Data Exchange for Remote Identification Cohort Documents- Index

From: Jenniss, Stephen (FAA)
Sent: Tuesday, January 21, 2020 1:44 PM
To: Jacob Ruytenbeek
Cc: Harrison, Tenisha (FAA); Nair, Casey (FAA); Yezzo, Christine (FAA)
Subject: Airmap RemoteID Memorandum of Understanding Executed
Attachments: FAA UAS Remote ID Data Exchange ConUse v1.0.pdf; FAA_MOU_Remote ID_FINAL_fillable (AirMap 1.7.20) executed.pdf

Follow Up Flag: Follow up
Flag Status: Flagged

Welcome to the Remote ID RFI Cohort! Please find attached a fully executed MOU regarding your participation. Also find attached the Remote ID Concept of Use (ConUse) for "FAA Data Exchanges with UAS Service Suppliers". This document will frame the discussions of the Remote ID Cohort; note the FAA's recently released FAA NPRM for Remote ID will not be discussed, please place your comments on the proposed rule in the Federal Register. The first cohort meeting is scheduled for 26-27 February in the Washington, D.C. area. Subsequent meetings are planned approximately monthly for 24-25 March, 28-29 April, 27-28 May, and so on moving forward throughout the year. The FAA requests that each participating organization send nominally three representatives in person to each meeting to cover the areas of program management, technical implementation, and legal issues. Cohort meetings will likely subdivide into working groups as needed. Please come to the first meeting prepared to discuss:

- How Remote ID USSs and the FAA will interface to implement Remote ID
- How Remote ID USSs will share data with the general public
- USS Governance: MOA, Performance Rules, privacy and data protection, etc.
- Technical performance such as capacity, quality of service, availability

Additionally, effective immediately, administration of these MOUs will be handled by Contracting Officer Tenisha Harrison; FAA ACQ-350. Please contact Tenisha Harrison at [redacted] for all related matters to this Cohort.

The FAA looks forward to working with you on this initiative.

Thanks,
Steve Jenniss
Contracting Officer
Acquisition & Grants Division, AAQ-630
W J Hughes Technical Center
Atlantic City Int'l Airport, NJ 08405
[redacted]

FAA ATO

Remote Identification (Remote ID) of Unmanned Aircraft Systems

Concept of Use (ConUse):

FAA Data Exchanges with UAS Service Suppliers (USS)

17 January 2019

Version 1.0

Revision History

Version	Description
1.0	First release.

Contents

Index of Figures

1 Introduction

1.1 Background

Unmanned Aircraft Systems (UAS) are part of a burgeoning industry for both private and public actors to accomplish a variety of tasks including package delivery, search and rescue operations, aerial inspections, real estate activities, media activities, disaster response, and recreational activities. UAS are rapidly being integrated into the National Airspace System (NAS). The FAA is using a risk-based approach to determine which UAS can operate safely in the NAS and using a phased incremental approach to establish operational requirements pursuant to statutory authority granted by Congress.[1]

Beginning in 2016 with the publication of 14 CFR Part 107, Operation and Certification of Small Unmanned Aircraft Systems ("Part 107"),[2] the FAA has enacted regulations and programs to integrate UAS into the NAS. One such program is the Low Altitude Authorization and Notification Capability (LAANC), which allows Part 107 and (as of 2019) recreational flyers[3] to request and receive automated access to fly in controlled airspace.[4] However, due to the growing presence and potential utility of UAS, more programs and capabilities are needed.

The backdrop to any integration of UAS into the NAS is the safety of the general public. Safety is the most important aspect of the FAA's role in aviation. The next step in safe integration is Remote Identification (Remote ID) for UAS. Section 376 of the FAA Reauthorization Act of 2018[5] requires the FAA to assess remote identification of UAS for risk reduction and mitigation. The FAA recently published a Notice of Proposed Rulemaking (NPRM) for Remote Identification of Unmanned Aircraft Systems.[6]

Successful implementation of Remote ID will provide identification of UASs flying in the NAS, which will help promote public safety and increased efficiency of the NAS. Remote ID is also a step toward future UAS capabilities including UAS Traffic Management (UTM), beyond visual line of sight (BVLOS), and automated operations.

1.2 Problem Statement

1.2.1 Remote ID in General

No standardized, regulated remote identification scheme currently exists for UAS. Remote Identification is a necessary step in integrating UAS into the NAS. Remote ID would allow for better FAA awareness of unmanned aircraft flying in the airspace and would assist the FAA, law

---

[1] See 49 U.S.C. § 44807

[2] See 81 FR 42063 and 14 CFR Part 107 for complete rule

[3] See 49 U.S.C. § 44809

[4] Specifically: Class B, Class C, or Class D airspace or within the lateral boundaries of the surface area of Class E airspace designated for an airport.

[5] See FAA Reauthorization Act of 2018, Pub. L. 115-254 (18/10/2018)

[6] FAA, NPRM "Remote Identification of Unmanned Aircraft Systems," Federal Register 84 FR 72438, 12/31/2019.

enforcement, and security agencies to carry out their duties with respect to UAS operations. Remote ID would also assist the public by making UAS identification generally available, increasing transparency and proper accountability.

1.2.2 Data Exchanges in Specific

If Remote ID is to be effective in the decades ahead, it would need to be built on a foundation of modern, flexible, well-accepted technology. Data exchanges frame this challenge in the context of a constantly connected world. The implementation of Remote ID would need to specify the technical details of how these data exchanges should be constructed and operated.

Furthermore, data exchanges address another Remote ID problem: what stakeholder architecture should be used to deploy the Remote ID capability? (That is, what would the division of roles be among stakeholder systems and interactions?) Data exchanges have proven effective on recent programs such as LAANC by creating options for commercial providers meet the needs of the flying public and interested parties in partnership with the FAA.

1.3 Purpose

This Concept of Use (ConUse) is intended to address the technological capabilities of Remote ID, specifically, what data exchange programs and systems would the FAA need to define to realize the Remote ID capability? The FAA expects to establish partnerships and technical arrangements (networks, software, interfaces, etc.) to fulfill the technological requirements of a Remote ID capability. In particular, this ConUse focuses on the technological requirements of "network Remote ID." Network Remote ID refers to internet-based data exchanges between operating UAS, UAS Service Suppliers (USS), and recipient stakeholders such as the FAA, other federal agencies, and local authorities. Network Remote ID is intended to be available wherever Remote ID-equipped UAS are able to connect to the internet to transmit Remote ID messages.

The intended audience for this ConUse focuses on stakeholders that would connect with FAA network Remote ID systems, primarily UAS Service Suppliers (USSs) intending to provide remote ID services to UAS pilots.

The primary purpose of this ConUse is to drill into the high-level requirements for network Remote ID data exchanges. This ConUse illustrates different users of Remote ID and how this new capability would interact with them. This ConUse assumes the conditions as proposed in the Remote ID Notice of Proposed Rulemaking (Remote ID NPRM), but the FAA recognizes that these conditions and requirements may change following public comment and the development of a Final Rule. As the Remote ID concept matures, this ConUse will be adjusted accordingly to provide a context in which to discuss decisions and tradeoffs in the implementation of the technology that supports the Remote ID rulemaking.

