



May 16, 2016

VIA ELECTRONIC FILING

Ms. Marlene H. Dortch, Secretary
Federal Communications Commission
445 Twelfth Street, SW
Washington, DC 20554

Re: *Wireless Telecommunications Bureau and Office of Engineering and Technology
Establish Procedure and Deadline for Filing Spectrum Access System (SAS)
Administrator(s) and Environmental Sensing Capability (ESC) Operator(s)
Applications, GN Docket No. 15-319*

In response to the Public Notice from the Wireless Telecommunications Bureau ("WTB") and the Office of Engineering and Technology ("OET") in the above-captioned docket,¹ CTIA[®] hereby submits the attached proposal to develop and manage an independent Spectrum Access System ("SAS") and Environmental Sensing Capability ("ESC").

The creation of the new Citizens Broadband Radio Service ("CBRS") in the 3.5 GHz band has the potential to add much-needed capacity to meet the ever-increasing demand for wireless broadband connectivity, and SASs and ESCs will play an integral role in ensuring the success of that band. The Commission has done much work to detail the requirements necessary for the SAS, ESC, and CBRS Devices to coordinate the most efficient uses of designated frequencies. We are committed to working with the FCC and federal agencies to ensure this experiment in spectrum sharing is a success. While many details on how such operations will work remain unclear, the wireless industry stands ready to partner with the Commission to see if this novel type of spectrum sharing is viable and can benefit U.S. consumers.

As detailed throughout our proposal, CTIA is well equipped to be a SAS Administrator and an ESC Operator given its background, experience, expertise, and approach, and is committed

¹ See *Wireless Telecommunications Bureau and Office of Engineering and Technology Establish Procedure and Deadline for Filing Spectrum Access System (SAS) Administrator(s) and Environmental Sensing Capability (ESC) Operator(s) Applications*, Public Notice, 30 FCC Rcd 14170 (2015); see also *Wireless Telecommunications Bureau and Office of Engineering and Technology Extend "First Wave" Filing Deadline for Spectrum Access System (SAS) Administrator(s) and Environmental Sensing Capability (ESC) Operator(s) Proposals*, Public Notice, GN Docket No. 15-319, DA 16-397 (rel. Apr. 14, 2016).



to complying with the Commission's orders and Part 96 rules in executing these functions. We look forward to working with all stakeholders to leverage our technology leadership in the mobile data services arena to help bring about the successful roll-out of CBRS service in the 3.5 GHz band.

Respectfully submitted,

/s/ Paul Anuszkiewicz

Vice President, Spectrum Planning

Thomas C. Power
Senior Vice President, General Counsel

Thomas Sawanobori
Senior Vice President and Chief Technology Officer

Scott K. Bergmann
Vice President, Regulatory Affairs

CTIA
1400 Sixteenth Street, NW, Suite 600
Washington, DC 20036
(202) 785-0081



CTIA's Proposal to be Designated as a Spectrum Access System Administrator and an Environmental Sensing Capability Operator

Introduction

Almost exactly a year ago, the Federal Communications Commission ("FCC" or "Commission") adopted a Report and Order that created a new Citizens Broadband Radio Service ("CBRS") and rules for commercial use of 150 megahertz of spectrum in the 3550-3700 MHz band for mobile broadband use.¹ Throughout the proceeding, CTIA continually demonstrated its support for the 3.5 GHz band as a promising opportunity for deployment of innovative technologies, including small cells, to meet the explosive growth in demand for mobile broadband services. Indeed, Americans now use more than 11.1 billion megabytes of data every day and mobile data traffic is expected to grow six-fold between 2015 and 2020.² More licensed spectrum is therefore needed to meet this demand.

By opening up the 3.5 GHz band for mobile broadband use, the Commission has the potential to make available a significant source of spectrum that the U.S. wireless industry may use to continue to meet consumers' ever-growing desire for better, faster, and more ubiquitous mobile broadband services. The 3.5 GHz spectrum is well-suited for small cell deployment, which is already a \$1 billion industry that can help address ongoing capacity needs in high-traffic areas.³ These small cells are key to creating

¹ See *Amendment of the Commission's Rules with Regard to Commercial Operations in the 3550-3650 MHz Band*, Report and Order and Second Further Notice of Proposed Rulemaking, 30 FCC Rcd 3959 (2015) ("3.5 GHz Order"); see also *Amendment of the Commission's Rules with Regard to Commercial Operations in the 3550-3650 MHz Band*, Order on Reconsideration and Second Report and Order, FCC 16-55, GN Docket No. 12-354 (rel. May 2, 2016) ("3.5 GHz Reconsideration Order" and "3.5 GHz Second R&O").

² Thomas Sawanobori and Dr. Robert Roche, *Mobile Data Demand: Growth Forecasts Met: Significant Growth Projects Continue to Drive the Need for More Spectrum*, CTIA (June 22, 2015), <http://www.ctia.org/docs/default-source/default-document-library/062115mobile-data-demands-white-paper-new.pdf>; *US Mobile Data Traffic Will Grow 6-Fold from 2015 to 2020*, CTIA (Feb. 16, 2016), <http://www.ctia.org/your-wireless-life/how-wireless-works/wireless-quick-facts/us-mobile-data-traffic-will-grow-6-fold-from-2015-to-2020>.

³ Small Cell Market Worth \$1B, CTIA (Mar. 3, 2016), <http://www.ctia.org/your-wireless-life/how-wireless-works/wireless-quick-facts/small-cell-market>.



ultra-dense network configurations and can support next-generation 5G wireless technologies, delivering faster speeds, providing higher device density, enabling massive connectivity for billions of sensors, wearables, and devices, and unlocking new services and applications.⁴ The 3.5 GHz band thus has the potential to play an important role in helping the U.S. wireless industry continue its success story.

In order to facilitate a wide variety of users, business opportunities, and deployment models, the Commission adopted a three-tier framework for the 3.5 GHz band, consisting of Incumbent Access, Priority Access, and General Authorized Access (“GAA”) users.⁵ For this unprecedented spectrum access model to work, there must be careful coordination between and among frequency users within the band to prevent interference. The proper functioning of the Spectrum Access System (“SAS”) and associated Environmental Sensing Capability (“ESC”) will be crucial to ensuring the successful interaction of the three tiers of users in this band.

Administration of the SAS and operation of the ESCs must therefore be undertaken by an entity or entities with the ability to perform the functions required for such extensive coordination. As demonstrated herein, given its history and experience in addressing various spectrum, technology, cybersecurity, and public advocacy projects and initiatives over the past 15 years,⁶ CTIA is confident that it can discharge the roles and responsibilities of a Spectrum Access Administrator and ESC Operator.

