

Proposal to Conduct a Public Field Trial and for Initial Commercial Deployment

GN Docket No. 15-319

Key Bridge Wireless LLC
Jesse Caulfield, CEO
1750 Tysons Blvd., Suite 1500
McLean, VA 22102
Phone: +1 (703) 542-4140
<http://keybridgewireless.com>

Document Information

Document status	Public
Version	1.0.1
Date printed	September 10, 2018
Copyright	© 2018 Key Bridge Wireless LLC. All Rights Reserved

Opening letter

Key Bridge Wireless LLC (fmr Key Bridge Global LLC, dba “Key Bridge”, “Key Bridge Wireless”) is pleased to submit this supplement to our original proposal to administer a Spectrum Access System (SAS) in the 3.5 GHz frequency band.¹

Key Bridge TV white space SAS technology, first tested and certified by the Commission in 2013, has been in successful commercial operation for over five years. Our CBRs SAS solution builds on this foundation and has been extensively tested in a controlled lab environment. In this document we propose to extend the scope of testing to include evaluation of our commercial spectrum access system in a real-world setting through several short term, limited geographic, private commercial deployments.

The goal of the our initial commercial deployment field trials is to collect detailed performance and operational status information from our CBRs SAS. The product of the effort will be a set of comprehensive reports describing the quality and quantity of SAS operations and affirming system compliance with Commission rules plus all relevant commercial specifications and standards.

We thank the Commission for this opportunity and are happy to provide any additional information the Commission may require to evaluate our proposal.

/s/

Jesse Caulfield, CEO

Key Bridge Wireless LLC

¹ See Key Bridge *Proposal to Administer a Spectrum Access System* (“Key Bridge SAS Proposal”), GN Docket 15-319 submitted 05/13/16 at <https://ecfsapi.fcc.gov/file/60001841834.pdf>

1 ICD project overview

Key Bridge proposes to conduct SAS initial commercial deployment testing in one public field trial and three real world settings. We have carefully selected client partners and use case settings to ensure complete coverage of all Part 96 functionality and also to fully exercise our SAS solution with complex and demanding operating scenarios that will be encountered during real world commercial use. Each scenario will stress and test the most important, complex and critical SAS functions required for successful commercial operation.

Because ESC services are not yet available all of the ICD evaluations are located in the interior of the United States, away from the coast. The locations are also well outside NTIA coastal exclusion zones and DPA protection zones.²

We believe that each of the ICD evaluations will contribute to an effective SAS test as each supports the unique demands of highly variant use cases while preserving secure, stable and equitable multi-tier spectrum sharing.

1.1 Commercial partners

Key Bridge is a neutral operator of spectrum administration infrastructure and supports several different CBRS manufacturers and trials.

Key Bridge has **partnered with Nokia** for our initial commercial deployment effort. Nokia is well known to the Commission with a strong track record of pioneering research and technology development for shared spectrum use in wireless networks. Nokia is also a manufacturer of CBRS capable wireless infrastructure.

Key Bridge has also **partnered with Amazon** web services to provide our cloud-hosted SAS service in support of the ICD. Amazon Web Services (AWS) provides companies of all sizes with an infrastructure web services platform in the cloud. Amazon is a prime supplier of hosted infrastructure solutions for commercial and government applications.

1.2 Project duration

We believe **eight weeks** operation of the SAS and other CBRS infrastructure components is a sufficient duration to produce a substantive and meaningful report for the Commission. We therefore propose to conduct ICD testing for not less than eight and not more than 10 weeks beginning as soon as the Commission will allow.

2 See NTIA, *Letter to FCC on Commercial Operations in the 3550-3650 MHz Band*, (NTIA Letter) GN Docket 12-354 received March 24, 2015. Referencing the *NTIA Letter* Enclosure 1: Key Bridge ICD locations are selected to lie outside the original Fast Track exclusion zone (yellow line). Referencing the *NTIA Letter* Enclosure 2: Key Bridge ICD locations are not near any ground based radar locations or other locations separately communicated to SAS administrators by the DoD.

All of the described ICD use cases are either currently in operation or in the last stages of procurement and provisioning. **Key Bridge is prepared to begin ICD testing and evaluation immediately.**

Key Bridge would like to begin ICD testing **on or about November 1st, 2018** and continue through December. If the Commission agrees with this timing Key Bridge could then provide the Commission with a comprehensive report of CBRS commercial operations and ICD learnings in mid-January, 2019.

1.3 Administration and data collection

Referencing our original SAS proposal as background, the Key Bridge SAS is realized as a modular, cloud-hosted computer application.³ Essential SAS functions, such as system administration, user access, device registration, and spectrum access services are provided by separate components.

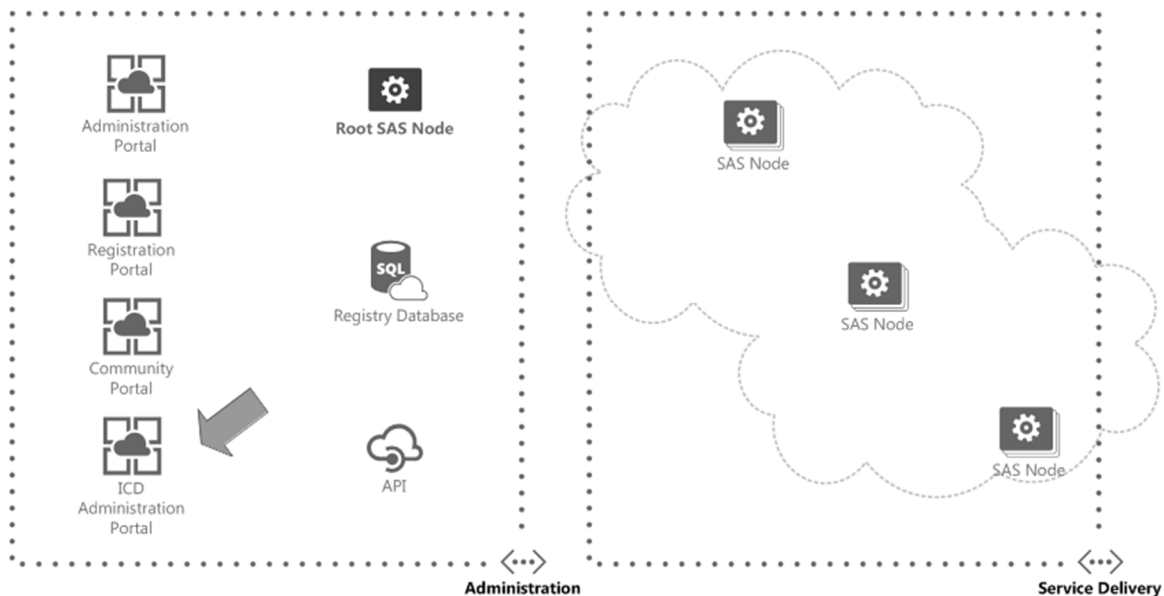


Illustration 1: Key Bridge will operate a temporary ICD administration portal.

