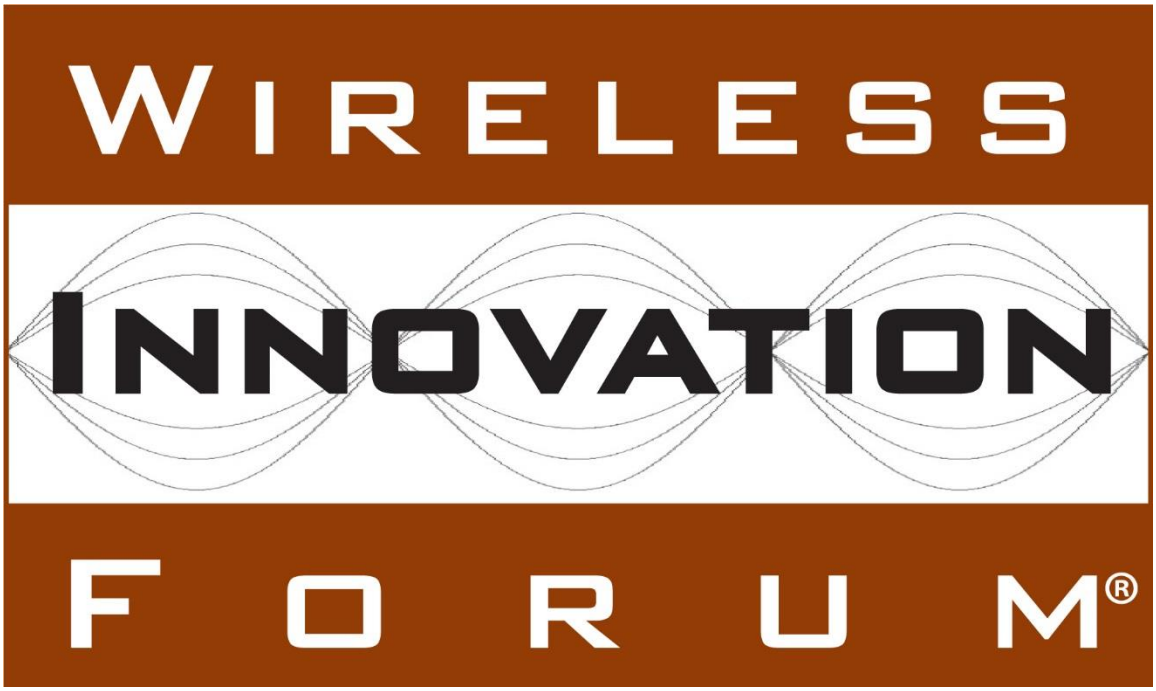

CBRS Operational Security

Document WINNF-15-S-0071

Version V1.0.0
21 June 2016

TERMS, CONDITIONS & NOTICES

This document has been prepared by the Spectrum Sharing Committee to assist The Software Defined Radio Forum Inc. (or its successors or assigns, hereafter "the Forum"). It may be amended or withdrawn at a later time and it is not binding on any member of the Forum or of the Spectrum Sharing Committee.

Contributors to this document that have submitted copyrighted materials (the Submission) to the Forum for use in this document retain copyright ownership of their original work, while at the same time granting the Forum a non-exclusive, irrevocable, worldwide, perpetual, royalty-free license under the Submitter's copyrights in the Submission to reproduce, distribute, publish, display, perform, and create derivative works of the Submission based on that original work for the purpose of developing this document under the Forum's own copyright.

Permission is granted to the Forum's participants to copy any portion of this document for legitimate purposes of the Forum. Copying for monetary gain or for other non-Forum related purposes is prohibited.

THIS DOCUMENT IS BEING OFFERED WITHOUT ANY WARRANTY WHATSOEVER, AND IN PARTICULAR, ANY WARRANTY OF NON-INFRINGEMENT IS EXPRESSLY DISCLAIMED. ANY USE OF THIS SPECIFICATION SHALL BE MADE ENTIRELY AT THE IMPLEMENTER'S OWN RISK, AND NEITHER THE FORUM, NOR ANY OF ITS MEMBERS OR SUBMITTERS, SHALL HAVE ANY LIABILITY WHATSOEVER TO ANY IMPLEMENTER OR THIRD PARTY FOR ANY DAMAGES OF ANY NATURE WHATSOEVER, DIRECTLY OR INDIRECTLY, ARISING FROM THE USE OF THIS DOCUMENT.

