

APPENDICES



TABLE OF CONTENTS

APPENDIX 1: SELECT FEDERATED WIRELESS BIOGRAPHIES 1

 I. Executive Leadership Team 1

 II. Technical Leadership 2

 III. Founders and Advisors 4

APPENDIX 2: OWNERSHIP STRUCTURE 7

APPENDIX 3: TERMINATION AND CONVEYANCE OF SPECTRUM ACCESS SYSTEM SERVICES 8

 I. Introduction 8

 A. Purpose and Scope 8

 II. Design 8

 III. Summary 9

APPENDIX 4: ACCESS PROTOCOLS AND PROCEDURES 10

 I. Purpose and Scope 10

 II. References 11

 III. Role Based Access Control 11

 A. Access Procedures 11

 B. Administrative Access 12

 C. General Public Access 12

 IV. CBSD Registration Data 12

 A. Category A & B CBSDs 12

 B. Category B CBSDs 13

 C. Data Obfuscation 13

 D. Operational Security 13

 V. Web Based GUI 13

 A. Search Form 13

 B. CBSD Registration Information 14

 VI. CBSD Owners and Certified Professional Installers 14

 VII. Non-Federal Incumbent and GWBL Users 15

 VIII. FCC Access 15

 A. Web Based GUI 15

 IX. Response to Government Entity Instructions 16

 A. Contact Information and 24/7/365 Availability 16



- B. Government Entity Validation..... 17
- C. Procedures and Protocols..... 17
- X. Summary..... 17
- APPENDIX 5: DATABASE INFORMATION..... 19
 - I. Purpose and Scope 19
 - A. References..... 19
 - II. Database Information Design 19
 - A. FSS Earth Stations..... 20
 - B. Grandfathered Wireless Broadband Licensees (“GWBLs”)..... 20
 - C. Exclusion Zones and Protection Zones 21
 - D. Equipment Authorization 21
 - E. Census Tracts..... 21
 - F. Canadian and Mexican Borders 21
 - G. GeoData..... 22
 - H. Priority Access Licenses 22
 - I. Secondary Market 22
 - J. CBSD Records 23
 - K. Owner Records 23
 - L. Professional Installer 24
 - M. ESC Sensors..... 25
 - N. Data Synchronization Process 25
 - III. Summary..... 25
- APPENDIX 6: INFORMATION RETENTION..... 26
 - I. Scope and Purpose 26
 - II. References 26
 - III. Data Privacy and Confidentiality 26
 - IV. Database Architecture..... 27
 - A. Incumbent Information 27
 - B. Non-Incumbent Information 28
 - C. SAS Transaction Records..... 28
 - D. ESC Data 29
 - V. Summary..... 29



APPENDIX 7: ERROR RESOLUTION AND INTERFERENCE REPORTING POLICY31

- I. Purpose and Scope31
- II. References31
- III. Identification of Data Inaccuracies31
- IV. Data Resolution Procedures.....32
- V. Interference Resolution Procedures33
- VI. Summary34

APPENDIX 8: SAS CHANNEL AVAILABILITY35

- I. SAS Architecture Supporting Frequency Assignment35
 - A. Databases36
 - B. Frequency Assignment Procedure36
- II. References42

APPENDIX 9: DEFINITION OF USE AND SECONDARY MARKETS44

- I. Overview.....44
- II. Terminology44
- III. Specifics of Solution.....45
 - A. SAS PAL Channel Assignment Under Steady-State Conditions47
 - B. PPA Protection/Allowance of GAAs48
- IV. References50

APPENDIX 10: COMMERCIAL FSS INCUMBENT AND GRANDFATHERED WIRELESS SERVICE PROTECTIONS52

- I. Protection of Fixed Satellite Service Earth Stations.....52
 - A. Overview of FSS Protection Methodology.....52
 - B. Required Inputs54
 - C. Azimuth and Elevation Angles Between FSS Earth Stations and CBSD Devices56
 - D. Antenna Gains58
 - E. Aggregate Interference Calculations61
 - F. CBSD Assignments62
- II. Protection of Existing Operators in the 3650-3700 MHz Band62
- III. References62



APPENDIX 11: PRIORITY ACCESS LICENSE CHANNEL ASSIGNMENT PLAN64

- I. Overview..... 64
- II. Band Plan 64
- III. Rules Applicable to PAL Channel Assignment..... 64
- IV. Proposed Methodology for Determining Steady-State PAL Frequency Assignments 65
- V. Extensions 66
- VI. References 66

APPENDIX 12: CBRS MEASUREMENT REPORT67

- I. Introduction 67
 - A. Purpose and Scope 67
 - B. Background 67
 - C. Assumptions and Constraints 67
- II. Functional Requirements..... 68
- III. Existing Measurement Frameworks..... 68
 - A. LTE Measurement for Mobility and Load Balancing..... 69
 - B. LTE Measurement for SON Management and Configuration 71
 - C. LTE Minimization of Drive Test (“MDT”)..... 71
- IV. CBRS Measurement System Design 73
 - A. SAS-CBSD Measurement Report Support 73
 - B. Proposed Measurement Report Framework..... 74
 - C. Proposed LTE Specific Measurement Metrics 76
 - D. Other Proposed Measurement Metrics 79
- V. Summary 80
- VI. References 81

APPENDIX 13: REGISTRATION 82

- I. Introduction 82
 - A. Purpose and scope..... 82
 - B. Background 82
 - C. Assumptions and Constraints 82
- II. Functional Requirements..... 83
- III. Registration Pre-Requisites..... 84
 - A. Owner pre-Registration 84



- B. Professional Installer pre-Registration86
- C. PAL Licensee pre-Registration87
- D. PAL Lessee pre-Registration89
- E. CBSD Authentication.....89
- IV. CBSD Registration91
 - A. Single Step CBSD Registration92
 - B. Multi-Step CBSD Registration94
- V. CBSD Spectrum Inquiry Procedure97
- VI. Summary.....98
- VII. References99
- APPENDIX 14: CERTIFIED PROFESSIONAL INSTALLERS 100
 - I. Overview..... 100
 - II. Professional Installer Certification Program 100
 - III. Handling CPIs during Registration..... 101
 - IV. Minimizing the Impact of Errors to the SAS via CPIs 102
 - A. Minimize the amount of information that is entered manually during registration..... 102
 - B. Minimize the likelihood of an error being introduced to the system during manual registration. 102
 - C. Maximize the likelihood of detecting errors post-registration and minimize the time required to correct errors. 102
- APPENDIX 15: SECURITY POLICIES AND PROCEDURES 104
 - I. Introduction 104
 - II. Security Implementation Plan..... 105
 - III. Database Security and Preventing Unauthorized Access..... 106
 - A. SAS Database Security 106
 - B. Database Threats 106
 - C. Threat Mitigation 108
 - D. Preventing Unauthorized Access 112
 - E. Security Event Monitoring and Incident Response..... 112
 - IV. Security Features to Comply with Part 96 Rules 113
 - A. Plan to Meet Requirements for Part 96..... 113
 - B. Public Key Infrastructure 114

- C. Transport Security Protocol 115
- D. Blacklisting..... 115
- V. FCC ID Verification..... 116
- APPENDIX 16: ENVIRONMENTAL SENSING CAPABILITY..... 118
 - I. Overview..... 118
 - II. ESC System Design Principles..... 118
 - III. ESC Architecture 118
 - A. ESC Sensor Design..... 119
 - B. ESC Decision System 124
 - IV. Deployment 128
 - V. Incumbent Activity Position Estimate Uncertainty 129
 - VI. Security 132
 - VII. References 133
- APPENDIX 17: TERMS OF SERVICE..... 134
- APPENDIX 18: PRIVACY POLICY 140
- APPENDIX 19: PROPAGATION MODEL IMPLEMENTATION 148
 - I. Introduction 148
 - II. NTIA Propagation Model..... 149
 - A. Executive Summary of NTIA Propagation Model (“NPM”) and NTIA Methodology 149
 - B. Land Clutter Categories..... 149
 - C. NPM High Level Operation..... 151
 - III. Extended HATA (EHATA) Propagation Model..... 153
 - A. Scenario 1 ($d \leq 100\text{ m}$)..... 153
 - B. Scenario 2 ($100\text{ m} < d < 1\text{ km}$) 153
 - C. Scenario 3 ($1\text{ km} \leq d \leq 80\text{ km}$)..... 154
 - D. Scenario 4 ($d > 80\text{ km}$) 155
 - E. Antenna Effective Height..... 156
 - F. Terrain Undulation Parameter 157
 - G. Isolated Ridge Correction (“IRC”) 160
 - H. Rolling Hilly Correction (“RHC”)..... 163
 - I. Fine Rolling Hilly Correction (“FRHC”)..... 164



- J. Terrain Slope correction ("TSR") 165
- K. Mixed Land-Sea Correction ("LSC") 167
- L. Location Variability 168
- M. Suburban Loss Correction ("SLC") 169
- N. Corrected NPM 169
- O. ITM Urban Factor ("UF") 169
- IV. Irregular Terrain Model 170
 - A. Interpolation for Elevation 172
 - B. Indoor Penetration Loss 172
- V. References 172



APPENDIX 1: SELECT FEDERATED WIRELESS BIOGRAPHIES

I. Executive Leadership Team

Iyad Tarazi, Chief Executive Officer

Iyad Tarazi joined Federated Wireless from Sprint Corp., where he served as Vice President of Network Development and led the Network Vision network modernization project. Responsibilities included overseeing the development and integration of new products and technologies within Sprint's networks and managing Sprint-Nextel's technology integration labs. Prior to the Sprint-Nextel merger, Iyad led Nextel's Network Engineering organization, managing network planning, integration performance engineering, testing, and core deployment initiatives.

Iyad also held positions with MCI and served as a Board member for CafeX Communications, which specializes in collaborative software development. Iyad has a Masters in Engineering Management from Southern Methodist University and a B.S. in Electrical Engineering from the University of Maryland.

Kurt Schaubach, Chief Technology Officer

Kurt Schaubach brings 25 years of wireless industry experience to Federated Wireless, where he plays a key role in developing technologies and new business strategies to create the next-generation architecture of broadband wireless.

Previously, Kurt served in various engineering roles at the National Rural Telecommunications Cooperative ("NRTC"), NextWave Wireless, LCC International, and Southwestern Bell. He has also served as a technology consultant to wireless network operators, equipment manufacturers, and semiconductor suppliers.

Kurt was a founding member of a publicly traded wireless broadband and multimedia software company and led the acquisition and integration of two wireless infrastructure companies. Kurt has been active in spectrum development, management, and policy matters throughout his career. He currently serves on the Commerce Spectrum Management Advisory Committee ("CSMAC"). Kurt received his B.S. and M.S. in Electrical Engineering from Virginia Tech.

Sepehr Mehrabanzad, Senior Vice President of Engineering

Sepehr Mehrabanzad brings over 20 years of product development experience to Federated Wireless. No stranger to start-ups or to spectrum, Sepehr came from Sentient Wireless, a company he co-founded with a focus on shared spectrum operation for wireless networks. Sepehr was also a founding member of Airvana, a leader in 3G mobile broadband development, where he was responsible for all engineering activities for consumer small cell product development. As the founding engineer there, he was initially responsible for radio node software architecture and implantation, and later became Vice President of Engineering for the 3G broadband macro cellular product line built for Nortel & Ericsson and deployed globally. Subsequently, he became Vice President of Engineering for consumer small cell product development. At last count, there are over 1.5 million small cells shipped by Airvana, complete with a centralized management system that accounts for RF performance and spectrum allocation. During his tenure, Sepehr expanded the



engineering capabilities from a few engineers into a multidisciplinary organization delivering full-featured, complex hardware and software solutions.

Prior to founding Airvana, Sepehr was with Motorola-Codex and Racal-Milgo. While at Motorola, he was a leading contributor in the successful commercial launch of ITU's standards for V.92 high-speed modems. Sepehr is a Senior Member of the Institute of Electronics and Electrical Engineers ("IEEE") and holds 15 patents in the fields of wireline and wireless communications. He completed his education at the Georgia Institute of Technology, where he earned a M.S. in Electrical Engineering, B.S. in Electrical Engineering, and a B.S. in Applied Mathematics.

Sarosh Vesuna, Senior Vice President of Corporate Development and Strategic Alliances

Sarosh brings more than 25 years of experience in leading innovative networking companies and creating strong business alliances. Before joining Federated Wireless, Sarosh served as vice-president and general manager of Meru Network's enterprise networking business, responsible for the overall revenue, go-to-market direction, business strategy, and partnerships.

Prior to joining Meru, Vesuna held executive roles at Motorola and Symbol Technologies, where he was responsible for wireless protocol architecture, joint ventures and acquisitions, OEM, technology partnerships, and the overall direction of the WLAN and VoIP businesses. He co-authored the IEEE 802.11 WLAN protocol and co-founded the Wi-Fi Alliance, where he served on the Board of Directors. Vesuna has an MSEE from the Pennsylvania State University, and has completed executive education from MIT Sloan and the Stanford Graduate School of Business. Vesuna also holds 10 U.S. Patents.

Ken Stewart, Senior Vice President Sales and Business Development

Ken Stewart has 20 years of global experience in technology innovation, business development, emerging markets and sales, in both start-up and mature corporations. Prior to joining Federated Wireless, Ken was Senior Vice President of Sales at GridPoint, where he was responsible for enterprise and channel sales of their cloud-based energy management platform. Ken previously held positions at Syniverse, NeuStar and MACH, successfully leading those companies' efforts to establish and build their business in the Asia Pacific region. Ken holds an M.B.A. in International Business from Saint Leo University, a B.A. from Saint Leo University, and a Certificate in Innovation Management from the University of Maryland – Robert H. Smith School of Business.

II. Technical Leadership

Sam MacMullan, Ph.D., Director of Architecture, Cognitive RF Group

Dr. Sam MacMullan joined Federated Wireless as the Director of Architecture for the Cognitive RF Group, leading the company's spectrum sensing and SAS cognitive engine development efforts. He has 25 years of experience generating algorithms and software/hardware implementations for commercial and military communication systems.

Prior to joining Federated, Dr. MacMullan was the founder and President of ORB Analytics, developing spectrum sensing, location analytics, and radio resource management solutions. Prior to ORB Analytics, he was co-founder/CTO of Radiospire Networks, creating an ultrawideband ("UWB")



wireless product for high-definition audio and video cable replacement. He has also held leading roles at Qualcomm, Texas Instruments, MIT Lincoln Laboratory, and JHU/APL. He received a Ph.D. from Notre Dame, M.S. from Johns Hopkins, and B.S. from Cornell, all in electrical engineering.

Masoud Olfat, Ph.D., Director of Technology, Standards, and Regulatory

Dr. Masoud Olfat joined Federated Wireless in May 2015, and is responsible for the development of technology and standards for the 3.5 GHz shared Spectrum CBRS system, and supporting technical regulatory developments.

Before joining Federated Wireless, Dr. Olfat worked for about 20 years in several positions responsible for LTE technology, standard, and network development at LightSquared, LTE and WiMAX technology and network development at Clearwire, Sprint and Nextel, as well as technology development for multimedia communication. He has participated actively in several standard organizations, such as IEEE802.16, WiMAX, ITU, 3GPP LTE, and 5G development in the LTE community. He has published several papers, authored several book chapters and been granted about 30 patents and has submitted another 30 patents waiting for issuance. has also held adjunct faculty positions with University of Maryland at College Park. Masoud holds a Ph.D. degree in Wireless Communications and Signal Processing from the University of Maryland at College Park.

James Ni, Ph.D., Director of SAS Systems

Dr. James Ni joined Federated Wireless in March 2014 as the Senior System Architect responsible for the architecture, design and development of the Federated Wireless SAS systems. Prior to joining Federated Wireless, James worked in various System Architect roles at Verizon, Genband Communications, and Tata/Taqua, respectively, for more than 7 years, and in various Principal and Senior Software Development roles for over 12 years with Airvana, Convergent Networks, and Lucent/Ascend/Cascade Communications. James holds a Ph.D. degree in Wireless Networking and Coding Theory from Warwick University in the U.K.

Farhad Bassirat, Ph.D., Director of Product Qualification & Certification

Dr. Farhad Bassirat joined Federated Wireless as the Director of Product Qualification and Certification in July 2015. Prior to this, Farhad worked as Director of Operation for Ericsson, managing LTE Test and Certification in Sprint's network. Farhad has worked in the wireless industry for over 25 years, managing Wireless Product Development (TDMA, CDMA, WiMAX, and LTE), Test, and Deployment teams throughout the world. He is the recipient of 13 U.S. patents, and holds a Ph.D. from the University of Kent at Canterbury.

Matthew Probst, Ph.D., Director of Cloud Services

Dr. Matthew Probst is responsible for the security, scaling, and cloud-centric architecture of Federated Wireless services. Prior to joining Federated Wireless, Matthew designed the architecture for VMWare's public cloud IaaS, PaaS, and SaaS offerings. He also spent 12 years architecting IaaS and PaaS offerings for NTT Communications with a focus on scale, security, and availability. He holds a Ph.D. in Computer Science from the School of Computing at the University of Utah, and an M.B.A. from the Marriott School of Management at Brigham Young University.

III. Founders and Advisors

T. Charles Clancy, Ph.D., Founder and Advisor

Dr. Charles Clancy is an Associate Professor in the Bradley Department of Electrical and Computer Engineering of Virginia Polytechnic Institute and State University (Virginia Tech), and is Director of the Ted and Karyn Hume Center for National Security and Technology. In this role, Dr. Clancy is responsible for leading Virginia Tech's collaboration with national security organizations within the U.S. federal government and industry. Additionally, he is involved in developing and expanding the university's role in cyber-security research and education. His current research interests include wireless security and electronic warfare.

Prior to joining Virginia Tech in 2010, Dr. Clancy spent seven years working for the US Department of Defense in a variety of research, engineering, and operations roles. The majority of his time was spent as a researcher with the Laboratory for Telecommunications Sciences, a federal research laboratory at the University of Maryland. There he led government research programs in wireless communications, with an emphasis on software-defined and cognitive radio. His research focused on efficient use of commodity processors for software-defined radio, and security implications involved in military use of cognitive radio technologies. During this time, Dr. Clancy was also heavily involved in wireless authentication and authorization protocol standardization, and held leadership positions within the Internet Engineering Task Force.

He is a Senior Member of IEEE and has produced over 80 technical publications.

Dr. Clancy received his B.S. in Computer Engineering from the Rose-Hulman Institute of Technology, his M.S. in Electrical Engineering from the University of Illinois, Urbana-Champaign, and his Ph.D. in Computer Science from the University of Maryland, College Park.

Robert McGwier, Ph.D., Founder and Advisor

Robert G. McGwier, Ph.D., serves as Technical Director of Federated Wireless, Inc. Dr. McGwier is the Director of Research for the Ted and Karyn Hume Center for National Security and Technology, and Research Professor in the Bradley Department of Electrical and Computer Engineering at Virginia Tech.

At Virginia Tech, he leads the overall execution of the Center's research mission, and leads the university's program development efforts in national security applications of wireless and space systems. His area of expertise is in radio frequency communications and digital signal processing. Before joining Virginia Tech, Dr. McGwier spent 26 years as a Member of the Technical Staff at the Institute for Defense Analyses' Center for Communications Research in Princeton, N.J., where he worked on advanced research topics in mathematics and communications supporting the federal government. His work on behalf of the federal government has earned him many awards, including one of the intelligence community's highest honors in 2002. Dr. McGwier is an avid amateur radio operator (call sign N4HY) and has previously served as the Vice President of Engineering for the Amateur Radio Satellite Corporation as well as a member of its Board of Directors. He is a member and former Director of the Tucson Amateur Packet Radio. He won the Dayton Amateur Radio Association Technical Award in 1990 and the Central State VHF Society Chambers Award in 2007 for his work in software defined radio and its application to amateur radio.

Dr. McGwier received his Ph.D. in applied mathematics from Brown University.



Jeffrey H. Reed, Ph.D., Founder and Advisor

Dr. Jeffrey H. Reed is the Willis G. Worcester Professor in the Bradley Department of Electrical and Computer Engineering at Virginia Tech. He currently serves as Founding Director of Wireless@Virginia Tech, one of the largest and most comprehensive university wireless research groups in the US. In 2010, he founded the Ted and Karyn Hume Center for National Security and Technology and served as its interim director.

Dr. Reed's area of expertise is in software radios, smart antennas, wireless networks and communications signal processing. He has authored, co-authored, or co-edited ten books and proceedings, contributed to six books, and authored or co-authored over three hundred journal and conference papers. His book on Software Defined Radio is considered one of the earliest and most comprehensive books on the subject. In September 2014, his book on Cellular Networks was published by Wiley and IEEE Press and is a comprehensive review of fundamentals and cellular network operations.

Dr. Reed has served on panels, coordinated numerous workshops & conferences, and served on advisory groups for the Department of Commerce, DoD, State of Virginia, and NSF as well as technical advisory boards for many companies. Recently he served as associate editor for the Proceedings of the IEEE issues on cognitive radio.

Dr. Reed is currently the principal investigator on an NSF project to examine enforcement and regulatory technologies for spectrum sharing between commercial wireless and government users. Since joining Virginia Tech in 1992, Dr. Reed has been PI or co-PI on over 100 different sponsored research projects covering areas such as software radio, cognitive radio, ultrawideband, and channel modeling.

Dr. Reed served on the President's Council of Advisors on Science and Technology Working Group on how to transition federal spectrum for commercial economic benefits. In 2014, Dr. Reed was selected to be a member of CSMAC, the advisory group on spectrum issues for the U.S. Department of Commerce.

In 2005, Dr. Reed became a Fellow to the IEEE for his contributions to software radio and communications signal processing and for leadership in engineering education. In 2013, he received the International Achievement Award from the Wireless Innovations Forum for the impact of his accumulated research. In 2014, Dr. Reed served as co-general chair for the IEEE Dynamic Spectrum Access Network conference.

Dr. Reed received his B.S., M.S., and Ph.D. degrees from the University of California, Davis.

Joseph Mitola III, Ph.D., Founder and Advisor

Dr. Mitola, Fellow of the IEEE, is recognized globally as "the Godfather" of software radio and cognitive radio technologies on which smart phones are based, and brings over 40 years of experience to his role as co-founder of Federated Wireless.

His seminal research and publications on software radio, software-defined radio, and cognitive radio, including his book, Software Radio Architecture and Cognitive Radio Architecture (Wiley 2006), on which the U.S. Department of Defense (DoD) based dynamic spectrum access and the Federal Communications Commission (FCC) based spectrum sharing.

Dr. Mitola serves as Subject Matter Expert for Virginia Tech's Hume Center for National Security and Technology.



From 2008-2012, Dr. Mitola was Vice President for the Research Enterprise of Stevens Institute of Technology, Hoboken, N.J., and worked for The MITRE Corporation from 1993-2008.

Earlier in his career (1974-1993) Dr. Mitola held positions of technical leadership with E-Systems, Harris Corporation, Advanced Decision Systems, and ITT Corporation.