For the ICD process Key Bridge will temporarily add and operate a **customized ICD administration portal** to receive all ICD test data and to assemble test data into a collection of ICD test reports. This new portal is shown in the general SAS architecture diagram in Illustration. It will be provisioned in and will operate as part of the SAS administration domain.

1.4 Test report content, organization and format

During ICD each SAS component will be configured to provide finely detailed logging information, as described in the Proposal, and to forward that information to the customized ICD administration portal for handling.⁴

³ See *Key Bridge SAS Proposal* at section 5.2 SAS Infrastructure. See specifically Illustration 5, which is modified in this document to show the placement of a temporary “ICD administration portal” component.

⁴ See *Key Bridge SAS Proposal* at 7.1.2 Logging.

The ICD administration portal will be configured to collect operating logs and ICD extended test data and metrics from each of the various Key Bridge SAS components. The information collected will include detailed status and transaction logs, event information and notifications, time-series operating metrics, and other component or function-specific measurements.

The collected information will be stream processed in near real time on the ICD administration portal and organized according the high-level, notional SAS architecture as described in our original SAS Proposal and shown here in Illustration for convenience.⁵

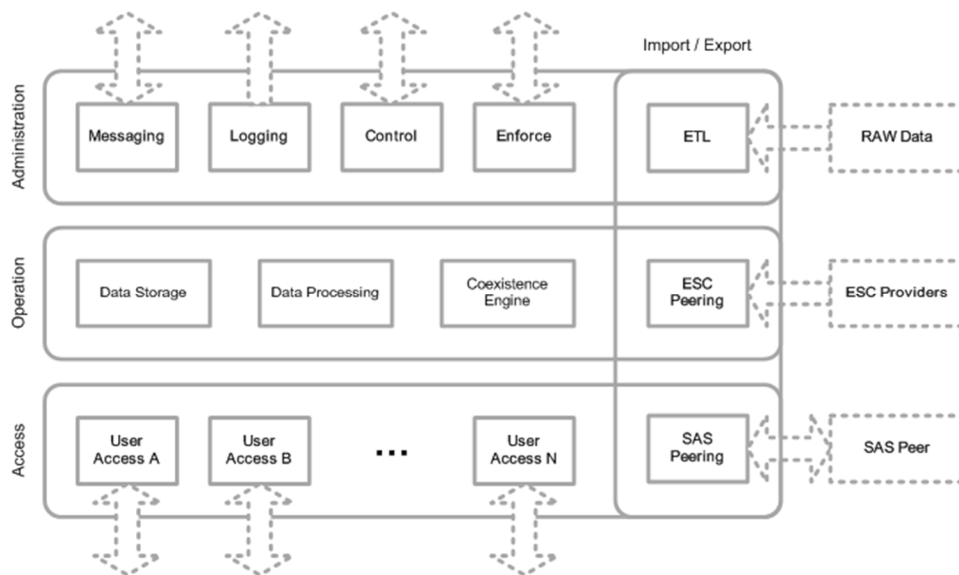


Illustration 2: A high-level, notional SAS Node architecture.

Referencing Illustration to further describe the data collection and organization strategy with an example, all logs, events and metrics referencing the *Coexistence Engine* module will be processed and organized together while all information related to the *SAS Peering* module will be processed and organized together but independently of the *Coexistence Engine* module. This organizing approach follows our general implementation strategy of developing SAS functional components as self contained software modules that inter-operate according to fixed interface contracts.

The collected information will be analyzed by module and by function to provide a comprehensive view of each SAS module plus a comprehensive evaluation of the SAS supporting a larger communications ecosystem.

For example, Key Bridge will provide a test report of the *Coexistence Engine* using data collected from all ICD use cases. The report will include tables, charts and graphs to describe the functions, performance and Part 96 compliance of this SAS module operating in isolation.

As another example, referencing Illustration 14 in the *Key Bridge SAS Proposal*, we will provide an ICD test report that details user access services such as a CBSD channel assignment transaction.⁶ This

⁵ See *Key Bridge SAS Proposal* at 5.3 SAS Node and Illustration 6: A high-level notional SAS Note architecture.

and other functional reports will combine captured information from all SAS components supporting the transaction and include tables, charts and graphs to describe the entire transaction process, its aggregate and component performance, and Part 96 compliance.

Key Bridge will provide all ICD reports to the Commission in one or more PDF documents plus in an easily browsed and searchable online format.

2 SAS operations

During ICD Key Bridge will typically provision and operate **two SAS instances per use case** operating in a master/slave high availability configuration. Additionally, Key Bridge will provision and operate two coequal **master SAS instances** supporting inter-client peering plus external peering and message exchange with other SAS administrators.