⁴ Thomas K. Sawanobori, *The Next Generation of Wireless: 5G Leadership in the U.S.*, CTIA (Feb. 9, 2016), http://www.ctia.org/docs/default-source/default-document-library/5g_white-paper-web.pdf.

⁵ 3.5 GHz Order ¶¶ 4-6. As CTIA expressed previously, the Commission’s rules should provide certainty with respect to the rights of Priority Access licensees. Among other things, CTIA has encouraged the Commission to foster investment and innovation in the 3.5 GHz band by increasing license terms for PALs and including a renewal expectancy, revising the PAL auction structure, modifying technical rules, and adopting a workable definition of when PAL spectrum is in “use.” Such policies would put the 3.5 GHz band and Priority Access licensees in a stronger position to succeed. See, e.g., Letter from Brian M. Josef, Assistant Vice President, CTIA, to Marlene H. Dortch, Secretary, FCC, GN Docket No. 12-354 (dated Mar. 21, 2016); Petition for Reconsideration of CTIA, GN Docket No. 12-354 (filed July 23, 2015); Comments of CTIA, GN Docket No. 12-354 (filed July 15, 2015).

⁶ See Appendices A and B, attached hereto.



Proposal

1) **Spectrum Access System and Environmental Sensing Capability Duties and Responsibilities.**

1.1) **A detailed description of the scope of the functions that the SAS and/or ESC would perform.**

1.1.1) **Spectrum Access System Roles and Responsibilities.**

The SAS is an essential element of the CBRS system for the commercial use of the 3.5 GHz band. An illustrative end-to-end CBRS architecture⁷ is shown in Figure 1.

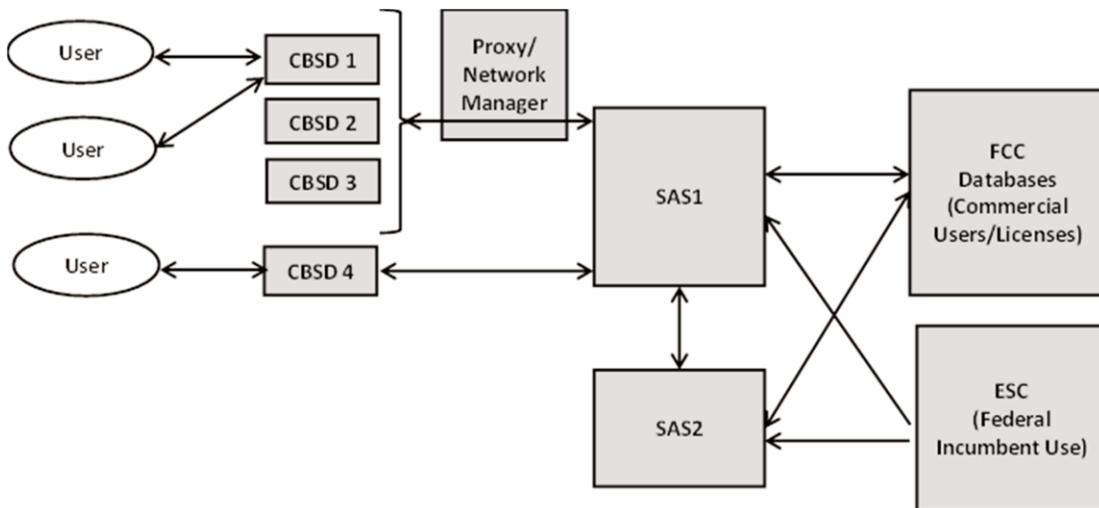


Figure 1: CBRS Architecture

The requirements of the SAS can be categorized broadly into the following categories:

- General Responsibilities;
- SAS Functional Requirements;
- SAS Monitoring and Management of Spectrum Use; and

⁷ See SAS to CBSD Protocol Technical Report-B, Document WINNF-15-P-0062, Version V1.0.0 (Mar. 30, 2016), <http://groups.winnforum.org/Reports> ("SAS-to-CBSD Technical Report").



- Issues related to the Initial Launch and Evolution of the SAS and Band Plan.

Specifically, CTIA proposes, consistent with the Commission's guidance,⁸ that as an authorized SAS Administrator, it would perform at a minimum the following core functions:

- Determine the available frequencies and maximum power limits at a given geographic location and assign them to CBRS devices ("CBSDs");
- Communicate and instruct a CBSD to cease operations as soon as technically possible, but no more than 300 seconds.
- Determine the maximum permissible radiated transmission power level for CBSDs at a given location and communicate that information to the CBSDs;
- Register and authenticate the identity and location of CBSDs;
- Enforce Exclusion and Protection Zones, including any future changes to such Zones, to ensure co-existence between CBRS users and incumbent federal operations;
- Communicate with the ESC and ensure that CBSDs operate in a manner that does not interfere with federal users;
- Ensure that CBSDs protect non-federal incumbent users consistent with the rules;
- Protect Priority Access licensees from harmful interference from other CBRS users;
- Facilitate coordination among GAA users to promote a stable spectral environment;
- Ensure secure and reliable transmission of information between the SAS, ESC, and CBSDs;
- Interface with an approved ESC with relevant and necessary sensing information reported by its own sensor network or by CBSDs if available;
- Allow protected grandfathered wireless broadband licensees to register until the end of the grandfather period;
- Facilitate among SASs the coordination and exchange of information necessary to avoid conflicting frequency assignments; and

⁸ See, e.g., 3.5 GHz Order ¶¶ 316; see also 3.5 GHz Reconsideration Order ¶¶ 64, 151.



- Abide by current and future operational international agreements established with Mexico and Canada. The terms of these agreements shall be implemented by the SAS.

1.1.2) Environmental Sensing Capability Roles and Responsibilities.

Working in conjunction with the management of CBSDs by an approved SAS, the ESC enables CBRS users to operate near the coastline on a channel or frequency not being used by federal radar systems. CTIA commits to protect the security and confidentiality of federal operations by ensuring that the ESC does not store, retain, transmit, or disclose any information on the locations or movements of any federal systems.

In addition, CTIA ensures, consistent with the Commission's guidance,⁹ that the ESC shall at a minimum:

- Accurately detect federal frequency use in the 3550-3700 MHz band and adjacent frequencies;
- Communicate information about detected frequency use to an approved SAS;
- Maintain security of detected and communicated signal information;
- Comply with all Commission rules and guidelines governing the construction, operation, and approval of ESCs;
- Be available at all times to immediately respond to requests from authorized Commission personnel for any information collected or communicated by the ESC; and
- Ensure that the ESC does not store, retain, transmit, or disclose operational information on the movement or position of any federal system or any information that reveals other operational information of any federal system.