1.4 Scope

This ConUse focuses on developing technical requirements for the FAA network-connected aspects of Remote ID. For the purposes of this ConUse, elements of the proposed framework for Remote ID such as proposed operating or manufacturing requirements are incorporated into this ConUse as assumptions that are subject to change following the notice and comment process and finalization of the Remote ID rule.

There are several related capabilities (beyond Remote ID) which may be mentioned but are fundamentally out of scope for this document. These include detect-and-avoid (DAA), beyond visual line of sight (BVLOS) operations, and UAS Traffic Management (UTM). Although Remote ID may be an initial building block for some of these capabilities, this ConUse does not provide any authoritative definition of these capabilities.

Finally, as specified in the Remote ID NPRM, the proposed requirements of the proposed Remote ID rule are independent of other statutes and regulations that may be binding on UAS operators and related parties. For example, complying with the proposed Remote ID rule would not change the requirement for a commercial operator flying a small UAS to also comply with 14 CFR Part 107. Remote ID compliance discussed in this document should not be interpreted as replacing any other regulatory requirements.

2 Referenced Sources

- Federal Aviation Administration, Notice of Proposed Rulemaking "Remote Identification of Unmanned Aircraft Systems," Federal Register 84 FR 72438, 31 December 2019
- Federal Aviation Administration, Advisory Circular: 107-2, "Small Unmanned Aircraft Systems (sUAS)", 21 June 2016
- Federal Aviation Administration, "Integration of Unmanned Aircraft Systems into the National Airspace System, Concept of Operations v2.0", September 2012
- FAA Reauthorization Act of 2018, Pub. L. 115-254 (Oct. 18, 2018)
- FAA Extension, Safety, and Security Act of 2016, Pub. L. 114-190 (July 15, 2016)
- FAA ANG-C2, "Remote ID Use Cases For Request for Information Package", Version 1.0, 17 December 2018

3 Operational, Technological, and Strategic Context

3.1 State of UAS Identification

Figure 1: UAS identification relative to other transportation

The UAS era is in full swing in the U.S. and is only expected to continue growing rapidly. The FAA's Aerospace Forecast FY 2019-2039[7] estimates over a million UAS in the private and commercial fleet in 2019 and another million will be added by 2023. Furthermore, fleet composition will shift strongly from occasionally-used private UAS to business-driven commercial UAS. Fueled by smarter, smaller, cheaper flight systems, new applications continue to emerge and mature, from agriculture to package delivery. However, new UAS capabilities come with new potential for harm. An incident at Gatwick in December 2018 demonstrated how a single UAS could disrupt the lives of over 100,000 people and cost airlines alone over $60 million.

Proposed UAS identification involves many industry, government, and private stakeholders. Remote identification would need to be produced for recreational operations, commercial operations (e.g. survey, agriculture), emergency services, law enforcement operations, and so forth. Remote identification information would be consumed for purposes such as infrastructure protection, manned flight, law enforcement, and airspace awareness.

The FAA is responsible for regulating and developing policy to ensure the safety and efficiency of navigable airspace. This includes regulations to identify and protect aircraft, protect individuals and property on the ground, use navigable airspace efficiently, and prevent collisions between aircraft.[8] On 31 December 2019, the FAA published the Remote ID NPRM, proposing requirements for the remote identification of unmanned aircraft systems. This document provides a conceptual overview of the technical underpinning for remote identification as proposed in that NPRM. The proposed capability uses both broadcast technology using unlicensed radio spectrum ("broadcast"), and modern information exchange to a network of UAS Service Suppliers (USS) over the internet ("network").

The network Remote ID concept incorporates elements such as:

- USS-to-FAA data exchanges,
- information management and privacy policies, and
- roles and responsibilities for interagency (and federal, state & local) interconnections.

---

[7] FAA, 2019. "FAA Aerospace Forecast: Fiscal Years 2019-2039", Document #TC19-002.

[8] See 49 U.S.C. § 40103

The range of Remote ID data exchange stakeholders and considerations calls for rigorous, detailed concept design.

3.2 Near-Term Solution Can Leverage Existing Technologies

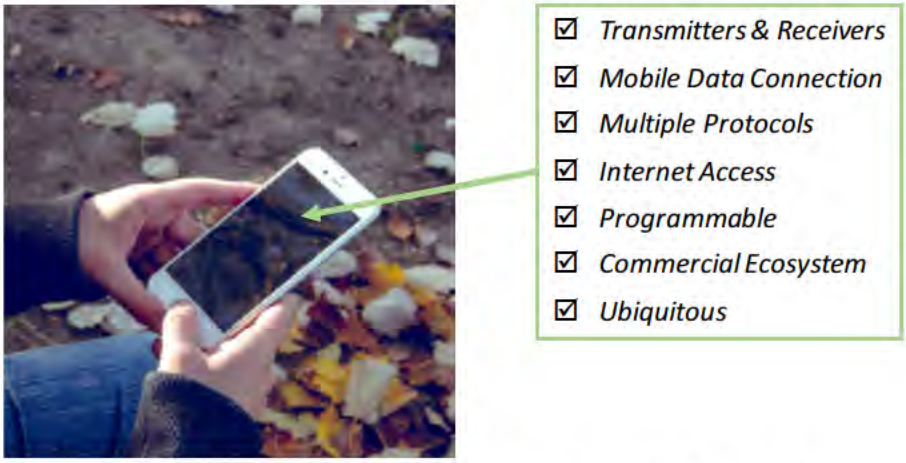


Figure 2: Existing technology offers foundation for Remote ID

Initial Remote ID technical elements focus on leveraging existing technology. There are many reasons to do so:

- **Achieving initial capability more quickly:** Technical standards typically require years to complete, followed by fabrication, testing, and qualification periods. If existing protocols and components can be used, Remote ID will reach initial capability much faster.
- **Reducing the cost of concept development:** The cost of new and customized parts is much higher than the cost of mass-produced components. Although Remote ID is in the concept exploration phase, the capability can be matured with low-cost and readily available technology.
- **Technological alignment:** Critical elements of Remote ID align with existing technologies. Mobile networking is already ubiquitous in vast areas. As demonstrated by LAANC, system-to-system exchanges of UAS operations information is highly compatible with internet and cloud infrastructure.