Recipients of this document are requested to submit, with their comments, notification of any relevant patent claims or other intellectual property rights of which they may be aware that might be infringed by any implementation of the specification set forth in this document, and to provide supporting documentation.

This document was developed following the Forum's policy on restricted or controlled information (Policy 009) to ensure that that the document can be shared openly with other member organizations around the world. Additional Information on this policy can be found here: http://www.wirelessinnovation.org/page/Policies_and_Procedures

Although this document contains no restricted or controlled information, the specific implementation of concepts contain herein may be controlled under the laws of the country of origin for that implementation. Readers are encouraged, therefore, to consult with a cognizant authority prior to any further development.

Wireless Innovation Forum ™ and SDR Forum ™ are trademarks of the Software Defined Radio Forum Inc.

Table of Contents

List of Figures

CBRS Operational Security

1 Introduction

The overall security concept for the 3550-3700 MHz Citizens Broadband Radio Service (CBRS) includes operational security of the Citizens Broadband Service Devices (CBSDs), Spectrum Access Systems (SASs) and Environmental Sensing Capabilities (ESCs). Operations security (OPSEC) is a military discipline that enables mission success by preventing inadvertent compromise of sensitive or classified activities, capabilities, or intentions at the tactical, operational and strategic levels. This is distinct from the operational security of the CBRS, which encompasses a wider range of security disciplines, including cybersecurity. Cybersecurity includes protection of data in transit and at rest from attack through communications security, physical security, personnel security, and supply chain risk management.

This document addresses both requirements to preserve incumbent operations security as required by the Federal Communications Commission (FCC) for operation in the 3550-3700 MHz CBRS band and operational security of the CBRS with the exception of CBRS Communications Security (COMSEC) addressed in WINNF-15-S-0065 and the cybersecurity threat model for the overall ESC/SAS described in WINNF-15-P-0089.

2 Regulatory Requirements

The FCC Part 96 rules address OPSEC risk mitigation in three sections:

> 96.55 – Information Gathering and Retention – (c) The SAS shall only retain records of information or instructions received regarding federal Incumbent User transmissions from the ESC in accordance with information retention policies established as part of the ESC approval process.
>
> 96.63 – Spectrum Access System Administrators – (n)(2) Ensure that the SAS does not store, retain, transmit, or disclose operational information on the movement or position of any federal system or any information that reveals other operational information of any federal system that is not required by this part to effectively operate the SAS.
>
> 96.67 - Environmental Sensing Capability – (c)(7) Ensure that the ESC … does not store, retain, transmit, or disclose operational information on the movement or position of any federal system or any information that reveals other operational information of any federal system that is not required by this part to effectively operate the ESC.

This document does not address CBRS COMSEC issues. These are addressed in WINNF-15-S-0065.

3 Threat Model

The security threat model for the overall ESC/SAS is described in WINNF-15-P-0089.