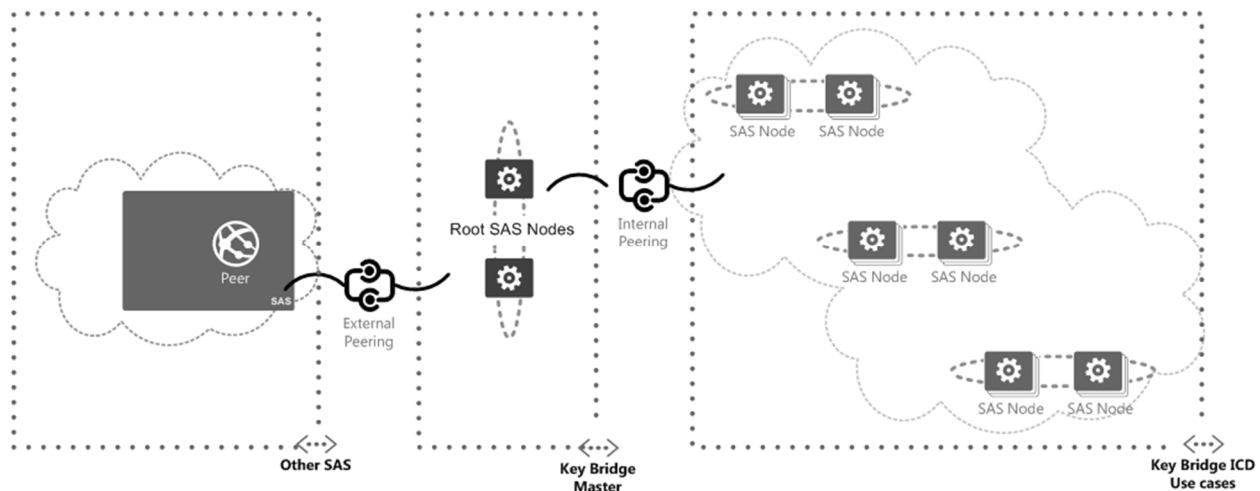


Illustration 3: Key Bridge ICD will evaluate a complete SAS configuration and ecosystem.

The Key Bridge SAS configuration for ICD is our configuration for normal commercial operations and will fully exercise and stress all aspects of the SAS, beginning with basic Part 96 conformance and compliance and extending to support the unique configuration and performance requirements of complex real-world communications scenarios.

All Key Bridge SAS instances operate on private or virtual private networks. No communication between Key Bridge SAS instances traverses the open Internet. Furthermore, all information exchanged between Key Bridge SAS instances is signed and encrypted to ensure strong counter-party authentication with message confidentiality.

6 See Key Bridge SAS Proposal at 6.4 SAS User Access Services. This section details how a CBSD channel query is processed and handled by the SAS in a single transaction, which SAS modules are involved, and what is their general function.

2.1 User Registration Process

Key Bridge SAS authorization is provided by the Java Authentication and Authorization Service (JAAS), the Java implementation of the standard Pluggable Authentication Module (PAM) information security framework. The Key Bridge SAS is configured by default to use Key Bridge's user access manager for user authentication and authorization. The SAS can also be configured to use a client's user authentication and authorization service via standard, open protocols, depending upon the client's preference.

During the ICD all SAS user authentication and authorization will employ Key Bridge own user authentication and authorization service and will benefit from Key Bridge's standard know your customer (KYC) processes.

During ICD a SAS administrator can create and pre-authorize new user accounts to access that administrator's SAS instance or instances. Alternatively, a SAS administrator can establish authorization criterion to accept users that have self-registered accounts with Key Bridge. Both account creation processes includes automated information validation followed by external information confirmation processes such as an emailed token or SMS message, as examples. Additional automated and manual identity validation steps can be added as required by the SAS administrator including the exchange of public and private cryptographic keys, the issuance of a shared secret token, or binding with a two-factor authentication provider, for example.

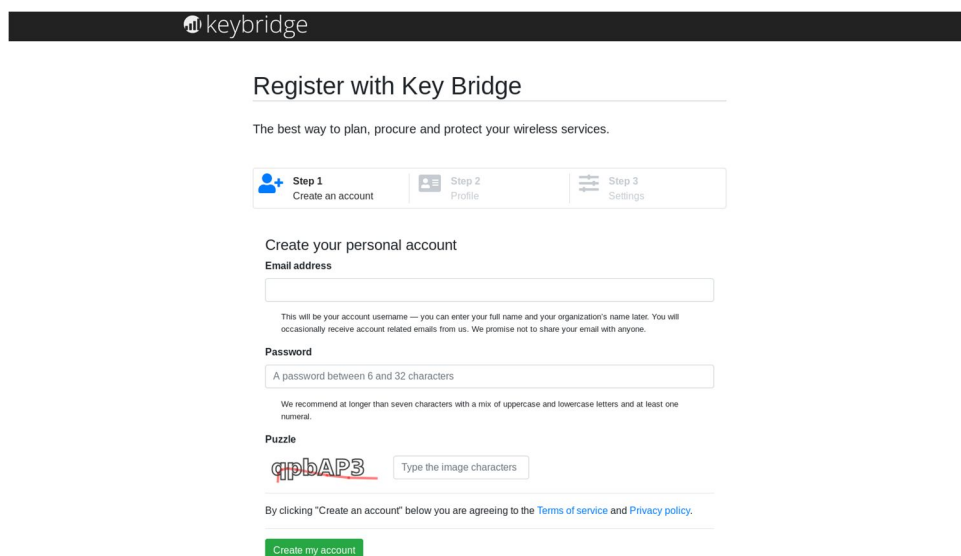
The image shows a web browser window with the Key Bridge logo at the top. The main heading is "Register with Key Bridge". Below it is a subheading: "The best way to plan, procure and protect your wireless services." There are three steps in a progress bar: "Step 1 Create an account" (active), "Step 2 Profile", and "Step 3 Settings". The "Create your personal account" section contains an "Email address" field with a note: "This will be your account username — you can enter your full name and your organization's name later. You will occasionally receive account related emails from us. We promise not to share your email with anyone." Below this is a "Password" field with a note: "A password between 6 and 32 characters" and a recommendation: "We recommend at longer than seven characters with a mix of uppercase and lowercase letters and at least one numeral." There is a "Puzzle" section with a CAPTCHA image and a "Type the image characters" input field. At the bottom, there is a note: "By clicking 'Create an account' below you are agreeing to the Terms of service and Privacy policy." and a green "Create my account" button.

Illustration 4: User accounts can be self-registered or created by the SAS administrator.

Different SAS instances support different client communities and, accordingly, each ICD client SAS instance is configured to only allow access for users authorized for that specific client community. Access authorization is locally administered in the SAS with account associations, roles and privileges established by the SAS administrator.

2.1.1 User sign in

Once an account is created and validated a user with the correct credentials can sign in to their respective SAS web portal using their user name and password, plus any additional authentication steps specific to their configuration such as cryptographic keys or entering a two-factor authentication token.

2.1.2 User account management

Key Bridge provides users with complete user account management functionality, including password reset, change and lost password recovery, security status, audit trail, access privileges, etc.

2.2 SAS-CBSD Communications

The SAS to CBSD communications and SAS data processing is described in detail in Section 6.4 of our SAS Proposal.⁷

In the Proposal we reference our intention to implement and employ protocols then under development within the Wireless Innovation Forum. The development of the SAS to CBSD protocol within the Wireless Innovation Forum is now completed.⁸ Our own software implementation is also completed and has kept pace with the various updates and improvements to this protocol.