3.3 Leverage a USS-Centric Architecture

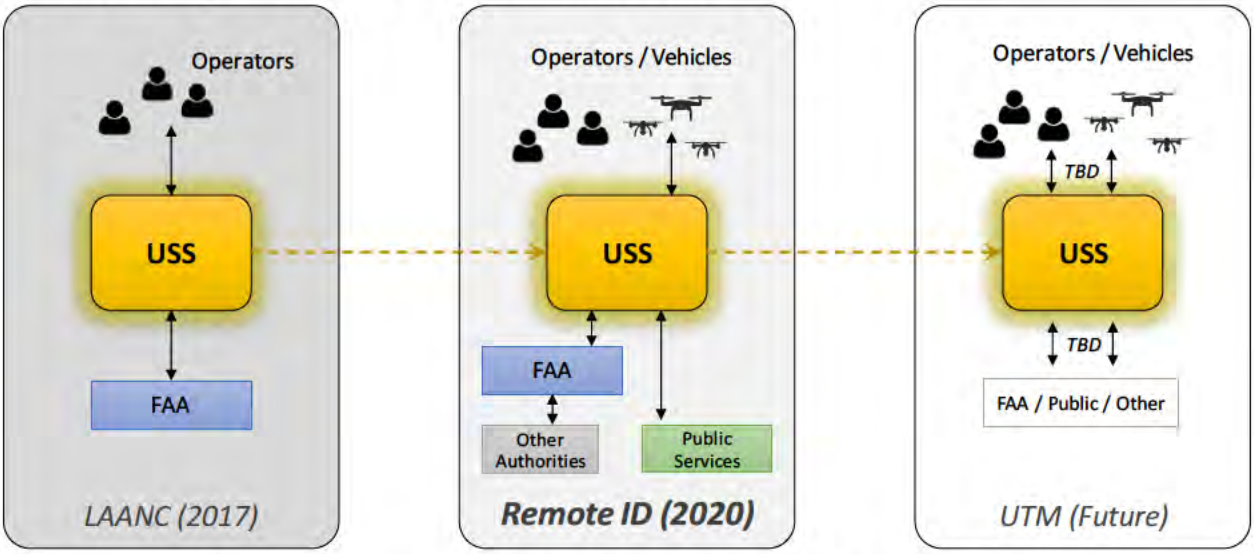


Figure 3: The UAS Service Supplier (USS) is central to recent capability architectures

In the interest of governance efficiency and stimulating commercial development, the FAA has increasingly made efforts to introduce capabilities in the framework of a public-private collaboration. In the UAS domain, this has produced the concept of UAS Service Suppliers (USSs), which are entities which are qualified by the FAA to provide specific UAS related services to the UAS community. The USS model has been implemented in LAANC (a fielded capability) and designed into current UTM initiatives.

Based on the success of the USS model, the FAA is investigating Remote ID capabilities with USSs as a fundamental building block. Provided that the capability architecture ensures the information exchanges, non-government roles such as USSs are beneficial and desirable. Several aspects of the proposed Remote ID capability draw on the precedent of LAANC:

- **USSs interface directly with operators, rather than the FAA interfacing directly with operators.** This has proved effective in LAANC, as USSs can rapidly introduce and evolve a diverse ecosystem of operator-facing interfaces that are customized and packaged for various operator subgroups.
- **The FAA would define and manage common requirements for USS qualification.** A combination of signed agreements as well as performance and technical requirements ensure that USSs fulfill their responsibilities within their defined role.
- **The capability can be defined in terms of information exchanges, in which USSs can be successfully integrated as a broker.** Operators provide certain information to USSs, USSs provide certain information to FAA, and FAA provides certain information to other federal government partners.

The Remote ID NPRM proposes connection to Remote ID USSs as an operating requirement for UAS operators; therefore, this ConUse examines the role of a network Remote ID USS as part of the concept architecture. Network Remote ID USSs link operators and operator systems with FAA Remote ID systems via APIs accessible over the internet. Consequently, Remote ID USSs

are vital stakeholders in the Remote ID capability development process, both representing their commercial interests and, by extension, the interests of the operators they serve.

4 Major Uses of Network Remote ID

4.1 End Use Actors

4.1.1 UAS Pilots

This ConUse assumes that for network Remote ID, the UAS pilot would source the original data that feeds the overall capability. In this role, the pilot would have certain responsibilities, such as:

1. Only fly with compliant equipment.
2. Ensure that equipment is functioning properly.
3. Connect over the internet to a Remote ID USS.

Flying with compliant equipment would mean purchasing and using UAS that have been manufactured to meet performance requirements enumerated in the Remote ID rule. For the purposes of this ConUse we assume Remote ID UAS would be manufactured to meet the performance requirements as proposed in the Remote ID NPRM, but recognize that these requirements may be subject to change in the Final Rule. Individual Remote ID UAS would be registered with the FAA by manufacturer, model, and serial number. We expect that following the compliance dates of the Final Rule for Remote ID, some remote pilots would continue to fly functioning legacy (pre-Remote-ID) UAS, however pilots would be responsible for operating within the regulatory requirements for UAS without Remote ID (e.g. at an FAA-Recognized Identification Area – FRIA).

Pilots are ultimately responsible for flying a drone that is transmitting the Remote ID message and so would be required to observe any self-test or status indications built into the UAS designs that would alert them to a change in Remote ID capability. Example indications could include:

- Network: “Connected”, “Searching”, or “Fault”
- Internet: “Connected” or “Not Connected”
- USS: “Connected” or “Not Connected”

UAS with faulty network Remote ID functionality would not be allowed to operate, unless they are operated within the rules applicable to non-equipped UAS (e.g. at a FRIA/Part 89 Site). Intentionally tampering with Remote ID capabilities would be a violation of the proposed rule.

Concerning network coverage, pilots would have a responsibility under Remote ID to connect to a USS over the internet. This would often mean mobile data access of some type. For example, if a standard Remote ID UAS connects to the internet using LTE, the pilot would be responsible to acquire a corresponding LTE plan. Similarly, if a Remote ID UAS design relies on integration with a smart device (e.g. phone or tablet) that has internet access, the pilot would be responsible to ensure that he or she is using a compatible smart device before conducting an operation with the standard or limited Remote ID UAS. (Standard and limited Remote ID UAS types are covered in Section 5.2.) Future Remote ID configurations could include designs that include

network access and coverage in the UAS purchase, which could make things simpler for pilots. This topic is discussed further in Section 5.4.

4.1.2 National Security and Law Enforcement

Figure 4: UAS enforcement faces unique difficulties

The FAA would be able to use remote ID data to fulfill its role as the civil enforcement authority for the airspace. Additionally, remote ID data would be useful for various federal, state, and local authorities to assist them with threat discrimination. Furthermore, four Federal departments have the authority to deploy counter-UAS systems to detect and mitigate threats posed by UAS.

Law enforcement authorities need effective ways to access and use Remote ID information. There are three major avenues to provide this information: (1) by receiving broadcasts directly using local hardware, (2) through inter-agency sharing, and (3) through a commercial service. Broadcast Remote ID is not detailed in this ConUse; inter-agency sharing and commercial services are part of the data exchanges described in this ConUse.

4.1.3 General Public

There are a range of reasons why members of the general public might have a legitimate need for public Remote ID information:

- Reporting unsafe and/or illegal flight,
- Reporting property violations, and
- Gaining awareness of local traffic for potential conflicts.

Private citizens could subscribe to services connected to Remote ID that focus on providing public information relevant to their concerns – such as displaying local drone traffic. This type of service would consolidate information from Remote ID USSs and/or other sources and contextualize it. For example, a private citizen could have a web portal that shows local drone activity and SMS alerts for activity in particular areas of concern. Drone activity is generally benign. Nonetheless, a capability such as this serves to inform the general public in appropriate ways.

General public users may include:

- Homeowners

- Property managers
- Infrastructure operators (power plants, factories, etc.)
- Commercial (farms, tourism attractions, etc.)
- Etc.

4.1.4 Other Manned and Unmanned Pilots

Figure 5: Especially in certain areas, UAS/manned conflict risk is substantial

Network Remote ID provides a basis for wide-area situational awareness. Manned aircraft and associated users could procure services from USSs tailored to providing public Remote ID information within space and time boundaries relevant to their flights. For example, a fleet of manned aircraft could set up services that notify a dispatcher (and/or provide a display) of all UAS operations within 10 miles of their flight trajectories. This would give the operator advanced notice of unusually high UAS densities.