⁹ *Wireless Telecommunications Bureau and Office of Engineering and Technology Establish Procedure and Deadline for Filing Spectrum Access System (SAS) Administrator(s) and Environmental Sensing Capability (ESC) Operator(s) Applications*, Public Notice, 30 FCC Rcd 14170, 14173-74 (2015) ("Notice").



1.1.3) Citizens Broadband Radio Service Device (CBSD) requirement.

With respect to interference protection to Incumbent Users and Priority Access Licensees, two categories of CBSDs are being defined based on their maximum conducted power – Category A and Category B CBSDs.

Category A CBSDs will be limited to a maximum EIRP of 30 dBm in 10 megahertz, and may be used for indoor or outdoor deployments.

Category B devices are authorized for outdoor deployment as small cells, as well as in configurations such as non-line-of-sight backhaul. Category B CBSDs are also authorized to operate at higher power than Category A CBSDs, providing greater flexibility and ensuring ongoing compatibility with existing 3650-3700 MHz operations. As the Commission clarified in the *3.5 GHz Reconsideration Order*, Category B devices can operate at a maximum allowable EIRP of 47 dBm/10 MHz, and the peak-to-average power ratio (“PAPR”) of any CBSD transmitter output power must not exceed 13 dB.¹⁰

CTIA's SAS will support both CBSD categories for GAA and Priority Access use, consistent with the rules adopted in the *3.5 GHz Order*, *3.5 GHz Second R&O*, and *3.5 GHz Reconsideration Order*, as applicable.

1.2) A demonstration that the prospective SAS Administrator or ESC operator possesses sufficient technical expertise to administer/operate an SAS and/or ESC, including the qualifications of key personnel who will be responsible for operating and maintaining the SAS and/or ESC.

CTIA is confident about its technical expertise to administer, manage, and operate a SAS and an ESC. CTIA personnel that will be involved in administering, operating, and managing the SAS and ESC may include, but are not limited to:

- Thomas Sawanobori, SVP and CTO
- Paul Anuskiewicz, VP Spectrum Planning

¹⁰ *3.5 GHz Reconsideration Order* ¶¶ 69, 75-77, 83. The amendment to the maximum allowable EIRP for non-rural Category B CBSDs “mak[es] the power levels allowed for both non-rural and rural deployments the same.” *Id.* ¶ 75.



- John Marinho, VP Technology & Cybersecurity
- Mark Sargent, VP Certification Programs
- Eshwar Pittampalli, Ph.D., Director Wireless Technology

Further details about CTIA's past performance and technical experience are attached as Appendix A. Biographies of the above-listed personnel are attached as Appendix B.

1.3) The prospective SAS Administrator or ESC operator must demonstrate that it is financially capable of operating an SAS and/or ESC for a five-year term. The proposal must include a description of the prospective SAS Administrator or ESC operator's business structure including ownership information. To the extent that the proponent will rely on fees to support its operations, the proposal should also describe the fee collection process and the entities from which the fees will be collected.

CTIA, an international nonprofit membership organization that has represented the wireless communications industry since 1984, is well positioned financially to operate a SAS and ESC for the initially authorized five-year term and beyond. CTIA receives strong financial support from a diverse group of member companies representing all aspects of the wireless ecosystem including wireless carriers and their suppliers, as well as providers and manufacturers of wireless data services and products. In addition, CTIA provides several revenue-generating services at the request of, and for the benefit of, its members, which generate diversified annual income to ensure the continued healthy operation of the Association.

CTIA's membership includes the five largest U.S. wireless carriers as well as numerous regional and local wireless carriers. CTIA's Board of Directors is made up of senior executives from 35 member companies.¹¹ With members from wireless carriers and their suppliers to providers and manufacturers of wireless data services and products, the association brings together a dynamic group of companies that enable consumers to lead a 21st century connected life.

¹¹ A complete list of CTIA's Board of Directors is available at <http://www.ctia.org/about-us/board-of-directors>.



CTIA has conducted an extensive analysis of the anticipated operations cost of the SAS and ESC, and will support those operations via a reasonable fee structure sufficient to ensure those costs are covered. Member customers will be invoiced on a quarterly basis or otherwise agreed basis for SAS services provided.

1.4) A description of how data will be securely communicated between the SAS and its associated ESC and how quickly and reliably these communications will be accomplished.

The secure communication policies require a Public Key Infrastructure ("PKI"), which will govern communications within the CBRS ecosystem and provide authentication and authorization for messages exchanged within the SAS ecosystem.

The SAS ecosystem will address the security concerns at every level of connectivity between and among various functional elements. In a fully deployed system, there will be several peer-to-peer interconnected SAS operators and domain proxy operators representing a network of CBSDs. In addition, there will be CBSDs that will be directly connected to a SAS, not represented by a domain proxy, which must be authenticated and provided secure communications.

The architecture, requirements, and specifications for these communications are currently being defined in the Wireless Innovation Forum™ ("WInnForum"), a multi-stakeholder forum, and CTIA is an active member contributing to the development of these definitions and protocols.

1.5) Technical diagrams showing the architecture of the SAS and/or ESC and a detailed description of how each function operates and how each function interacts with the other functions.

The diagrams below are derived from various WInnForum Working Group documents.¹² The functional description of various major elements is stated in response to question 1.1.1 above.

¹² See generally WInnForum, Report Work Products, <http://groups.winnforum.org/Reports>.