During ICD our intention is to support only the most recently published version of the protocol.⁹

⁷ See *Key Bridge SAS Proposal* at Section 6.4 SAS User Access Services.

⁸ See The Software Defined Radio Forum Inc. *Signaling Protocols and Procedures for Citizens Broadband Radio Service (CBRS): Spectrum Access System (SAS) – Citizens Broadband Radio Service Device (CBSD) Interface Technical Specification*, WINNF-TS-0016 (*SAS to CBSD Protocol*)

⁹ At the time of this writing the current version of document WINNF-TS-0016 is v1.2.1 published January 03, 2018

2.3 Professional Installation

As no Certified Professional Installer (CPI) presently exists Key Bridge will test and evaluate our implementation of industry processes for ICD device registration and administration during ICD.

We will test a new process wherein already validated users may self-register as a certified professional installer. This process will include the completion of an online form, presentation of appropriate industry (e.g. WINNForum) standardized credentials and additional attestations.

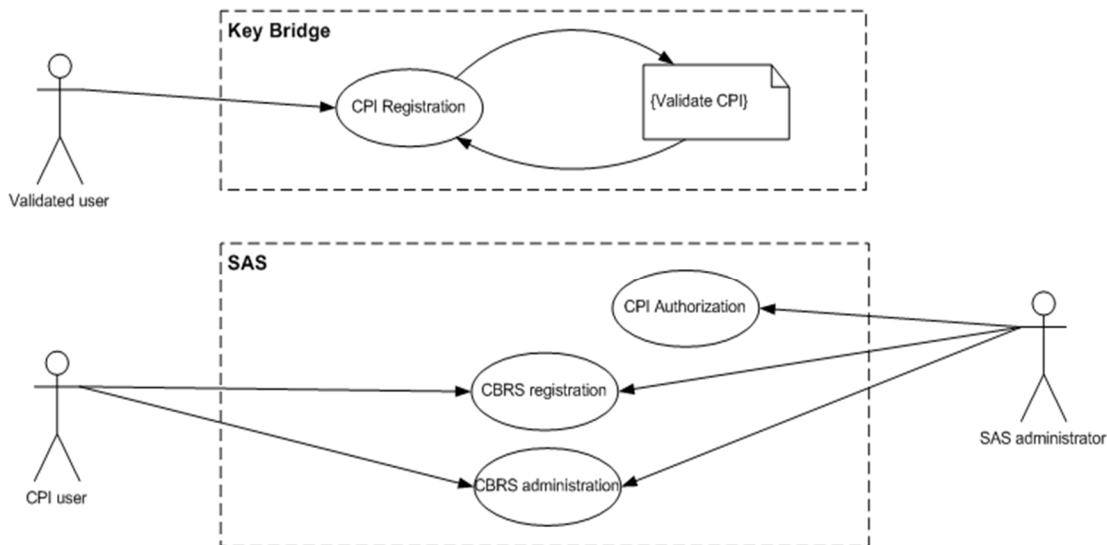


Illustration 5: Professional installers self-register with Key Bridge and are authorized by the SAS administrator.

Once established as a CPI by Key Bridge a SAS administrator can authorize the CPI user to configure CBSDs in the SAS.

Once authorized in the SAS the CPI user can access SAS resources for CBSD registration and administration, including web forms to enter individual CBSDs or web forms to upload bulk CBSD registration data files.

During ICD Key Bridge will provide active oversight of all CBSD registrations. Each device registration will be confirmed by Key Bridge to match the actual installed configuration prior to authorization for service.

2.4 SAS-SAS Interoperability

SAS to SAS interoperability and peering is described in detail in Section 7.3.2 of our SAS Proposal.¹⁰



Illustration 6: The Key Bridge SAS supports internal plus external peering and message exchange.

In the Proposal we reference our intention to implement and employ protocols then under development within the Wireless Innovation Forum. The development of the SAS to SAS protocol within the Wireless Innovation Forum is now completed.¹¹ Our own software implementation is also completed and has kept pace with the various updates and improvements to this protocol.

During ICD Key Bridge will seek to peer and to coordinate data sharing with other SAS operators, per their availability, using the most recent most recently published SAS-SAS peering protocol version.¹²

¹⁰ See *Key Bridge SAS Proposal* at 7.3.2 SAS to SAS Peering.

¹¹ See The Software Defined Radio Forum Inc. *Signaling Protocols and Procedures for Citizens Broadband Radio Service (CBRS): Spectrum Access System (SAS) - SAS Interface Technical Specification Document* (WINNF-TS-0096) at Section 5, SAS-SAS Procedures and Section 6, SAS-SAS Synchronization.

¹² As of this writing the current version of document WINNF-TS-0096 is v1.2.0 dated October 20, 2017.

2.5 SAS Utilization of Commission Databases

The Key Bridge general strategy for extract, transform and load (ETL) of Commission databases is detailed in our SAS proposal.¹³

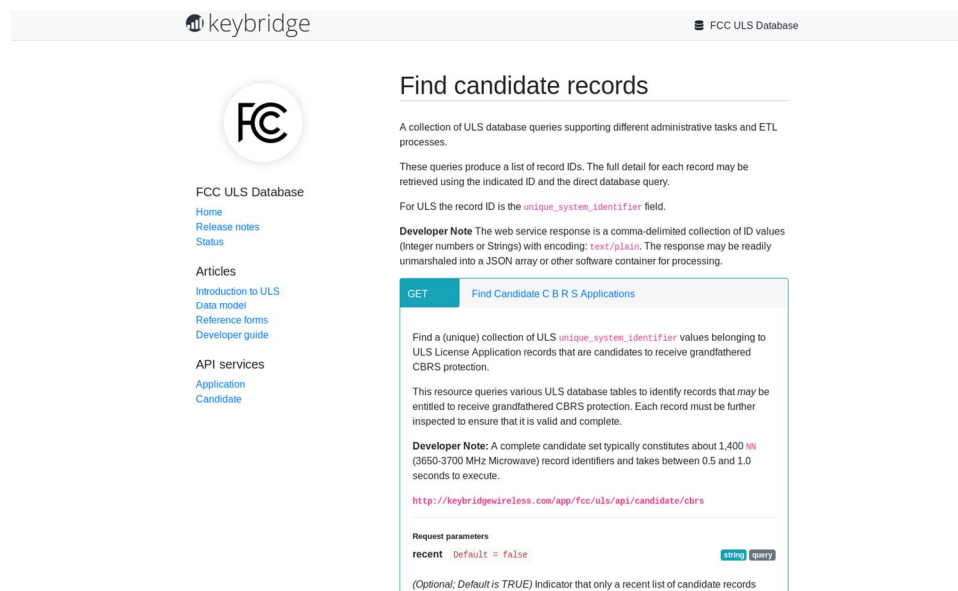


Illustration 7: Key Bridge maintains cleaned and normalized versions numerous FCC databases such as ULS.