4.2 Intermediary Actors

As a general capability architecture, each of the boxes in Figure 6 is an intermediary for Remote ID.

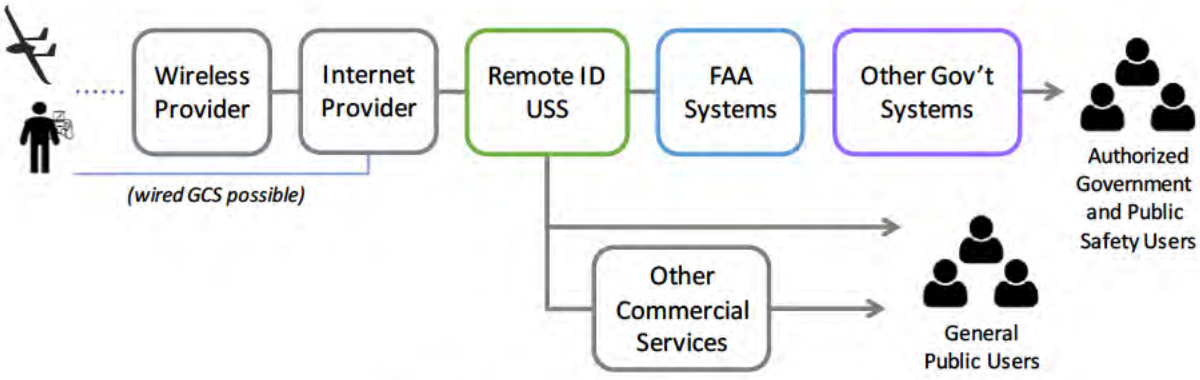


Figure 6: Remote ID Intermediaries

Each intermediary is discussed in the following sections.

4.2.1 Wireless and Internet Providers

Typically, the first link between UAS and Remote ID networks would be a wireless provider. (Note that the UAS ground control station (GCS) could have a wired connection. In that case, wireless provisioning is bypassed.) Wireless providers may or may not offer services specifically for UASs or Remote ID. In many cases, Remote ID may operate over standard mobile data networks– the wireless provider may be unaware that Remote ID data (in particular) is passing over the connection. On the other end of the spectrum, wireless services could be integrated with Remote ID USS offerings. See Section 5.4 for more detail.

The next intermediary link would be an internet provider. An explicit connection to the internet is necessary for Remote ID, as Remote ID USSs offer their interfaces on the internet (see NPRM). In many cases, internet provision could be integrated with wireless provision. The conventional example of major mobile data carriers (LTE, GSM, 3G, 5G, etc.) illustrate this model – members of the general public can procure services that give them access to a mobile network and the internet (via that network) under a single provider plan.

Wireless and internet services would not necessarily be integrated, especially looking forward to long-term Remote ID configurations. For example, the wireless UAS connection could be a high-performance command and control (C2) link with a separately configured internet provider.

The FAA would not directly regulate wireless or internet provider services as used for Remote ID. However, the FAA would make determinations as necessary concerning whether or not a particular wireless and/or internet provider service (or class of services) is acceptable for Remote ID compliance.

4.2.2 Remote ID UAS Service Suppliers (USSs)

The Remote ID UAS Service Supplier (USS) would be the critical intermediary for the network Remote ID concept. Remote ID USSs would be qualified by the FAA to offer remote ID services and would serve as a link between UAS and FAA systems. Only qualified Remote ID USS could serve in this capacity. Remote ID USSs fulfill Remote ID regulatory requirements on behalf of the pilots that utilize their services.[9]

In order to be qualified as a Remote ID USS, the entity would have to agree to certain rules and procedures. The USS would be required to provide certain data streams, protect certain data, and retain certain data for possible later queries from the government. Once a Remote ID USS is qualified by the FAA, it would be able to offer remote ID services to UAS operators.

Although the largest and best-known Remote ID USSs may serve the flying public in general, some Remote ID USSs (commercial or governmental) may choose to offer services solely to their own organization's fleet.

4.2.3 Other Commercial Services

As UAS applications evolve, the types of USS services may evolve with them. Some services related to but not included in the Remote ID function could potentially include:

[9] Remote ID USSs must be qualified by the FAA specifically to offer remote ID services. A USS qualified to offer other services such as LAANC must still obtain FAA qualification for Remote ID before it can become a Remote ID USS.

- Aggregating public Remote ID information,
- Displaying Remote ID information in various contexts to various types of users, and
- Smart (automated) monitoring of UAS information for various applications.

Although other commercial services may use data points that overlap with the data provided by Remote ID USS, but only those USS qualified by the FAA to provide Remote ID services would be Remote ID USS and qualified to offer Remote ID services to the public in a way that satisfies the proposed operator regulatory requirements under the proposed part 89.

4.2.4 FAA Systems

The FAA would qualify Remote ID USS and would set up and oversee the exchange of Remote ID data with USSs. The FAA would also retain the ability to correlate remote ID data gathered by the USSs with other information available to the FAA such as the registration system in order to provide information to other authorized government and public safety users. Section 5.7.3 discusses the exchange of data from the FAA to other government users in greater detail.

Additionally, the FAA would use the Remote ID messages collected via the USSs to further its mission to ensure the safety and efficiency of the airspace.

FAA systems would perform another critical role in the core functionality of Remote ID: authentication of Remote ID USSs. This topic is discussed in more detail in Section 5.7.

4.2.5 Federal Government Systems

The FAA would provide a system-to-system interface (not directly to end users) for other federal government stakeholders for authorized uses. These other federal government stakeholders likewise would have an intermediary role in conveying Remote ID information to their user bases.

For example, DHS might need Remote ID information as part of its efforts to secure critical infrastructure. DHS would then implement a system to connect to the FAA and manage DHS users and functions, to convey the appropriate information and capabilities to DHS personnel (for example, Aviation Enforcement Agents).

Similarly, DOI might need Remote ID to monitor UAS traffic in areas where it is managing fires or other natural disasters. DOI may want to implement its own Remote ID system to connect to the FAA and enable DOI personnel (for example, Fire Management Officers) to access the information and capabilities they need.

4.2.6 State and Local Government Systems

State and local government stakeholders represent an important in-the-field presence with respect to Remote ID capabilities. For example, local police might be the first to hear about a potential crime involving a UAS in a given municipality. Under the planned Remote ID capability architecture, state and local authorized government systems would be able to receive Remote ID message information and correlated data from the FAA systems by going through the appropriate federal government agencies.

For example, local police departments could be connected to federal Department of Justice systems to gather appropriate information for their missions. If a local police officer receives a

report that a UAS damaged a building, that police officer could retrieve Remote ID information for that location and time via the Department of Justice (which in turn connects to the FAA). In this manner, authorized police activity could retrieve not only public Remote ID information but also non-public information (such as UAS registration information) that could be vital to an effective investigation.

Similarly, local first responders could retrieve Remote ID information via FEMA/DHS, National Guard units could retrieve information via the Department of Defense, and so forth.