Dr. Mitola received the B.S. degree in electrical engineering from Northeastern University, Boston, MA; the M.S.E. degree in stochastic optimal control from The Johns Hopkins University, Baltimore, MD; and the Licentiate and doctorate degrees in teleinformatics from KTH, The Royal Institute of Technology, Stockholm, Sweden.

Jeannie Diefenderfer, Advisor

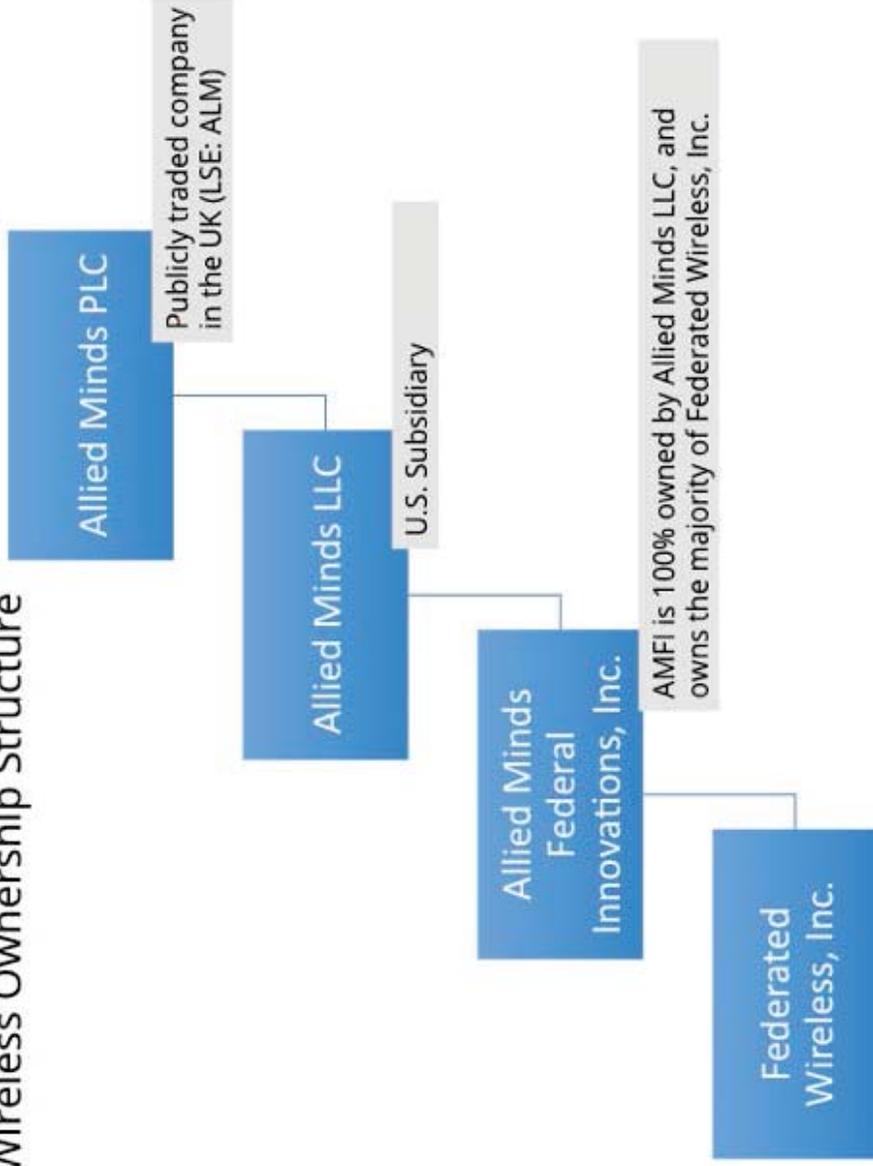
Jeannie Diefenderfer, a former executive at Verizon Wireless, is an advisor to the Federated Wireless executive leadership team. Based in New York City, Ms. Diefenderfer is a globally respected telecommunications executive with over 28 years of technical and operational experience.

Ms. Diefenderfer spent more than 10 years in executive leadership positions at Verizon Communications, including leading a 10,000-person global customer care organization for the company's largest enterprise customers. During her three-year tenure managing a \$10 billion+ purchasing program as Chief Procurement Officer, Ms. Diefenderfer achieved over \$1 billion dollars in savings for Verizon. In addition, as the Senior Vice President of Global Engineering and Planning, she implemented a network capital program of more than \$10 billion to expand Verizon's global backbone network across six continents.

Ms. Diefenderfer is a member of the Accenture Network Advisory Council, independent director of the boards of MRV Communications (MRVC: NASDAQ) and Westell Technologies (WSTL: NASDAQ), an advisor to Vasona Networks, and is a Trustee of Tufts University.

APPENDIX 2: OWNERSHIP STRUCTURE

Federated Wireless Ownership Structure





APPENDIX 3: TERMINATION AND CONVEYANCE OF SPECTRUM ACCESS SYSTEM SERVICES

I. Introduction

A. Purpose and Scope

In compliance with sections 96.63(g) and 96.55(b) of the Commission’s rules, Federated Wireless has implemented procedures to securely transfer some or all of the information in its Spectrum Access System (“SAS”) to another approved entity in the event a Federated Wireless customer elects to discontinue SAS services, or in the event that Federated Wireless does not continue as the SAS Administrator at the end of its term. While the SAS-to-SAS communication protocol and synchronization procedures enable sharing of Citizens Broadband Radio Service Device (“CBSD”) registration records, these procedures are not sufficient to complete the transfer of CBSDs and the associated user account registrations from one SAS to another.

II. Design

Federated Wireless will securely transfer the information in the SAS, along with the IP addresses and URLs used to access the system, and a list of registered CBSDs, to another approved entity (“recipient SAS”) under the following circumstances: (1) in the event a Federated Wireless customer elects to discontinue SAS services; or (2) in the event that Federated Wireless does not continue as the SAS Administrator at the end of its term. The following process will be applied:

1. The customer(s) and/or user(s) will confirm to Federated Wireless that it has established a relationship with the recipient SAS. A user account with the recipient SAS is required to enable an account transfer.
2. Federated Wireless will export the related user data fields from its SAS database or create an Application Program Interface to its system for direct access. Federated Wireless will provide the structure and syntax for the database fields so the recipient SAS can correctly interpret the data. Generally, the database export will be provided in a format that is widely used in industry **[***BEGIN CONFIDENTIAL INFORMATION***]** **[***END CONFIDENTIAL INFORMATION***]** for the recipient to import. The data export process and/or direct database access through the established API will comply with the security functionalities described in Section II.F of the main body of the Application.
3. Federated Wireless will further export retained data, such as historical records related to customer/user transmissions.
4. Federated Wireless will provide a capability to redirect or repoint the CBSDs to the recipient SAS or, as needed, the IP addresses and URLs used to access the Federated Wireless system.
5. Additional information, such as owner account and billing data, Category B CBSD registration data, and the Device Installation Record (“DIR”) as described in Appendix 13: Registration,



will not be transferred as these records either reside in third-party databases or are the responsibility of the recipient SAS Administrator to obtain from the user.

III. Summary

Federated Wireless has established procedures to securely transfer the information in its SAS to another approved entity in the event a Federated Wireless customer elects to discontinue SAS services, or in the event that Federated Wireless does not continue as the SAS Administrator at the end of its term.

APPENDIX 4: ACCESS PROTOCOLS AND PROCEDURES

I. Purpose and Scope

Federated Wireless has established role-based access protocols and procedures for its Spectrum Access System (“SAS”). This permits the wide variety of differing stakeholders in the CBRS ecosystem to access only the types of data they need while preserving the security or privacy of other stakeholders. The following summarizes these roles and levels of access where as described in the Error Resolution and Interference Reporting Policy Appendix, Error Reports also support reporting of interference.

Authorized Federated Wireless users with a need to access data in the SAS for purposes of development, maintenance, and updates, such as the lead software architect, cloud services support engineers, and network operations personnel, have administrative-level access to view, edit, or modify any and all data in the SAS pursuant to database maintenance and error resolution procedures.

Verified employees of the Federal Communications Commission (“FCC” or “Commission”) have access to view any and all data in the SAS pursuant to their oversight of the ecosystem. Commission-initiated modifications or changes to the data in the database need to be conveyed to Federated Wireless according to the SAS Error Resolution and Interference Reporting Policy. Additionally, Commission users may view spectrum availability at locations via this interface.

Verified owners of CBRS Devices (“CBSDs”), Certified Professional Installers (“CPIs”), and verified owners of Incumbent systems have complete access to view data associated with their own system. For systems other than the ones they own, these users can only view information registration information with identifying information removed. To correct errors or modify data, owners of CBSDs and CPIs may initiate an Error Report or update their records via Registration Messages in the SAS-CBSD protocol. Owners of incumbent systems can correct errors via the Error Resolution process or by updating records stored in Commission databases via processes established by the Commission. These users may view spectrum availability via Spectrum Inquiry messages in the SAS-CBSD protocol.

Members of the general public may access the SAS to view registration data, but with all owner-identifying information removed or obfuscated. These users may initiate an Error Report as part of the Error Resolution Process and may view spectrum availability via Spectrum Inquiry messages in the SAS-CBSD protocol.

Further, in certain situations, federal government entities may need to interact with Federated Wireless for operations such as spectrum reclamation. In order to facilitate this, Federated Wireless has established a set of protocols and procedures to respond to instructions from federal government entities, including the President of the United States. These internal protocols and procedures enable Federated Wireless to comply with all government entity instructions in a timely manner.

The remainder of this document reviews the Federated Wireless SAS Access processes and procedures for the following classes of users:

- Administrative Access
- General Public Access to Obfuscated CBSD Registration Data



- Commission Access to CBSD and Spectrum Data
- CBSD owners and CPI Access to review their own CBSD Registration Data and SAS-calculated PAL Protection Areas (“PPAs”) that the SAS administers and self-report smaller protection contours
- Non-federal Incumbent Access to review and verify their system information within the SAS and to request additional interference protection
- Grandfathered Wireless Broadband Licensee (“GWBL”) Access to review and verify their system information within the SAS
- Responses to Instructions from Designated Government Entities

II. References

- The procedures described herein comply with sections 96.53(o), 96.55(a)(2), 96.55(a)(3), 96.63(j), 96.63(l), 96.63(k), 96.63(n), 96.63(m), 96.55 (d) of the Commission’s rules.
- “CBRS Operational Security”, Wireless Innovation Forum, Working Document WINNF-15-S-0071-V0.3.7, March 2016
- Additional information can be found in Appendix 6: Information Retention, Appendix 5: Database Information, and Appendix 17: Terms of Use.

III. Role Based Access Control

Federated Wireless employs role-based access control to govern access to the SAS data. Users are only able to see the information they are authorized to view based on their role. The following roles are supported:

- Administrative users
- General public users
- CBSD owners and CPIs for CBSDs that the SAS administers
- Non-federal Incumbent Users (e.g., FSS earth station licensees)
- GWBL users
- FCC users

A. Access Procedures

The Federated Wireless SAS provides limited and appropriate access to SAS data to users based on the defined roles through a web based graphical user interface (“GUI”).

All users must create a user account with the Federated Wireless SAS to access this GUI and obtain information. This includes creating a user identity, a user account with secure login, and consenting to Federated Wireless’s Terms of Use Agreement.

- a) User identity information will include name, address, phone number, and contact email. User account type will also need to be specified and this will be one of the four defined roles (General public, CBSD owner/CPI, non-federal Incumbent User, GWBL user, FCC user). If the account type is the owner of CBSDs managed by the SAS or a CPI, the identity information



will include owner/CPI registration data as defined in the Database Information Appendix so the user identity is tied back to the owner/CPI record. If the account type is a non-federal Incumbent User, the incumbent type (Fixed Satellite Service, "FSS") will need to be specified as part of user registration.

- b) User account creation will be verified via the email provided. For non-federal Incumbent Users, Federated Wireless will both verify the supplied user information against the data stored in the SAS's FSS database and contact the user directly to verify their identity, contact information, and incumbent status before an account is created.
- c) The Terms of Use Agreement ("ToU") includes language stating that CBSD registration information may not be used for competitive purposes. The ToU will also include provisions for Federated Wireless to suspend, block, or cancel accounts that abuse policies.

A user account can be created free of charge. Federated Wireless will retain the user account information and electronic consent to the ToU.

[*BEGIN CONFIDENTIAL INFORMATION***]**

[*END CONFIDENTIAL**

INFORMATION*]**

B. Administrative Access

Authorized Federated Wireless users with a need to access data in the SAS for purposes of development, maintenance, and updates, such as the lead software architect, cloud services support engineers, and network operations personnel, have administrative-level access to view, edit, or modify any and all data in the SAS pursuant to database maintenance and error resolution procedures. This provides access to all data and logs within the Federated Wireless SAS, information about cloud management, software maintenance, and network operations.

C. General Public Access

Federated Wireless makes CBSD registration records available to the general public. No identity data is shown to these general users.

IV. CBSD Registration Data

The Federated Wireless SAS retains the following CBSD registration information. This only pertains to CBSDs that the SAS administers.

A. Category A & B CBSDs

- Geographic location
- Antenna height above ground level
- CBSD class (Category A/B)
- Requested Authorization Status (Priority Access License ("PAL")/General Authorized Access ("GAA"))



- FCC ID number
- Call sign
- Air interface technology
- Manufacturer’s serial number
- Sensing capabilities
- User contact information
- Deployment profile (indoor/outdoor)
- Secure information to associate CBSD with the Owner (may be provided through Owner pre-Registration)

B. Category B CBSDs

- Antenna gain
- Beamwidth
- Azimuth
- Downtilt angle

C. Data Obfuscation

All identifiable information that can tie CBSD registration data back to the identities of the licensees and/or CDSO owners is not exposed to the general public. Thus, in accordance with section 96.55(a)(3), the identities of licensees providing information is obfuscated for any public disclosures. The registration data not exposed to the general public includes:

- Call sign
- User contact information

D. Operational Security

Per the Wireless Innovation Forum (“WINNF”) Operational Security requirements as defined within WINNF-15-S-0071, there will be a 7-day delay from the time that a CBSD registers with the SAS and when this registration data will be available to the general public.¹

V. Web Based GUI

A public web page will be available for the users to interact with and view CBSD registration information. All users will need to login to the GUI based on their SAS account credentials. Once logged in, the GUI will contain a form where a user can enter the following parameters to search against and retrieve CBSD registration data that the SAS stores.

A. Search Form

¹ Wireless Innovation Forum, *CBRS Operational Security*, Working Document WINNF-15-S-0071 (Aug. 2015).



CBSD Parameter	Description
Latitude	Latitude of the CBSD location. Limited to locations within the USA.
Longitude	Longitude of the CBSD location. Limited to locations within the USA.
Radius	Radius in miles

The response to the query will be a table that includes the CBSD registration information identified above that fits within the search criteria. The information reported will correspond to the information access privileges of the specific user. A sample response that will be shown on the web page is as follows:

B. CBSD Registration Information

FCC ID	Category	Authorization	Air Interface	Serial Number
abc123	B	GAA	LTE	abcd1234

Latitude	Longitude	Height	Azimuth	Downtilt	Gain	Beamwidth
38.882546	-77.113393	6	270.5	3	16	30

VI. CBSD Owners and Certified Professional Installers

Federated Wireless makes CBSD registration records available to CBSD owners and CPIs with no data obfuscated. This pertains to CBSDs that the SAS administers and allows owners to review their own CBSDs’ registration data. Once a CBSD owner logs into the GUI they will see a table of their own CBSD records including identity information such as call sign and user contact information. They will also see the same search form that general public users have access to and will be able to carry out a search for CBSD registration records. Access to all other records where the user is not the CBSD owner will be treated the same as general public users.

If the CBSD authorization status is a PAL, the owner will be shown details of the PAL the SAS is managing.

The GUI for the CBSD owner will also be used for PAL licensee review of SAS calculated PPAs and for the self-reporting of smaller protection contours by the Licensee (or CBSD owner). Specifically, the GUI will include data entry fields to permit the Licensee (or CBSD owner) to specify the geo-coordinates of the smaller protection contour.



VII. Non-Federal Incumbent and GWBL Users

Federated Wireless makes SAS data pertaining to non-federal Incumbent Users and GWBL Users available to such users. This allows such users to review their own system's information within the SAS. Once a non-federal Incumbent User or GWBL User logs into the GUI they will see a table of their records including identity information. They will also see the same search form that general public users have access to and will be able to carry out a search for CBSD registration records. Access to all other records will be treated the same as general public users.

The GUI for the non-federal Incumbent User will also be used to receive reports of interference and requests for additional protection. Reports of interference entered and verified through the GUI exposed to the non-federal Incumbent User will be immediately communicated to the Federated Wireless SAS operations center for diagnosis and resolution. Further information regarding the Federated Wireless SAS operations center is provided in Section IX.A. below.² The GUI will also include data entry fields to permit the FSS earth station licensee to request additional interference protection. As described further in Appendix 10, the FSS earth station licensee will furnish its request as adjustments to parameters or protection criteria applied in the FSS interference calculation algorithm.

VIII. FCC Access

Federated Wireless will immediately respond to requests from authorized Commission personnel for any and all information stored by the SAS. This includes:

- CBSD registration data including identity information
- Spectrum inquiries showing the availability of channels/frequencies in a given geographic area.

For FCC users, there is no data obfuscation and registration record details include licensee identities.

A. Web Based GUI

FCC users will need to login to the GUI based on their registration. Once logged in, the GUI will contain a similar search form shown to general public users where a user can enter parameters to search against and retrieve CBSD registration data that the SAS stores. In addition to the search parameters available to general public users, authorized FCC users will also be able to search for CBSD registration data associated with a particular user or just view all CBSD records in the database. The response to FCC users will include user contact information and call sign, which are not exposed to general public users.

In addition to searching and examining full CBSD registration records, FCC users will also be able to carry out spectrum inquiries showing the availability of channels/frequencies in a given geographic area. The form for this will be as follows:

² Upon request, Federated Wireless will provide the FSS earth station licensee similar contact options as otherwise provided to government entity users. The Federated Wireless operations center will be available 24/7/365 to respond to FSS earth station licensee interference reports.



1. Spectrum Inquiry Search Form

CBSD Parameter	Description
Latitude	Latitude of the CBSD location. The allowed range is from - 90.000000 to +90.000000
Longitude	Longitude of the CBSD location. The allowed range is from - 180.000000 to +180.000000.
Authorization Status	"PAL" or "GAA"
CBSD Category	"A" or "B"
Deployment profile	Indoor or outdoor
Height	In AGL
Peak EIRP	In dBm
Antenna Gain	In dBi. Only necessary for Category B CBSDs.
Antenna Beamwidth	In Degrees. Only necessary for Category B CBSDs.
Azimuth Angle	In Degrees. Only necessary for Category B CBSDs.
Downtilt Angle	In Degrees. Only necessary for Category B CBSDs.

The response to the query will be a table that shows channel availability based on the parameters, showing all frequencies available. Appendix 8: SAS Channel Availability details how channel availability is determined by the SAS and this is the same approach used by the SAS for spectrum inquiries.

IX. Response to Government Entity Instructions

Federated Wireless has established protocols and procedures to support requests and respond to instructions from federal government entities including the Commission and President of the United States or another designated federal government entity issuing instructions pursuant to 47 U.S.C. § 606. These include 24/7/365 availability and government entity validation.

A. Contact Information and 24/7/365 Availability

The contact information for Federated Wireless’s SAS and ESC operations center will be available on the company’s publicly accessible web page. This includes the network operations center’s (“NOC”) manager, phone number, email address, and postal address. Federal government entities can access this information anytime from the web page and use it to contact Federated Wireless for SAS and ESC operations.



Federated Wireless can be contacted by federal government entities on a 24/7/365 basis. Once a government entity contacts Federated Wireless, the company will respond to the request in a timely manner commensurate with the priority and urgency of the situation communicated by the entity.

For immediate response, government entities should contact Federated Wireless via the provided phone number. Calls to this phone number are broadcasted to the NOC manager and a designated support engineer to ensure there is always someone available to respond to these requests. Action will be taken immediately on phone requests and the government entities making the request will be provided with status updates on the resolution via phone and email.

Requests made via email are also broadcasted to the NOC manager and a designated support engineer, and Federated Wireless will respond to such requests within 12 hours. Government entities making email requests will be provided with status updates on the resolution via email.

B. Government Entity Validation

Upon contact by a federal government entity, Federated Wireless will validate that the request is coming from an actual government entity. This procedure will be followed to ensure that the request is a valid request and only once this is confirmed will Federated Wireless continue with the requested operation.

C. Procedures and Protocols

The Federated Wireless SAS complies with the WINNF's procedures for addressing requests from federal government entities. This includes providing all federal government entities capabilities to reach the SAS Administrator in situations of exceptional circumstances and immediately sharing all instructions received from government entities with all other SAS Administrators to effect a coordinated response across the ecosystem when needed.

Federated Wireless has established training processes and procedures that will be used to ensure all relevant Federated Wireless staff properly respond to validated requests from government entities. Federated Wireless has established a comprehensive internal incident response plan to deal with such situations so there is a documented course of action depending on the issue at hand.

X. Summary

Federated Wireless has established a set of protocols and procedures using role-based access controls to ensure that users are only able to access data that they are authorized to see based on their role.

In addition, Federated Wireless has also established a set of protocols and procedures to respond to federal government entities, including the President of the United States, as necessary. These internal protocols and procedures enable Federated Wireless to comply with all government entity instructions in a timely manner. These policies and procedures are summarized in Table 1 where Error Correction Reports also permit the reporting of interference conditions.



Table 1: Summary of Federated Wireless SAS Access Policies

User Class	Data Access	Access for Error Correction	Spectrum Availability Access
Administrative	<ul style="list-style-type: none"> All data and logs 	<ul style="list-style-type: none"> Complete access 	<ul style="list-style-type: none"> All Access
Federal Communications Commission	<ul style="list-style-type: none"> All CBRS-related data 	<ul style="list-style-type: none"> Error Reports 	<ul style="list-style-type: none"> User Interface for Spectrum Inquiries SAS-CBSD Spectrum Inquiries
CBSD Owner / CPI	<ul style="list-style-type: none"> All registration data for own system Delayed registration data with identifying information removed for other systems 	<ul style="list-style-type: none"> Error Reports SAS-CBSD Registration Message 	<ul style="list-style-type: none"> User Interface for Spectrum Inquiries SAS-CBSD Spectrum Inquiries User Interface to view SAS computed PAL Protection Areas and self-report smaller PPA boundaries
General Public	<ul style="list-style-type: none"> Delayed registration data with identifying information removed 	<ul style="list-style-type: none"> Error Reports 	<ul style="list-style-type: none"> User Interface for Spectrum Inquiries SAS-CBSD Spectrum Inquiries
Non-federal Incumbent (FSS earth station licensee)	<ul style="list-style-type: none"> All registration data for own system Delayed registration data with identifying information removed for other systems 	<ul style="list-style-type: none"> Error Reports SAS-CBSD Registration Message 	<ul style="list-style-type: none"> User interface for interference reporting and protection requests User Interface for Spectrum Inquiries SAS-CBSD Spectrum Inquiries
GWB Licensee	<ul style="list-style-type: none"> All registration data for own system Delayed registration data with identifying information removed for other systems 	<ul style="list-style-type: none"> Error Reports SAS-CBSD Registration Message 	<ul style="list-style-type: none"> User Interface for Spectrum Inquiries SAS-CBSD Spectrum Inquiries
President of the U.S. or Designee	<ul style="list-style-type: none"> Data-related to compliance with directives 	<ul style="list-style-type: none"> Error Reports 	<ul style="list-style-type: none"> Data-related to compliance with directives

APPENDIX 5: DATABASE INFORMATION

I. Purpose and Scope

Federated Wireless maintains a repository of data required by the Spectrum Access System (“SAS”) to perform its functions. This includes data acquired from Federal Communications Commission (“FCC”) databases, the National Telecommunications and Information Administration (“NTIA”), and other government records. The data includes information such as FCC equipment authorization, Priority Access License (“PAL”) assignments, exclusion zones and protection zones, secondary market lease notification information, CBSD records, and owner records. All data stored by the SAS is only for the purpose of effective SAS operations and does not include any operational data on the movement or position of any federal system or any information that reveals operational data of any federal system that is not required by the SAS. The SAS also does not retain network operational information of CBRS users unless required to effectively perform SAS operations or to comply with the information retention requirements of Part 96.