Since 2010 Key Bridge has successfully operated a ETL capability that retrieves (i.e. extracts), processes (i.e. transforms) and imports (i.e. loads) data from the FCC's Universal Licensing System (ULS), Consolidated Database System (CDBS), Equipment Authorization System (EA) and International Bureau Filing System (IBFS) into our own local databases. All records imported from the FCC into Key Bridge database via ETL process are examined, cross-referenced and validated. Any invalid or inconsistent records are identified and logged, and these logs are shared with Commission staff. Over the years the Commission has benefited from this feedback generated by our rigorous data validation processes with thousands of records identified for correction and clean-up.

Key Bridge is presently developing additional ETL functions to copy other FCC data sources specific to CBRs operation. During ICD Key Bridge will continue to mirror all Commission databases and also import all newly published Commission data sources.

¹³ See Key Bridge SAS Proposal at 7.1.5 Extract-Transform-Load

2.6 DPA Protection

The Key Bridge SAS is “DPA Enabled” in conformance with the FCC’s DPA Waiver Order.¹⁴

Because DPA boundaries and DPA protection neighborhood distances are still being refined we have developed and maintain a dedicated resource specifically to ensure that all Key Bridge SAS instances have and utilize the most recent DPA configurations provided by DoD / NTIA.

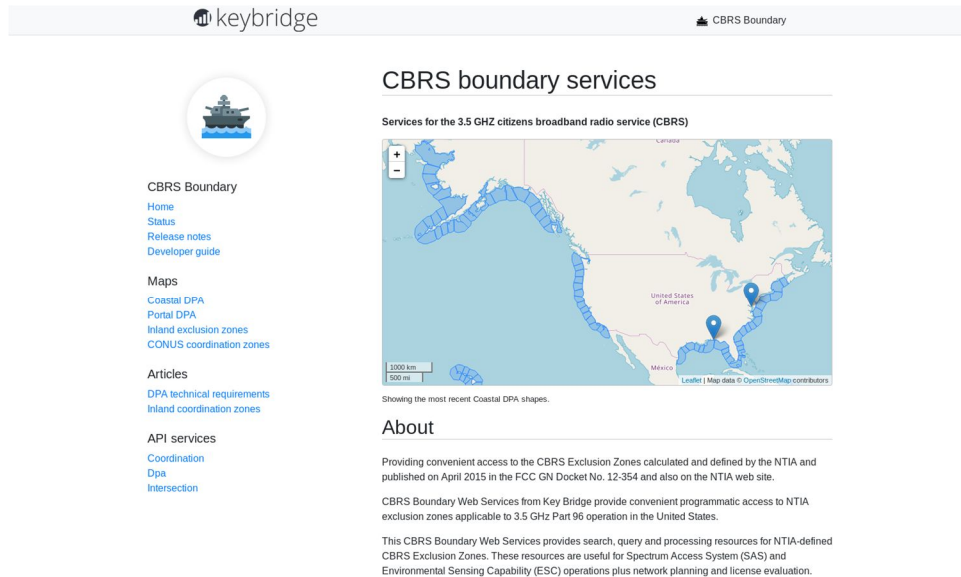


Illustration 8: Key Bridge maintains a centralized, publicly available repository for all officially published CBRS boundaries.

The Key Bridge SAS protects federal incumbents according to the agreed upon procedures identified in the most recent CBRS requirements and requirements document published by the Wireless Innovation Forum.¹⁵

Key Bridge implements the strategy for DPA protection and ESC sensor protection described in the *CBRS Requirements Document* under Section 4.1 SAS General Requirement at R2-SGN-03, R2-SGN-23 and R2-SGN-24, with calculated aggregate interference according to the procedures laid out at R2-IPM-03 thru R2-IPM-05, at minimum.¹⁶

¹⁴ See *Promoting Investment in the 3550-3700 MHz Band*, Order, DA 18-538 (WTB/OET May 22, 2018), 2018 WL 2387489 (*DPA Waiver Order*).

¹⁵ See The Software Defined Radio Forum Inc. *Requirements for Commercial Operation in the U.S. 3550-3700 MHz Citizens Broadband Radio Service Band; Working Document* (WINNF-TS-0112) (*WINNF Requirements Document*). As of this writing the most recent published version is 1.4.1 published January 16, 2018. As of this writing the most recent (un-published) working version is v1.5.0r5.0.

¹⁶ See *WINNF Requirements Document* at pages 11, 22, 23, 33, 34, respectively.

2.7 Incumbent Protection Implementation

Our strategy for protecting federal incumbent users is described in detail in Section 6.6 of our SAS Proposal, and protecting non-federal incumbent users is described in detail in Section 6.7 of our SAS Proposal.¹⁷ The Proposal was later supplemented with two method of procedure documents detailing our approach for protecting FSS Earth stations and grandfathered wireless services.¹⁸

During the ICD, CBRS operations will avoid to the extent possible all geographic areas where incumbent protections may be necessary. Regardless, Key Bridge will proactively coordinate with all parties to ensure stable and interference-free operations and will promptly response and work to mitigate any notice or complaint of interference.



Illustration 9: Key Bridge will generate emulated incumbent protection records for ICD.

Because the ICD configurations are selected specifically to avoid known incumbent operations it is unlikely any incumbent protection events will be triggered. To exercise this capability Key Bridge will therefore manually generate emulated incumbent operation records and manually insert these into the SAS to evaluate their influence of CBRS operations and to confirm correct, rules compliant behavior of all affected systems.

Key Bridge has already tested this process and will reuse software and processes from the WINNF test harness to generate and load emulated incumbent records into the SAS.