5 Key Elements

5.1 Dual-Mode Strategy: Network and Broadcast

There are two technological strategies for UAS identification. The first is a traditional aircraft approach: a broadcast transmitter (broadcast Remote ID). The second is a more modern, "internet of things" (IoT) approach: connect to the internet and report the identification message (network Remote ID). Remote ID incorporates both strategies. This ConUse focuses on network Remote ID (while acknowledging that the proposed rule would require broadcast Remote ID in addition to network for standard remote ID UAS).

Although Remote ID incorporates both network and broadcast technologies, not every UAS would be required to be equipped with both. The Remote ID NPRM addresses three types of UAS, categorized in the sections below.

5.2 Remote ID UAS Types

For the purposes of Remote ID, small UAS fall within the three type categories shown in the table below.

Remote ID Type	Description	Operating Restrictions
Standard	Operates with both Remote ID network connection and broadcast.	
Limited	Network only (from control station or vehicle).	UAS may not fly more than 400' from the control station; VLOS operations only.
Non-equipped	Manufactured before Remote ID, amateur-built without Remote ID, or other special classes.	Limited to FAA Recognized Identification Areas (FRIA) or specially authorized by Administrator.[10]

Note that UAS operators continue to be bound by the operating rules under which they are operating, so any restrictions they may be subject to under 14 CFR part 107, 91, 135, etc. or any conditions and limitations under an exemption or waiver held by the operator would still apply regardless of type of UAS.

[10] UAS not required to be registered would not be subject to the remote ID requirements, therefore there will be some UAS that are not required to equip and will not be limited to the FRIAs.

5.2.1 Standard Remote ID UAS – Both Broadcast and Network

Standard Remote ID UAS would be manufactured to meet particular performance requirements by following an FAA-accepted means of compliance for UAS with both broadcast and network capability. The FAA anticipates there will be multiple means of compliance for manufacturers to choose from (see Section 5.5).

Standard Remote ID UAS are the least constrained type of UAS with respect to Remote ID operational restrictions. For example, unlike limited Remote ID UAS, there would be no range restriction imposed by the proposed Remote ID regulations. (As noted above, other operating rules would continue to apply.)

As a standard remote ID UAS operation is in progress, network coverage and/or the associated internet connection could fluctuate. However, the UAS must connect to a Remote ID USS whenever possible. It is the operator's responsibility to make reasonable efforts for internet availability and/or mobile data to achieve coverage. The proposed rule would require the UAS to initiate a connection to one or more Remote ID USSs whenever it falls within this coverage.

Regardless of the status of an internet connection, standard Remote ID UAS always continuously produce a Remote ID broadcast per its accepted design. This is an important aspect of standard Remote ID UAS, and it is the only type to require broadcast. Remote ID broadcast serves several purposes:

- backup to Remote ID networking should coverage fail,
- providing information to local parties that are not receiving network-based near-real-time messages, and
- support some degree of local aircraft-to-aircraft operational deconfliction.

If broadcast capability is lost during the operation, the operator would be required to terminate the intended operation and land the UAS as soon as safely practicable.

5.2.2 Limited Remote ID UAS – Network Only

Limited Remote ID UAS would also be manufactured to a specific set of performance requirements using an FAA-accepted means of compliance. Limited Remote ID UAS would only have network capability and would not broadcast the remote ID message elements. As Limited Remote ID UAS would transmit a message that does not include location data for the unmanned aircraft (the message does include location data for the control station), the proposed rule would require that limited Remote ID UAS would not be able to operate further than 400' from their control station (the location of their operator). This range restriction would be built into the UAS itself. This ensures that, even if a local observer does not have Remote ID information via a network-connected mechanism, they have a reasonable chance of identifying the UAS operator by looking around. For example, a law enforcement officer attempting to interdict a dangerous operation should have a good chance of spotting the operator if the officer is close enough to spot the UAS.

If network connectivity is lost at any time during the flight – whether due to lack of coverage or equipment failure – the UAS has no functional Remote ID capability. The operator would be required to land the UAS as soon as safely practicable. Additionally, a limited remote ID UAS

would not be capable of taking off if it were unable to transmit the remote ID message to a Remote ID USS.

5.2.3 Non-Equipped UAS

Remote ID would likely trigger a significant shift among commercially-available small UAS. If a small UAS is larger than 0.55lbs and manufactured for operation in the United States, it would need to have Remote ID capability for operation in most locations. Additionally any UAS under 0.55 lbs intended for operation under Part 107 would require Remote ID. This means that most off-the-shelf UASs are anticipated to come equipped with at least limited Remote ID capability.

However, a subset of UAS will remain non-equipped with Remote ID. Most of these will be one of three types (setting aside exceptions authorized by the Administrator such as UAS performing sensitive security missions):

- **Less than 0.55lbs.** Even these would only be allowed to operate in most locations for non-commercial purposes (see applicable regulations for exact definition).
- **Amateur-built.** Small UAS that are largely built by a person "solely for their own education or recreation" (see NPRM).
- **Legacy UASs.** Small UAS that were manufactured and sold prior to the establishment of Remote ID may be operating without Remote ID capabilities.

UAS without remote ID capability would be limited to flying at an FAA Recognized Identification Area (FRIA) and within visual line of sight. FRIAs are areas where remote ID equipment is not required, however, any equipped UAS (standard remote ID UAS or limited remote ID UAS) would still be required to remote ID even when in the FRIA. Additionally, the FRIA does not provide any exception to existing operating rules, so the flights there would still be bound by whatever statutes or regulations apply to the operation. Because each FRIA is held by a community-based organization, the FAA expects that most FRIAs will be the same hobbyist fields that have existed for model aviators for many decades. The FAA expects to make digital charts available that identify FRIAs.

Operating within the confines of a FRIA, the identification area itself serves the function of remotely identifying the UAS – all stakeholders are made aware that UAS operations could be taking place at any time within that airspace volume.

5.3 Remote ID Information Content

The Remote ID NPRM proposes standardized messages containing identification information. A Remote ID message would contain the fields in the table below. (Note that Aircraft Location is not required for Limited Remote ID UAS.)

Remote ID Required Fields	Description	Limited	Standard
Serial Number or Session ID	*Unique identifier for the UAS*	✓	✓
Control Station Location	*Latitude, longitude, barometric altitude*	✓	✓
Aircraft Location	*Latitude, longitude, barometric altitude*		✓
Time Stamp	*UTC, corresponding to location data*	✓	✓
Emergency Status of UAS	*Identifies special flight situations*	✓	✓

Performance tolerances for the proposed Remote ID messages are as follows:

Remote ID Information	Tolerance (Limited and Standard)
Location	+/- 100' of true position (95% probability)
Altitude	+/- 20' of true barometric pressure altitude
Maximum Latency	<1s between location measurement and transmission
Minimum Rate	>= 1 message / sec

5.3.1 Session IDs

Session IDs may be used in both broadcast and network messages. The use of session IDs allows operators an optional additional layer of information protection. If serial numbers are always transmitted "in the clear" (especially over broadcast technology), there is the possibility that some parties might be able to aggregate usage data and other contextual information to identify UAS operators. With session IDs, the public Remote ID message does not correlate directly to the serial number (at least, not in publicly available data). In addition, operators can change session IDs with every flight. This reduces the potential for their collected data to be used in undesired applications.

