SAS and ESC in a secure manner. To protect the exchange of information and communications between the SAS and ESC, TLS—a protocol created to provide authentication, confidentiality, and data integrity between two communicating applications—will be used with the PKI structure.

F. SENSING METHODOLOGY

Federated Wireless has developed a methodology to accurately and reliably detect federal Incumbent User transmissions. Sensors will provide coarsely time-stamped quantized RSSIs in 10 MHz channels where the RSSI exceeds a detection threshold. These RSSI measurements will be used by the ESC Decision System to activate Protection Zones and manage CBSD frequency assignments and use.

1. Sensor Types

The Federated Wireless ESC sensor is a dedicated, purpose-built "listening device" that operates independently of CBSD infrastructure or CBRS EUDs. The sensor performs signal processing using the known properties of radars in the 3550-3650 MHz band to accurately and reliably detect those federal Incumbent User transmissions, as it is important that the sensor be able discern federal Incumbent User transmissions from other uses of the band, such as transmissions by CBSDs or EUDs.

The components comprising the Federated Wireless sensor include:

- Polycarbonate Weatherized Enclosure #1:
    - Sensor Device
    - Internal Antenna (180 beam width and 6 dBi Gain)
- Polycarbonate Weatherized Enclosure #2:
    - AC/DC Convertor
    - AC Surge Protector

  - Battery Backup
  - Wireline or Wireless Modem/Router
  - Power over Ethernet ("POE") injector
- Bracket/Harness to install these units on poles and against walls.

2. Sensing Method

The Federated Wireless ESC Detection System relies on coarsely time-stamped, quantized RSSI measurements to determine a detection threshold for federal Incumbent User activity. The ESC Decision System interpolates RSSI measurements reported by the sensors to estimate RSSI at each coastline location. The threshold detection methodology exploits the reciprocal properties of RF propagation as described in detail in NTIA Report 16-521.[155] That is, the methodology relies on the observation that propagation loss from an at-sea radar to a sensor location will be equal to or less than the propagation loss from the sensor location to the same radar receiver. As a result, the ESC Decision System need only establish an appropriate signal reception level (*i.e.*, the detection threshold) *from* the radar system transmission to determine if the aggregate signal transmissions from CBSDs *to* the radar will exceed an acceptable limit (*i.e.*, -6 dB I/N). To establish the detection threshold, the ESC Decision System models the propagation loss from the location of each CBSD location to a location on the coastline where the at-sea propagation loss reciprocity can be applied. Using this approach, the only signal processing done by the ESC and sensor is interpolation of the quantized RSSI measurement and comparison of the interpolated data against a computed detection threshold.

[155] *See* NTIA Radar Detection Report. The report recommends an approach to ESC sensing, and was released shortly before the filing deadline for prospective ESC operators. Federated Wireless was generally aware of and collaborated with NTIA and ITS on aspects of the study which is manifested in the use of the propagation loss reciprocity approach in the ESC sensing methodology proposed here. The NTIA study, at p. 25 – 27, summarizes the application, and potential benefits of, the proposed approach and presents recommendations for future work. Among those recommendations is the treatment of aggregate interference from CBSDs, which Federated Wireless believes it has addressed in its proposal.

At no point during a detection event does the Federated Wireless ESC Detection System predict or estimate the at-sea propagation loss, which would be an input to a geolocation computation of the federal incumbent system. At no point (*e.g.*, within the system or a subsystem) is the location of a federal Incumbent User accurately estimated or tracked in the Federated Wireless ESC. In this manner, the Federated Wireless ESC does not reveal any information pertaining to the location or movement of any federal incumbent system.

3. Sensor Sensitivity

As described in Appendix 16: Environmental Sensing Capability, detector performance for the Federated Wireless sensor hardware has been simulated and verified in laboratory testing. Simulations demonstrate that a probability of detection of 99% under normal operating conditions is achieved with, on average, one false alarm every 370 days. The associated sensor receive sensitivity is found to be well in excess of what is required for detecting in-band federal transmissions over a maximum propagation loss in excess of 180 dB.

4. Sensor Resiliency to Front-End Saturation and Burn-Out

As described in Appendix 16: Environmental Sensing Capability, the Federated Wireless sensor hardware has been designed with overload protection circuitry to prevent front-end saturation and burn-out from in-band (3550-3650 MHz) and adjacent bands operating in close proximity of the sensor. The ESC sensor also includes alarms, remotely monitored by the ESC Operating Center, to indicate sensor hardware failure should one occur.

G. SENSOR COMMUNICATIONS

1. Sensor Communication Methods

The sensor will communicate with the ESC software platform using a secure, low-latency wireline or wireless connection. The specific connection type will be based on deployment factors

such as availability, cost, and connection reliability. The same level of communications security can be maintained regardless of the physical medium employed.