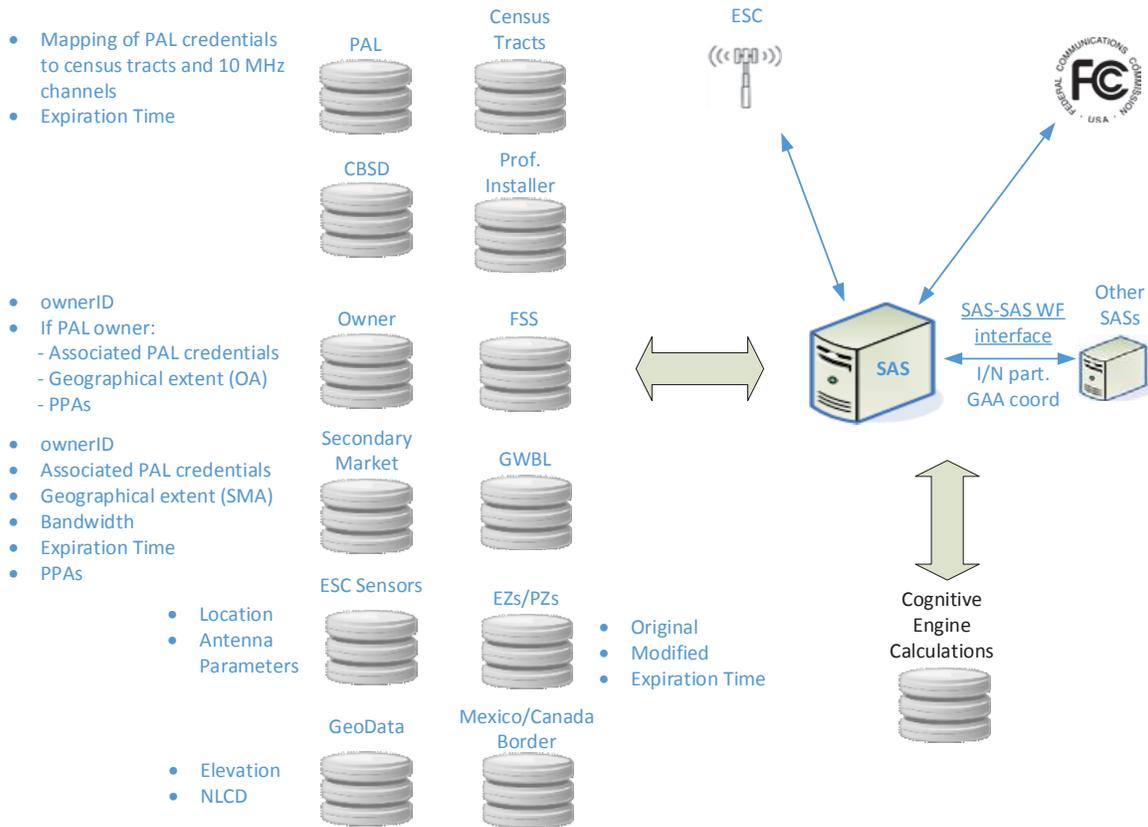
A. References

- The information provided here details Federated Wireless’ compliance with sections 96.57(c), 96.63(a), 96.63(b), and 96.66(a)(2) of the Commission’s rules.
- WINNF-15-P-0062-1.0.0, “SAS to CBSD Protocol Technical Report-B”, Version 1.0.0, March 2016
- Appendix 11: PAL Channel Assignment Plan
- Appendix 9: Definition of Use and Secondary Markets

II. Database Information Design

As noted above, Federated Wireless connects to a number of databases to acquire data. Once data is acquired from these various external data sources, the data is then aggregated and stored in Federated Wireless’ SAS databases so it can be utilized by the SAS for its operations and in support of the Information Gathering and Retention requirements of section 96.55. Figure 1 shows the database design.

Figure 1: Database design



A. FSS Earth Stations

SAS maintains a database with Fixed Satellite Service (“FSS”) earth station parameters needed for SAS incumbent protection calculations and to comply with section 96.55(a). Accessing the FCC’s database on protected FSS sites¹ populates this database.

B. Grandfathered Wireless Broadband Licensees (“GWBLs”)

The Federated Wireless SAS database for GWBL devices will follow the FCC’s determinations based on the record generated by the Wireless Telecommunications Bureau (“WTB”) in Public Notice DA 15-1208 and complies with section 96.21. Section 96.21 indicates that the SAS is responsible for protecting GWBL base or fixed stations registered in the FCC’s Universal Licensing System (“ULS”) on or before April 17, 2015 and constructed, in service, and fully compliant with the rules in Part 90, subpart Z, as of April 17, 2016. The Wireless Innovation Forum (“WINNF”) established a Task Group to address questions raised in DA 15-1208. This Task Group suggested the establishment of a central third-party database maintained by a multi-stakeholder group and that includes registration details on all Wireless Internet Service Provider (“WISP”) deployments in 3.65 - 3.70 GHz. The Task

¹ <http://licensing.fcc.gov/cgi-bin/ws.exe/prod/ib/forms/reports/swr030b.hts?set=#earthReport>



Group recommended GWBL protection based on the information contained in ULS along with additional data contained in the third-party database including whether a particular transmitter is a base station or CPE.

Federated Wireless anticipates the WTB release of a Notice that defines the methods for SAS access of GWBL device registration records in ULS and, if applicable, third-party databases. Federated Wireless further expects the Notice to also provide interface mechanisms to such databases and any additional SAS requirements pertaining to this database such as updating frequency and SAS-to-SAS data exchange. The Federated Wireless SAS will comply with the requirements related to GWBL protection contained in Part 96 and in the anticipated Notice.

C. Exclusion Zones and Protection Zones

The boundaries of several Exclusion Zones (“EZs”) must be maintained for protection of federal Incumbent Users, as required by section 96.53(e). In particular, section 96.15(a)(3) states that EZs shall be maintained along the Coastline, as shown at ntia.doc.gov/category/3550-3650-mhz, around federal radiolocation sites as set forth at ntia.doc.gov/category/3550-3650-mhz (96.15(a)(3)) and an 80 km radius around the federal radiolocation sites listed in 47 C.F.R. § 90.1331 and 47 C.F.R. § 2.106, US 109 (section 96.15(b)(2)). We denote the EZs obtained from the above sources as “Original Exclusion Zones” and these are maintained as Keyhole Markup Language (“KML”) files.

As per section 96.15, the Commission may temporarily extend or modify EZs and Protection Zones (“PZs”) 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
- Expiration Data and Time of Modified Exclusion Zone

Upon expiration of the modified EZ, the SAS enforced EZ will revert back to the original EZ. As per section 96.15, EZs shall be converted to PZs once Environmental Sensing Capabilities (“ESC”) are approved.

D. Equipment Authorization

The SAS connects to the FCC’s Equipment Authorization System (“EAS”) to get a list of valid devices and their associated FCC IDs. The FCC ID of any CBSD seeking SAS services is verified against this data to ensure it is a valid device prior to it being authorized as part of the CBSD Registration Process.

E. Census Tracts

Several SAS functions, *e.g.*, Priority Access License (“PAL”) management, rely on knowledge of census tract boundaries. Accessing the online database provided by census.gov populates a database with such boundaries.

F. Canadian and Mexican Borders

For the Television White Space (“TVWS”), the FCC pointed TVWS Database (“TVDB”) operators to GIS files for the US-Canada and US-Mexico borders.² The Federated Wireless SAS stores KML data

² <https://www.fcc.gov/general/white-space-database-administration-q-page>



derived from these files, which is used in enforcing protections in compliance with current and future international agreements.

G. GeoData

*****BEGIN CONFIDENTIAL INFORMATION*****

*****END CONFIDENTIAL INFORMATION*****

H. Priority Access Licenses

The Federated Wireless SAS maintains a database that maps each PAL to a census tract and 10 MHz channel.³ This database is initially populated based on the third-party defined PAL Channel Assignment Plan. The PAL needs to be associated with one or more CBSDs before these CBSDs can request channel grants from their serving SAS.

The associated database field for a unique PAL License (“PAL ID”) would include the following pieces of information and parameters for each PAL:

- a. Establishment of a system-wide unique PAL Protection Area (“PPA”) ID number;
- b. An encrypted token or security feature that allows automated SAS authentication (from any SAS) of any PAL ID when presented during normal automated channel requests from CBSD devices;
- c. The original PAL owner from the auction results;
- d. The PAL initiation date (from auction);
- e. The PAL termination date (from auction),
- f. The census tract and block identity (identification numbers);
- g. The ‘M’ vertex points that define the original PAL census tract boundaries; and
- h. The PAL state (purchased, pending, claimed, valid, PAL expired, PAL revoked, PAL pending enforcement).

I. Secondary Market

The 2nd R&O provides a framework for secondary market transactions and Federated Wireless will provide the functionality required to accept leasing notifications and support leasing arrangements. As part of this framework, a Priority Access Licensee can establish a Spectrum Management Lease Agreement (“SMLA”) with another entity (“Lessee”). Before Lessee CBSDs can operate in the CBRS band, the SAS will confirm that the Lessee has been certified by the Commission and Federated Wireless will electronically obtain the following additional information:

³ <https://www.fcc.gov/general/white-space-database-administration-q-page>



- a. Notification from the Licensee of the SMLA
- b. Lessee contact information including name, address, telephone number, fax number, e-mail address;
- c. Lessee FCC Registration Number (“FRN”);
- d. Name of Real Party in Interest and related FRN;
- e. The specific spectrum leased (in terms of amount of bandwidth and geographic area involved) including the call sign(s) affected by the lease; and the duration of the lease.

The SAS will also confirm that the lease will not violate the 40 MHz PAL spectrum aggregation limit, and confirm that the lease area is within the Licensee’s Service Area but outside its PPA. The SAS will store the SMLA notification information and synchronize this information, including information about the expiration, extension, or termination of leasing arrangements, with the Commission databases at least once a day consistent with the requirements of section 96.66.

J. CBSD Records

The SAS maintains records with all CBSD information. This information is created via a variety of methods including through SAS-to-CBSD exchanges, entered into the SAS by a Professional Installer via an industry-standardized interface, and obtained over the SAS-to-SAS interface. The rate for SAS-to-SAS exchanges is currently being defined in WINNF and Federated Wireless will support any frequency requirement mandated by the FCC for this exchange.

K. Owner Records

CBSDs must be associated with an owner, who is required to register with the SAS. The owner may be an individual or legal entity (e.g., corporation, non-profit, governmental agency) that owns and is responsible for one or more CBSDs.

As described in Appendix 9: Definition of Use and Secondary Markets, the SAS will maintain PPAs for each owner based on an Engineering Definition of Use.

As part of owner registration, the owner has to provide the following information to the SAS:

- Owner legal identity (corporate or individual),
- Owner Mailing Address (contact address), or designated agent contact address,
- Owner’s Physical address (may or may not correspond to the Mailing Address)
- Owner’s Legal Address (may or may not correspond to the Mailing Address)
- Owner’s Email Contact Address,
- Owner’s Phone Number (contact, or of designated agent),
- Designated Agent (if applicable)
- Number of owner pre-shared authentication keys being requested (default is one)

After the owner has provided the above necessary contact information, the system must provide the owner with:

- A system wide unique Owner Registration Identify (“OR-ID”),
- A method to authenticate the Owner when accessing the Owner account (e.g., password),
- One or more unique and secure Owner Registration Pre-shared Authentication Key(s), that were requested during owner registration. The Pre-shared Authentication Key(s) will later be input into the CBSD(s) to allow the SAS to properly



associate a registering CBSD with its owner. This is to ensure the CBSD is linked to a valid owner and to ensure registration occurs with the Owner’s permission. The use of more than one pre-shared authentication key number per owner would allow the owner to create sub-groupings of CBSDs, which may be useful for large networks.

During registration, the owner must acknowledge that operations are subject to the Part 96 rules, and also acknowledge that it accepts the risk of interference from federal Incumbent User operations. Upon owner registration, the SAS shall record the following information about the owner in its owner database:

- Registration date,
- Registration expiration or term
- Registration state (valid, expired, pending enforcement, revoked),
- Registering Agent (FCC, SAS, or other agent),
- Whether Registration Fee is Paid or not. This information is optional and could include a credit card transaction that may help to serve as an identity check and a mailing address check to prevent fraudulent or fictitious registrations and mailing addresses. This credit card transaction may be a separate transaction for the Owner License, or may be the purchase transaction for the CBSD itself.

L. Professional Installer

For CBSDs that are installed by a Certified Professional Installer (“CPI”), the CPI is required to be registered with a professional installer certifying body database, which the SAS must be able to access. The rules also “encourage” an accreditation program for professional installers. The SAS must provide CPIs with a system-wide unique CPI Identity and a method to authenticate the Installer when accessing the CPI account. The installer will then use this information when they enter the CBSD Device Installation Record into the CBSD or provide it to the SAS Administrator. Moreover, these two sets of data shall be recorded by the SAS accessible database. The Certified Professional Installer Registration (“CPIR”) process requires the CPI to provide the following information to a SAS-accessible centralized database:

- a. Legal identity (name),
- b. Mailing address,
- c. Legal address,
- d. Email contact,
- e. Phone contact,
- f. Accredited certification number from a training program,
- g. License initiation date, termination date

In general, CPI data required for storage as part of the WINNF/community-defined CPI program will be maintained for the requisite time period.



M. ESC Sensors

An ESC operator of a dedicated sensor network may request SAS interference protection of one or more of its sensors. An ESC operator that requests protection shall provide the location and height of the protected sensor to a SAS. Such requests shall be shared between SASs. The ESC sensor location and height data will be stored in the ESC sensor database.

N. Data Synchronization Process

The Federated Wireless SAS synchronizes with the necessary FCC databases at least once every 24 hours by default to pull and push the latest updates. The databases included in this daily sync are the FCC’s Equipment Authorization System (“EAS”) and Universal Licensing System (“ULS”). The sync rate is fully configurable to support more frequent updates if necessary. Each database synchronization service is individually configurable and extensible to allow the Federated Wireless SAS to comply with changing Commission requirements and Industry Standards for data freshness and data format on a database-by-database basis. Federated Wireless will support any update rate requirement mandated by the FCC. Federated Wireless complies with the FCC’s published mechanisms for accessing data. This includes the documentation published for accessing ULS and EAS. **[***BEGIN CONFIDENTIAL INFORMATION***]**

[*END CONFIDENTIAL**

INFORMATION*]**

III. Summary

Federated Wireless maintains a repository of data required by the SAS to perform its functions, which includes data acquired from FCC databases, NTIA, and other government records. This data stored by the SAS is only for the purpose of effective SAS operations and does not include any operational data on the movement or position of any federal system or any information that reveals operational data of any federal system that is not required by the SAS. The SAS also does not store network operational information of CBRS users unless such information retention is required to effectively perform SAS operations or to comply with the information retention requirements of Part 96.

APPENDIX 6: INFORMATION RETENTION

I. Scope and Purpose

Federated Wireless has established an information retention policy in order to retain any information necessary to operate as a Spectrum Access System (“SAS”) Administrator. This includes, but is not limited to, federal Incumbent User Exclusion Zones and Protection Zones, registration information for protected Fixed Satellite Service (“FSS”) earth stations, registration data for Grandfathered Wireless Broadband Licensees (“GWBLs”), current information on registered Citizens Broadband Radio Service Devices (“CBSDs”), and Spectrum Manager Lease Agreements (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 defined period of time.

II. References

- The information provided here details Federated Wireless’ compliance with sections 96.17(d), 96.53(e), 96.55(a), 96.55(b), 96.55(c), 96.55(e), 96.63(a), 96.63(n), and 96.66(a) of the Commission’s rules.
- Appendix 4: Access Protocols and Procedures
- Appendix 15: Security
- Appendix 10: Commercial FSS Incumbent and Grandfathered Wireless Service Protections

III. Data Privacy and Confidentiality

Federated Wireless will comply with the FCC’s rules and regulations relating to data privacy and confidentiality while maintaining the privacy and confidentiality needs of our customers.

Given the diverse interests of this community, Federated Wireless believes that a multi-stakeholder group, such as the Wireless Innovation Forum (“WINNF”) should establish requirements and standards for information gathering and retention, and Federated Wireless believes that the essential core principles are as follows:

1. CBSD registration information shared among SASs shall be used to comply with the requirements of section 96.55(a)(2) and may not be used for other purposes.
2. SAS Administrators shall be separately responsible for complying with section 96.55(a)(3), and in complying SAS Administrators shall disclose to the general public registration information only for those CBSDs that the SAS administers.
3. Registration information encompasses the Required, Conditional, and Optional parameters in the Registration Message defined as defined by the WINNF SAS-CBSD Protocol.

IV. Database Architecture

[*BEGIN CONFIDENTIAL INFORMATION***]**

[*END CONFIDENTIAL**

INFORMATION*]**

A. Incumbent Information

The Federated Wireless SAS retains all necessary data as defined in Appendix 5: Database Information for protection of federal and non-federal Incumbent Users. This data is retained for 60 months.

1. Federal Incumbent Users

- Exclusion Zones as defined by the National Telecommunications and Information Administration (“NTIA”) along the Coastline and around federal radiolocation sites are maintained by the SAS and updated when notified by the Commission.
- Protection Zones based on the presence of an approved Environmental Sensing Capability (“ESC”) that the SAS is utilizing.

2. Non-Federal Incumbent and Grandfathered Users

- FSS earth station details that the SAS pulls from the FCC’s databases. This data is synchronized and updated as defined in Appendix 5: Database Information.
 - The earth station’s geographic location
 - Antenna gain
 - Azimuth and elevation antenna gain pattern
 - Antenna azimuth relative to true north



- Antenna elevation angle
- GWBLs

B. Non-Incumbent Information

The Federated Wireless SAS retains all necessary information not pertaining to federal Incumbent User transmissions for 60 months. This data includes:

- CBSD Registration Data
 - Geographic location
 - Antenna height above ground level
 - CBSD class (Category A/B)
 - Requested Authorization Status (Priority Access License (“PAL”)/General Authorized Access (“GAA”))
 - FCC ID number
 - Call sign
 - User contact information
 - Air interface technology
 - Manufacturer’s serial number
 - Sensing capabilities
 - Deployment profile (indoor/outdoor)
 - Antenna gain
 - Beamwidth
 - Azimuth
 - Downtilt angle
- Secondary market data
 - Spectrum Manager Lease Agreement Notification
- Secure information to associate the CBSD with the Owner (may be provided through Owner pre-Registration)
- Professional Installer data

C. SAS Transaction Records

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 WINNF SAS-to-CBSD TS
- Channel assignments by the SAS to CBSDs
- FSS earth station interference report events
- FSS earth station requests for additional interference protection
- Owner self-reports of PAL Protection Area (“PPA”) boundaries



As detailed in Federated Wireless' Terms of Use , the SAS retains acknowledgement records by all entities registering CBSDs that they understand the risk of possible interference from federal Incumbent User radar operations in the band. This acceptance of the policy is retained indefinitely and is not subject to the 60-month storage period.

D. ESC Data

For federal Incumbent User transactions, the ESC notifies the SAS of a federal Incumbent 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.
- A deactivation time for this protection.

[*BEGIN CONFIDENTIAL INFORMATION***]**

[*END CONFIDENTIAL INFORMATION***]**

The ESC itself does not retain incumbent detection events past the cessation of incumbent activity.

V. Summary

Federated Wireless has established an information retention policy in order to retain any information necessary to operate as a SAS Administrator. This complies with all of the Commission's rules on information retention including data privacy and confidentiality. **[***BEGIN CONFIDENTIAL INFORMATION***]**

[*END CONFIDENTIAL INFORMATION***]**



APPENDIX 7: ERROR RESOLUTION AND INTERFERENCE REPORTING POLICY

I. Purpose and Scope

Since the interference protections and services provided by the Federated Wireless Spectrum Access System (“SAS”) depend on the accuracy of the data stored in its database, Federated Wireless is keenly interested in quickly resolving any errors in our SAS database. This document describes the processes and procedures Federated Wireless has established to rapidly remediate data inaccuracies upon identification and to proactively identify errors in data sources to minimize the introduction of errors to the Federated Wireless database. Additionally, this document describes the process Federated Wireless will follow to resolve Interference Reports, particularly those related to reports of interference by FSS earth station licensees.

II. References

- The information provided here details Federated Wireless’ compliance with section 96.17(f) and 96.63(f) of the Commission’s rules.
- Appendix 4: Access Protocols and Procedures
- Appendix 13: CBSD Registration and Registration Verification
- Appendix 14: Certified Professional Installers
- Appendix 12: CBRS Measurement Report

III. Identification of Data Inaccuracies

The Federated Wireless SAS Database is fully compliant with Part 96 and stores data from a variety of sources including the following.

- Current information on registered Citizens Broadband Radio Service Devices (“CBSDs”)
- Federal Incumbent User Exclusion Zones and Protection Zones
- Geographic locations and configuration of protected Fixed Satellite Service (“FSS”) locations
- Grandfathered Wireless Broadband Licensees (“GWBLs”)
- Owner registration data
- Certified Professional Installer (“CPI”) data
- Secondary Market data

A key element of the Federated Wireless SAS error mitigation strategy is preventing errors from entering into the SAS in the first place. Thus for each of the preceding data sources, the Federated Wireless SAS takes steps to proactively detect and remediate errors as they enter the database. For instance, the Federated Wireless SAS performs basic checking of CBSD data during the registration process⁶, performs basic error checking on data from Federal Communications

⁶ Appendix 13: Registration; Appendix 14: Certified Professional Installers



Commission (“FCC “ or “Commission”) databases, and uses data gleaned from Measurement Reports to attempt to detect CBSDs whose actual operating parameters differ from the registered parameters.⁷

Additionally, the Federated Wireless SAS design encourages external parties to identify data errors and bring them to our attention via the following methods:

- Data issues identified by the Commission as they access the SAS database based on the access control policies in place for their roles as defined in Appendix 4: Access Protocols and Procedures will be communicated to Federated Wireless via a contact form on the webpage or by calling Federated Wireless. This form will prefill the identity and contact information of the FCC user based on their user account.
- Data issues identified by third parties (such as the general public, CBSD Owners, CPIs, and non-federal Incumbent Users) accessing the SAS database as constrained by the access control policies in place for their roles as defined in [1] will be communicated to Federated Wireless via a contact form on the webpage. This form will prefill the identity and contact information of the user based on their user account. Third party users with roles of CBSD owners, CPIs, and non-federal Incumbent Users are able to identify issues with their own registered data on the SAS.