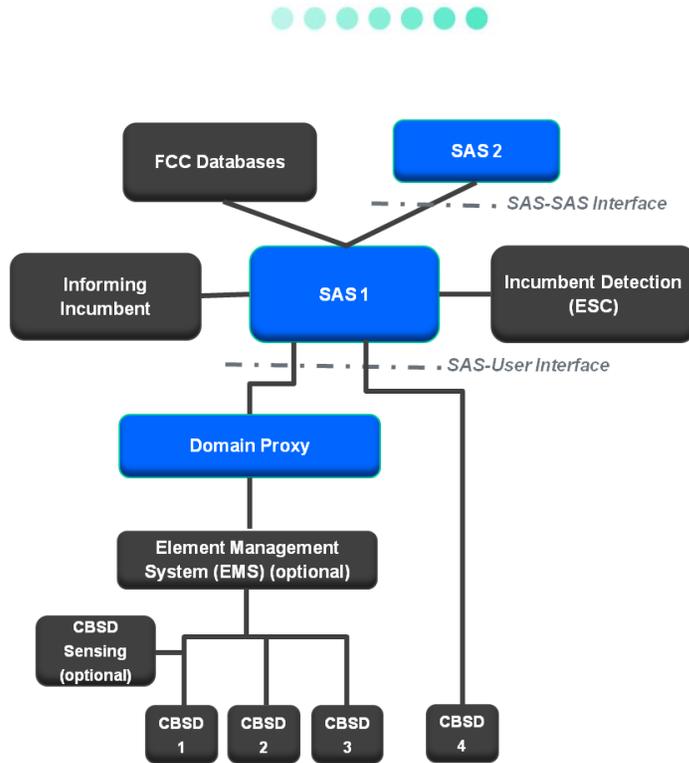


Figure 2: SAS Functional Architecture

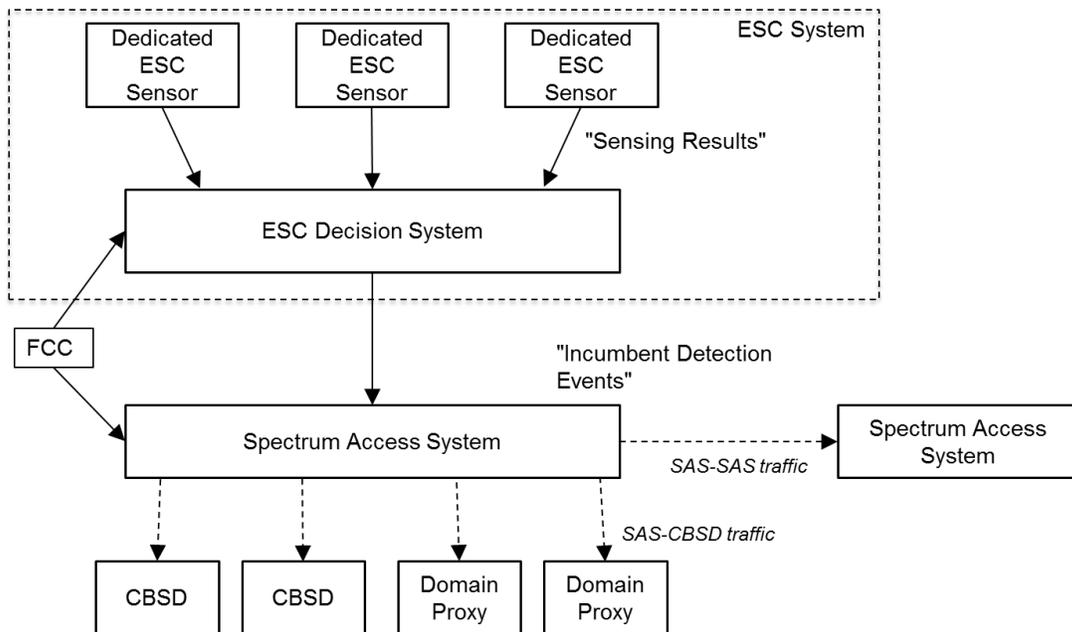


Figure 3: ESC Functional Architecture



1.6) A description of the propagation model and any other assumptions that the prospective SAS Administrator or ESC operator proposes to use to model operations and facilitate coordination in the band.

The propagation model is an empirical mathematical model depicting the behavior of a radio wave propagation for a given frequency, distance and other surrounding conditions. Different models have been developed to meet the needs of different conditions. These models are derived from massive data collected for a given terrain. This data is purely numerical in nature. For a given model, the collected data should be of sufficient quantity to predict the behavior of radio signals for any given scenario. Thus, the radio model essentially can predict likely behavior of a radio link in a given scenario.

There are several models that are developed and used to engineer the needs of practical deployment scenarios. Some of these models include, but are not limited to:

- Indoor applications
- Outdoor applications
- Attenuation models based on the environment
- Line-of-sight models
- Terrain models
- Urban models
- Sub-urban models
- Rural models
- Longley-Rice models
- Extended Hata models

Given that the 3.5 GHz band deployment is anticipated to address hotspot capacity needs and indoor applications, it is believed that there is not a strong need for a traditional broader RF engineering analysis in regard to various propagation models. A small cell used either to meet hotspot capacity enhancement needs or indoor application needs will be confined to a few hundred-meter radius coverage, limiting the need for an exhaustive consideration of various propagation models. For such a need, one would focus on fixed urban or suburban or other radio propagation models



for most deployment scenarios. CTIA will explore coordinating with other SASs to agree on using the same propagation models for consistency of results.

1.7) A description of the methods that will be used to update software and firmware and to expeditiously identify and address security vulnerabilities.

Over-the-air ("OTA") programming is the recommended option to be considered to update the software, firmware, and configuration settings of functional elements of the system under consideration. An advantage of an OTA system is that one central location can send an update to all of the affected functional elements. These updates will follow the best practices established by the industry for maintaining the security, privacy, and integrity needs of the system as well as consumers.

To keep up with the requirements of responding to the evolving needs of the system, OTA configuration has become increasingly important as new updates can be passed on without requiring a site visit to each and every remote functional element location.

Various standardization bodies have been established to help develop, oversee, and manage OTA programming. One of them is the Open Mobile Alliance ("OMA").¹³

To provision parameters in a remote functional element over the air, the element needs to support a provisioning client capable of receiving, processing, and setting the parameters. For example, a Device Management client in a device will enable it to receive and provision applications or update its connectivity parameters.

CTIA intends to adopt the best practice methods that are currently being defined in the WInnForum to rapidly address and eliminate security vulnerabilities through firmware and software updates delivered over the air, as needed.

¹³ See Open Mobile Alliance, www.openmobilealliance.org.



1.8) An affirmation that the prospective SAS Administrator and/or ESC operator (and its respective SAS and/or ESC) will comply with all of the applicable rules as well as applicable enforcement mechanisms and procedures.

CTIA will implement the rules specified in the WInnForum SAS to CBSD Technical Report.¹⁴ Additionally, with respect to this requirement, CTIA is committed to support:

- § 96.53 Spectrum access system purposes and functionality
- § 96.55 Information gathering and retention
- § 96.57 Registration, authentication, and authorization of Citizens Broadband Radio Service Devices
- § 96.59 Frequency assignment
- § 96.61 Security
- § 96.63 Spectrum access system administrators
- § 96.65 Spectrum access system administrator fees
- § 96.67 Environmental sensing capability

Additionally, CTIA will also support the amendments to parts 1, 2, 95, and 96 of Title 47 of the Code of Federal Regulations, as specified in the *3.5 GHz Order*, *3.5 GHz Second R&O*, and the *3.5 GHz Reconsideration Order*.

¹⁴ See SAS-to-CBSD Technical Report.



2) Spectrum Access System Duties and Responsibilities.