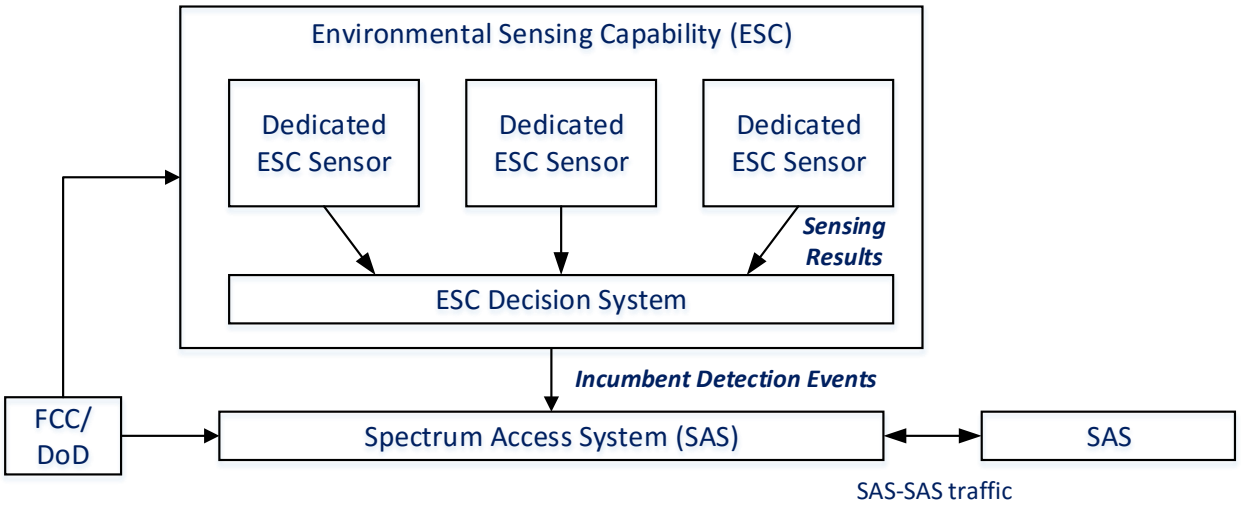

Figure 1 Overall architecture for the ESC, with sensors sending data to the SAS

The threat model under consideration for CBRS OPSEC is where an Internet-connected device is able to probe the Spectrum Access Server (SAS) ecosystem through spectrum access queries and as a result learn information about military operations at a higher level of fidelity than can be reliably discovered from other Internet-connected sources such as news reports about naval activity.

We make the following minimum assumptions about the adversaries' capabilities:

- adversary can enroll into the General Authorized Access (GAA) tier of SAS service and as a result has the necessary credentials to make spectrum authorization requests from one or more SAS providers;
- adversary has the ability to make requests from multiple source IP addresses using multiple GAA credentials, for example leveraging a BotNet;
- adversary has sufficient computational resources to make probabilistic inferences about incumbent activity based on received authorizations; and
- adversary can perform a denial of service (DoS) or distributed DoS (DDoS) against Internet-connected SAS interfaces.

4 Operational Security Requirements

The following are the OPSEC properties proposed within the scope of the threat model and regulatory requirements.

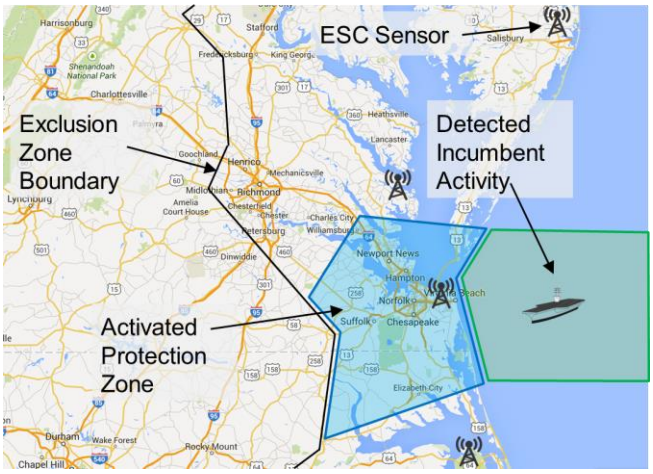

Figure 2 Relationship between incumbent detection, protection zone, and NTIA-defined exclusion zone

4.1 Environmental Sensing Capability Requirements

The ESC is responsible for detecting incumbents, and is envisioned as a network of dedicated listening devices deployed within the FCC exclusion zones. Figure 1 shows the overall components of the ESC architecture. At present the Wireless Innovation Forum does not intend to standardize a protocol between the SAS and ESC, and as a result this document serves to put requirements around the implementation of an ESC such that it meets the FCC and Department of Defense (DoD) requirements for incumbent detection and protection of incumbent privacy.

The overall concept of operations is show in Figure 2. The ESC detects an incumbent and within a subset of the FCC-defined exclusion zone SASs shall reduce the aggregate interference.

Sensors may be configured to directly send incumbent detection events to the SAS or to a component which contains detection logic that supports functions such as sensor redundancy and management.

********** Proposed New Text **********

R2-ESC-[SENSOR CONSTRAINTS]

The ESC shall meet the following requirements:

1. Sensors shall not store or transmit any time-series data for detected incumbent signals.

2. Sensors shall not store or transmit any incumbent radar signal characteristics other than the minimum required for incumbent radar activity determination.

3. Sensors shall not convey timing information whose accuracy and precision is sufficient to enable geolocation techniques.