To use a limited-duration session ID instead of a serial number, the operator must obtain the session ID from a Remote ID USS. The Remote ID USS would assign a unique session ID and provide it to the operator. The Remote ID USS also sends the session ID assignment to the FAA (over secured internet connection). The FAA is the only party other than the USS that receives and has access to the correlation between the session ID and serial number. Rules will be developed for session ID format and duration of assignment.

Session IDs offer protections to limit visibility of information as appropriate. Members of the general public who receive Remote ID messages would not necessarily have the UAS serial number, but they would have a unique UAS identifier (the session ID) which can be used for

reporting. The USS, as the source of the session ID, would have access to both the session ID and serial number. Protection of this information would be governed by legal agreements the USS makes with the FAA. The FAA would have access to the same information (session ID and serial number), and additionally the FAA would be the only party that could correlate serial numbers to registration and other regulatory information. Neither USSs nor the general public would have access to registration information.

5.4 UAS Networking for Remote ID

Remote ID capabilities utilize a network-based link between the UAS and a USS. This persistent link is the basis of network Remote ID. A Remote ID network connection allows an operator to transmit Remote ID messages to a Remote ID USS using an internet connection. The USS in turn would transmit it on to the FAA, which can provide it to federal government stakeholders and – by extension – local law enforcement and other authorized parties. As a mechanism for disseminating information to all affected stakeholders, network Remote ID is more comprehensive, allows for archiving of remote ID message data, and better aligns with modern technology than broadcast Remote ID. Working with a USS also enables operators to use session IDs in both broadcasts and network messages.

Network Remote ID requires an internet connection. It is not expected that UAS will be connected everywhere in U.S. airspace. Particularly where internet is provided by mobile data coverage, it is anticipated that coverage will be better near populated areas with infrastructure and poor in remote locations.

As described in the NPRM, exact equipment and protocol details would be captured in specific Means of Compliance (MOC) documentation. The MOC could stipulate the equipment requirements on the manufacturer in a vendor-neutral way. For example, an MOC could specify that UASs manufactured under that MOC are equipped with LTE (or HSPA, WiMAX, etc.). The NPRM's proposed operating rules require an operator to connect to the internet using that UAS to transmit to a Remote ID USS, therefore for that transmission to occur, the operator would have to procure an adequate mobile networking plan with compatible ground infrastructure. See NPRM for the details of these proposed rules.

5.4.1 Near-Term Example of UAS Networking

The earliest and simplest forms of Remote ID UAS Networking are likely to take the approach of leveraging connectivity already available in commercially-available control stations. Frequently this takes the form of a "phone on a controller" configuration as shown in Figure 7. This is expected to be an early configuration because it is possible for many existing UAS products with only a software upgrade.

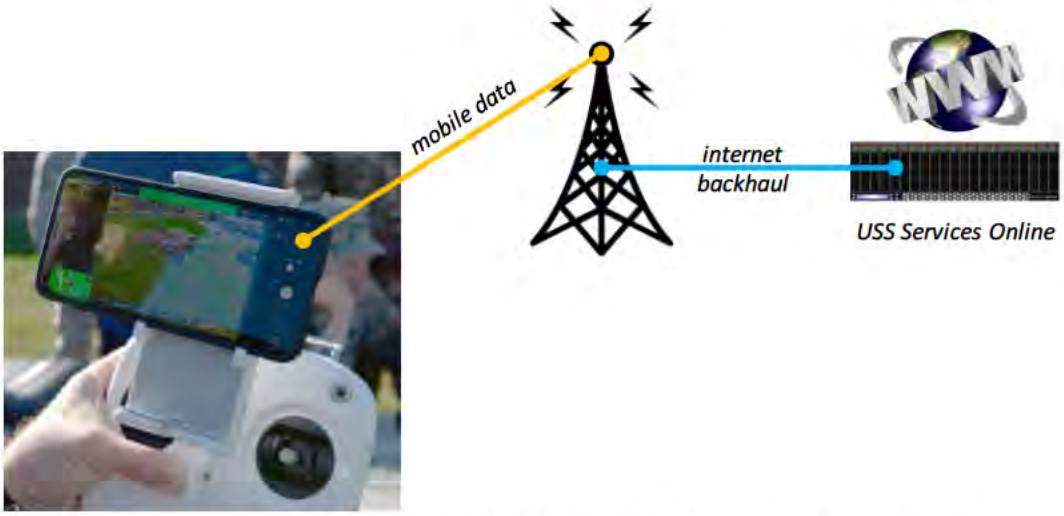


Figure 7: Remote ID Network – Early Configuration (Integrated Smart Device)

Configurations such as this usually involve a controller app running on a smart device, which already has access to the smart device's mobile data connection. In general, for this model to work for Remote ID compliance, the operator will have to provide for two fundamental services:

1. Internet connection, likely through mobile data for their smart device
2. Remote ID service account with a USS

The first, internet connection, could be provided under an existing smartphone or tablet mobile data plan. The operator would be required by the proposed rule to maintain internet service, and if his/her UAS is designed to connect to the internet via a mobile data, acquiring that internet service would require acquiring mobile network coverage. This ConUse assumes that where internet is provided through mobile data, that operators will acquire and maintain coverage equivalent to a standard mobile plan from a major carrier.

Second, the operator would have to establish a service account with a Remote ID USS to support their UAS flights in compliance with Remote ID. The USS would deploy servers on the internet that accept connections from operator UASs. In addition, USSs may also develop integrated Remote ID software that runs on the control station smart device (a client-side application). Or, a standard (multi-USS) application might run on the controller and be directed to the USS interface on the internet. A range of architectures are possible. USS services could vary from multi-faceted and expensive to simple and virtually free.

Remote ID encourages redundant connection options to improve network coverage. At the data coverage level, in the near-term model, this could take the form of standard roaming services that many mobile data providers already incorporate in their services. At the USS services level, this could take the form of cloud-based redundancies to ensure that Remote ID services are virtually always available. Note that USSs are online entities that normally address availability concerns with cloud redundancy and similar methods. Internet-based companies do not have inherent geographic limitations in the same way that mobile data providers do.

If two or more mobile data companies offer UAS-specific plans based on LTE (for example), roaming could be part of the fielded solution. Any UAS with compatible equipment could automatically make a Remote ID network connection, regardless of which company is providing

coverage. Note that UAS configurations that use a connected smart device for internet access (such as a smart phone with a plan from a major provider) would normally have this roaming feature by default.

5.4.2 Mid-Term Example of UAS Networking

In the mid-term, Remote ID could take the form of embedding conventional mobile networking technology on the airborne vehicle ("phone on a drone"). This is associated with the mid-term because, in general, it would require newly manufactured aircraft equipment. (New hardware design, not just a software upgrade.)