As discussed in more detail below, CTIA has both the intent and technical ability to comply with the requirements and core functions for serving as a SAS Administrator, including compliance with Part 96, subpart F of the Commission's rules.¹⁵

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

CTIA's policy on how the SAS will retain, secure, and verify information from the CBSDs is governed by the requirements set forth in the Commission's rules:

- A SAS must employ protocols and procedures to ensure that all communications and interactions between the SAS and CBSDs are accurate and secure and that unauthorized parties cannot access or alter the SAS or the information it sends to a CBSD.
- Communications between CBSDs and a SAS, between an ESC and a SAS, between individual CBSDs, and between different SASs, must be secure to prevent corruption or unauthorized interception of data.
- A SAS must be protected from unauthorized data input or alteration of stored data.
- A SAS must verify that the FCC identification number supplied by a CBSD is for a certified device and must not provide service to an uncertified device.

The overall security concept for the 3550-3700 MHz CBRS, as mentioned earlier, includes operational security ("OPSEC") and communications security ("COMSEC") of the CBSDs, SASs, and ESCs. The OPSEC of the CBRS 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, and personnel security.

¹⁵ See Notice at 14174, 14175-76.



COMSEC is the prevention of unauthorized access to telecommunications traffic that is transmitted or transferred over communications media. There are several COMSEC disciplines, including:

- Cryptographic security – encrypts the payload so that it becomes unreadable unless it is decrypted by an authorized recipient with proper decrypting key. This also prevents the potential tapping of the data during the transmission.
- Emission Security – stops unauthorized reception and interception of data
- Physical security – ensures the security of the physical location of the site, database, or equipment.

CTIA intends to follow the best practices set forth for both OPSEC and COMSEC in the WinnForum, a multi-stakeholder forum, and other relevant industry fora (e.g., National Institute of Standards and Technology (“NIST”) Framework, Department of Homeland Security National Coordinating Center for Communications - COMM-ISAC, and FCC Communications Security, Reliability and Interoperability Council).

2.2) A demonstration that the SAS will be capable of resolving various sources of interference between and among Citizens Broadband Radio Service users and/or Incumbent users.

CTIA is committed to complying with the emissions and interference limits adopted by the Commission, which were designed to promote effective coexistence of different users in the band.¹⁶ In particular, CTIA shall implement:

- -13 dBm/MHz from 0 to 10 megahertz from the SAS assigned channel edge.
- -25 dBm/MHz beyond 10 megahertz from the SAS assigned channel edge down to 3530 MHz and up to 3720 MHz.
- -40 dBm/MHz below 3530 MHz and above 3720 MHz.

Additionally, the deployed systems will maintain the support of Category A CBSDs that will be limited to a maximum EIRP of 30 dBm in 10 megahertz, but will be required to

¹⁶ CTIA notes that it is further committed to complying with any revised interference protection requirements adopted by the Commission as a result of reconsideration of the 3.5 GHz Order.



operate in accordance with instructions from the SAS, which for interference prevention reasons, may authorize a lower power level (see FCC Rule § 96.41 and Part 96, Subpart F).

With respect to Category B devices, CTIA understands that Category B devices may be used for outdoor applications in configurations including non-line-of-sight backhaul. CTIA notes the difference in power limits between the Category B and Category A devices as set forth in Commission's Rules and the *3.5 GHz Order*.

To mitigate interference, the SAS expects its respective registered CBSDs to provide signal strength and location information for use in determining interference levels. To make sure these metrics are in place, CTIA is involved in the deliberations of appropriate standards and best practices for defining such parameters in the multi-stakeholder forum.

Additionally, the area within the Priority Access licensee's default protection contour, as calculated by the SAS in accordance with Section 96.25 (or smaller, self-reported protection contour), will be protected from interference in accordance with sections 96.25 and 96.41 (d).¹⁷ To protect CBSDs authorized to provide service on a Priority Access basis, the SAS will not authorize other CBSDs whether Priority Access or GAA – on the same channel in geographic areas and at maximum power levels that will cause aggregate interference in excess of -80 dBm/10 MHz channel within a PAL Protection Area.¹⁸

The emission power measurements will be performed using either RMS-detection or peak detection.¹⁹

¹⁷ See *3.5 GHz Reconsideration Order* ¶ 138 (referencing *3.5 GHz Second R&O* ¶¶ 164-197).

¹⁸ *3.5 GHz Reconsideration Order* ¶ 138.

¹⁹ See *3.5 GHz Reconsideration Order* ¶ 103.



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

CTIA recognizes the need to protect incumbent fixed satellite service (“FSS”) earth stations from harmful interference. To ensure protection of incumbent FSS earth stations, CTIA will consider technical factors such as:

- Actual EIRP density of CBSD and End User Device transmitters;
- Location, antenna pattern, and orientation of those transmitters;
- FSS earth station receiver characteristics (including location, antenna gain, elevation and azimuth of the main antenna beam); and
- Relative distance, mutual orientation, surrounding terrain and the propagation channel(s) between an FSS earth station and potential interfering transmitters.

In the context of the CBRS, CTIA expects to implement a realistic and predictable path loss between CBSDs and FSS earth stations resulting in smaller protection distances. Also, CTIA agrees to receive and respond to interference complaints from FSS earth station licensees.²⁰ Regarding protecting grandfathered wireless broadband licensees, CTIA will take steps to maximize protection for these licensees until the end of grandfather period.

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

The Commission may determine to approve multiple SAS Administrators. In such an event, because each CBSD will only be required to contact a single SAS, there is a need for SASs to share accurate registration information necessary to avoid conflicting assignments. Therefore, CTIA as a SAS Administrator will cooperate with other SAS Administrators to develop a standardized process for coordinating all SAS operations and avoiding conflicting assignments, thus maximizing shared use of available frequencies while enabling ease of operations for SAS customers, ensuring continuity of

²⁰ See 3.5 GHz Reconsideration Order ¶ 147.



service to all registered CBSDs, and sharing data collected from registered CBSDs that is necessary to avoid conflicting assignments. CTIA is working with WinnForum members regarding the existence of controls to ensure sensitive SAS customer data, including information on CBSD operations, is not used for any other purpose other than as needed to enable SAS operations. This extends to data exchanged with other SAS Administrators.

CTIA also commits to coordinate with other SASs to facilitate non-interfering use by CBSDs connected to other SASs, maximize available GAA frequencies by assigning Priority Access Licenses ("PALs") to similar channels in the same geographic regions, and perform such other functions necessary to ensure that available spectrum is used efficiently. CTIA, as a SAS Administrator, will share information on the CBSDs and licensees managed by its SAS to the extent necessary to facilitate the effective coordination of all approved SASs.