4. Sensors shall only report quantized received signal strength indication (RSSI) measurements.

5. Sensors shall not employ highly directional antennas for purposes of precision angle of arrival (AoA) estimation

****

The intent of these requirements is to prevent the ESC from performing any form of precision geolocation. Without phase coherency and highly directional antennas and leveraging only quantized RSSI measurements, the ESC will be unable to use techniques such as AoA and TDoA to geolocate incumbent activity.

4.1.1 ESC Position Estimate Uncertainty

It is required, for OPSEC purposes, that ESCs and SASs not reveal any information pertaining to the movement or position of any federal system. Thus, ESC operators and SAS Administrators interfacing with one or more ESCs must ensure at all points in their design that the location of incumbent activity cannot be accurately estimated or tracked. This relates to the direct calculation of position estimates as well as the availability of intermediate variables that, if combined, could be used to form a position estimate.

Given proposed ESC design constraints (e.g., R2-ESC-[SENSOR CONSTRAINTS]) and performance requirements (e.g., R2-ESC-[DETECTION THRESHOLD] and R2-ESC-[FIGURES-OF_MERIT]), initial analysis of candidate ESC designs suggests a likely position estimate uncertainty of roughly 65 nautical miles.

********** Proposed New Text **********

R2-ESC-[ESC POSITION ESTIMATE UNCERTAINTY]

During the certification process, ESC operators and SAS Administrators interfacing with one or more ESCs shall quantify the incumbent activity position estimate uncertainty in their designs. This relates to the direct calculation of position estimates as well as the availability of intermediate variables that, if combined, could be used to form a position estimate.

****

4.1.2 Supply Chain Considerations

ESC operators need to realize that their ESC design supply chain (e.g., parts, system integration) may introduce cyber security risks. Hence, ESC operators need to have a strategy to minimize supply chain risk while allowing review of their ESC design methodology.

********** Proposed New Text **********

R2-ESC-[SUPPLY CHAIN]

During the certification process, ESC operators shall describe how they manage and allow review of cyber security risks in their ESC design supply chain.

4.1.3 Limited Reconfigurability

ESC operators need to realize that an adversary may intrude and tamper with fielded ESC sensors or ESC Decision Systems in an attempt to prevent ESC from satisfying OPSEC requirements, obstruct ESCs ability to protect 3.55-3.7 GHz federal Incumbent Users from harmful interference, and/or to repurpose the sensor to detect federal Incumbent Users outside 3.55-3.7 GHz. Hence, ESC operators need to have a strategy to limit reconfigurability of their deployed ESC solutions, restrict tampering of the software and hardware, and limit remote access vulnerability. ESC operators also need to have a strategy to detect (e.g., using a host-intrusion detection system) and respond to intrusions.

R2-ESC-[RECONFIGURABILITY]

During the certification process, ESC operators shall describe how they limit reconfigurability and remote access vulnerability of their ESC designs and detect and respond to tampering anywhere in their ESC design.

****

4.2 Protection Zone Activation

When a federal Incumbent User is detected, aggregate interference shall be reduced by reassigning spectrum grants to CBSDs from a channel that would cause interference to one that would not cause interference. (R0, 96.15/96.53) Given that SAS Administrators must make anonymized spectrum grant information publicly available, SAS shall make it difficult to infer detailed information about incumbent activity from this publicly available data.

To accomplish this, the SAS shall seek to reduce the correlation between such reassignments and geographic regions. This can be accomplished through a number of ways, including:

1. reassigning all users in a pre-defined protection zone to a new channel using pre-computed interference criteria; or

2. randomly reassigning a subset of users over one or more protection zones to a new channel in sufficient number to meet real-time estimates of interference criteria.

Regardless of the approach used, the probability density of channel reassignments within any affected area shall be uniform from the coastline up to the edge of the NTIA-defined exclusion zone boundary to minimize the fidelity of any inferred information regarding incumbent activity.

********** Proposed New Text **********

R2-ESC-[PROTECTION ZONE ACTIVATION]

During the certification process, a SAS implementation shall have a documented and approved approach to preserve OPSEC concerns in its protection zone activation strategy.

****

4.3 Exclusion/Protection Zone Activation Obfuscation

As per Part 96 rules (96.15(iii)(5) and 96.15(iii)(6)) the FCC will, as necessary, add or modify Exclusion Zones or Protection Zones to protect current and future federal Incumbent Users. The FCC may also temporarily extend or modify Exclusion Zones and Protection Zones to protect temporary operations by federal Incumbent Users. Federal Incumbent Users will coordinate with the Commission prior to the beginning of any non-emergency operation requiring additional protection. Such modifications will be communicated to the SAS along with the expiration date and time of any modification.