IV. Data Resolution Procedures

Once a data inaccuracy has been identified, Federated Wireless will respond to and resolve the error in less than 12 hours.

If the data issue is identified during a database sync process with the FCC databases, the SAS will employ the following procedure:

- Contact the Commission via email to inform them of the error found.
- Correct the inaccuracies, if obvious, by updating or removing the data as needed so it aligns with what is being acquired from the FCC databases.
- Otherwise, wait for a correction from the Commission while using the last known set of good data.

Upon every database sync, the SAS validates all the data it acquires and makes the necessary changes in the SAS database based on the latest information it gets. This consolidation is done in real time as part of the sync process. When an error is detected autonomously, *e.g.*, when validating registration data or from analysis of Measurement Reports, the Federated Wireless SAS will contact the owner of the system to correct the error. If found during CBSD registration, the error will be signaled to the CBSD via error codes returned by the SAS. CBSDs found with errors affecting interference calculations will have all transmission grants suspended until errors are resolved.

If the data issue is identified by the Commission or third parties that have access to view some or all of the SAS database, these users can notify Federated Wireless through an Error Report form on the webpage. Federated Wireless will verify the claims by checking against the source of the

⁷ Appendix 12: CBSD Measurement Report



data and update the SAS database as needed to resolve the identified errors. This error resolution will be complete within 12 hours of notification of the issue and the notifying party will be updated via email of the resolution status.

If a third party user has the role of a CBSD owner or CPI and identifies data issues with their own data, these users can resolve the errors instantaneously by going through the process of re-registering their device(s). Such users can also go through the contact form process for error resolution.

All error reports and actions taken by the Federated Wireless SAS in response to Error Reports are logged and stored as a SAS Transaction.

V. Interference Resolution Procedures

Outside of egregiously incorrect information (e.g., attempting to register a CBSD at a location outside of the U.S.), the first chance that a SAS will have to detect many 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 federal or non-federal system
- SAS-CBSD protocol Measurement Reports (for CBSDs), which can be used to autonomously infer unexpected levels of interference
- 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:

1. 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.
2. 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.
3. 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 propagation model computations and terrain databases, etc.). 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 spectrum and geographic definitions of applicable interference regions around each protected user are defined in the associated Appendices, *e.g.*, the applicable interference coordination region for an FSS site from the site location consistent with section 96.17.⁸

VI. Summary

Federated Wireless has established processes and procedures to detect and respond to data issues in a timely manner. Through this process, the Federated Wireless SAS is able to remediate data inaccuracies as soon as they have been identified so it can continue to operate with the proper data, as required by the Commission. While errors with CBSDs are being addressed, spectrum grants for those CBSDs are suspended to protect the Citizens Broadband Radio Service ecosystem. Similarly, Federated Wireless has established procedures to resolve Interference Reports designed to ensure protection of Incumbent Users while continuing to maximize spectrum access.

⁸ 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.



APPENDIX 8: SAS CHANNEL AVAILABILITY

[*BEGIN CONFIDENTIAL INFORMATION***]**



[*END CONFIDENTIAL INFORMATION***]**



APPENDIX 9: DEFINITION OF USE AND SECONDARY MARKETS

[*BEGIN CONFIDENTIAL INFORMATION***]**

[*END CONFIDENTIAL INFORMATION***]**



**APPENDIX 10: COMMERCIAL FSS INCUMBENT AND GRANDFATHERED WIRELESS
SERVICE PROTECTIONS**

[*BEGIN CONFIDENTIAL INFORMATION***]**

[*END CONFIDENTIAL INFORMATION***]**

APPENDIX 11: PRIORITY ACCESS LICENSE CHANNEL ASSIGNMENT PLAN

I. Overview

This document describes the methods by which a Spectrum Access System (“SAS”) Administrator will assign channels to Priority Access Licensees (“PALs”) when no federal Incumbent User activity is present. When federal Incumbent User activity is present, the SAS may temporarily adjust these assignments following the [1] methodology. Specifically, this document describes how Owner Areas (“OAs”) are determined.

II. Band Plan

While the Commission wisely declined to formally define a band plan, Part 96 specifies the following constraints relevant to spectrum assignment to PALs.

- Section 96.13 (a) - Each PAL shall be authorized to use a 10 megahertz channel in the 3550-3650 MHz band.
 - Section 96.13 (a)(1) - No more than seven PALs shall be assigned in any given License Area at any given time.
- Section 96.13 (b) - The 3650-3700 MHz band shall be reserved for Grandfathered Wireless Broadband Licensees and GAA Users.
- Section 96.31 - Priority Access Licensees may aggregate up to four PAL channels in any License Area at any given time.

To facilitate development of the Citizens Broadband Radio Service (“CBRS”), the Wireless Innovation Forum (“WINNF”) developed a common band plan¹¹ that complies with these and other relevant rules. 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. For example, Channel 1 is a PAL channel from 3550 – 3560 MHz, Channel 2 3560 – 3570 MHz, and so on.

III. Rules Applicable to PAL Channel Assignment

Rather than assigning specific frequencies to PAL auction winners as part of the auction process, section 96.25(b)(2) specifies that channels must be assigned by the SAS. This is critical to the dynamic protections needed for Part 96’s design for ESC-enabled coexistence with offshore naval radar in shoreline regions and to support the Federal Communications Commission’s (“FCC” or “Commission”) goals of maximizing spectrum efficiency and utilization.

Part 96 further defines several rules that guide SAS allocation of 10 MHz channels to PALs, *e.g.*:

- Geography – section 96.25(b)(1) - Each PAL consists of a single License Area

¹¹ Reference [2]



- Contiguous Geographic Areas – section 96.25(b)(1)(i) - An SAS must assign geographically contiguous PALs held by the same PAL licensee to the same channels in each geographic area, to the extent feasible.
- Contiguous Channels – section 96.25(b)(1)(i) - An SAS must assign multiple channels held by the same PAL licensee to contiguous channels in the same License Area, to the extent feasible
- Section 96.31 – PAL licensees may aggregate up to four PAL channels in any License Area at any given time.
- Section 96.13 - No more than seven PALs shall be assigned in any given License Area at any given time.
- Section 96.11 (a)(3) – PAL licensees may be assigned frequencies in the 3550-3650 MHz frequency range, effectively making 10 channels available for making up to seven 10 MHz PAL channel assignments.

However, Part 96 only requires that a SAS make a best-effort to satisfy these requirements when Incumbent Users are present, specifically relaxing the requirements on contiguous geographic areas and channels as follows:

- Section 96.25(b)(1)(i) - The SAS may temporarily reassign individual PALs held by the same licensee to different channels, so that geographical contiguity is temporarily not maintained, to the extent necessary to protect Incumbent Users or if necessary to perform its required functions under subpart F.
- Section 96.25(b)(2)(i) - The SAS may temporarily reassign individual PALs to non-contiguous channels to the extent necessary to protect Incumbent Users or if necessary to perform its required functions under subpart F

Furthermore, PAL license terms are for relatively long time periods - three years¹² –though the Commission may open PAL application windows at other times as announced via Public Notice.

Thus, during typical operation, channel assignments to PAL licensees by the SAS represents a complex integer programming problem, albeit one that nominally only must be solved once every three years or after out-of-cycle Commission auctions as announced via Public Notice. However, coordinating the derivation of the solution to this problem of this across multiple SAS Administrators could be complicated. Furthermore, even SAS Administrators with the best of intentions may inadvertently give the appearance of making a determination of a PAL frequency assignment in a way that favors a PAL licensee, thereby inviting complaints of frequency determinations being made in a discriminatory manner, in violation of section 96.59(a).

IV. Proposed Methodology for Determining Steady-State PAL Frequency Assignments

Recognizing the challenges and constraints posed by the rules, we propose the following process.

- The FCC conducts the auction, whether in-cycle (every three years) or at other times at the Commission's choosing.

¹² 47 C.F.R. §§ 96.25(b)(3); 96.27(a).



- At the conclusion of the auction and prior to PAL use commencing, an independent party with appropriate expertise is contracted by the community to solve the integer programming problem of assigning “steady-state” frequencies to PA Licenses 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 proposed solution will be presented to the PAL owners for review and comment.
- Upon community approval, the solution is provided to all SAS Administrators for implementation and to the FCC as part of a public record and to facilitate secondary market transactions. The format(s) for the records provided to the SAS Administrators and to the FCC will be specified as part of the third party’s contract. These records define the OAs described elsewhere in this proposal.
- Adjustments to the solution can be made at later points as agreed to by the PAL-SAS community

V. Extensions

This methodology could be readily extended as deemed desirable by the PAL-SAS community in a variety of ways, including the following:

- Alternate PAL band plans - In areas where time-varying incumbent activity is expected, *e.g.*, Norfolk or San Diego, alternate PAL channel mappings could be pre-computed
- Additional objectives for subsequent and out-of-cycle auctions - When a previous static PAL band plan exists prior to auction, the third party’s optimization routine could be given additional guidance, such as to minimize changes to existing frequency band plans.
- The community may also decide to adjust channel assignments following transfers or assignments of PALs consistent with Part 1. As with subsequent or out-of-cycle auctions, this could be conducted in a way to minimize changes to existing frequency band plans.

VI. References

1. Appendix 16: Environmental Sensing Capability
2. “Requirements for Commercial Operation in the U.S. 3550-3700 MHz Citizens Broadband Radio Service Band”, Working Document, WINNF-15-S-0112, Version V0.45, 30 March 2016

APPENDIX 12: CBRS MEASUREMENT REPORT

I. Introduction

A. Purpose and Scope

The scope of this document is to explain the measurement framework, measurement metrics, and the mechanisms by which the metrics are collected and reported to the Federated Wireless Spectrum Access System (“SAS”). The document also briefly explains how each metric can be used by the SAS to adjust the Radio Environment Map (“REM”). The exemplary framework, measurement, and metrics are based on LTE technology but the concepts are readily extensible to other technologies that may be deployed in the 3.5 GHz band.

B. Background

According to the Federal Communications Commission’s (“FCC” or “Commission”) Report & Order [1], the SAS is a centralized management system for spectrum allocation and interference management in the Citizens Broadband Radio Service (“CBRS”) spectrum band at 3550-3700 MHz. In order to perform an efficient interference management and spectrum allocation, the SAS must obtain four sets of information, some static and some in a dynamic fashion. These are: (a) FCC databases, the National Telecommunications and Information Administration (“NTIA”), and other government authorized records; (b) Sensor Data and analysis; (c) CBRS Device (“CBSD”) Registration Records used for SAS REM calculations; and (d) field measurement reports from CBSDs.

The information provided to the SAS through FCC databases, NTIA, other government records, and CBSD Registration records is static information that enables the Federated Wireless SAS to calculate the REM using certain propagation models and network deployment scenarios. However, unless CBSDs actively update their registration records, the SAS will not be able to update the interference environment and the REM. The only dynamic inputs to the SAS are the CBSD active measurement reports to allow the SAS to update its understanding about the interference map and the adjustment in its understanding of radio environment. This dynamic REM adjustment is essential for the SAS to manage CBSD to Incumbent User, General Authorized Access (“GAA”) user to Priority Access License (“PAL”) user, and PAL to PAL interference, as well as facilitate a fair GAA spectrum allocation.

The FCC [1] has mandated that CBSDs provide some sort of measurement report. However, the requirement has not explicitly identified the required metrics and measurement configuration. This document outlines the requirement, proposed framework, and proposed measurement metrics.

C. Assumptions and Constraints

One of the principles of the FCC’s Report & Order [1] is the radio technology neutrality of the CBRS framework. Therefore, the measurement report configuration shall be flexible and expandable enough to address technology neutrality, and shall not necessarily assume any radio technology in the CBRS framework. In other words, the measurement framework, and the SAS-CBSD or SAS-Domain Proxy interface protocols must be developed to assume interoperability between the SAS and CBSDs using different underlying radio technologies.

Therefore, even though the framework shall be able to address any radio technologies and their corresponding measurement metrics, to define the detailed measurement report, we need to



make an assumption on the underlying radio technology to in order to define measurement metrics and their exact definition. To this end, we have assumed the radio technology is 3GPP LTE [2]. This is a realistic and reasonable assumption, since LTE is currently the only active and viable mobile radio technology which has defined operation in the 3550-3700 MHz band, through LTE bands 42 and 43.

However, 3GPP LTE has defined specific measurement metrics provided by the CBSDs and End User Devices (“EUDs” or “UEs”), and limited the set of measurement metrics that can be reported through LTE management framework. Therefore, to avoid a major change to the 3GPP LTE standard, the CBRS measurement framework should follow the 3GPP LTE constraints.

Moreover, the SAS shall be able to exchange measurement configurations and measurement reports from different CBSDs manufactured by different vendors. Therefore, it is essential to design a standard measurement framework to allow interoperability between the Federated Wireless SAS and CBSDs implemented by different manufacturers.

Federated Wireless intends to implement the measurement framework and specific measurement metric designed by the Wireless Innovation Forum (“WINNF”), as a basic solution. However, using the expandable WINNF model, the Federated Wireless SAS will be able to extend the measurement metrics to optimize its REM design and interference management scheme.

II. Functional Requirements

The FCC’s Report and Order [1] provides a description of measurement reports, and the functional requirement is specified in section 96.39(d) of the Commission’s rules.

- FCC Report and Order, para. 237: We require that CBSDs be able to measure and report on their local interference levels and issues as set forth in the proposed rules. We encourage industry to develop detailed metrics regarding issues like received signal strength, packet error rate, and technology specific parameters of signal and interference metrics. These metrics could be developed by an industry multi-stakeholder group. Such guidance could be incorporated in the SAS Approval process described in section III(H)(3)(b) or incorporated independently by authorized SAS Administrators, subject to Commission review. This requirement is separate from sensing requirements associated with ESC, discussed in section III(I).
- Section 96.39(d): “Signal Level Reporting: A CBSD must report to an SAS regarding received signal strength in 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.”

As stated above, the requirement in section 96.39 (d) describes the measurement metrics, the channels by which the metrics are measured, and measuring entity (CBSD or EUD).

III. Existing Measurement Frameworks

For LTE technology, measurements are performed for three main reasons:

- For mobility and load balancing reasons;

- To manage, configure, and optimize the network using LTE management layer and SON systems; and
- Minimization of Drive Test (“MDT”)

A. LTE Measurement for Mobility and Load Balancing

In LTE, the measurements are mainly performed by the UEs for mobility control or for load balancing. The measurement configuration elements can be signaled via the RRCConnectionReconfiguration message from the eNB to the UEs.

Measurement commands are provided by eNB to order the UE to start measurements, modify measurements or stop measurements. Three reporting criteria are used: event-triggered reporting, periodic reporting, and event-triggered periodic reporting. Moreover, depending on the measurement type, the UE may measure and report either its own serving cell, or other listed cells (such as neighboring cells). The measurement report itself could include the listed cells only (*i.e.*, the list is a white-list), or all detected cells. LTE allows inter-technology measurement to be performed (for example an LTE UE measuring other cells using other Radio Access Technologies (“RAT”) such as UMTS for inter-RAT mobility.

The UE triggers one of the LTE pre-defined events when one or more cells meets a specified entry condition as specified in the definition of the event. However, the eNB can influence the entry condition by setting the value of some configurable parameters used in these conditions, for example changing the thresholds or offset, or defining a hysteresis.

Also, the UE may be configured to provide a number of periodic reports after having triggered an event. Of course, the report amount and the report interval would be specified by the eNB.

The eNB can send the measurement configuration, so that the UE performs either Intra-frequency, or Inter-frequency LTE or inter-RAT measurements. The measurements performed by a UE for intra/inter-frequency mobility can be controlled by the eNB, using broadcast or dedicated control. In RRC_IDLE state, a UE follows the measurement parameters defined for cell reselection specified by the E-UTRAN broadcast. In RRC_CONNECTED state, a UE follows the measurement configurations specified by RRC directed from the eNB. Intra-frequency neighbor (cell) measurements are performed by the UE when the current and target cell operates on the same carrier frequency. The UE should be able to carry out such measurements without measurement gaps. Inter-frequency neighbor (cell) measurements are performed by the UE when the neighbor cell operates on a different carrier frequency, compared to the current cell. The UE should not be assumed to be able to carry out such measurements without measurement gaps. The UE may need to perform neighbor cell measurements during downlink (“DL”)/uplink (“UL”) idle periods that are provided by DRX or packet scheduling (*i.e.*, gap-assisted measurements).

For measurements within LTE, the following three major metrics are considered for UE measurement in the DL

- Reference Signal Received Power (“RSRP”): The RSRP measurement provides a cell-specific signal strength metric. This measurement is used mainly to rank different LTE candidate cells according to their signal strength and is used as an input for handover and cell reselection decisions. RSRP is defined for a specific cell as the linear average over the power contributions (in Watts) of the Resource Elements (“Res”) which carry cell-specific RS within the considered measurement frequency bandwidth. Normally the RS transmitted on the first antenna port are used for RSRP

determination, but the RS on the second antenna port can also be used if the UE can determine that they are being transmitted. If receive diversity is in use by the UE, the reported value is the linear average of the power values of all diversity branches.

- Carrier Received Signal Strength Indicator (“RSSI”): The LTE carrier RSSI is defined as the total received wideband power observed by the UE from all sources, including co-channel serving and non-serving cells, adjacent channel interference and thermal noise within the measurement bandwidth. UE LTE carrier RSSI is not reported as a measurement in its own right, but is used as an input to the LTE RSRQ measurement.
- Reference Signal Received Quality (“RSRQ”): This measurement is intended to provide a cell-specific signal quality metric, and is used as an input for handover and cell reselection decisions, especially in scenarios for which RSRP measurements do not provide sufficient information to perform reliable mobility decisions.

The RSRQ is defined as

$$RSRQ = \frac{N \times RSRP}{RSSI}$$

where N is the number of Resource Blocks (“RBs”) of the LTE carrier RSSI measurement bandwidth. The measurements in the numerator and denominator are made over the same set of resource blocks. While RSRP is an indicator of per Orthogonal Frequency Division Multiplexing (“OFDM”) tone wanted signal strength, RSRQ additionally takes the interference level into account due to the inclusion of RSSI. RSRQ therefore enables the combined effect of signal strength and interference to be reported in an efficient way. Even though RSRQ is not the same as SINR, but it resembles the SINR in LTE networks.

In the UL, the LTE eNB can measure the following metrics:

- RSSI:
 - Co-channel RSSI: If eNB is not in operation, co-channel RSSI becomes equivalent to interference power.
 - Non-co-channel RSSI presenting pure interference to the serving eNB
- SINR (“Signal to Interference-plus-Noise Ratio”)
 - SINR on UL control channels (“PUCCH”) or shared UL data channel (“PUSCH”)
- UL received interference power

Moreover, some eNBs can either measure RSRP and RSRQ (like certain home eNB in neighborhood listening mode), or can collect these measurements from UE and report statistics of these metrics. One metric that is defined by LTE to be measured by home-eNBs is carrierRSSI defined as below [4]:

- CarrierRSSI: RSSI over the carrier frequency range from CarrierARFCN_{DL} as the lower bound and (CarrierARFCN_{DL} + CarrierChWidth) as the upper bound. CarrierARFCN_{DL} is the lower bound of the LTE Absolute Radio Frequency Channel

Number (“ARFCN,” determining the center frequency of the channel Bandwidth to be measured) in MHz in the DL direction that HeNB is requested to measure. CarrierChWidth is the Number of ARFCNs in downlink direction starting from CarrierARFCNDL that Home eNB is requested to measure. The range bounded by CarrierARFCNDL as the lower bound and (CarrierARFCNDL + CarrierChWidth) as the upper bound expresses the total carrier frequency range to be measured.

B. LTE Measurement for SON Management and Configuration

In the LTE Self-Organizing Network (“SON”) architecture, Automatic Neighbor Relation (“ANR”), automatically collected measurements from multiple sources (e.g., from UEs, individual network elements, and on an end-to-end basis from advanced monitoring tools) provide accurate real time and near real time data upon which these algorithms can operate to provide performance, quality, and/or operational benefits.

ANR is an automated approach of maintaining Neighbor Relation in LTE and is one of the most important features for SON. ANR will remove, or at least minimize, the manual handling of neighbor relations when establishing new eNBs and when optimizing neighbor lists. This will increase the number of successful handovers and lead to less dropped connections due to missing neighbor relations. It allows automatic discovery and setup of neighbor relations when a UE moves from a serving eNB to another (target) eNB. ANR also automatically sets up of the LTE unique X2 interface between eNBs, primarily used for handover.

The basic building block of ANR is the measurement performed by the UEs. The UE reports all detected Physical Cell Identities (“PCIs”) that fulfill the measurement criteria set by the eNB at RRC connection. The UE may also measure on legacy radio technologies if it supports multi-mode operation. If there is an unknown cell included in the measurement report, then ANR may begin actions to make the cell known and potentially enable handover to the cell.

Another aspect of SON functionality is the Inter Cell Interference Coordination (“ICIC”) Radio Resource Management (“RRM”). The objective of SON is the self-configuration and self-optimization of control parameters of RRM ICIC schemes for UL and DL ICIC. SON based ICIC requires the exchange of messages between the eNBs of various cells, via X2 interface, for interference coordination. By means of ICIC related Performance Measurements (“PM”) analysis, the SON function may properly tune ICIC configuration parameters like reporting thresholds/periods and resource preference configuration settings in order to make the ICIC schemes effective with respect to Operator’s requirements.

C. LTE Minimization of Drive Test (“MDT”)

Traditional drive test procedures to determine coverage for various locations is expensive in terms of staff, time and equipment needed. Without manual drive test, a limited measured information for actual user distribution and their mobility and application mixes are available in any area, such as in-building areas. Also, a manual correlation and post processing of drive test data with network parameters including transmit power, antenna azimuth/tilt/gain, is needed in order to obtain meaningful information. LTE has developed an automated solution by involving UEs in the field to reduce the operator costs for network deployment and operation. In this feature, actual UE data are used to help measure coverage vs. position, etc. This approach has even more advantages over manual drive test, helping measure dropped calls versus position. Coordinated acquisition of UE and network measurements provides significant potential improving the performance of the

system. MDT measurements could be reported either offline in non-real-time mode or immediately by UEs in connected/active state.