The SAS-SAS interface defines the methods and protocols that govern the communication, coordination, and information exchange between two SAS implementations.

In addition, CTIA notes that the requirements on these interfaces are set forth in the Part 96 of the Commission's rules, which include:

- Cooperate to develop a standardized process for coordinating operations with other SASs, avoiding any conflicting assignments, maximizing shared use of available frequencies, ensuring continuity of service to all registered CBSDs, and providing the data collected pursuant to section 96.55.²¹
- Coordinate with other SAS Administrators including, to the extent necessary, sharing information, facilitating non-interfering use by CBSDs connected to other SASs, maximizing available General Authorized Access frequencies by assigning PALs to similar channels in the same geographic regions, and other functions necessary to ensure that available spectrum is used efficiently consistent with this part.²²

²¹ 47 C.F.R. § 96.63(h).

²² 47 C.F.R. § 96.63(i).



It is further noted that the communications between CBSDs and a SAS, between an ESC and a SAS, between individual CBSDs, and between different SASs, must be secure to prevent corruption or unauthorized interception of data. A SAS must be protected from unauthorized data input or alteration of stored data.²³ As a SAS Administrator, CTIA will make all information necessary to effectively coordinate operations between and among CBSDs available to other SAS Administrators.²⁴ In no event will the information stored in the SAS database be used for any commercial use except to serve the needs of the functional operation of the CBRS system.

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

CTIA is committed to performing all SAS Administrator Part 96, subpart F functions. For certain specific expertise, if deemed necessary in the future, CTIA may partner with another entity that is well recognized in the industry as a subject matter expert to complement CTIA's resources and will file supplemental information as necessary to update the Commission on this process.

If multiple SASs are authorized by the Commission, CTIA will follow the data transfer schedule guidelines that are being defined in the multi-stakeholder forum.

²³ 47 C.F.R. § 96.61(b).

²⁴ 47 C.F.R. § 96.55(a)(2).



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

CTIA will comply with the architecture of the CBRS system shown in Figure 1 and adhere to the information flows identified below:

- SAS Discovery
 - Successful operation
 - Abnormal conditions
- CBSD Registration
 - Successful operation
 - Unsuccessful Operation
- CBSD Spectrum Inquiry
 - Successful operation
 - Unsuccessful Operation
- Grant Request
 - Successful operation
 - Unsuccessful Operation
- CBSD Heartbeat Request
 - Successful operation
 - Unsuccessful Operation
- CBSD Spectrum Relinquishment
 - Successful operation
 - Abnormal conditions

From a temporal criteria point of view, if a CBSD ceases to operate on a Priority Access basis – or discontinues service for more than seven days – the SAS will alter the PAL Protection Area accordingly. If a CBSD discontinues service and is later reactivated on



a Priority Access basis, the SAS will expeditiously re-establish the PAL Protection Area around that CBSD.²⁵

The SAS-SAS data transfer is guided by the standards that are being developed by the multi-stakeholder forum.²⁶ The SAS-to-SAS Technical Report describes the protocol by which SASs exchange information as required by the 3.5 GHz Order in order to facilitate access to the band by CBSDs connected to other SASs, coordinate operations between and among such CBSDs, provide a stable radio frequency environment for Priority Access licensees, and other functions required for orderly spectrum administration and the fulfillment by the SAS of the responsibilities given it under Part 96 of the FCC's. CTIA is committed to following the protocols defined in the SAS-to-SAS Technical Report to support SAS-to-SAS communications.

Some of the topics that are covered in the SAS-to-SAS Technical Report include, but are not limited to:

- SAS-SAS information exchange elements
 - SAS-SAS exchange entities and names
 - SAS Administrator Exchange Record
 - ESC Administrator Exchange Record
 - SAS Implementation Exchange Record
 - ESC Implementation Exchange Record
 - Domain Proxy Exchange Record
 - CBSD Device Type Exchange Record
 - CBSD Exchange Record
 - Incumbent Exchange Record
 - Zone Exchange Record
 - CBSD Operator Exchange Record
 - Professional Installer Exchange Record
 - Coordination Event Exchange Record
- SAS-SAS Exchange Mechanisms:

²⁵ See 3.5 GHz Second R&O ¶ 195.

²⁶ See Interim SAS to SAS Protocol Technical Report-A, Document WINNF-15-P-0051, Version V1.0.0 (Jan. 26, 2015), <http://groups.winnforum.org/Reports> ("SAS-to-SAS Technical Report").



- Providing metadata-only in response to time-range requests
- Time basis for time-range requests
- Wildcard time-range requests

If a CBSD ceases to operate on a Priority Access basis – or discontinues service for more than seven days – it must inform the SAS of this change in status and the SAS must alter the PAL Protection Area accordingly.

The communication protocol between the SAS and ESC is currently being defined in WinnForum, a multi-stakeholder forum. CTIA is committed to supporting this protocol when it is published.

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

CTIA affirms that it will abide by Section 96.55 of the Commission's rules and will only retain records and information or instructions received regarding federal transmissions from the ESC in accordance with information retention policies established as part of the ESC approval process.

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

CTIA, as a SAS Administrator, affirms that it will implement best practices for OPSEC and COMSEC. More details regarding CTIA's policy on how the SAS will ensure that unauthorized parties cannot access or alter the SAS or otherwise corrupt the operation of the SAS in performing its intended function can be found in the response to question 2.1 above.



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

The fundamental asset that CTIA will utilize to accommodate support of geographically and spectrally adjacent operations is interference mitigation. The SAS will calculate estimated cumulative aggregate interference based upon reported locations of CBSDs, reported power levels of each CBSD and the radio model for the specific area (urban, suburban, rural, etc.). In the event interference calculations result in unacceptable levels of interference, the SAS will act to either move CBSDs to alternate non-interfering channels or reduce CBSD power levels. The goal of this interference calculation is to make sure that Tier 1 (*i.e.*, Incumbent Access) and Tier 2 (*i.e.*, Priority Access) users are protected and the neighboring Priority Access users are protected from the GAA users being served.

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

The CTIA SAS will make its records available to authorized Commission personnel upon written request from such personnel.



3) Environmental Sensing Capability Duties and Responsibilities.

As discussed in more detail below, CTIA has both the intent and ability to comply with the requirements and core functions for serving as an ESC Operator, including compliance with Part 96, subpart G of the Commission's rules.²⁷

- 3.1) A description of the methods (e.g., interfaces, protocols) that will be used by the ESC to communicate with the SAS. It must include a description of the security methods or protocols that will be used to ensure that unauthorized parties cannot access or alter the ESC or otherwise corrupt the operation of the ESC in performing its intended functions.**

The methods (e.g., interfaces, protocols) that will be used by the CTIA ESC to communicate with the SAS will follow the guidelines set forth by the WInnForum, which are currently under development.