¹⁷ See *Key Bridge SAS Proposal* at Section 6.6 Protecting Federal Incumbent Users and Section 6.7 Protecting Non-Federal Incumbent Users.

¹⁸ See *Key Bridge CBRS Method of Procedure, Protecting FSS Earth Stations* and *CBRS Method of Procedure, Protecting Grandfathered Wireless Services*. Both filed 09/27/16 in GN Docket 15-319 in response to FCC response for supplemental information.

2.8 Interference Reports and Mitigation

Our strategy for accepting, processing and sharing reports of interference follows the DoD's Joint Spectrum Interference Resolution (JSIR) process and employs the DoD's Standard Spectrum Resource Format (SSRF).¹⁹ The Standard Spectrum Resource Format (SSRF) is a government specification published by the Military Communications Electronics Board and is issued under the authority of DOD Directive 5100.35. SSRF is aligned with the National Telecommunications and Information Administration (NTIA) Office of Spectrum Management's Data Dictionary (OSMDD) and the North Atlantic Treaty Organization (NATO) Spectrum Management Allied Data Exchange Format – eXtensible Markup Language (SMADEF-XML). The specification defines standard data elements for the automated exchange of radio-frequency (RF) spectrum-related data that includes, among other things, interference reports. The SSRF specification is formally endorsed by members of the Wireless Innovation Forum.²⁰

Key Bridge has implemented the SSRF interference reporting and JSIR (resolution) processes as a modular extension to our online ticketing and issue resolution system. For the ICD we will provision and administer a ticketing system instance dedicated exclusively for CBRS trials. We will use this resource to test and evaluate the efficiency of the SSRF and JSIR processes as they apply to commercial CBRS operations.

During the ICD we do not anticipate interference complaints will be raised by a CBSD device or network owner or user. However the ticketing system supports web-based tools to enable reporting of interference incidences by any concerned party and will raise reported events to the attention of SAS administrators via an online portal plus using conventional messaging such as email and text messaging.

During ICD the Key Bridge SAS administrator will be directly responsible and accountable for accepting and promptly resolving any reports of interference.

¹⁹ See *Key Bridge SAS Proposal* at Sections 11 and 12 Appendix.

²⁰ See The Software Defined Radio Forum Inc. *Endorsement of Standard Spectrum Resource Format*. (WINNF-14-R-0019) version v1.0.0 published January 12, 2015. Filed 09/27/16 in GN Docket 15-319 in response to FCC response for supplemental information.

3 Public field trial

Key Bridge proposes to provision and manage a complete spectrum access system and portal for public experimentation and evaluation. The SAS will be configured to support user self-registration and configuration of all aspects, including limited administration. The SAS database will be populated with a collection of thousands of software emulated CBRS devices and other CBRS components configured to provide emulated broadband commercial wireless Internet across a multi-state region.

The specific use case is broadband wireless Internet and the evaluation results will be generally applicable to any type of CBRS data service including wireless Internet, enterprise and campus data, public safety communications, and home networking, as examples.

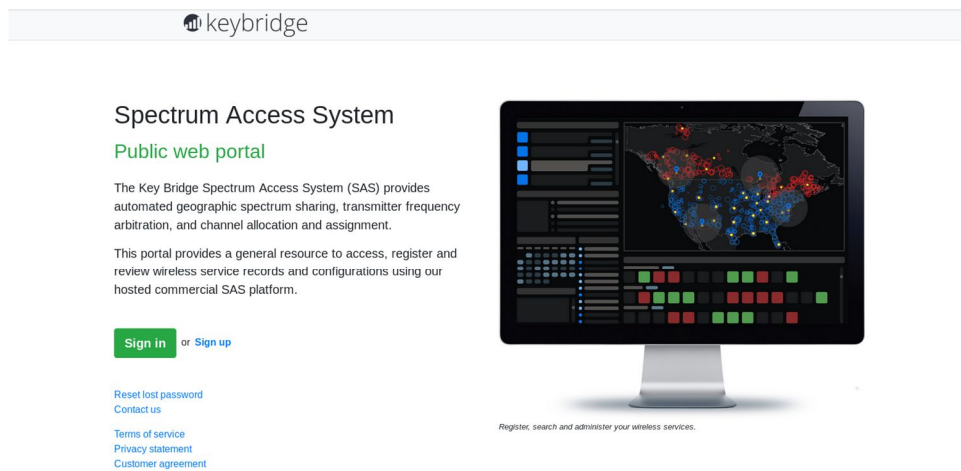


Illustration 10: The SAS web portal provides public access to SAS data and features.

Most CBRS infrastructure – and spectrum access systems in particular, will typically be invisible to the public user. Once deployed the public will rarely have an opportunity to see a SAS in operation, explore how a SAS is configured and administered, or evaluate how a SAS performs and responds to user configurations and input.

This generic ICD configuration will allow us to evaluate all aspects of the SAS, from the new user onboarding process, SAS portal security, user interface aesthetics to how the SAS supports large numbers of users each making simultaneous configuration changes while attempting to establish and preserve a stable spectrum environment for emulated wireless devices. We will specifically evaluate:

- User self-registration. We will evaluate how users can self register accounts with Key Bridge, receive or exchange security credentials, and use those credentials to access a spectrum access system portal.
- System load. We will pre-provision a complete SAS instance with thousands of emulated CBSDs controlled by fully functional software agents. Registered users may then modify CBSD

configurations, delete CBSDs, create and provision new CBSDs, and manipulate existing CBSD operating channels and status.

- System integrity. We will evaluate how various CBRS processes, implemented in the SAS as complete, isolated transactions, interact with each other by blocking, queuing and pipelining system resources. We will evaluate how different processes compete for common resources and ensure correct or expected behavior sequences.
- User interface. We will confirm correct user interface configuration and programming, and identify any UI bugs or issues where necessary information is not presented or incorrectly rendered.