Secure communications between the Federated Wireless ESC software platform (*i.e.*, the ESC Decision System) and fielded sensors will be satisfied using an industry-recognized PKI, which is comprised of a hierarchical set of roles, policies, and procedures needed to mutually authenticate, create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption. The purpose of this PKI structure is to facilitate legitimate electronic communications between the SAS and ESC in a secure manner. To protect the exchange of information and communications between the SAS and ESC, TLS —a protocol created to provide authentication, confidentiality, and data integrity between two communicating applications— will be used with the PKI structure.

Similar to operational concepts for CBSDs, each sensor will register and authenticate with the ESC and it will operate under the direct control of the ESC. A sensor will cease its operation if the communications link to the ESC software platform is lost or compromised.

2. Verification of Sensor Operation and Communications

As described previously, the Federated Wireless ESC solution uses RSSI measurements collected from multiple sensors to monitor for federal transmissions. If a single sensor fails, its performance degrades, or it ceases to communicate, the ESC Decision System can utilize measurements derived from other normally functioning sensors to detect the presence of a federal Incumbent User and activate or manage Protection Zones. The network of sensors provides resilience in the ESC system that ensures continued system availability in the event of a component failure.

To verify sensor operation and communication, the sensor hardware module and sensor installation site will be remotely monitored 24/7 by the Federated Wireless NOC. Alarms at the

NOC will be activated if a sensor ceases operation due to hardware or power failure; the sensor performance is impacted or degraded; communications with the sensor is degraded or fails; if the sensor enclosure is tampered with; or upon unauthorized access to the site location. The NOC will employ industry-standard troubleshooting and event escalation procedures, and technicians will be dispatched to resolve alarm events. Trouble resolution times will be based on the severity of the alarm event or outage. Outage information will be supplied to the ESC Detection System. If ESC detection capability is compromised or degraded as a result of the outage the ESC Detection System will, as a fail-safe mechanism, activate a Protection Zone using the procedures described in Section III.D.2 until service is restored.

Additional measures Federated Wireless will employ to ensure high availability of the ESC include the following:

- At locations where federal incumbent activity is expected to be high (*e.g.*, Norfolk-Virginia Beach, VA or San Diego, CA) redundant sensors will be deployed to support standby failover.
- Qualified field technicians will be available on a regional basis to reduce travel time to sensor locations for on-site troubleshooting, maintenance, or repair.
- An inventory of spare components (*e.g.*, sensor hardware, antenna, power supply, etc.) will be maintained at regional depots.
- Regular sensor hardware and site checks will be performed by qualified technicians to address maintenance issues before they become service-impacting.

CONCLUSION

Federated Wireless looks forward to the opportunity to serve as a SAS Administrator and ESC operator. The innovative regulatory framework for the CBRS will bring to market the myriad benefits of spectrum sharing first identified by PCAST in 2012. The request for, and submission of, SAS Administrator and ESC proposals is yet another crucial milestone reached in the march toward launch of commercial services in the CBRS. That these proposals are being submitted within one year of the first Report and Order in this proceeding speaks well of the Commission's leadership, the cross-industry stakeholder collaboration in developing standards and solutions, and the building excitement and momentum toward launch of the CBRS.

Respectfully submitted,

/s/

Kurt Schaubach
Chief Technology Officer
Federated Wireless, Inc.
4301 North Fairfax Drive
Suite 301
Arlington, VA 22203

May 16, 2016

PROPOSAL COMPLIANCE

To aid in the Commission's review and evaluation of the compliance of the proposed SAS and ESC systems, this following indicates which section(s) of this proposal are responsive to the requirement.

All proposals must at a minimum include the following information:

Requirement from Application Procedures PN	Relevant Document Section(s)
A detailed description of the scope of the functions that the SAS and/or ESC would perform.	I.A.1
A demonstration that the prospective SAS Administrator or ESC operator possesses sufficient technical expertise to operate an SAS and/or ESC, including the qualifications of key personnel who will be responsible for operating and maintaining the SAS and/or ESC.	I.B.1 Appendix 1
The prospective SAS Administrator or ESC operator must demonstrate that it is financially capable of operating an SAS and/or ESC for a five year term. The proposal must include a description of the prospective SAS Administrator or ESC operator's business structure including ownership information. To the extent that the proponent will rely on fees to support its operations, the proposal should also describe the fee collection process and the entities from which the fees will be collected.	I.B.2 Appendix 2
A description of how data will be securely communicated between the SAS and its associated ESC and how quickly and reliably these communications will be accomplished.	I.A.2 II.C II.F III.E
Technical diagrams showing the architecture of the SAS and/or ESC and a detailed description of how each function operates and how each function interacts with the other functions.	I.A.2
A description of the propagation model and any other assumptions that the prospective SAS Administrator or ESC operator proposes to use to model operations and facilitate coordination in the band.	I.A.3 II.D Appendix 19
A description of the methods that will be used to update software and firmware and to expeditiously identify and address security vulnerabilities.	I.A.4 II.F III.D.4 Appendix 15 Appendix 16
An affirmation that the prospective SAS Administrator and/or ESC operator (and its respective SAS and/or ESC) will comply with all of the applicable rules as well as applicable enforcement mechanisms and procedures.	I.C.3 I.C.5 I.C.6 I.C.11