Measurements supported for MDT performance using different modes of reporting include:

- RSRP and RSRQ measurement by UE with periodic, event A2, or Radio Link Failure as reporting triggers.
- Power Headroom (“PH”) measurement by UE
- Uplink signal strength/SINR measurement by eNB

The MDT measurement collection task may be initiated in two distinct ways: (1) A management-based MDT task is sent from the LTE management system (“OAM”) towards a PLMN or a limited region within a PLMN without targeting a specific UE; and (2) Signaling based MDT task is sent from the OAM and initiated towards a specific UE and a PLMN or a limited region within a PLMN by the signaling trace activation messages from core network nodes.

(a) Broadband Forum TR-196

The Broadband Forum is a non-profit corporation organized to create guidelines for broadband network system development and deployment.

A Femto Access Point (“FAP” or “Femtocell”) is a small-scale cellular base station, typically designed for use in a home or small business. The FAP is a small-scale cellular base station designed specifically for indoor coverage. As such, it communicates with the user’s mobile handset over the standards-based radio interface using licensed spectrum and further connects to the mobile network infrastructure over the fixed broadband connection.

In TR-196 Issue 2 [6], the Broadband Forum has defined a Radio Environment Measurement (REM) Process for FAP. There are three main purposes for the REM process in [6]. They are:

- Location verification: The surrounding cell information (e.g., macro cells) can be used as a “fingerprint” of the area in which the FAP is located in order for the O&M system to verify its location against the location the FAP owner subscribed the service with (e.g., street address of the owner). The previous section that discusses location verification covers this.
- Neighbor list (“NL”) configuration; The scanning of the DL information (physical radio level information and broadcast information) is gathered from the nearby cells to build the neighbor list. This is a part of the FAP configuration so that it can broadcast appropriate set of NL to the UEs. The next section will cover this.
- Parameter value selection: The scanning of the DL information (both physical radio level and broadcast information) from the nearby cells is useful for the parameter selection process within the FAP. If the FAP is provided with a choice of multiple values or range of values, the nearby cell information can be used to avoid collision or to minimize interference in the area. Some of the examples are Primary Scrambling Code, Maximum FAP Transmit Power, Maximum UL Transmit Power, etc.

IV. CBRS Measurement System Design

A. SAS-CBSD Measurement Report Support

The WINNF, in its Stage 2 Technical Report [7], defines the protocol for SAS and CBSD communication. According to this, after the SAS discovery, the CBSD has to register itself with the SAS, either directly or through a Certified Professional Installer. Upon successful registration at the SAS, its state is change to “Registered”, at any time it could inquire the available spectrum form the SAS, followed by a spectrum grant request by the CBSD. When the CBSD receives the spectrum grant, its state is modified to “Granted”. Regardless whether the CBSD is transmitting signals at the granted spectrum or not, it is mandated to send a “HeartBeat Request” message to the SAS with the SAS-designated period “HearbeatDuration”. The objective of sending “Heartbeat Request” is two-folded: First, it indicates to the SAS that the CBSD is still alive, and therefore intending to use the granted spectrum. Second, since the SAS-CBSD interface uses a RESTFUL HTTP protocol, it is more efficient to initiate all SAS-CBSD communications by the CBSD (pull), and not by the SAS (push). Therefore, the HeartBeat message provide a mechanism for SAS-CBSD communication while the CBSD is in “Granted” or “Transmission” start. Figure 1 depicts the CBSD state transition diagram.

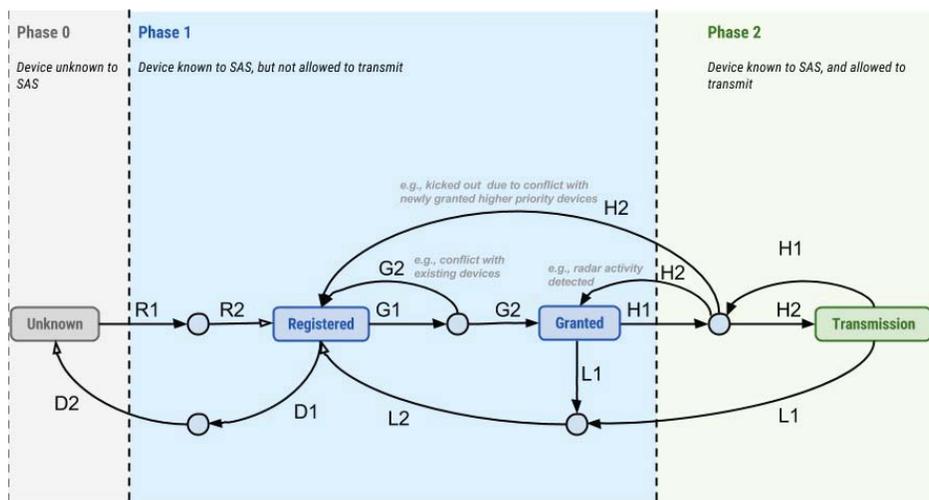


Figure 1: CBSD State Transition Diagram

When the “Heartbeat Request” message is sent by the CBSD, the SAS responds with a “Heartbeat Response” message, in which the SAS could optionally include an object named “MeasReportConfig” containing SAS’s desired measurement configuration. In the succeeding “HeartBeat Request”, the CBSD has to include the measurement report using an object called “measReport”. The detail contents of “MeasReportConfig” and “measReport” have not yet been determined.

BEGIN CONFIDENTIAL INFORMATION

[*END CONFIDENTIAL**

INFORMATION*]**

V. Summary

The Federated Wireless SAS is designed to manage and control the interference to the incumbents and PAL users in CBRS. Moreover, it is aimed to provide fair and optimized channel allocation to GAA and PAL users, in a dynamic and channel/ interference variant environment. The two methods to control the interference and provide efficient channel assignment are: 1) SAS's radio environment calculation, by knowing the location and power and hardware specifications of CBSDs, and assuming a realistic channel and propagation model; and 2) using the measurement report from the CBSDs. The FCC R&O [1] requires all CBSDs to report some type of measurement metric to the SAS. The measured and reported metrics could vary, depending on the underlying radio technology. Some of the LTE-specific metrics are RSRP, RSRQ, DL RSSI, CarrierRSSI, and some of the non-LTE specific metrics are Pre-HARQ PER or BER, call drop rate, handover success rate, SINR, DL Transmit power, UL transmit power, UE power headroom, etc. All of these metrics can be measured and reported during CBSD operation. However, the only metric that can be measured by the CBSD



in silent mode is the CarrierRSSI measured by the CBSD. Therefore, the industry has decided to use CarrierRSSI as the only model used in the first phase of CBRS certification. Federated Wireless has proposed and is implementing a flexible measurement framework that is expandable to any number or types of measurement metrics and would pursue standardization and certification of that model.

VI. References

1. *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 (2015).
2. www.3gpp.org
3. 3GPP TS 36.213 v13.0.1, "Evolved Universal Terrestrial Radio Access (E-UTRA); Physical layer procedures", January 2016 <http://www.3gpp.org/dynareport/36213.htm>
4. 3GPP TS 36.214v13.0.0, "Evolved Universal Terrestrial Radio Access (E-UTRA); Physical layer; Measurements", January 2016 <http://www.3gpp.org/dynareport/36214.htm>
5. 3GPP TS 32.592v13.0.0, "Telecommunication management; Home enhanced Node B (HeNB) Operations, Administration, Maintenance and Provisioning (OAM&P); Information model for Type 1 interface HeNB to HeNB Management System (HeMS)", January 2016 <http://www.3gpp.org/DynaReport/32592.htm>
6. Broadband Forum TR-196: "Femto Access Point Service Data Model, Issue 2", November 2011, https://www.broadband-forum.org/technical/download/TR-196_Issue-2.pdf
7. WINNF-15-P-0062 V0.3.6, "SAS to CBSD Protocol Technical Report-B," March 2016, <http://groups.winnforum.org/p/do/si/topic=801>

APPENDIX 13: REGISTRATION

I. Introduction

A. Purpose and scope

The scope of this document is to explain the process for registering a Citizens Broadband Radio Service (“CBRS”) device (“CBSD”) with the Federated Wireless Spectrum Access System (“SAS”). According to the First Report & Order [1], every CBSD operating in the 3.5 GHz band using the CBRS framework must register with a SAS. This document describes the registration process, the registration protocol, and the registration parameters conveyed by the CBSD.

The current Wireless Innovation Forum (“WINNF”) protocol defines the CBSD registration process based on an individual CBSD registering with the SAS. However, owners of multiple CBSDs may seek to register collections of CBSDs via a Domain Proxy, the protocols for which are still being defined by WINNF. The Federated Wireless SAS will implement the registration of collections of CBSDs via a Domain Proxy when the process is finalized in the WINNF.

B. Background

According to the FCC Report and Order [1], before a CBSD can begin any channel allocation requests with the SAS, or any transmit in the 3.5 GHz band, the CBSD must be registered with the SAS. Providing the SAS with CBSD location, type, and other configuration information is critical to the implementation of the interference protections and other procedures of the CBRS band.

The FCC R&O [1] has outlined the minimum required registration parameters to be included in the CBSD registration process. In addition, a CBSD is generally owned and might be deployed by either a Priority Access License (“PAL”) licensee or a General Authorized Access (“GAA”) user. Therefore, the CBSD registration process includes several pre-requisite steps, including Owner pre-Registration (“OR”), PAL Licensee pre-Registration for CBSDs using PAL licenses, and Certified Professional Installer (“CPI”) pre-Registration (“CPIR”) mandated for all category B CBSDs and optional for Category A CBSDs.

As stated above, the CBSD registration is required before a CBSD can start a spectrum request or commence radio operation in the CBRS band. However, the WINNF has defined two procedures for completion before a CBSD can request a spectrum grant. They are the Registration Procedure (and all its pre-requisite steps as described in Section 3 below), and the optional Spectrum Inquiry Procedure.

This document outlines the CBSD registration process, multi-step registration, parameters included in the registration, different registration mechanisms, and pre-requisite pre-registration stages.

C. Assumptions and Constraints

To define the registration process, the following should be assumed:

- a) The SAS-CBSD Protocol is completely defined
- b) The roles, responsibilities, process, and operation of CPIs are completely defined.
- c) The process for owner pre-registration is defined
- d) The process for PAL licensee pre-registration is defined
- e) The parameters required for CBSD registration are agreed and completed.
- f) The SAS has to provide an interface or a portal to allow professional installers

Federated Wireless intends to implement the registration framework and specifications developed by WINNF as a basic solution.

II. Functional Requirements

The description of registration requirements is stated in Paragraph 232, 233, and 333 in FCC Report and Order [1], and the functional requirement is specified in Part 96 Section 96.39 (c), and 96.45 (a).

Paragraph 232: The Citizens Broadband Radio Service framework depends on SAS authorization of commercial use and protection of incumbents. In order to perform this function, it is essential for the CBSD to provide the SAS with necessary information about its operations prior to transmission. We therefore require that as part of registration, the CBSD should provide the SAS with a number of operational parameters, including geographic location, antenna height above ground level (meters), CBSD operational category (Category A/Category B), requested authorization status, unique FCC identification number, user contact information, air interface technology, unique serial number, and additional information on its deployment profile (e.g., indoor/outdoor operation). All information provided by the CBSD to the SAS must be true, complete, correct, and made in good faith, and failure to provide such information will void the user's authority to operate the CBSD.

Paragraph 233: We adopt additional registration requirements for Category B CBSDs. Pursuant to section 96.45, Category B CBSDs must register all information required under section 96.39 as well as antenna gain, antenna beamwidth, antenna azimuth for sector site, and antenna height above ground level. These additional requirements could provide the SAS with information necessary to perform effective propagation and interference mitigation analyses on these higher power devices. This will help ensure the effective coexistence of all tiers of user operating in the band. If any of the required registration information changes, the CBSD shall update the SAS within 60 seconds of such change.

Paragraph 333: We find that registering, authenticating, and authorizing CBSDs is an essential component of the SASs responsibilities. As described in section III(F)(2)(b), CBSDs must report information on their technical specifications, location, and the identity of their authorized operators or licensees to the SAS. The SAS must, in turn, verify this information to ensure that CBSDs are used only by authorized users in accordance with the Commission's rules. The SAS must also verify that the FCC ID of any CBSD seeking to provide Citizens Broadband Radio Services is valid prior to authorizing it to begin providing service. We reiterate that individual CBSDs are not required to interface with the SAS so long as the required information is communicated by an aggregation point or network control device. We also note that these requirements do not apply to End User Devices. SASs must not collect, track, or store information on End User Devices or their users without user consent.



The precise methods used to register, authenticate, and authorize CBSDs may be determined during the SAS approval process described in section III(H)(3)(b).

Section 96.39(c): “(c) Registration with SAS: A CBSD must register with and be authorized by an SAS prior to its initial service transmission. The CBSD must provide the SAS upon its registration with its geographic location, antenna height above ground level (in meters), CBSD class (Category A/Category B), requested authorization status (Priority Access or General Authorized Access), FCC identification number, call sign, user contact information, air interface technology, unique manufacturer’s serial number, sensing capabilities (if supported), and additional information on its deployment profile required by sections 96.43 and 96.45. If any of this information changes, the CBSD shall update the SAS within 60 seconds of such change, except as otherwise set forth in this section. All information provided by the CBSD to the SAS must be true, complete, correct, and made in good faith.”

Section 96.45(a): Category B CBSDs must be professionally installed.

As stated above, the requirement in section 96.39(c) describes the registration parameters, the channels by which the metrics are measured, and the applicable measuring entity (CBSD or EUD).

III. Registration Pre-Requisites

Before a CBSD can begin automated channel allocation requests with the SAS, the CBSD must be registered with the SAS. This is a rather complex process, pursuant to which several separate pre-registration procedures or enrollments may be required. This section describes these procedures.

We may analogize the registration process to registering a car and obtaining a driver’s license. In this context, owner pre-registration as described below is equivalent to obtaining a driver’s license for the entity that owns the CBSD and plans to operate it. The CBSD registration is equivalent to registering the specific car. Finally, the PAL pre-registration is equivalent to obtaining a Commercial Driving License (“CDL”) to perform additional operations beyond those authorized by the standard driver’s license, such as operating large commercial vehicles, etc.

A. Owner pre-Registration

CBSDs must be associated with an owner, who is required to pre-register (enroll) with the system. The owner may be an individual or legal entity (e.g., corporation, non-profit, governmental agency) who owns and is responsible for one or more CBSDs. Owner registration with a certified SAS is expected to be a manual process (for example, via a Web Interface). The owner pre-registration process is depicted in Figure 1.

During the owner Pre-Registration process, the SAS Administrator and the CBSD Owner shall exchange information that establishes a secure mechanism to verify the CBSD Owner identity and to establish the relationship between the CBSD and its owner. This procedure could be completed via the following approaches:

1. By the SAS providing a number of unique and secure owner pre-shared (“PSK”) authentication keys to facilitate association of the CBSD being registered with the corresponding owner.
2. The owners supply the fingerprint of all of their CBSDs, and public keys as a per-CBSD token to the SAS following the Owner Registration process. The SAS Administrator keeps this database, and matches the fingerprint of the CBSDs (e.g., using CBSD Serial Number) provided during CBSD registration to validate the CBSD and owner association.

It is important to note that Federated Wireless considers any post-manufacturing data entry into the CBSDs by individuals a potential security risk unless the communication and interface between the CBSD and individuals follows a tight logical and physical security. One such example is when the CBSDs are under the control of a Mobile Network Operator (“MNO”) management system, and are behind Domain Proxy (“DP”). Therefore, Federated Wireless prefers to implement the second approach. However, it is open to other approaches if such approaches ensure the security of the communications.

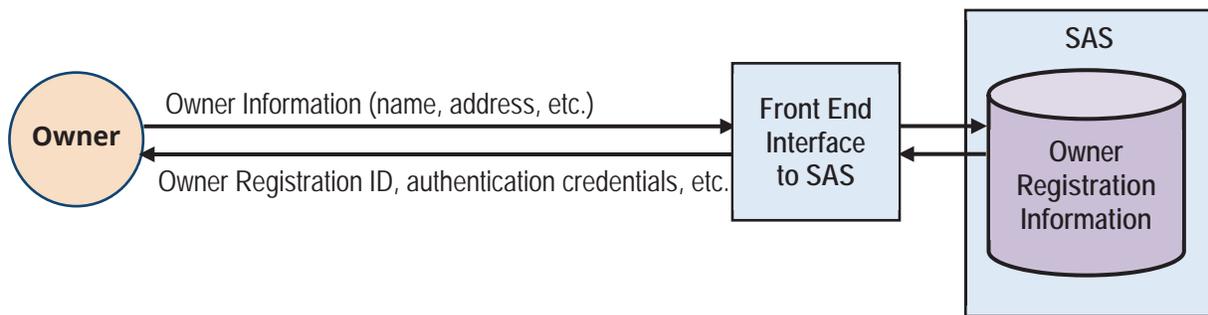


Figure 1: Owner Pre-Registration including a secure mechanism for CBSD-Owner Association

As part of the owner pre-registration process, the owner has to provide the following information to the SAS:

- Owner legal identity (corporate or individual),
- Owner Mailing Address (contact address), or designated agent contact address,
- Owner’s Physical address (may or may not correspond to the Mailing Address)
- Owner’s Legal Address (may or may not correspond to the Mailing Address)
- Owner’s Email Contact Address,
- Owner’s Phone Number (contact, or of designated agent),
- Designated Agent (if applicable)

After the owner has provided the above contact information, the system must provide the owner with:

- A system wide unique Owner Registration Identify (“OR-ID”),
- A method to authenticate the Owner when accessing the Owner account (e.g., password)

Information is exchanged between the CBSD owner and the SAS Administrator to establish a secure mechanism to associate the CBSD and the owner identity. This mechanism will be used to allow the SAS to properly associate a registering CBSD with its owner. This is to ensure the CBSD is linked to a valid owner and to ensure registration occurs with the owner's permission. The mechanism would allow the owner to create sub-groupings of CBSDs, which may be useful for large networks.

During registration, the owner has to acknowledge that operation of the CBSD(s) is subject to the requirements of Part 96 [1], and also acknowledge and accept the risk of interference from federal operations in the band [1, § 96.55(e)]. Upon owner registration, the SAS shall record the following information about the owner:

- Registration date,
- Registration expiration or term
- Registration state (valid, expired, pending enforcement, revoked),
- Registering Agent (FCC, SAS, or other agent),
- Whether Registration Fee is Paid or not. This information is optional and could include a credit card transaction that may help to serve as an identity check and a mailing address check to prevent fraudulent or fictitious registrations and mailing addresses. This credit card transaction may be a separate transaction for the Owner License, or may be the purchase transaction for the CBSD itself.

The SAS must validate the owner credentials (whether an individual or business) to ensure the owner is who they represent themselves to be and has provided valid contact and address information. For an individual, this may include using a credit card to validate name and contact address. Moreover, the Owner shall be able to update owner information and be able to register or deregister CBSDs to their account.

B. Professional Installer pre-Registration

For the CBSDs that are installed by a CPI, the CPI is required to pre-register with a professional Installer certifying body database, which the SAS must be able to access. The rules also "encourage" an accreditation program for professional installers [1, para. 222]. The installer pre-registration process is depicted in Figure 2.

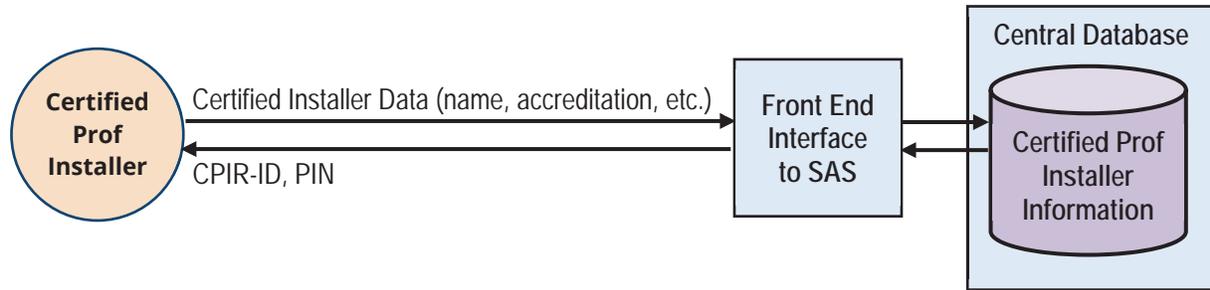


Figure 2: CPI Pre-Registration

The FCC Rules require that Category B CBSDs be installed by a CPI, while Category A CBSDs may or may not be installed by a CPI [1, § 96.45 (b)].

The SAS must provide CPIs with a system-wide unique CPI Identity and a method to authenticate the CPI when accessing the CPI account. This information will then be used by the CPI when they enter the CBSD Device Installation Record into the CBSD or provide it to the SAS Administrator. Moreover, these two sets of information shall be recorded by the SAS accessible database.

The Certified Professional Installer Registration (“CPIR”) process requires the CPI to provide the following information to a SAS-accessible centralized database:

- Legal identity (name),
- Mailing address,
- Legal address,
- Email contact,
- Phone contact,
- Accredited certification number from a training program,
- License initiation date, termination date

This set of information could be provided to the SAS in two ways: First, through a secure CPI communication mechanism provided by the SAS Administrator, and after authenticating the identity of the CPI by the SAS Administrator. The second approach is to embed this information into the CPI certificate and, through the CPI authentication process, the SAS Administrator could extract this information from the certificate. The Federated Wireless SAS implementation is able to accept either approach.

C. PAL Licensee pre-Registration

The FCC is planning to auction PALs on the basis of census tracts. A census tract is variable in size and is based on population, ideally 4,000 people. Even though the census tracts may change over time based on census surveys, it is assumed that after a PAL auction, the census tract will remain fixed for the duration of the license term.

According to the FCC R&O [1], the spectrum allocated to a PAL must be used by the licensee, and if the SAS recognizes the spectrum allocated for PAL is not in use by the licensee, the SAS can authorize GAAs to temporarily operate on that spectrum. Therefore, the PAL protection might be limited to a smaller area than the census tract defined by the PAL. The FCC R&O has envisioned the concept of “use it or share it,” and defined actual “use” using engineering concepts and the general view that protection areas can be determined and enforced by the SAS. As a result, to support this concept, and the concept of secondary market transactions, the CBSD registration process might entail the explicit definition of the new PAL Protection Area (“PPA”).

The PAL (or PPA) needs to be associated with one or more CBSDs before it can request channel grants from the serving SAS and attempt to assert PAL rights to protected and reserved channels in a specific protected area.

For CBSDs using PAL credentials, the PAL licensee is required to pre-register or enroll the PAL and the specific protection area with the SAS. As a result of the PAL pre-registration process, a PAL license ID number (“PAL-ID”) and a security feature for authentication would be provided. Figure 3 depicts the PAL pre-Registration process. Federated Wireless’ proposed PAL channel assignment process is outlined in [3].

Similar to the owner case, Federated Wireless considers any post-manufacturing data entry into the CBSDs by individuals a potential security risk unless the communication and interface between the CBSD and individuals follows a tight logical and physical security. Therefore, Federated Wireless accepts the PAL credentials either through DP, or through CBSDs if the security of the owner entering information into the CBSDs is assured.