- 3.2) A description of the sensing methodology it (the ESC) will use to detect federal transmissions and determine that the spectrum needs to be evacuated. This description must include a detailed description of the type of sensors to be used (i.e., infrastructure or device based), the sensing architecture to be employed, the sensing thresholds, any processing of sensor data, sensor sensitivity, and sensor resiliency to receiver front-end saturation and burn-out. The prospective ESC operator must also provide a description of the safeguards that will be used to “ensure that the ESC does not store, retain, transmit, or disclose operational information on the movement or position of any federal system or any information that reveals other operational information of any federal system that is not required to effectively operate the ESC by Part 96.”**

The sensing methodology that the CTIA ESC network will use to detect federal transmissions and determine whether the spectrum needs to be evacuated is under development in the multi-stakeholder forum (i.e., WInnForum). Once finalized, CTIA will

²⁷ See Notice at 14174, 14176.



update this document, if necessary, to include a detailed description of the type of sensors to be used (*i.e.*, infrastructure or device based), the sensing architecture to be employed, the sensing thresholds, any processing of sensor data, sensor sensitivity, and sensor resiliency to receiver front-end saturation and burn-out. This architecture will be completely consistent with the architecture that is currently being defined in the multi-stakeholder forum.

The ESC sensors will be spaced along the coast at station-to-station distances that are practical (*i.e.*, on the order of a few tens of kilometers); they will be located with radio frequency line-of-sight coverage from one to the next along the shore, running as close as possible to the shoreline.

The ESC sensors that will be deployed will have a sensitivity level sufficient to detect the presence of an incumbent radar signal.

CTIA will ensure that appropriate safeguards are put in place to ensure that the ESC does not store, retain, transmit, or disclose operational information on the movement or position of any federal system or any information that reveals the locations or movements of any federal system.

3.3) *A description of the methods (e.g., interfaces, protocols) that will be used by sensors to communicate with the ESC and the procedures, if any, that it plans to use to verify that all sensors can communicate with the ESC in a timely and secure manner. It must include a description of the security methods or protocols that will be used to ensure that unauthorized parties cannot access or alter the ESC or individual sensors or otherwise corrupt the operation of the ESC in performing its intended functions.*

The methods (*e.g.*, interfaces, protocols) that will be used by the CTIA ESC sensors to communicate with the ESC, and the procedures used to verify that ESC sensors are able to communicate with the ESC, will follow the guidelines set forth by WINNForum, which are still in development. Such guidelines will also include a description of the security methods and/or protocols that will be used to ensure that unauthorized parties cannot access or alter the ESC or individual sensors or otherwise corrupt the operation of the ESC in performing its intended functions.



Appendix A

CTIA Background

CTIA is an international nonprofit membership organization that has represented the wireless communications industry since 1984. CTIA's membership includes the five largest U.S. wireless carriers as well as regional and local wireless carriers. CTIA's Board of Directors is made up of senior executives from 35 member companies. With members from wireless carriers and their suppliers to providers and manufacturers of wireless data services and products, the association brings together a dynamic group of companies that enable consumers to lead a 21st century connected life.

The association advocates on behalf of its members at all levels of government. CTIA also coordinates the industry's voluntary efforts to provide consumers with a variety of choices and information regarding wireless products and services. This includes voluntary industry guidelines; programs that promote mobile device recycling and reuse; and wireless accessibility for people with disabilities.

Past Performance and Technical Experience

CTIA provides technology leadership in the mobile data services arena ranging from government advocacy to consumer education to improve the quality of life for everyone. Some of the noteworthy accomplishments of CTIA include:

AWS Cost Sharing Clearinghouse Development

CTIA developed a process to enable industry-accepted spectrum clearing cost-sharing for the 2.1 GHz band. The process, which was developed with Comsearch, fairly determines how the cost of relocating wireless operations from one band to another should be shared among the parties involved, thereby accelerating the expansion of the amount of spectrum available for commercial mobile radio service. CTIA's process determines when cost-sharing is triggered, notifies the parties involved, and includes resolution of any disputes that may arise.



Common Short Code Administrator

Common Short Codes (“CSCs”) are special numbers (usually five-six digits), shorter than 10-digit telephone numbers, that are used to address SMS and MMS messages from selected service providers’ to the mobile phones of wireless subscribers. Short codes are widely used for value-added services such as television program voting, charity donations, and many other applications.

CTIA, in its capacity as the CSC Administrator (“CSCA”), supports all aspects of code acquisition and monitors code compliance with the Acceptable Use Policy (“AUP”). Any violations of the AUP by a user may result in penalties, up to and including the inability to register new CSCs or to renew existing CSCs, and the suspension of CSC campaigns on the network(s) of one or more wireless carriers. This role has provided CTIA with expertise and experience in interfacing and working with mobile eco-system players.

CTIA and Global Certification Forum Wireless Device Evaluation

CTIA and the Global Certification Forum (“GCF”) have agreed to a common process for evaluating the over-the-air (“OTA”) performance of new wireless devices. This agreement allowed GCF to incorporate CTIA’s “Test Plan for Wireless Device Over-the-Air Performance” into its Performance Measurement process. The agreement also allows the organizations to work together on future updates of the test plan to ensure that the needs of network operators and device vendors throughout the world are being addressed.

Today, CTIA’s “Test Plan for Wireless Device Over-the-Air Performance” is part of the CTIA and PCS Type Certification Review Board (“PTCRB”) certification programs. The test plan defines a standard method to measure a wireless device’s antenna performance. By simulating the network environment, the wireless device is put through a rigorous testing process to evaluate how well it can transmit and receive a wireless signal.

For GCF, Performance Measurement is an optional scheme that complements GCF Certification and allows manufacturers to quantify and report on agreed aspects of the



performance of a mobile device. Performance Measurement relies on test criteria developed by recognized standards bodies, including 3GPP. GCF's current use of the CTIA OTA test plan establishes a single benchmark for device vendors and network operators throughout the world.

9-1-1 Location Accuracy

From location-awareness to sharing texts, images, video, and voice, wireless services enhance how first responders approach and handle emergencies. The wireless industry has a strong history of taking steps to continually improve public safety functions and wireless 9-1-1 services.