Activation drills may be used by the FCC and/or DoD to obfuscate actual Exclusion/Protection Zone modifications.

********** Proposed New Text **********

R2-ESC-[EXCLUSION ZONE/PROTECTION ZONE ACTIVATION OBFUSCATION]

SAS providers shall enforce Exclusion/Protection Zone modifications due to FCC or DoD Activation Drills, e.g., reassign CBSD frequencies as necessary given the modified Exclusion Zones or Protection Zones.

****

For reference, it is assumed that all SASs will be given the same Exclusion/Protection Zone modifications.

4.4 Authorization Limiting

Repeated queries to the SAS ecosystem requesting spectrum authorizations may allow someone to map incumbent activity. To address this SAS providers shall implement authorization limiting techniques when assigning spectrum to users. These potentially include:

1. to the extent possible, provide the same CBSD device the same allocation to avoid repeated “catch and release” adversary tactics; and

2. do not authorize more spectrum than can be reasonably used by a CBSD device in multiple, fragmented authorization requests; and

3. impose a minimum time separation between CBSD spectrum requests from the same CBSD device but at locations separated by more than 50 meters (horizontal) and/or 3 meters (vertical)

********** Proposed New Text **********

R2-ESC-[AUTHORIZATION LIMITING]

During the certification process, a SAS implementation shall have a documented and approved authorization limiting approach.

****

Colluding CBSD devices or devices with multiple virtual identities can allow an adversary to increase the rate at which they make requests. This threat shall be principally addressed through robust enrollment and revocation procedures.

4.5 Obfuscating Incumbent Episodes

An incumbent episode is defined as the interval between when an incumbent activity first and last crosses the minimum threshold for ESC detection. OPSEC best practices can utilize temporal and spatial obfuscation of the precise time and location when the incumbent activity ends.

********** Proposed New Text **********

R2-ESC-[OBFUSCATING INCUMBENT EPISODES]

During the certification process, a SAS implementation shall have a documented and approved approach to obfuscate the reported time when an incumbent episode ends.

****

4.6 Public Release of CBSD Registration Information

As per 96.55 - Information Gathering and Retention – (a)(3) SAS Administrators shall make CBSD registration information available to the general public. This information could potentially be used by an adversary to determine operational information about a federal system.

********** Proposed New Text **********

R2-ESC-[OBFUSCATING INCUMBENT EPISODES]

For OPSEC purposes, the SAS shall not make CBSD registration information available to the public any earlier than 7 days from when the information is collected by the SAS.

****

4.7 Channel Availability Lists – Incumbent Frequency Obfuscation

SAS is permitted to provide CBSDs with a range of available frequencies, allowing the CBSDs to select and utilize a subset of these available channels. An OPSEC concern is that the SAS provided list of available channels could be used by an adversary to determine the incumbent frequency. For instance, if the SAS provided list excludes the incumbent frequency, an adversary may be able to infer information regarding the incumbent frequency.

One approach to obfuscate the incumbent frequency is for SAS, in the CBSD Spectrum Request procedure, to provide the CBSDs with a set of available frequencies that sometimes or always includes the incumbent frequency. If then the CBSD grant request includes operation on the incumbent frequency, SAS may direct that CBSD to choose a different frequency from a revised set of available channels that does not include the incumbent frequency. As per 96.39(e), "If directed by the SAS, a CBSD that receives a range of available frequencies or channels from an SAS must promptly report to the SAS which of the available channels or frequencies it will utilize." Thus, after SAS directs the CBSD to report its channel use and the chosen channels include the incumbent frequency, SAS can redirect the CSBD to a new frequency. To avoid having this frequency reassignment reveal information regarding the incumbent frequency, SAS could randomly choose to direct CSBDs to new frequencies even if the utilized frequency is not an incumbent frequency.

********** Proposed New Text **********

R2-ESC-[CHANNEL AVAILABILITY LISTS]

During the certification process, a SAS implementation shall have a documented and approved approach to obfuscate the incumbent frequency in its channel availability lists and channel reassignment mechanisms.

****