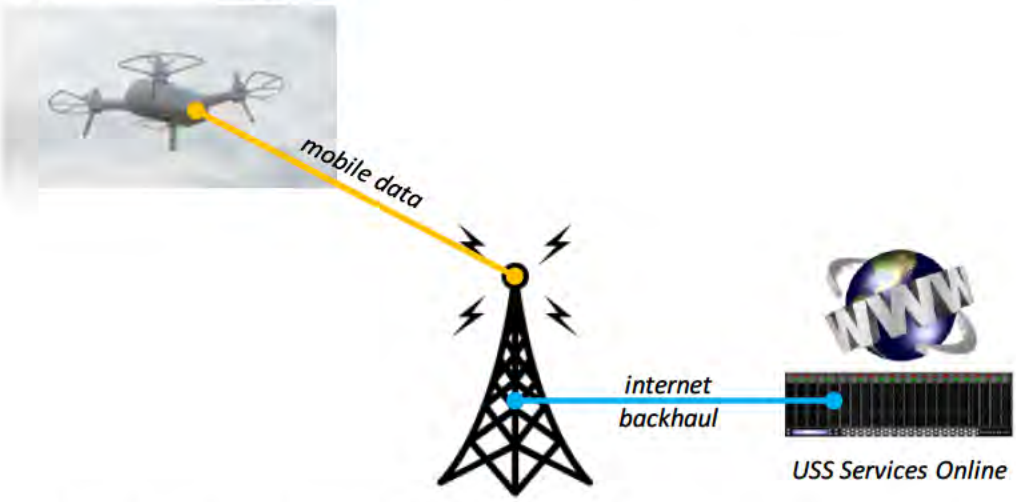


Figure 8: Remote ID Network – Mid-term Configuration (Mobile Data on Vehicle)

As in the near-term case, the operator still needs to provide for an internet connection and a USS account for online services. However, internet provided through mobile data coverage is not necessarily as standardized since it is not necessarily localized in a conventional smart device such as a phone or tablet. There are several ways in which mobile data could be integrated into this Remote ID configuration:

- **Phone or tablet equivalence.** The UAS vehicle could be designed to appear just like a phone or mobile-networked tablet on a mobile carrier's network. In that case, coverage would be procured in the same manner as adding a conventional phone or tablet to a service plan.
- **New service class for UASs on conventional plans.** Mobile carriers and manufacturers could collaborate to define a "drone" device class. Presumably this would have some modified characteristics as it appears on a mobile network (for example, other standard services like SMS disabled; possibly optimized for low latency). This would allow operators to add a UAS to their plan as a specific device type. This approach requires compatible efforts on the part of both manufacturer and mobile carrier.
- **Integrated mobile data services.** Under this approach, operators do not necessarily need to have a conventional mobile data plan. They could procure mobile data services specifically for their UAS as part of their USS plan, manufacturer support plan, or other bundle. Presumably under this approach, USSs (or other stakeholders) would establish a business-to-business relationship with a mobile data carrier – or some other form of business integration such that the services can be bundled.

5.4.3 Long-Term Example of UAS Networking

The near- and mid-term examples of Remote ID networking presented in the prior two sections are *not* expected to phase out in the foreseeable future. Rather, the "phone on a controller" and "phone on a drone" configurations are expected to settle as classes of Remote ID compliant UAS designs.

In addition, in the long-term, new and more advanced configurations are anticipated. An example discussed here is a long-endurance fixed-wing small UAS designed for BVLOS applications. Anticipating that standards for the command and control (C2) link will be higher than for visually tracked sUAS, we can assume a dedicated low-latency wireless link is available. While designed for C2, it can also be used as a link in the Remote ID networking capability. The general design is shown in Figure 9.

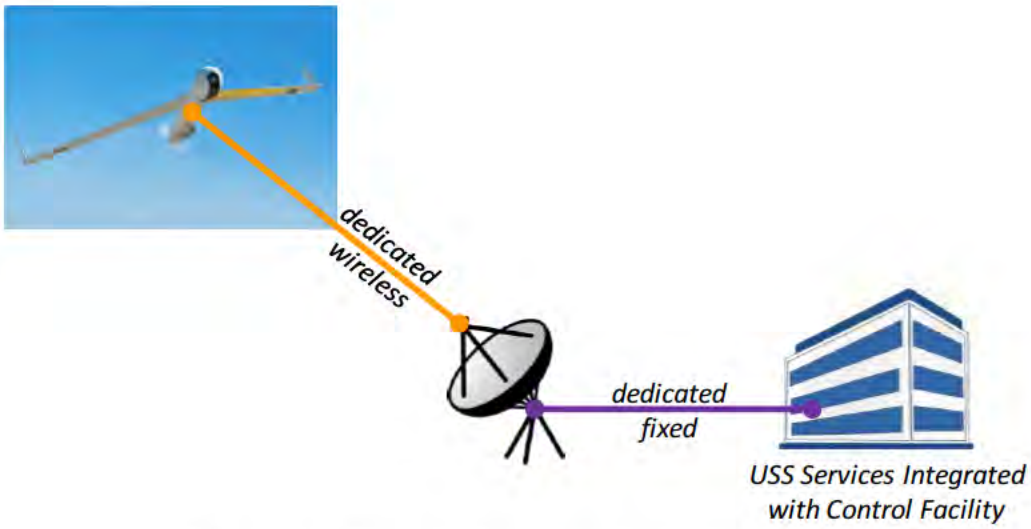


Figure 9: Remote ID Network – Long-Term Configuration (with BVLOS)

Time will tell the fielded range of solutions that might fit with part or all of this general pattern. One possible configuration is described as follows:

- **USS offers integrated C2 and Remote ID.** Either by partnerships or directly, the USS would ensure wireless data coverage infrastructure for the flight area (ground towers, satellite, etc.). The USS also includes sufficient ground networking infrastructure to the operator's control location.
- **Aircraft equipped for compatibility.** The UAS itself is equipped with compatible radio gear that connects both C2 and Remote ID through the USS network. The USS does not necessarily need to be concerned with the C2 protocols (presumably they will match the operator's control stations, conveyed over some standard network packaging), but the USS will manage Remote ID directly. That is, Remote ID information from the aircraft goes to the USS for management. The operator only needs to be concerned with C2.
- **Full flight operations management.** Although not shown, operational concepts have emerged involving control link handoffs. For example, an operator at the launch site handles takeoff and flight of the first few minutes, then transfers control to a remote operator. A

similar handoff is repeated for landing / retrieval. The USS may need to include supplemental modes of networking to ensure Remote ID connectivity and coverage during all phases of flight.

5.5 Qualification of Manufacturing and Operational Configurations

5.5.1 Establishing a Means of Compliance

Manufacturers would meet the remote ID performance requirements of the rule for standard or limited remote ID UAS by using a means of compliance (MOC) that has been accepted by the FAA. The Remote ID NPRM explains the process for FAA acceptance of a means of compliance. The FAA would evaluate any MOC submitted for acceptance and either accept or deny the MOC based on whether it satisfactorily meets all Remote ID performance requirements.

5.5.2 Manufacturing UAS with a Declaration of Compliance

Manufacturers would file a declaration of compliance (DOC) declaring that the UAS, or a range of UAS by serial number, meet the performance requirements of the rule and that they have followed an FAA-accepted MOC. The DOC confirms that the UAS was produced in accordance with a MOC and would link an approved MOC to a range of manufacturer serial numbers. The production requirements and DOC process as proposed are described in the Remote ID NPRM.

5.6 Built-In Test, Monitoring, and Failure Management

As part of Remote ID compliance, UAS would be required to have a built-in self-test to detect degraded conditions. Some of the critical degraded conditions could be:

- loss of network connectivity
- failure of broadcast equipment

Monitoring refers to ability of the operator to maintain awareness of degraded conditions. Appropriate indicators would be designed into UAS controls to fulfill Remote ID-related functions. Some degraded conditions require action on the part of the operator – actions which there is no general way to automate. For example, if a limited Remote ID UAS loses Remote ID network connectivity, the operator would need to land it as soon as practicable. There are safety factors and decisional tradeoffs to be considered in the landing process which only the operator could manage.