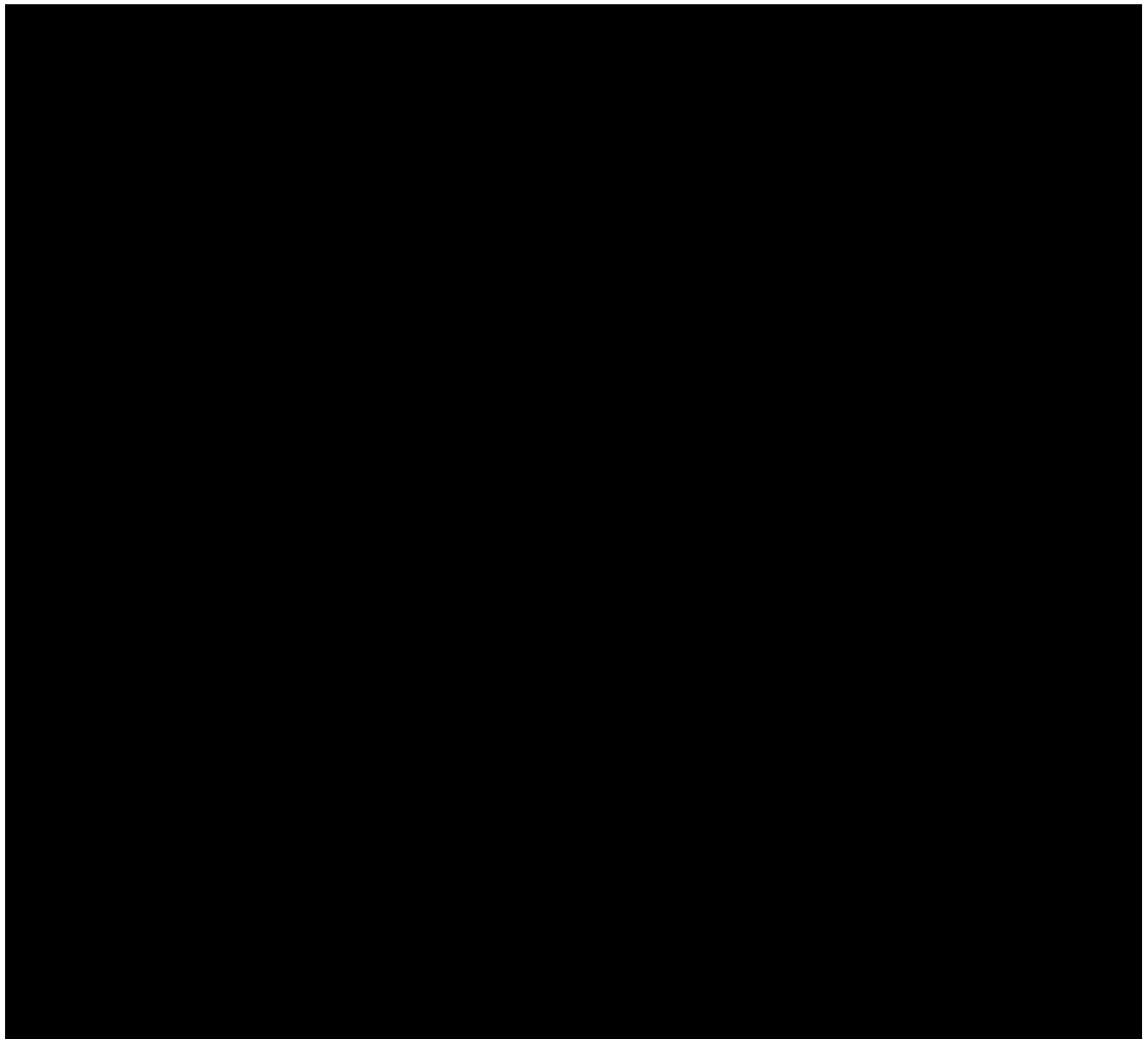
3.1 Field trial configuration

In this initial commercial deployment Key Bridge proposes to provision and operate one self-contained spectrum access system with a database containing numerous pre-provisioned CBSDs. The SAS will communicate via direct network connection with a second server emulating the CBSDs as independent and autonomous software agents.

In addition to the preceding descriptions for Part 96, Subpart F conformance, this initial commercial deployment will include the following unique configurations.

SAS-CBSD Communications	<p>CBSDs for this scenario are emulated software agents and will not transmit RF energy in any way. CBSD agents communicate with the SAS via standard protocols.</p> <p>Users will be able to add, edit and remove CBSD registrations. Users will be able to set and update CBSD channels and evaluate how those changes affect neighboring devices and the aggregate spectrum environment.</p>
SAS-SAS Interoperability	<p>The public field trial SAS will be provisioned in a self-contained virtual private network and will not transmit information to any external systems.</p> <p>SAS-SAS interoperability will not be evaluated on the public field trial SAS.</p>
DPA Protection	<p>In support of the public field trial Key Bridge will provide a separate capability to manually enable and disable individual DPAs. The SAS will be configured to reset all user configured DPA status on a daily basis.</p>
Incumbent Protection	<p>The public field trial SAS will include a special administrative</p>

Implementation	<p>capability to manually create new incumbent records and then to add these records to the SAS database to enable their protection.</p> <p>The SAS will be configured to purge all user created incumbent protection records on a daily basis.</p>
Interference Reports and Mitigation	<p>Users may freely create, edit and respond to entries using the interference reporting system. This will be configured so that users can experiment with the capability and provide constructive feedback.</p> <p>Key Bridge will not monitor or respond to interference reports created on the field trial SAS.</p>