SAS proposals must also provide the following information:

Requirement from Application Procedures PN	Relevant Document Section(s)
A detailed description of how the SAS will retain, secure, and verify information from CBSDs (including location data), licensees, associated ESCs, and other SASs.	II.B Appendix 5 Appendix 6
A demonstration that the SAS will be capable of resolving various sources of interference between and among Citizens Broadband Radio Service users and/or Incumbent users	II.D II.E.8 II.E.9 Appendix 10 Appendix 16
A description of how the SAS will ensure that non-federal FSS earth stations and grandfathered 3650-3700 MHz licensees are protected from harmful interference consistent with the rules.	II.D.5 Appendix 8 Appendix 10
A description of how coordination will be effectuated (e.g., through data synchronization) between multiple SASs, if multiple SASs are authorized, and how quickly this synchronization of data will be accomplished.	II.E
If the prospective SAS Administrator will not be performing all SAS functions, it must provide information on the entities operating other functions and the relationship between itself and these other entities. In particular, it must address how the Commission can ensure that all of the requirements for SAS Administrators in Part 96, subpart F are satisfied when SAS functions are divided among multiple entities, including a description of how data will be transferred among these various related entities and SASs, if multiple SASs are authorized, and the expected schedule of such data transfers (i.e., real-time, once an hour, etc.).	II.A
A description of the methods (e.g., interfaces, protocols) that will be used by: (1) CBSDs to communicate with the SAS; (2) the SAS to communicate with CBSDs; (3) the SAS to communicate with other SASs; and, if applicable, (4) the SAS to communicate with one or more ESCs. The prospective SAS Administrator must also describe the procedures, if any, which it plans to use to verify that a CBSD can properly communicate with the SAS.	II.C Appendix 13 Appendix 16
An affirmation that, consistent with section 96.55 of the Commission's rules, the SAS will only retain records and information or instructions received regarding federal transmissions from the ESC in accordance with information retention policies established as part of the ESC approval process.	I.C.4 III.D.6 Appendix 6
A description of the security methods that the prospective SAS Administrator plans to use to ensure that unauthorized parties cannot access or alter the SAS or otherwise corrupt the operation of the SAS in performing its intended functions, consistent with the Commission's	II.F.1 Appendix 4 Appendix 9

rules.	
Descriptions of dynamic use-case scenarios for how the SAS will manage and assign spectrum resources to ensure that geographically and spectrally adjacent operations are coordinated consistent with the Commission's rules. Use case scenarios should include the methodology and protection approach for cases of radio interference due to adjacent blocking, out-of-band emissions, and aggregate co-channel interference. Describe how multiple SASs will coordinate the calculation of aggregate interference for protecting Incumbent users and Priority Access licensees.	II.D Part II. Section G.
A description of the methods that the SAS will use to make information stored or retained by the SAS available in response to a request from authorized Commission personnel.	I.A.2 II.B.10 Appendix 4

ESC proposals must also include the following information:

Requirement from Application Procedures PN	**Relevant Document Section(s)**
A description of the methods (e.g., interfaces, protocols) that will be used by the ESC to communicate with the SAS. It must include a description of the security methods or protocols that will be used to ensure that unauthorized parties cannot access or alter the ESC or otherwise corrupt the operation of the ESC in performing its intended functions.	I.A.2 III.C Appendix 9 Appendix 16
A description of the sensing methodology it will use to detect federal transmissions and determine that the spectrum needs to be evacuated. This description must include a detailed description of the type of sensors to be used (i.e., infrastructure or device based), the sensing architecture to be employed, the sensing thresholds, any processing of sensor data, sensor sensitivity, and sensor resiliency to receiver front-end saturation and burn-out. The prospective ESC operator must also provide a description of the safeguards that will be used to "ensure that the ESC does not store, retain, transmit, or disclose operational information on the movement or position of any federal system or any information that reveals other operational information of any federal system that is not required to effectively operate the ESC by Part 96."	III.D III.F Appendix 16
A description of the methods (e.g., interfaces, protocols) that will be used by sensors to communicate with the ESC and the procedures, if any, that it plans to use to verify that all sensors can communicate with the ESC in a timely and secure manner. It must include a description of the security methods or protocols that will be used to ensure that unauthorized parties cannot access or alter the ESC or individual sensors or otherwise corrupt the operation of the ESC in performing its intended functions.	III.D III.E III.G Appendix 16