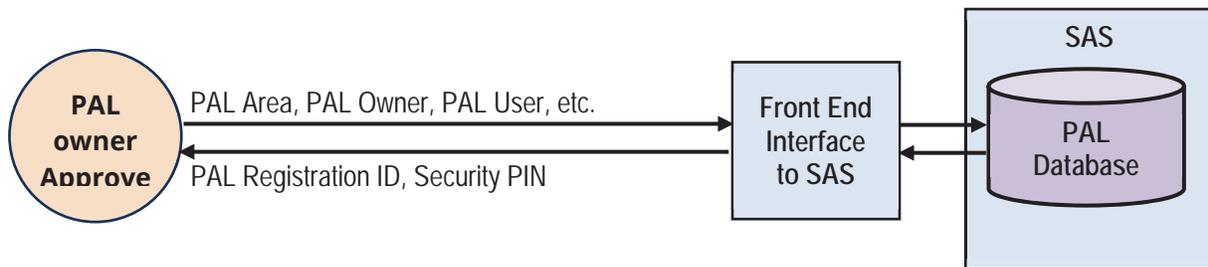


Figure 3: PAL Pre-Registration

The PAL pre-Registration process is not yet standardized in WINNF; however, the following provides Federated Wireless’s general thoughts:

The PALs may be further sub-divided into meaningful and usable PPAs that may correspond to useful areas (like a shopping mall, town center, airport area, etc.). These may be determined by the SAS when it models positioning of a group of CBSDs within that sub-area with their collective coverage and determines the size of the protected sub-area. The SAS doesn’t have to define the PPA, but if a PAL owner wishes to lease a portion of their service area, the PAL owner and lessee need to agree on the boundaries of the area being leased. These areas may be leased, sub-leased, brokered, or sold to other parties. Hence, the (OR-ID or a CBSD ID might not be associated to a PAL-ID permanently. Within one PAL, one or many non-overlapping PPAs may be defined. The PPA is then assigned a PAL-ID and authentication number, thus registering it (in the same format as the PAL-ID and security feature for authentication) with the SAS and the overall system.



The method for establishing the PPA is out of the scope of this document.

However, the PAL License ID registration process shall establish a unique PIN (or similar encrypted security feature) to allow any SAS to authenticate any PAL submitted as a credential from a requesting CBSD device.

The associated database field for a unique PAL License (PAL ID) could include the following pieces of information and parameters for each PAL. The information could be either entered by the PAL owners or be fetched from FCC database.

- a) Establishment of a system-wide unique PAL ID registration number that corresponds to a specific PPA according to section 96.32 in [4],
- b) An encrypted token or security feature that allows automated SAS authentication (from any SAS) of any PAL ID when presented during normal automated channel requests from CBSD devices,
- c) The original PAL owner from the auction results,
- d) The PAL initiation date (from auction),
- e) The PAL termination date (from auction),
- f) The census tract and block identity (identification numbers),
- g) The 'M' vertex points that define the original PAL census tract boundaries,
- h) The 'M' vertex points defining the PAL sub-area.
- i) The PAL state (purchased, pending, claimed, valid, PAL expired, PAL revoked, PAL pending enforcement).

D. PAL Lessee pre-Registration

Subject to section 96.32 of [4], a PAL licensee, is permitted to lease any portion of its its spectrum access or geographic area, outside of the PPA, for any bandwidth or time duration within the terms of the license with any entity that has provided a certification to the FCC.

Paragraph 1.9046 of [4] requires that the lessee first obtain an FCC Registration Number ("FRN") and submit a certification to the FCC that it meets the same eligibility and qualification requirements applicable to the licensee. Then the licensee must submit notification of the leasing arrangement to the SAS Administrator, by electronic filing. The notification or pre-registration must include the following information:

- a) lessee contact information including name, address, telephone number, fax number, e-mail address;
- b) lessee FRN;
- c) name of Real Party in Interest and related FRN;
- d) the specific spectrum leased (in terms of amount of bandwidth and geographic area involved) including the call sign(s) affected by the lease;
- e) the Duration of the lease

E. CBSD Authentication

To protect the exchange of authorization information and communications between the SAS and CBSDs, the CBSD and the SAS must authenticate each other before any communication, including registration. WINNF has adopted communications security policies governing SAS and

CBSD communications interfaces, including their mutual authentication. These policies describe a Public Key Infrastructure (“PKI”) which governs communications within the CBRS ecosystem and provides authentication and authorization for messages exchanged within the SAS ecosystem, through both the SAS-CBSD and the SAS-SAS communication interfaces. Figure 4 shows the position of the SAS-CBSD authentication process in the SAS-CBSD communication procedure.

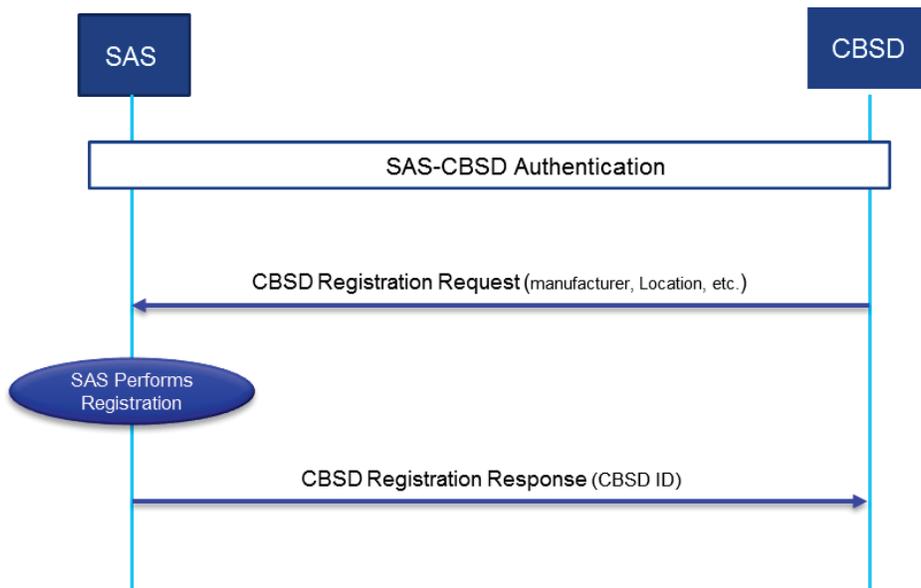


Figure 4: Authentication in SAS-CBSD Registration

PKI is a system which organizes credentials authenticated by a hierarchical structure containing a Root of Trust (“RoT”). The RoT signs credentials for trusted parties which authenticate their identities. Those parties may then sign credentials for another level of trusted parties. Figure 5 depicts the CBRS chain of trust that defines the RoT for the SAS or the CBSD RoT.

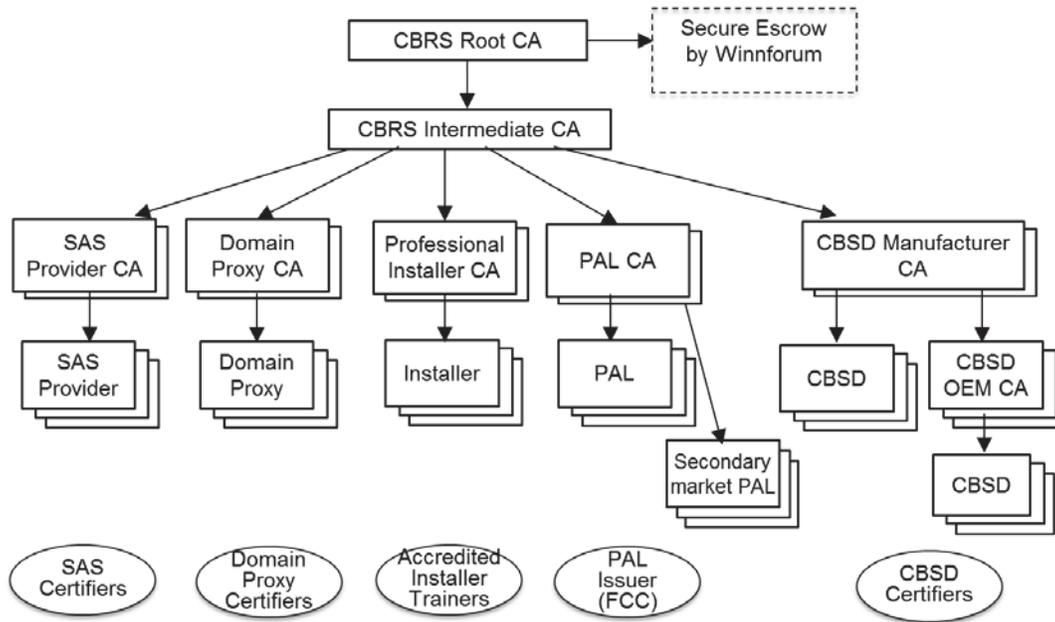


Figure 5: CBRS Chain and Root of Trust

Transport Layer Security (“TLS”) is the protocol selected for CBRS authentication. The TLS protocol provides authentication, confidentiality, and data integrity between two communicating applications and will utilize PKI to further ensure the security of the communications and authenticity of the communication elements.

As in Figure 4, before any communication occurs between the SAS and a CBSD, a TLS session is created between the two entities. The TLS session stays active as long as the procedure (such as registration procedure) is active. The authentication to the SAS is required between SAS and CBSD if the CBSD is directly communicating with the SAS, and is required for Domain Proxy and SAS if the CBSDs are under the control of a centrally-managed domain proxy. In the latter case, CBSDs have to be able to provide their authentication credentials or the Domain Proxy will be required to ensure their valid and authenticated status.

The details of the PKI and TLS processes, and how security is managed, are addressed in a different section of this application.

IV. CBSD Registration

CBSD registration is required by the FCC R&O [1] before a CBSD can make any spectrum grant request. Prior to CBSD registration, the SAS should have been discovered by the CBSD per the SAS discovery process being defined by the WINNF. CBSDs can register at the SAS in a single step through machine-to-machine registration or in a multi-step approach using CPs. As part of registration, the CBSD or CPI must provide installation parameters to the SAS. This section describes the procedures and parameters of each of these two approaches.

For a managed network with a Domain Proxy, the Domain Proxy can register on behalf of one or more CBSDs under its control. Each CBSD will still require its own CBSD Registration ID for its own parameters and location.



Upon completion of the CBSD registration procedure, a SAS needs to inform the CBSD Owner, CPI of the CBSD, other SASs, and if required, the FCC whether the registration is revoked, pending (e.g., due to incomplete information) or completed, whether the CBSD has been taken out of service (decommissioned), and whether the CBSD has any enforcement actions initiated against it or determined to be in effect.

The CBSD Registration could be categorized into two categories based on the number of stages required for registration completion. The first one is single step CBSD Registration, where the CBSD's position and installation parameters are either obtained (e.g., through GPS) or embedded in the CBSD, and the CBSD can convey them to SAS as a machine-to-machine automated protocol. The second one is multi-step registration, where in the first step, the CBSD performs a machine-to-machine protocol using manufacturer information, and in the second step, the CBSD or CPI uploads the location / installation information to the SAS. The single step registration could optionally apply to category A CBSDs, while category B CBSDs must use a multi-step registration.

A. Single Step CBSD Registration

Category A CBSDs may be installed by an owner or an authorized associate of the owner. Such CBSDs will initiate registration with the SAS. An owner-installed CBSD must be capable of automatically calculating its location (as defined by the FCC Rules) and providing that information as part of the CBSD registration process. Figure 4 depicts the single step CBSD Registration procedure.

1. Registration Process

The CBSD has to associate itself with an owner before the registration process. To this end, the Registration process shall either use the Owner Pre-Shared Key ("PSK"), previously established during the Owner Registration process, or the owner shall provide the list of associated CBSDs (CBSD fingerprints) during owner pre-registration, which shall allow any SAS to associate a registering CBSD with its corresponding registered Owner. Federated Wireless prefers the latter solution.

After successful authentication, if there is no Domain Proxy, the CBSD initiates registration by sending a CBSD Registration Request message to the SAS. Upon reception of the CBSD Registration Request, the SAS initiates the registration of the CBSD. The SAS responds to the CBSD with a CBSD Registration Response containing a CBRS-wide unique CBSD ID Information Element ("IE") along with an indication whether the registration succeeded or failed. The CBSD uses the CBSD ID parameter for all subsequent procedures with the SAS. If registration fails, there will be a Registration Response containing an error code. The CBSD ID shall have a one-to-one correspondence with the combination FCC ID + CBSD Serial Number and may be identical to that combination.

If the SAS determines the registration is incomplete, the SAS returns an error code indicating Registration Pending status. The CBSD periodically repeats the Registration Request until receiving a successful Registration Response from the SAS.

If the SAS determines the CBSD operating privileges have been revoked, the SAS returns an error code representing the CBSD as black-listed. When the CBSD operating privileges are restored, the CBSD may initiate a Registration Request.

If one of the parameters in the Registration Request is in error, the SAS returns an error code indicating a registration failure along with the faulty parameter(s). The CBSD passes the failure cause to the upper layers for resolution.



2. Registration Parameters

Prior to the SAS enabling spectrum use by the CBSD, Category A CBSDs shall provide the following information to the SAS. For single step registration, the information will be uploaded via the CBSD directly communicating with the SAS.

- a) CBSD Vendor,
- b) CBSD Serial number [1, § 96.39(c)],
- c) FCC Identification number [1, § 96.39(c)],
- d) Call Sign [1, § 96.39(c)],
- e) Secure information to associate CBSD with the Owner (maybe provided through Owner pre-Registration) CBSD Air Interface Technology, and the latest release of the technology supported by the CBSD [1, § 96.39(c)],
 - o Type includes: EUTRA (LTE), other values to be defined as appropriate
- f) CBSD Sensing capability [1, § 96.39(c)],
- g) CBSD installation location (Indoor or Outdoor) [1, § 96.43(b)],
- h) Location information [1, § 96.39(c) & para 219]:
 - o Latitude,
 - o Longitude,
 - o Antenna Height above ground level (AGL in meters),
- i) Other optional CBSD Installation Parameters (see below)
- j) Other optional vendor-specific information fields. The SAS shall allow CBSDs to provide optional vendor-specific information which can be used by the SAS. Examples include: CBSD model number, CBSD hardware version number, CBSD software and/or firmware version number, hardware characteristics, etc.

The optional CBSD installation parameters for Category A registration include

- a) Antenna Height Above Mean Sea Level (AMSL in meters)
- b) Accuracy of CBSD antenna horizontal location in meters, if it is smaller than the FCC requirement (50 meters)
- c) Accuracy of CBSD antenna vertical location in meters, if it is smaller than the FCC requirement (3 meters)
- d) 3-dB Antenna beamwidth in degrees [1, § 96.45(d)],
- e) Antenna azimuth pointing direction in degrees [1, § 96.45(d)],
- f) Antenna downtilt angle, both mechanical and electrical downtilts in degrees [1, § 96.45(d)],
- g) Peak Antenna Gain in dBi [1, § 96.45(d)]

The FCC ID, call Sign, CBSD Serial Number, and user ID identify the CBSD to SAS. The CBSD Category, air Interface, CBSD Manufacturer, sensing capability and installation parameters provide

specific information on the CBSD equipment configuration and capabilities. The maximum number of Grants parameter informs the SAS on the maximum number of grants the CBSD can use simultaneously (CBSD capability).

B. Multi-Step CBSD Registration

All Category B CBSDs must be installed by a CPI. Category A CBSDs unable to automatically (either by design or due to disadvantaged placement, such as indoor location) determine their location to within the accuracy prescribed in the FCC Rules must be installed by a CPI.

When the CPI is installing the CBSD (Category A or B), the CPI is required to provide additional information about the CBSD. The information may be entered into the CBSD (to be relayed to the SAS) or entered by a CPI via a mechanism provided by the SAS Administrator. The information provided by the CPI is site-specific. If a CPI accesses the CBSD to provide additional information, then s/he has to provide to the CBSD their associated CPI Registration ID. Figure 6 depicts a general multi-step CBSD registration. Figures 7 and 8 depict different scenarios for handling multi-step registration.

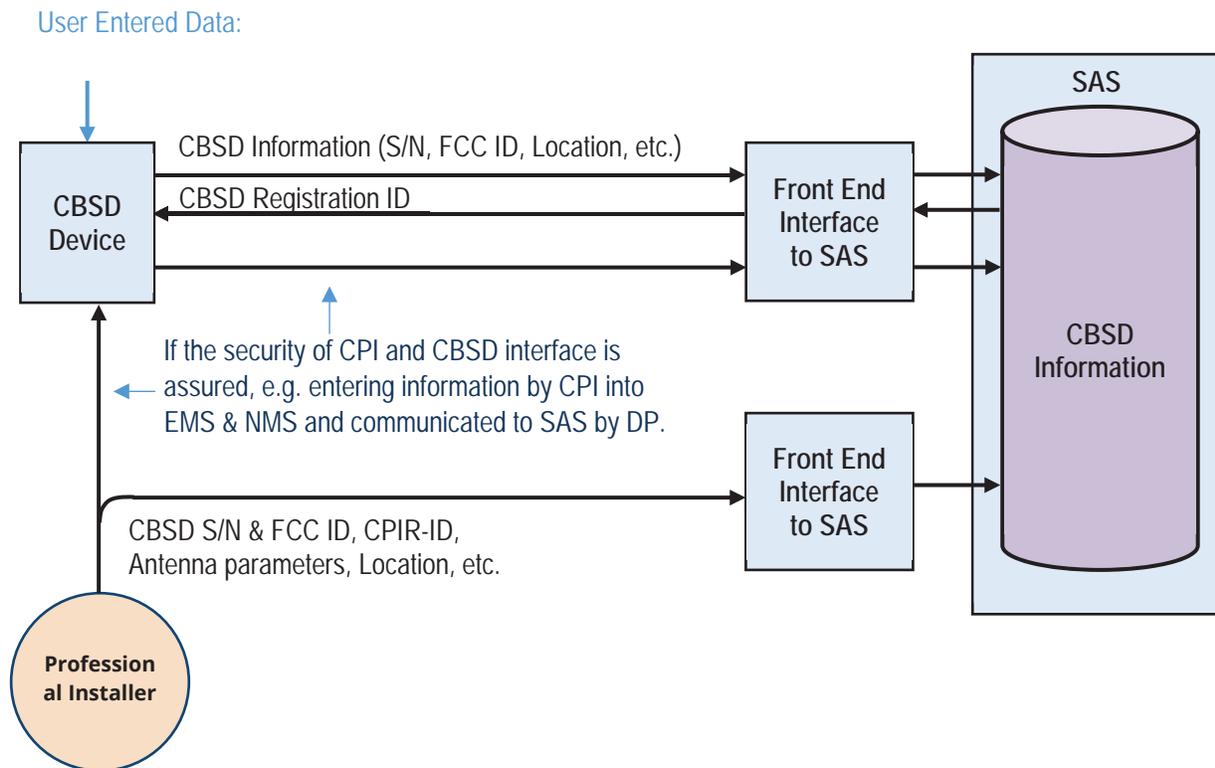


Figure 6: CBSD Multi-Step Registration

1. CBSD Machine-to-Machine Registration

The first step of CBSD multi-step registration is the Machine-to-Machine Registration after the CBSD and SAS are authenticated. As depicted in Figures 6, 7, and 8, similar to the single-step

process, the SAS receives the Registration Request, processes the fields of the request, and decides whether it wants to pursue the registration process or reject the request. The difference is that the set of parameters during machine to machine registration step is limited to the following:

- a) CBSD Serial Number [1, § 96.39(c)],
- b) FCC Identification Number [1, § 96.39(c)],
- c) Secure information to associate CBSD with the Owner (maybe provided through Owner pre-Registration)

Similar to the single-step process, the SAS would respond with a Registration Response message accepting or rejecting the request, based upon the limited information provided by the CBSD through machine-to-machine registration. If the registration request is successful, the SAS would include a CBSD ID in its response. This ID is used by the CPI in the second step to enter other related parameters or the CBSD.

2. CBSD Installation Record by Professional Installer

The second step of a multi-step registration requires the CPI to communicate with SAS via a mechanism provided by the SAS Administrator. In this case, the CPI shall provide the SAS or the SAS-accessible database with the CBSD serial number and FCC ID (to uniquely identify the CBSD), as well as the associated CPI Registration ID.

The SAS can access or receive CBSD information from CPI using two methods. In the first method, depicted in Figure 7, even before the CBSD starts the machine-to-machine registration with the SAS, the CPI has already entered the required information for the CBSD (or a group of CBSDs) through a secure mechanism provided by the SAS Administrator. In this case, upon receiving the Registration Request from the CBSD, the SAS would access the database and validate the information provided by the CBSD and CPI before it accepts or rejects CBSD registration. In this method, the SAS does not need to put the CBSD in pending mode, and the CBSD does not have to send the CBSD Registration Request for the second time.

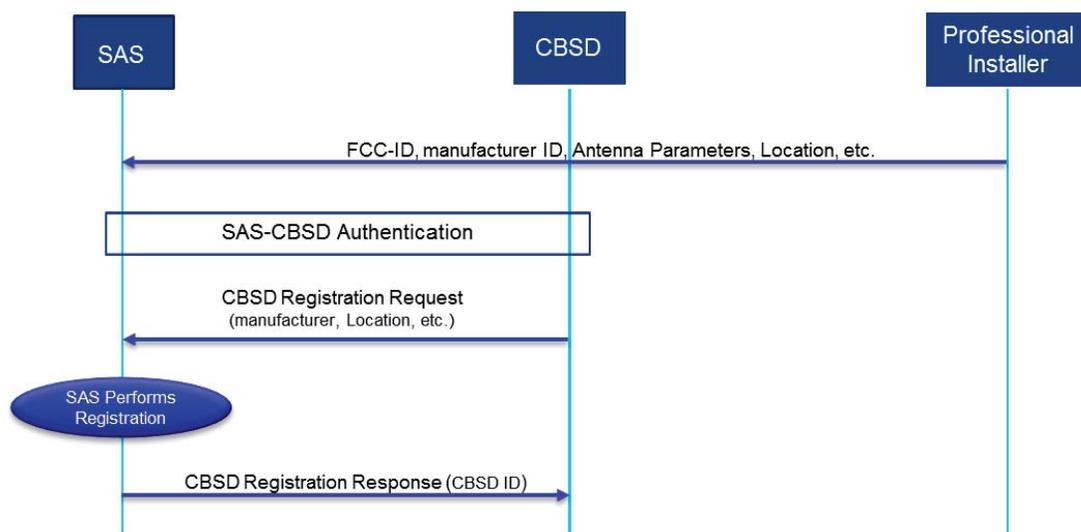


Figure 7: CBSD multi-step Registration method 1

In the second method, depicted in Figure 8, the SAS responds to the first Registration Request with a successful Registration Response that includes CBSID ID, but puts the CBSID in a pending state. The CPI uses CBSID ID to enter the installation parameters into the CBSID, which are transmitted to the SAS afterwards, possibly through a second Registration Request. The inclusion of the second Registration Request is not yet finalized by WINNF. Alternatively, the CPI can directly enter the installation parameters into the SAS through a mechanism provided by the SAS administrator. Finally, the SAS responds with a successful or failure Registration Response, using a process explained in Section 4.a. Once again, Federated Wireless considers any post-manufacturing data entry into the CBSIDs by individuals (the CPI in this case) a potential security risk unless the communication and interface between the CBSID and CPI follows a tight logical and physical security. Therefore, Federated Wireless prefers the second method, where the CPI directly provides the information to the SAS Administrator. However, when the interface between CBSIDs and CPI is secure, Federated Wireless will accept the information from the CBSID. One such example is when the CBSIDs are under tight and secure control of the MNOs, and the CPI can communicate with the MNO management system (Element Management System and Network Management System) and Domain Proxy.