In 2015, the FCC adopted new rules requiring nationwide wireless service providers to improve indoor 9-1-1 location accuracy when using mobile devices by delivering a dispatchable location that includes street address plus floor, suite, apartment or other location information. The FCC's Order included a requirement that an independently administered and transparent indoor Test Bed be established to test and verify that location technologies are capable of meeting the Commission's new location accuracy requirements for wireless calls to 9-1-1 emergency services. CTIA managed the establishment of Test Bed, LLC, which took on the Administrator-Executor role to facilitate the testing and validation of deployed and emerging wireless 9-1-1 location information technologies. This program is poised to test wireless 9-1-1 location information technologies under various conditions. These conditions include indoor environments representative of various topographies, morphologies, building styles and construction types. On March 31, 2016, the 9-1-1 Location Technologies Test Bed, LLC announced that LCC Design Services, Inc., a Tech Mahindra Company, was selected to administer the indoor 9-1-1 location accuracy test bed.

Additionally, the National Emergency Administration Database ("NEAD"), LLC was established by CTIA to launch the NEAD Platform, consistent with the FCC's 2015 Order on wireless E911 location accuracy requirements. The NEAD LLC was established to implement a national database of access point (e.g., Wi-Fi hotspots) and beacon (e.g., Bluetooth Low Energy) location information that will enable wireless service providers to deliver a dispatchable location that will help 9-1-1 call centers respond to emergencies.



Cybersafety and Cybersecurity

The wireless ecosystem today is dramatically different from what it was only five years ago with the constant introduction of a variety of new players and technologies. In order to protect the wireless industry from cybercriminals and cyber threats, the wireless ecosystem – network operators, device manufacturers and application/content developers – must work together. In June 2012, CTIA developed its Cybersecurity Working Group (CWG) for industry players to work together as much as possible to identify potential problems and determine the best course of action to minimize the impact of cyberthreats on consumers and companies.



Appendix B

Thomas (Tom) Sawanobori

Senior Vice President and Chief Technology Officer

Thomas (Tom) Sawanobori is CTIA's Senior Vice President and Chief Technology Officer. He is responsible for technology and technical matters concerning spectrum, network evolution, cybersecurity and device certification to benefit CTIA's members and to serve as a technical resource to policymakers. He has 22 years of technology planning, network engineering and operational experience for Verizon, including lead planner for Verizon Wireless' 4G LTE network.

Mr. Sawanobori was Vice President of Network Planning at Verizon, where he was responsible for technology planning and capital budget management. He led the technology evolution of the network including spectrum planning, 3G/4G technology, LTE and LTE-Advanced, and core network evolution. In addition to his career at Verizon, Mr. Sawanobori worked at Hughes Electronics on Navy Communications and Combat Systems. He served 5 years in the US Navy as a Submarine Warfare Officer and went on to complete 20 years total, retiring as a Commander in the Naval Reserve.

Mr. Sawanobori holds a Bachelor of Science in Mechanical Engineering from Duke University and a Master of Engineering from California State University-Fullerton.

Paul Anuskiewicz

Vice President, Spectrum Planning

Paul Anuskiewicz is CTIA's Vice President for Spectrum Planning. He is responsible for technology and technical matters concerning spectrum advocacy, spectrum allocation for the network evolution to 5G and other technical areas to aid CTIA's members and as a technical resource to policy makers. He has over 28 years of technology planning, network engineering and operational experience.

Prior to CTIA, Mr. Anuskiewicz was CEO of Caten McGuire, a wireless technology consulting firm responsible for developing and assessing wireless and technology strategy, implementing operational change, and for sourcing billions in infrastructure



and devices, for a wide variety of U.S. and international clients. Mr. Anuszkiewicz also served as CTO and VP of Network Operations for two U.S.-based cellular operators. Mr. Anuszkiewicz has served as a Board Member of PCIA for Microwave Clearing and has worked with international governments on regulatory and spectrum auction issues.

Mr. Anuszkiewicz holds a Bachelors Degree in Electrical Engineering from California State University and an MBA from the University of Dallas. He is a registered professional engineer.

John Marinho

Vice President, Technology & Cybersecurity

John Marinho joined CTIA as its Vice President of Technology and Cybersecurity in March 2012. Mr. Marinho's key responsibilities in the created role include leading CTIA's efforts to help the wireless industry secure its networks and devices against cybersecurity threats, educating policymakers on emerging technologies, and advocating for sensible and practical regulations that do not impose unintended consequences. He also serves as CTIA's primary liaison with government agencies on cybersecurity issues.

Mr. Marinho previously worked in Mobility Solutions at Dell, where he defined the end-to-end mobility solution for enterprise customers and certified the first secure Android implementation for the U.S. Department of Defense. Prior to Dell, Mr. Marinho held positions in Strategic Marketing, Product Management and Government Affairs at Alcatel-Lucent. During his tenure at Alcatel-Lucent/Bell Labs, he deployed the first wireless broadband 700MHz Public Safety system in Washington, D.C., and implemented numerous commercial wireless broadband networks for carriers around the globe. He has also worked at ITT and Canadian Marconi.

Mr. Marinho holds the Bell Labs President's Award for Innovation and was awarded several Bell Labs patents in the field of wireless network optimization, network design and RF technology. He is also the retired Chairman of the TIA TR45 Standards Committee that is responsible for wireless technology standards. Mr. Marinho is the recipient of the CTIA and TIA Industry Service Award for his efforts in setting wireless industry standards. Mr. Marinho has a MBA from Rutgers Graduate School of



Management, and graduated cum laude from New Jersey Institute of Technology in electrical engineering.

Mark Sargent

Vice President, Certification Programs

Mark Sargent is Vice President of Certification Programs at CTIA, where he oversees the U.S. wireless industry's certification programs for consumer wireless devices. In this position, he is also Chairman of CTIA's industry-wide Certification Program Working Group. Mr. Sargent has 30 years of experience in the telecommunications industry, having held various engineering, sales, marketing, product development and operations positions. Mr. Sargent received a BSEE from Pennsylvania State University and an MBA from Duke University.

Eshwar Pittampalli

Director, Wireless Technology

Eshwar Pittampalli is a Director of Wireless Technology at CTIA. Prior to joining CTIA, Dr. Pittampalli was a PARTNER in Alcatel-Lucent Corporate Marketing organization evangelizing Internet of Things (M2M). Prior to this role, he led the Alcatel-Lucent corporate market intelligence team as Senior Director forecasting global telecom market trends, sizing, shares supporting CFO's office, product groups and regions. A registered professional engineer with Master of Science and Ph.D. degrees in electrical engineering from the University of Oklahoma in Norman, Oklahoma. Dr. Pittampalli is also a Registered Patent Agent with a Mini-MBA from Wharton School of Business. In 2003, Dr. Pittampalli was awarded Bell Labs' highest honor, Bell Labs Fellow, for his outstanding technical contributions and leadership in advancing wireless communications technology and standards.