[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

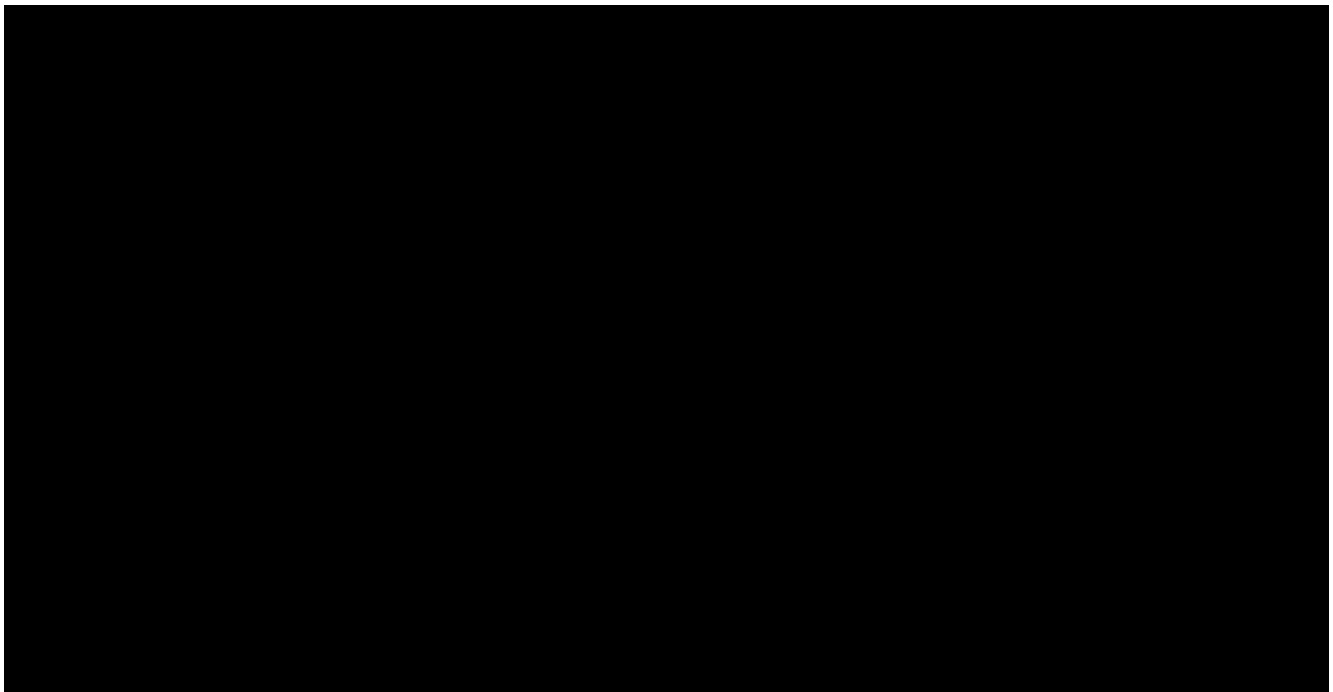
[REDACTED]

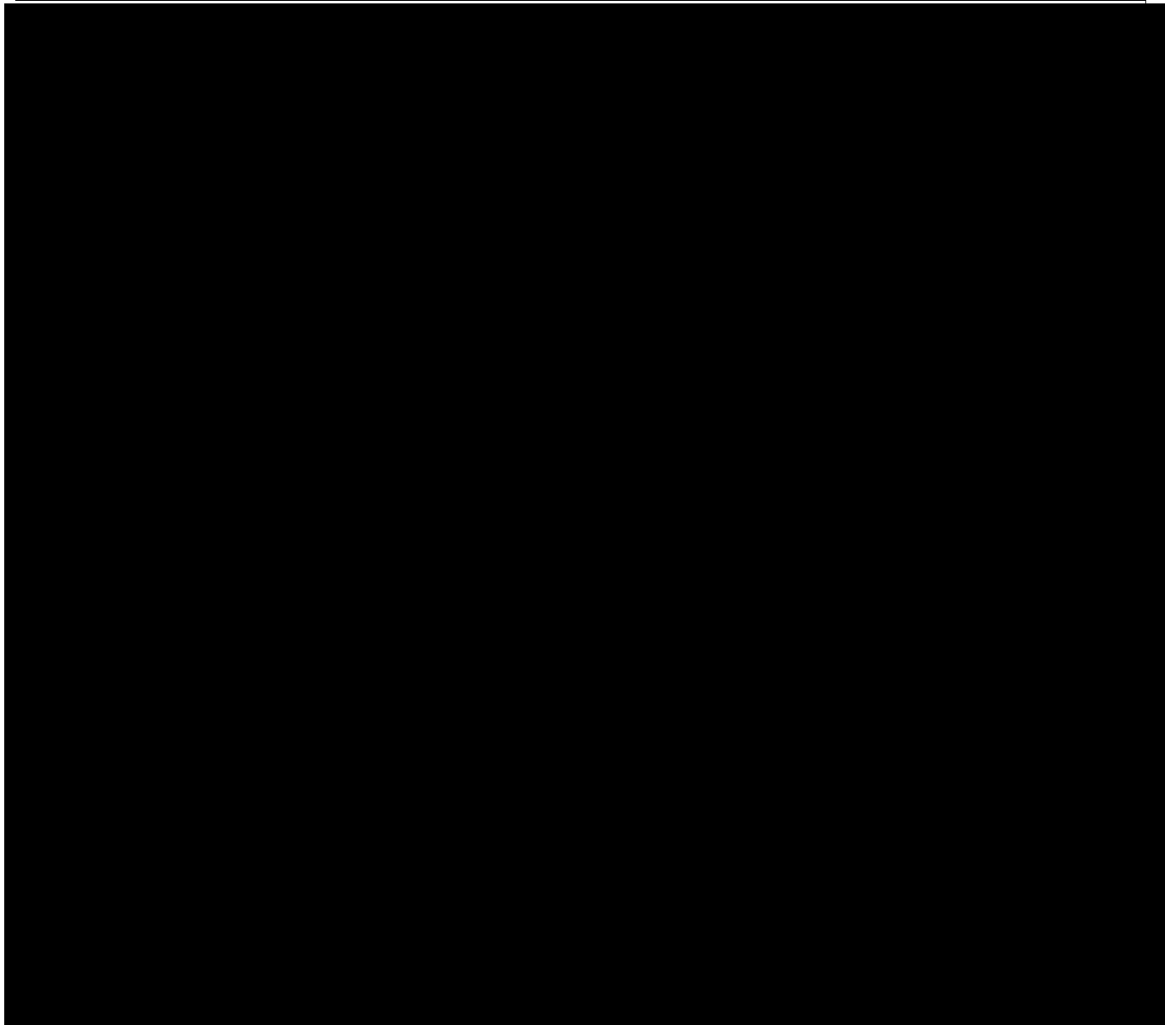
[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]





[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]



5 Conclusion

Key Bridge applauds the Commission's leadership and steady progress towards a successful launch of CBRN services in the United States. We are pleased to submit this supplement to our original proposal to administer a Spectrum Access System (SAS) in the 3.5 GHz frequency band. We are happy to provide any additional information and detail the Commission may require to evaluate this proposal.

We believe that the public field trial and each of the ICD projects described in this proposal will contribute essential data and help the Commission to fully evaluate commercial operation of the SAS. We kindly request the Commission to review and approve each.

We believe eight to 10 weeks is sufficient time to produce a substantive and meaningful report for the Commission, and we are prepared to begin ICD testing as soon as the Commission will allow.

/s/

Jesse Caulfield, CEO

Key Bridge Wireless LLC

__END__