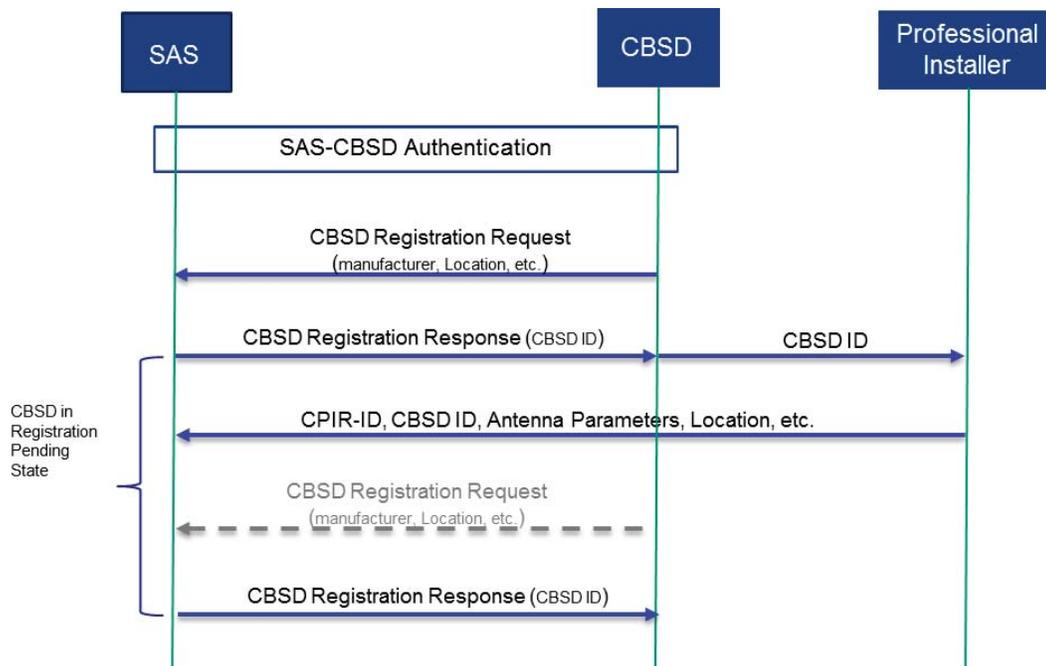


Figure 8: CBSID multi-step Registration method 2

The CPI might create a file named Device Installation Record (“DIR”), which includes all CBSID installation parameters transferred in the second step of CBSID registration, and upload that file into the SAS using a mechanism provided by the SAS Administrator.

The mandatory parameters included in DIR or directly entered into the SAS are the following:

- a) CBSID Vendor,



- b) Call Sign [1, § 96.39(c)],
- c) CBSD Air Interface Technology, and the latest release of the technology supported by the CBSD [1, § 96.39(c)],
 - o Type includes: EUTRA (LTE), other values to be defined as appropriate
- d) CBSD Sensing capability [1, § 96.39(c)],
- e) CBSD installation location (Indoor or Outdoor, required for Category A CBSDs that are installed by a CPI) [1, § 96.43(b)],
- f) Location information [1, § 96.39(c) & para 219]:
 - o Latitude,
 - o Longitude,
 - o Antenna Height above ground level (AGL in meters),
- g) CPI Registration ID (if information provided to the CBSD was manually entered by a CPI),
- h) 3-dB Antenna beamwidth in degrees [1, § 96.45(d)],
- i) Antenna azimuth pointing direction in degrees [1, § 96.45(d)],
- j) Antenna downtilt angle, both mechanical and electrical downtilts in degrees [1, § 96.45(d)],
- k) Peak Antenna Gain in dBi [1, § 96.45(d)]
- l) Other optional CBSD Installation Parameters (see below)
- m) Other optional vendor specific information fields. The SAS shall allow CBSDs to provide optional vendor specific information which can be used by the SAS. Examples include: CBSD model number, CBSD HW version number, CBSD SW and/or FW version number, hardware characteristics, etc.

The optional CBSD installation parameters included in the DIR or directly entered into the SAS are:

- a) Antenna Height Above Mean Sea Level (AMSL in meters)
- b) Accuracy of CBSD antenna horizontal location in meters, if it is smaller than the FCC requirement (50 meters)
- c) Accuracy of CBSD antenna vertical location in meters, if it is smaller than the FCC requirement (3 meters)

V. CBSD Spectrum Inquiry Procedure

As explained in Section 2, even though the FCC R&O [1] does not necessarily require CBSD registration before a CBSD can initiate a spectrum Grant Request, the Federated Wireless SAS requires the CBSD to register with the SAS prior to requesting a spectrum grant. This is essential, because the SAS cannot determine channel availability or the interference impact of the CBSD without having critical information about that CBSD, such as location, peak power, antenna characteristics, etc. However, WINNF has defined an intermediate optional step named "Spectrum Inquiry Procedure". 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. Since 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 files included in the Spectrum Inquiry Request are:

- CBSD ID
- A set of PAL Credentials: If the CBSD owner has PAL right, the PAL credential(s) should be included here. Credentials are formatted as an array of strings. This field is not included if the CBSD has no PAL right.
- A set of inquired Frequency ranges for which the CBSD seeks information

The SAS performs an assessment of channel availability for the frequency ranges indicated in the spectrum Inquiry Request. If the request succeeds, the SAS sends a spectrum Inquiry Response, including the CBSD ID, and the list of available channels and their types (PAL or GAA). If the parameter CBSD ID used in the Spectrum Inquiry Request message does not match with the PAL Credentials provided (e.g. the CBSD location does not match), the SAS fails the request and responds with an error message

The SAS does not reserve any channel allocations as part of the Spectrum Inquiry, nor does the SAS guarantee the information in the available channel object is still valid when the CBSD initiates a grant request. The CBSD should consider the information in the available channel object as an indication of the channels available to the CBSD.

If there is a Domain Proxy and the Domain Proxy is performing bulk Spectrum Inquiry Requests, the Domain Proxy aggregates information related to each applicable CBSD into an array of spectrum Inquiry Request objects. When the Domain Proxy receives the array of spectrum Inquiry Response objects from the SAS, the Domain Proxy matches the individual responses to the individual requests and takes the appropriate action, possibly involving the CBSD(s) and/or a separate CBSD element management system.

If the SAS determines an error with one of the parameters in the spectrum Inquiry Request message, the SAS returns a spectrum Inquiry Response message with an error code along with the faulty parameter(s). The CBSD passes the failure cause to the upper layers for resolution.

VI. Summary

According to the FCC Report and Order [1], before a CBSD can begin any channel allocation requests with the SAS, or any transmit in the 3.5 GHz band, the CBSD must be registered with the SAS. Providing the SAS with CBSD location, type, and other configuration information is critical to the implementation of the interference protections and other procedures of the CBRS band.

The FCC R&O [1] has outlined the minimum required registration parameters to be included in CBSD registration process. The parameters include information about the CBSD owner, FCC ID, technology to be used, and all hardware specifications that impact the power transmission and interference impact of CBSD transmission. Moreover, the CBDS needs to authenticate with the SAS to make sure no rogue CBSD accesses the CBRS spectrum. In addition, since each CBSD is generally owned and might be deployed by either a PAL licensee or a GAA user, the CBSD registration process requires a pre-requisite registration process including Owner pre-Registration, PAL Licensee pre-Registration for CBSDs using PAL licenses, and Certified Professional Installer pre-Registration (CPIR) mandated for all category B CBSDs and optional for category A CBSDs. If Category A CBSDs cannot



identify their own location using available positioning techniques (e.g. GPS), they have to be installed by a professional installer.

Moreover, the registration process might optionally include a spectrum inquiry procedure from the SAS. Using this procedure, the CBSD could obtain information about available channels for CBRS transmission, and their channel type (PAL or GAA).

VII. References

- [1] FCC Report and Order 15-47A1: "Amendment of the Commission's Rules with Regard to Commercial Operations in the 3550-3650 MHz Band", FCC, April 17 2015, https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-47A1.pdf
- [2] WINNF-15-P-0062 V0.3.6, "SAS to CBSD Protocol Technical Report-B," March 2016, <http://groups.winnforum.org/p/do/si/topic=801>
- [3] PAL Channel Assignment Appendix in FW's application
- [4] FCC Report and Order 16-55: "Order on Reconsideration and second Report and Order, , Amendment of the Commission's Rules with Regard to Commercial Operations in the 3550-3650 MHz Band", FCC, May 2 2016, <https://www.fcc.gov/document/35-ghz-order-recon-and-2nd-ro>

APPENDIX 14: CERTIFIED PROFESSIONAL INSTALLERS

I. Overview

To identify the location of indoor devices and to provide an additional layer of accountability and flexibility for higher power devices, professional installers are expected to be a critical component of the Citizens Broadband Radio Service (“CBRS”) ecosystem. However, adding professional installers to the ecosystem also introduces a number of issues including the following:

- Possibility of human error on data entry
- Inconsistency in the process the certified professional installers (“CPIs”) follow
- The opportunity for unauthorized users posing as CPIs to input data
- The opportunity for installers, once certified, to subsequently repeatedly provide erroneous information

This document discusses how the Federated Wireless Spectrum Access System (“SAS”) plans to work with CPIs to provide this valuable service to the CBRS ecosystem while minimizing the risks of introducing database errors and describes the following activities in more detail:

- Professional Installer Certification Program
- CPI pre-registration
- Handling CPIs during Registration
- Minimizing the Introduction of and Impact of Errors to the SAS via CPIs

II. Professional Installer Certification Program

The Wireless Innovation Forum (“WINNF”) is in the process of defining requirements for a Professional Installer Certification Program. Federated Wireless supports this effort. This CPI program will offer the following benefits:

- Trains all installers to follow a common set of processes and procedures, thereby ensuring the acceptability of installers across the ecosystem.
- Provides a mechanism by which the identity of installers can be authenticated during CBRS Device (“CBSD”) registration or during CBSD data modification subsequent to initial registration.
- Provides information needed for SAS Administrators to contact installers when corrective actions are required.
- Provides a means for the community to effectively audit the performance of installers by associating specific installations with specific installers, which can then be used as a basis for revoking or suspending an individual’s authorization to act as a CPI.

While the CPI program is open to all and the WINNF is expected to permit any entity to manage a CPI certification process, subject to satisfying the WINNF requirements, the Federated Wireless SAS will only accept manual installations from active CPIs certified by one of the WINNF-approved certification authorities.

As described in Appendix 13: Registration, each CPI is issued a unique, secure credential that allows the Federated Wireless SAS to authenticate the identity of the CPI and verify that the CPIs



certification is active with CPI certifications maintained in a Professional Installer certifying body database. This significantly reduces the opportunity for malicious data entry into the Federated Wireless SAS from unauthorized users¹³ and ensures consistency in the process by which CBSD parameters are determined by CPIs and entered into the Federated Wireless SAS.

III. Handling CPIs during Registration

For CBSDs that are installed by a CPI, the CPI is required to be pre-registered with a Professional Installer certifying body database which the SAS must be able to access. This pre-registration of CPIs allows the Federated Wireless SAS to authenticate the identity of the installer reported during registration and provides a means for the SAS to contact the installer if the SAS if needed post-registration. The CPI pre-registration happens after the identity and credentials of the CPI are verified by the SAS. CPI information could be provided to the SAS Administrator through a secure mechanism provided by the SAS Administrator, or could be embedded in the CPI certificate.

When the CPI is installing the CBSD (Category A or B), the CPI is required to provide additional information about the CBSD. The information may be entered into the CBSD (to be relayed to the SAS) or entered by a CPI via a mechanism provided by the SAS Administrator. The information provided by the CPI is site-specific. If a CPI accesses the CBSD to provide additional information, then s/he must provide to the CBSD their associated CPI Registration ID. It is important to note that Federated Wireless considers any post-manufacturing data entry into the CBSDs by CPIs a potential security risk unless the communication and interface between the CBSD and the CPI follows a tight logical and physical security. One such example is when the CBSDs are under the control of a Mobile Network Operator ("MNO") management system, and are behind a Domain Proxy ("DP"). Therefore, Federated Wireless prefers that the CPI directly provide the information to the SAS Administrator. However, when the interface between the CBSDs and the CPI is secure, Federated Wireless will accept the information from the CBSD. One such example is when the CBSDs are under tight and secure control of the MNOs, and the CPI can communicate with the MNO management system (Element Management System and Network Management System) and DP.

Following an initial step wherein automated registration information may be communicated to the SAS, the WINNF SAS-CBSD protocol¹⁴ specifies that the CPI will complete registration with the SAS via a mechanism provided by the SAS Administrator. The Federated Wireless SAS supports the following means for a CPI to input information into the Federated Wireless SAS:

- Direct entry of parameters via an interface provided by the CBSD manufacturer
- A secure web interface hosted by the Federated Wireless SAS for manual entry
- Uploading to the SAS via the CPI secure web interface a Device Installation Record ("DIR"), which includes all CBSD installation parameters

Throughout the CPI registration process, the Federated Wireless SAS checks for registration errors and messages back to the CPI to indicate which fields are in error.

¹³ See, for example, <https://twitter.com/JohnnyInterfere>

¹⁴ WINNF-15-P-0062-1.0.0, "SAS to CBSD Protocol Technical Report-B", Version 1.0.0, March 2016

IV. Minimizing the Impact of Errors to the SAS via CPIs

Unfortunately, manual input of registration data is subject to errors, which can significantly impact the SAS’s spectrum management process. To address this problem, the Federated Wireless SAS has adopted a strategy of defense-in-depth by taking the following three steps.

A. Minimize the amount of information that is entered manually during registration.

By allowing equipment vendors and owners to pre-configure and store parameters in devices or in online databases, the multi-step registration process¹⁵ reduces the number of parameters that have to be manually entered. However, GPS is not generally available indoors, so there remains the possibility of at least some manual data entry required by CPIs.

B. Minimize the likelihood of an error being introduced to the system during manual registration.

To minimize errors during registration, the Federated Wireless SAS performs basic checks of the validity of parameters (e.g., a sanity check) and when found to be out-of-bounds, flags these as errors for the owner or CPI to correct. This function is broadly consistent with other validations that Part 96 requires as part of registration, e.g., section 96.43(a), which dictates that Category A devices operated outdoors with antennas exceeding 6 meters in height above average terrain (“HAAT”) should be treated as Category B devices.

While the Federated Wireless SAS validates all input parameters (e.g., disallowing very high antenna heights), we illustrate this SAS function with location. First, the Federated Wireless SAS ensures that all input locations lie within the boundaries of the United States; this will eliminate entries of locations of 0,0 (off the coast of Africa) or entries that transpose latitude and longitude (frequently in Antarctica). Second, reported locations are screened against IP address-location mappings, which is generally sufficient to ensure that a CBSD is within the correct metropolitan area. Third, [***BEGIN CONFIDENTIAL INFORMATION***]

[***END CONFIDENTIAL

INFORMATION***] In each case, a location that appears not to make sense based on these validation criteria is flagged for the owner (automated registration) or CPI (manual registration) to correct during registration.

C. Maximize the likelihood of detecting errors post-registration and minimize the time required to correct errors.

The Federated Wireless SAS will be made aware of potential errors through the validated corrections of humans (including CPIs through the CPI interface wherein data can be updated) or through automated processes in the SAS. On the latter, as part of its spectrum enforcement responsibilities, the Federated Wireless SAS will continually scan for misconfigured devices as indicated by unexpected interference or unexpected KPI numbers reported via Measurement

¹⁵ Appendix 13: CBSD Registration and Registration Verification



Reports.¹⁶ The steps the Federated Wireless SAS takes to detect and quickly resolve errors in its database, including purging obsolete data, are described further in the Error Resolution Appendix.¹⁷

¹⁶ Appendix 12: CBRS Measurement Report

¹⁷ Appendix 7: Error Resolution and Interference Reporting Policy



APPENDIX 15: SECURITY POLICIES AND PROCEDURES

[*BEGIN CONFIDENTIAL INFORMATION***]**



[*END CONFIDENTIAL INFORMATION***]**



APPENDIX 16: ENVIRONMENTAL SENSING CAPABILITY

[*BEGIN CONFIDENTIAL INFORMATION***]**

[***END CONFIDENTIAL INFORMATION***]

APPENDIX 17: TERMS OF SERVICE

Draft**
Terms of Use
Subject To Change

** This draft of the Terms of Use complies with the requirements of the FCC Citizens Broadband Radio Service, 47 C.F.R. Part 96 (2015), specifically § 96.55(e) that:

"The SAS shall process and retain acknowledgements by all entities registering CBSDs that they understand the risk of possible interference from federal Incumbent User radar operations in the band."

While some of the provisions of these terms may change from time to time, Federated Wireless hereby represents that these terms shall always comply with 47 C.F.R. Part 96, including § 96.55(e), as well as any applicable laws or regulations.



SPECTRUM ACCESS SYSTEM ("SAS")

TERMS OF USE

Last modified: April 7, 2016

By using the Services you acknowledge that you understand the risk of possible interference from federal Incumbent User radar operations in the band.

Federated Wireless, Inc. ("**Federated**") with corporate offices at 4301 N Fairfax Drive, Suite 310, Arlington, VA 22203 has developed a revolutionary dynamic three-tiered Spectrum Access System (SAS), which enables carriers and other industry participants to cost-effectively unlock the tremendous value of licensed shared spectrum and enable the opportunity to add infrastructure for in-building broadband systems (the "**Services**"). Federated's ability to provide the Services is conditioned on receiving authority to operate the Services ("**Operating License**") from the Federal Communications Commission ("**FCC**"). If the Operating License is not granted, suspended or terminated for any reason, Federated shall have no obligations under these Terms to provide access to the Services. Whether capitalized or not, "**you**" and "**your**" means and refers to the person(s) or legal entity (whether the company, organization, educational institution, or governmental agency, instrumentality, or department) that has accepted these Terms under its own account and that is using the Services or otherwise exercising rights under these Terms. "**Your Application**" means one or more software programs developed by you that interfaces and/or accesses the Services including bug fixes, updates, upgrades, modifications, enhancements, supplements to, revisions, new releases and new versions of such software programs.

- 1. Agreement to Terms.** By using the Services, you are agreeing to these Terms of Use ("**Terms**"). In addition to these Terms, Federated provides certain technical guidelines ("**Guidelines**") that provide operational instructions on your use of the Services. The Guidelines are hereby incorporated into these Terms by this reference. If you are not authorized to accept these Terms, do not use the Services. If you do not agree to these Terms (including the Guidelines), you are not authorized to use the Services. Please read these Terms and the Guidelines carefully.
- 2. License Grant.** Subject to these Terms and any other commercial or other terms between you and Federated, Federated grants you a limited, non-exclusive, non-transferable, non-sublicensable license to access and use the Services via the Internet. All rights not expressly granted to you under these Terms are reserved by Federated. There are no implied rights.
- 3. Permitted Use of the Services.** You must use the Services consistent with the Guidelines. You may not misuse the Services. Your interference with the Services or attempts to access the Services using a method other than the interface and the instructions described in the Guidelines is a violation of these Terms. You may not use the Services to obtain Citizens Broadband Radio Service Device (CBSD) registration information for competitive purposes. Federated reserves the right to suspend or stop providing you with access to the Services if you do not comply with these Terms (including the Guidelines). Federated reserves the right to investigate suspected misconduct.



4. Limitations on Use of Services. No license is given to you for any software components (including any source code) that help enable the Services (the “**Software**”). These Terms do not grant you the right to use any branding or logos used in the Services. You shall not: (i) decompile, disassemble, re-program, analyze, reverse engineer any Software components or otherwise attempt to reconstruct, identify or discover any underlying ideas, underlying user interface techniques or algorithms, or source code, or disclose any of the foregoing (except to the extent such restriction is prohibited by law); (ii) except as expressly authorized herein, sell, rent, lease, license, sublicense or in any way redistribute any access to the Services; (iii) use the Services to create a service bureau, timesharing arrangement, or application service provider for the purpose of providing services similar to the Services; (iv) disclose the results of any benchmark or evaluation of the Services to any third party (whether or not obtained with Federated’s assistance) without Federated’s prior express written consent; (v) modify, adapt, translate or prepare derivative works of the Services; (vi) write or develop any other software program that is derived from the Services that is competitive with the Services; (vii) remove, obscure or alter Federated’s product identification, copyright notices, trademarks or other proprietary rights notices affixed to or contained within the Services; (viii) incorporate, link, or distribute the Services with any code or software licensed under the GNU General Public License (“GPL”), Lesser General Public License (“LGPL”), Mozilla, or any other open source license, in any manner that could cause or could be interpreted or asserted to cause the Services (or any modifications thereto) to become subject to the terms of the GPL, LGPL, Mozilla or such other open source license; or (ix) permit the Services to be used, examined, reviewed or inspected by others.

5. Regulatory Compliance.

5.1 By Federated. In providing the Services, Federated complies with FCC Citizens Broadband Radio Service, 47 C.F.R. Part 96 (2015) as well as the laws, regulations and policies of any other applicable regulatory bodies.

5.2 By You. You will fulfill any applicable regulatory requirements, including full compliance with all applicable laws, regulations, and policies related to your use of the Service and the manufacturing, marketing, sale and distribution of Your Application, and in particular the requirements of the FCC, including but not limited to FCC Citizens Broadband Radio Service, 47 C.F.R. Part 96 (2015), as well as the laws, regulations and policies of any other applicable regulatory bodies. You agree that you will not seek any regulatory marketing permissions or make any determinations that may result in the Services being deemed regulated or that may impose any obligations or limitations on Federated. By accepting these Terms and using the Services, you represent and warrant that you are in full compliance with any applicable laws, regulations, and policies, including but not limited to all FCC laws, regulations and policies, related to the manufacturing, marketing, sale and distribution of Your Application in the United States. You also represent and warrant that you will market Your Application only for its cleared or approved intended use/indication for use, and only in strict compliance with applicable regulatory requirements. If requested by the FCC or by another government body that has a need to review or test Your Application as part of its regulatory review process, you will provide Your Application to such entity for review purposes. You agree to promptly notify Federated of any complaints or threats of complaints regarding Your Application in relation to any such regulatory requirements, in which case Federated, solely in its discretion, suspend or terminate your access to the Services.



6. **Cooperation with Law Enforcement.** You understand that Federated may be required by law enforcement agencies to disclose information regarding your use of the Services and that Federated will comply with such requests.
7. **Ownership of Services.** You acknowledge and agree that the Services are owned by, and shall remain the sole property of Federated, that the Services contain, embody and are based upon worldwide patented or patentable inventions, trade secrets, copyrights and other intellectual property rights (collectively, “**Intellectual Property Rights**”) owned or licensed by Federated, and that Federated shall continue to be the sole owner of all Intellectual Property Rights in and to Services worldwide including, without limitation, any derivative works of the Services. These Terms do not convey to you title or ownership of the Services.
8. **Content.** Using the Services does not give you ownership of any Intellectual Property Rights in the content that you obtain from the Services (“**Content**”).
9. **Announcements and Communications.** Federated may send you service announcements, administrative messages, and other information in connection with your use of the Services. You may opt out of some of those communications.
10. **Accounts.** You may need a Federated account (“**Account**”) in order to use some of our Services. You may create your own Account, or your Account may be assigned to you by an administrator. If you are using an Account assigned to you by an administrator, different or additional terms may apply and your administrator may be able to access or disable your Account. To protect your Account, keep your password confidential. You are responsible for the activity that happens on or through your Account. Try not to reuse your Account password on third-party applications. If you learn of any unauthorized use of your password or Account, please contact Federated immediately.
11. **Privacy Policy.** Federated’s privacy policy for the Services is located at [\[Privacy Policy URL here\]](#) (the “**Privacy Policy**”). Please read and understand this Privacy Policy as it explains how Federated treats your personal data and protects your privacy when you use the Services. By using the Services, you agree to the Privacy Policy.
 - 11.1 Some of our Services allow you to upload, submit, store, and send content (“**Your Content**”). You retain ownership of any Intellectual Property Rights that you hold in Your Content.
 - 11.2 When you upload, submit, store, or send Your Content to or through our Services, you give Federated (and those Federated works with) a worldwide license to use, host, store, reproduce, modify, create derivative works (such as those resulting from adaptations or other changes Federated makes so that Your Content works better with the Services), communicate, publish, publicly perform, publicly display and distribute Your Content. The rights you grant in this license are for the limited purpose of operating, promoting, and improving our Services, and to develop new ones. This license continues even if you stop using the Services. Some Services may offer you ways to access and remove Your Content that has been provided to that Service. Make sure you have the necessary rights to grant Federated this license for any of Your Content that you submit to our Services.
 - 11.3 If you submit feedback or suggestions about our Services, Federated may use your feedback or suggestions without obligation to you.



- 12. Modifying and Terminating the Services.** Federated is constantly changing and improving the Services. Federated may add or remove functionalities or features, and Federated may suspend or stop a Service altogether. Federated may also create new limits to our Services at any time.
- 13. Modification of Terms.** Federated may modify these Terms including the Guidelines for many reasons including changes to the law or changes to the Services. You should look at the Terms regularly. Federated will post notice of modifications to these Terms on this page. Changes will not apply retroactively and will become effective no sooner than fourteen days after they are posted. However, changes addressing new functions for a Service or changes made for legal reasons will be effective immediately. If you do not agree to the modified Terms for a Service, you should discontinue your use of that Service.
- 14. DISCLAIMER OF WARRANTIES.** Federated provides the Services using commercially reasonable levels of skill. **FEDERATED DOES NOT MAKE ANY WARRANTIES, TERMS, REPRESENTATIONS OR STATEMENTS WHATSOEVER WHETHER EXPRESSED OR IMPLIED BY STATUTE, CUSTOM, USAGE OR OTHERWISE WITH RESPECT TO THE SERVICES, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTY OF TITLE, INTERFERENCE WITH YOUR ENJOYMENT OF THE SERVICES, OF NON-INFRINGEMENT, OF MERCHANTABILITY OR QUALITY, OF FITNESS FOR A PARTICULAR PURPOSE, OR ANY WARRANTY THAT THE PRODUCT IS ACCURATE OR COMPLETE, AND ALL SUCH WARRANTIES ARE HEREBY DISCLAIMED. THE SERVICES ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. YOU AGREE THAT NO COURSE OF DEALING OR PERFORMANCE OR USAGE OF TRADE SHALL APPLY TO THESE TERMS. YOU ACKNOWLEDGE THAT THE SERVICES MAY BE INTERRUPTED FROM TIME TO TIME AND THAT THE SERVICES MAY NOT BE ERROR-FREE. YOU ACKNOWLEDGE THAT YOU UNDERSTAND THE RISK OF POSSIBLE INTERFERENCE FROM FEDERAL INCUMBENT USER RADAR OPERATIONS IN THE BAND. YOU ACKNOWLEDGE THAT YOUR ONLY REMEDIES IN RESPECT OF ANY CLAIM WHATSOEVER THAT YOU MAY WISH TO BRING AGAINST FEDERATED ARE AS EXPRESSLY PROVIDED IN THESE TERMS.**
- 15. LIMITATION OF LIABILITIES.** WHEN PERMITTED BY LAW, FEDERATED SHALL IN NO CIRCUMSTANCES HAVE ANY LIABILITY WHATSOEVER TO YOU FOR:
- 15.1** ANY INDIRECT OR CONSEQUENTIAL LOSS OR ANY LOSS OF ACTUAL OR ANTICIPATED PROFIT, REVENUE OR GOODWILL OR LOSS OF USE OF THE SERVICES BY YOU OR FOR ANY OF YOUR LIABILITY TO ANY OTHER PARTY OF WHATEVER KIND HOWSOEVER ARISING (INCLUDING WITHOUT LIMITATION LOST PROFITS, LOSS OF BUSINESS REVENUE OR EARNINGS, LOST DATA (INCLUDING YOUR CONTENT), DAMAGES CAUSED BY DELAYS, OR A FAILURE TO REALIZE EXPECTED SAVINGS); OR
- 15.2** ANY OTHER LOSS OR DAMAGE SUFFERED BY YOU UNDER OR IN CONNECTION WITH THESE TERMS (WHETHER ARISING IN CONTRACT OR IN TORT OR OTHERWISE AND WHETHER AS A RESULT OF NEGLIGENCE OR OTHERWISE) EXCEPT TO THE EXTENT OF AN AMOUNT EQUAL TO THE AMOUNT YOU PAID FEDERATED TO USE THE SERVICES.
- 16. Indemnification.** You agree to indemnify and hold Federated, its licensors, successors, and affiliates, and, collectively, their respective partners, directors, officers, employees or agents, or anyone else who has been involved in the creation, production or delivery of the Services (collectively the "**Indemnified Parties**") harmless from and against all damages, cost, claims and liabilities (including reasonable attorney's fees) suffered or incurred by the Indemnified Parties as a consequence of any claims or proceedings made or brought against the Indemnified Parties by any person in connection with your use of the Services.

17. Termination.

- 17.1 Termination By Federated.** Federated may suspend or terminate your use of the Services with immediate effect by written notice given by Federated if (a) you commit any material breach of any Terms that (in the case of a breach capable of being remedied) shall not have been remedied within five (5) business days of a written request to remedy same; (b) Federated's Operating License is not granted, suspended or terminated for any reason; or (c) if you fail to provide payment to Federated for your use of the Services in breach of your commercial agreement with Federated.
- 17.2 Termination By You.** You may terminate your use of the Services with immediate effect by providing written notice to Federated provided that such termination is not in breach of your commercial agreement with Federated.
- 17.3 Rights and Obligations at Termination.** Upon expiration or termination of these Terms for any reason:
- a) The rights and licenses granted to you pursuant to these Terms, including but not limited to your access to the Services, shall cease.
 - b) Termination or expiration of this Agreement shall not release either party from:
 - 1) any liability which has already accrued to the other party hereto at the time of termination or expiration;
 - 2) any liability which thereafter may accrue with respect to any act or omission prior to termination or expiration; or
 - 3) any obligation which is expressly stated herein to survive termination or expiration.

Miscellaneous Provisions. A failure or delay to enforce any of these Terms shall in no way be construed to be a waiver of such Terms. In the event that any provision of these Terms shall be held to be invalid, the remaining provisions of these Terms shall be unimpaired. Where the context of any provision indicates an intent that it shall survive the termination of these Terms, then it shall so survive. There are no intended third party beneficiaries of any provision of these Terms. These Terms constitutes the entire understanding between the parties concerning the subject matter hereof and supersede all prior discussions, agreements and representations, whether oral or written and whether or not executed by the parties. All notices to Federated required hereunder shall be in writing and transmitted to Federated address set forth in the first paragraph of these Terms via courier, hand delivery, or registered mail. Notices shall be effective upon the date of confirmed delivery. The headings in these Terms are for convenience only and are in no way intended to describe, interpret, define, or limit the scope, extent, or intent of these Terms or any of its provisions. All personal pronouns used in these Terms, whether used in the masculine, feminine or neuter gender, shall include all other genders, the singular shall include the plural, and vice versa, as the context may require. These Terms shall be governed by the applicable federal laws and regulations of United States of America as well as the state laws of the Commonwealth of Virginia without regard to its conflict of laws provisions and you irrevocably agree to submit to the jurisdiction of the state courts located in Arlington, Virginia, or in the federal courts located in the Eastern District of Virginia.

APPENDIX 18: PRIVACY POLICY

Draft**
Privacy Policy
Subject To Change

** This draft of the Privacy Policy complies with the requirements of the FCC Citizens Broadband Radio Service, 47 C.F.R. § 96 (2015).

While some of the provisions of this policy may change from time to time, Federated Wireless hereby represents that these terms shall always comply with 47 C.F.R. Part 96



PRIVACY POLICY

Last modified: April 12, 2016

Federated Wireless, Inc. ("**Federated**", "**we**", "**our**" or "**us**") with corporate offices at 4301 N Fairfax Drive, Suite 310, Arlington, VA 22203 has developed CINC XP, a cloud-based application platform enabling next generation networks on shared spectrum (the "**Services**"). Whether capitalized or not, "**you**" and "**your**" means and refers to the person(s) or legal entity (whether the company, organization, educational institution, or governmental agency, instrumentality, or department) that has agreed to by using the Services accepts the terms of this privacy policy ("**Privacy Policy**").

Federated is committed to protecting and respecting your privacy. This Privacy Policy sets out how we process and retain your information provided to us as part of your use of the Services as well as other information generated or acquired by Federated and the Services. The content of this Privacy Policy is applicable to your use of the Services. We strongly recommend that you read this Privacy Policy carefully to understand our practices regarding your data.

The Services

The Services are built on Federated's dynamic three-tiered Spectrum Access System (SAS) and Environmental Sensor Capability (ESC). The Services support the Federal Communication Commission's (FCC) Report and Order (R&O) on commercial operations in the 3.5 GHz shared spectrum band to provide a true balance between the low cost and versatility of unlicensed spectrum and the quality and predictability of licensed spectrum.

Beyond the basic allocation and management of shared spectrum across the federal incumbent, priority access, and general authorized access tiers as defined by the FCC's R&O, the Services extend the standards even further to provide a range of enhanced shared spectrum, enabling Original Equipment Manufacturers (OEM) with the tools needed to operate wireless equipment on shared spectrum. Equipment manufacturers interface with the Services through a set of RESTful APIs to enable their equipment to access spectrum services which can then be used by Channel Partners and System Integrators to provide services to enterprises across industry verticals such as education, healthcare, retail, hospitality, etc., and even mobile network operators and service providers as a complimentary connectivity solution to the ever congested Wi-Fi through licensed shared spectrum. The Services include:

- APIs supporting SAS to Citizens Broadband Radio Service Devices (CBSD), SAS to Domain Proxy interfaces for spectrum allocation and management;
- Enhanced SAS services including spectrum optimization through multi-vendor coordination, enhanced interference management, active Priority Access License (PAL) & General Authorized Access (GAA) management, additional security & privacy services; and
- Web-based user interface showing a global view of the shared spectrum environment including spectrum availability, network planning through nationwide indoor/outdoor propagation modeling for 3.5 GHz, spectrum analytics including availability, and usage.



Our Commitment to Privacy

We take the responsibility of managing data and your trust in us very seriously. The physical security of our servers, networks, and equipment is equally as important as data security. We will not reduce your rights under this Privacy Policy without your explicit consent. We will post any Privacy Policy changes to our website, on the Cinq product homepage, located at [URL TBD]. We want our Privacy Policy to accurately describe what we can and cannot do with your data.

Types of Users Who Access the Services

The Services may be accessed and used by a number of different types of users. Each user type is defined by the role they play within the SAS ecosystem. The type of information that may be accessed by each type of user varies depending upon their role. The access rights for each user type is described in more detail below, in the Section titled The Way We Use Information. The types of users who may access the Services are:

- General Public Users -- any member of the public who creates an account on the Services ("**General Public Users**").
- FCC Employees -- FCC employees may register to use the Services. Once registered, Federated will verify the identity of the FCC employee. An FCC employee will not be permitted to use the Service until his/her identity as an FCC employee has been validated ("**FCC Users**").
- CBSD Owners ("**CBSD Owners**").
- Certified Professional Installers – these individuals will work on behalf of and manage accounts for CBSD Owners who have authorized them to work on their behalf ("**CPI**").
- Non-federal Incumbent Users (*e.g.*, Satellite Users (FSS) and Grandfathered Users (GWBL)) ("**non-federal Incumbent Users**").

In addition to the users of the Services set forth above, Federated is required under FCC regulations to share certain information with other SAS providers ("**SAS Administrators**") although other SAS Administrators are not users of the Services.

Information We Do Collect

This notice applies to all information collected by the Services (the "**Collected Information**"). For purposes of this Privacy Policy, all the information described in this section is considered Collected Information. Some of this information is requested by the Services during your installation and configuration process. Other information may be created during your use of the Services.

The Services comply with the requirements imposed on SAS providers under 47 C.F.R. Part 96 and as set forth in § 96.55 (Information gathering and retention), including but not limited to requirements that the Services collect the following information.

- The Services maintain current information on registered CBSDs such as their geographic locations and configuration of protected Fixed Satellite Service (FSS) locations (*see* § 96.55(a));
- The Services collect certain information from the CBSD upon its registration including its geographic location, antenna height above ground level (in meters), CBSD class (Category



A/Category B), requested authorization status (Priority Access or General Authorized Access), FCC identification number, call sign, user contact information, air interface technology, unique manufacturer’s serial number, sensing capabilities (if supported), and additional information on its deployment profile (see § 96.55(a)(1) and § 96.39(c)).

- For Category B CBSDs, the Service collects additional registration information such as antenna gain, beamwidth, azimuth, downtilt angle, and antenna height above ground level. (see § 96.45(d)).
- The Services store SAS transaction records including channel assignments by the Services to CBSDs and protection of non-federal Incumbent Users.
- For federal Incumbent User transactions, the Services only retain records received from the ESC based on the established ESC information retention policies.

The Services collect certain contact information and identifying information on each user who accesses the Services.

Federated’s system administrators have access to the Collected Information although it is against Federated’s policy for Federated system administrators to access this information unless they are required to do so as a part of supporting the Services.

In addition, we may collect other personal information from you when communicating with you as part of a technical support call or email conversation. Information may be requested verbally over the phone or in an email conversation.

Information We DO NOT Collect

The Services do 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 the Services. The Services do not store, retain, transmit, or disclose network operational information of users of the Services unless required to perform the Services or to comply with the information retention requirements of the FCC’s regulations. The Services do not collect any credit card information.

The Way We Use Information

Federated uses the Collected Information strictly in accordance with FCC regulations and strictly for the limited purposes of operating the Services. While Federated is required to make some of the Collected Information (excluding information collected from federal Incumbent Users) available to General Public Users, Federated is required to obfuscate the identities of those providing the Collected Information (see 47 C.F.R. § 96.55(a)(3)). Federated is required by FCC regulations to maintain certain Collected Information (excluding information collected from federal Incumbent Users) for at least sixty (60) months (see § 96.55(b)).

Table 1 *Accessing Data* below lists each type of user of the Service and describes how all the user types may access their data, and the type of data that each user group may access.

Table 1: Accessing Data

Type of User	Who May Access Their Data and How
General Public Users	No other types of users may access information on General Public Users.



	<p>General Public User information is not shared with other SAS Administrators.</p> <p>While Federated maintains contact information on each General Public User, Federated does not share this information with any third party and Federated does not use this information to contact General Public Users to send them marketing or other information on other Federated products or services.</p> <p>Federated may contact a General Public User related to supporting the Services.</p>
<p>CBSD Owners</p>	<p>CBSD and CBSD Owner information (except for identifying and contact information) is available for access from within the Services by General Public Users, other CBSD Owners, CPIs, and non-federal Incumbent Users. FCC Users may access all information about CBSDs and CBSD Owners including identifying and contact information. CBSD and CBSD Owner information is shared with other SAS Administrators except identifying and contact information. A CPI who manages an account for a CBSD Owner may access all such information including identifying and contact information.</p> <p>While Federated maintains contact information on each CBSD Owner, Federated does not share this information with any third party. Unless the CBSD Owner specifically “opts-out”, Federated may use this information to contact CBSD Owners to send them marketing or other information on other Federated products or services. CBSD Owners may opt-out during registration or by accessing their account profile information.</p> <p>Federated may contact CBSD Owners related to supporting the Services.</p>
<p>Certified Professional Installers (CPIs)</p>	<p>CPI account information is not accessible by General Public Users. CPI account information (except for identifying and contact information) is accessible by CBSD Owners, other CPIs, and non-federal Incumbent Users. FCC Users may access all information about CPIs including identifying and contact information. CPI information is not shared with other SAS Administrators.</p> <p>While Federated maintains contact information on each CPI, Federated does not share this information with any third party. Unless the CPI specifically “opts-out”, Federated may use this information to contact CPIs to send them marketing or other information on other Federated products or services. CPIs may opt-out during registration or by accessing their account profile information.</p> <p>Federated may contact CPIs related to supporting the Services.</p>



<p>Non-Federal Incumbent Users</p>	<p>Non-federal Incumbent User information is not accessible by General Public Users, CBSD Owners, CPIs, and other non-federal Incumbent Users. FCC Users may access all information about non-federal Incumbent Users including identifying and contact information. Non-federal Incumbent User information is not shared with other SAS Administrators.</p> <p>While Federated maintains contact information on each non-federal Incumbent User, Federated does not share this information with any third party and Federated does not use this information to contact non-federal Incumbent User to send them marketing or other information on other Federated products or services.</p> <p>Federated may contact a non-federal Incumbent User related to supporting the Services.</p>
<p>FCC Users</p>	<p>No types of users may access information on FCC Users, including other FCC Users. FCC User information is not shared with other SAS Administrators.</p> <p>While Federated maintains contact information on each FCC User, Federated does not share this information with any third party and Federated does not use this information to contact FCC Users to send them marketing or other information on other Federated products or services.</p> <p>Federated may contact a FCC User related to supporting the Services.</p>

We will ONLY disclose Collected Information maintained or generated by the Services to a regulatory body or law enforcement agency, and then only in circumstances where required by law or regulation or where a legitimate court order has been obtained from a court of competent jurisdiction.

We use non-identifying and aggregate information for internal purposes only to better design Federated products and services but we do not retain any identifying information as part of the aggregate information.

We do not share Collected Information with any outside parties except as provided in this section.

How Is Data Entered Into the Services and How Is It Corrected

Since the Service depends on the accuracy of the data stored in its database, Federated is keenly interested in quickly resolving any errors in the various databases that support our Services, including our SAS database. This section describes the processes and procedures Federated has established to rapidly remediate data inaccuracies upon identification.



Table 2 *Inputting and Updating Your Data* below lists each type of user of the Service and describes how all the user types may correct their account data. The table also describes how SAS transaction data may be corrected

Table 2: *Inputting and Updating Your Data*

Type of User	How Is Data Entered Into the Services and How Is It Corrected
General Public Users	Each General Public User’s account data is initially entered into the Services by self-populating their profile information via the Services’ configuration tool. Corrections to the account data may also be made directly by the General Public User using the same configuration tool.
CBSD Owners	<p>CBSD Owners’ account data is initially entered into the Service by self-populating their profile information via the Services’ configuration tool. This may be accomplished either directly by the CBSO Owner or by the CPI who is authorized by the CBSO Owner to act on its behalf. Corrections to a CBSO Owner’s account data may also be made directly by the either the CBSO Owner or by its authorized CPI using the same configuration tool.</p> <p>If a CBSO Owner or its authorized CPI identifies data issues with a CBSO device, these users can resolve the errors instantaneously by going through the process of re-registering their device.</p> <p>Any issues identified with a CBSO’s SAS transaction data needs to be corrected via the Error Resolution process described below in the Section titled, The Error Resolution Process and How to Contact Us.</p>
Certified Professional Installers (CPIs)	Each CPI’s account data is initially entered into the Service by self-populating their profile information via the Services’ configuration tool. Corrections to the CPI account data may also be made directly by the CPI using the same configuration tool. CPIs may also make changes to CBSO Owners’ account data for whom they are authorized. See the previous entry on CBSO Owners for more details.
Non-Federal Incumbent Users	<p>Non-federal Incumbent User’s account data is populated directly by Federated by using public sources for this information, including FCC databases. Non-federal Incumbent User’s account data may be changed by the non-federal Incumbent User’s authorized administrator by updating their profile information via the Services’ configuration tool.</p> <p>Any issues identified with a non-federal Incumbent User’s SAS transaction data needs to be corrected via the Error Resolution process described below in Section 0 (The Error Resolution Process and How to Contact Us).</p>
FCC Users	Each FCC User’s account data is initially entered into the Service by self-populating their profile information via the Services’ configuration tool. Corrections to the account data may also be made directly by the FCC User using the same configuration tool.



	Any issues identified by FCC Users with SAS transaction data needs to be corrected via the Error Resolution process described below in Section 0 (The Error Resolution Process and How to Contact Us).
--	--

Our Commitment to Data Security

To prevent unauthorized access, maintain data accuracy, and ensure the correct use of information, we have put in place appropriate physical, electronic, and managerial procedures to safeguard and secure the Collected Information as part of the Services.

The Error Resolution Process and How to Contact Us

Any issues identified with SAS transaction data needs to be corrected via Federated’s Error Resolution process, which is partially described here.

If the data issue is identified by the FCC or third parties that have access to view some or all of the SAS database, these users can notify Federated through an Error Report form located within the Services. Federated will verify the claims by checking against the source of the data and update the SAS database as needed to resolve the identified errors. This error resolution will be complete within 12 hours of notification of the issue and the notifying party will be updated via email of the resolution status.

If a CBSD Owner or Certified Professional Installer (CPI) identifies data issues with their own data, these users can resolve the errors instantaneously by going through the process of re-registering their device. Such users can also always file an Error Report form located within the Services to request error resolutions.

If you feel your privacy has been violated by your use of the Services, you may register your complaint with us and we will respond to your requests. To do so, please contact us as shown on our website at <http://www.federatedwireless.com/contact>.

Please contact us if you have any questions and comments regarding this Privacy Policy.



APPENDIX 19: PROPAGATION MODEL IMPLEMENTATION

[*BEGIN CONFIDENTIAL INFORMATION***]**

[***END CONFIDENTIAL INFORMATION***]