Failure management is the combination of automated and operator actions in response to a degraded condition. The proper response depends on the type of failure. The example above – landing in response to equipment failure – requires operator action in the decision loop. Other examples would be fully automatic. For example, UAS equipped with Remote ID would be designed to attempt network connectivity automatically; if network connectivity could not be achieved, limited Remote ID UAS would not take off. Standard Remote ID UAS could take off in this situation, but the pilot should be informed of the condition. If that same standard Remote ID UAS also lost broadcast capability, it would need to land as soon as practicable.

5.7 Remote ID Data Exchanges

Data exchanges are critical to the Remote ID concept. A data exchange in this context is a defined interface between two or more parties; specified data is transferred, in accordance with an established agreement between the parties. Participation is controlled. Data exchanges are a useful basis for system-to-system integration between dissimilar organizations. The data exchange concept was used successfully by the FAA and USSs to deploy the LAANC capability. Remote ID and future capabilities such as UTM are also expected to leverage data exchanges.

Note that this section is not comprehensive with respect to all data transfers between systems and end users that could occur in connection with Remote ID. For example, USSs would provide data to their customers, but this is not a system-to-system data exchange that needs to be centrally defined for Remote ID functionality. (Note, however, it would fall under data protection clauses to which the USS would agree.) There are many variants on other end uses and data transfers, such as pilots connected to public USS, law enforcement connected to public USS, law enforcement connected to government Remote ID systems, etc. Such exchanges and interfaces are not addressed here. Data exchanges in this section represent the most essential system-to-system Remote ID interfaces, which are fundamental to providing a collective capability.

5.7.1 USS-to-FAA Data Exchange

The Remote ID USS-to-FAA data exchange would build on proven technologies for system-to-system information exchange for national-scale operational integration, including:

- FAA cloud infrastructure hosting Remote ID services
- Online USS systems
- Industry-standard, secure interfaces
- 24/7 availability with backups and redundancies
- Automation of nominal processes
- Authentication and credentials administered by the FAA

UAS-to-USS data transfer would be periodic and frequent – one message per UAS per second, as detailed in the NPRM. USS-to-FAA data exchange presents a wider range of options and tradeoffs. For the USS-to-FAA interface, there are competing considerations:

- The FAA (and other government users) may not need every message, especially not redundant ones.
- Excessive bandwidth use is inefficient for systems on both sides.
- The USS can store messages for later retrieval if needed.
- A certain degree of near-real-time data is necessary for situational awareness.
- Data transfer requirements will be driven not only by the FAA, but also by other government stakeholders downstream of the FAA.

Figure 10 shows the general structure of the USS-to-FAA data exchange.

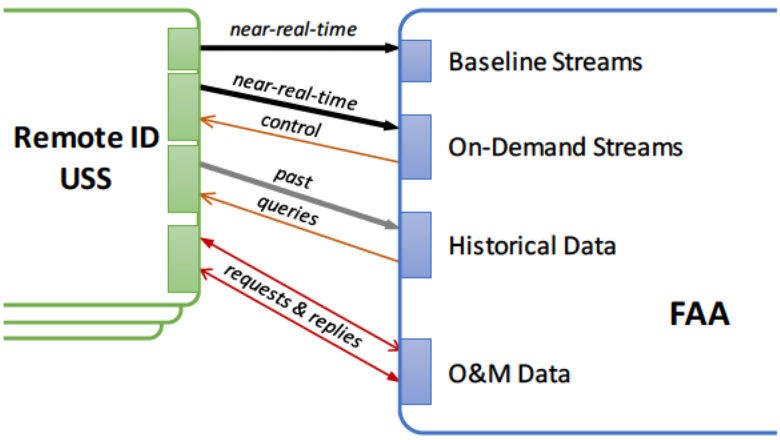


Figure 10: UAS-FAA Data Exchange Interface (General Design)

A "baseline stream" consists of certain data items which are always transmitted, in near real time, by the USS to the FAA. The baseline stream is the functional equivalent of a default subscription. This could include, for example, the first Remote ID message of any new operation and updates not less than every 1 minute during the operation. The frequency could be increased if the UAS is moving rapidly. For example, a message could be triggered if the distance since the last message exceeds 100ft. An exact algorithm for baseline stream inclusion has not been determined. It could vary with time as Remote ID policies develop. This ConUse establishes the concept of a baseline stream.

"On-demand streams" provide near-real-time data at a higher resolution (more frequent) than the baseline stream for specific operations of interest. Controls from the FAA to the USS would allow the FAA to configure these streams. For example, one on-demand stream could contain every available message (as it is received) in a sensitive area, such as over protected infrastructure or near an airport. Another stream could provide higher-resolution information on UAS of a certain class, such as over a given weight threshold. On-demand streams could have specified lifetimes or continue indefinitely until cancelled.

In contrast to the near-real-time streams described above, provision is also made for "historical data". Using this interface, the FAA could request stored information on any operations that occurred in the past 6 months. The historical query interface supports different definitions of scope and identification. Returns could include multiple UAS or single UAS, low-resolution or high-resolution data. A historical query capability is an important automation-oriented backstop for recovering past data for any reason – mitigating data loss, investigating incidents after the fact, and so forth.

One other type of data transfer is included here: operations and maintenance (O&M) information. Unlike the other data types, O&M data is not directly operational. It is a bidirectional exchange that allows USSs and the FAA to check each other's systems for status, comparing statistics, detecting inconsistencies, and probing failures.

5.7.2 USS-to-USS Data Exchange

The Remote ID concept incorporates an expectation that USSs provide public Remote ID information to each other and the general public. An obvious motivation for this information sharing is to provide operators and others with situational awareness of drone operations in the

vicinity (local situational awareness) – beyond what can be achieved via Remote ID broadcasts. (For example, limited Remote ID UAS would not broadcast at all.) One way to meet such a need is for a related service to specialize in Remote ID display to its user base, with a need to integrate all available sources. USS-to-USS sharing (and Remote ID USS sharing with other services/parties) could take many forms and have many motivations.

The general pattern for USS-to-USS (and related) data exchange is shown in Figure 11.

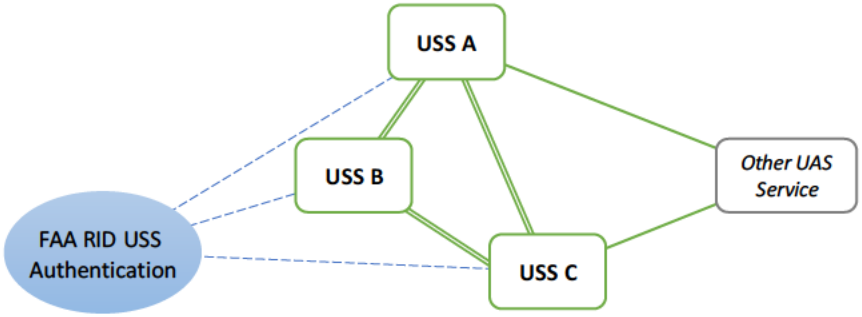


Figure 11: USS-to-USS and Related Data Exchanges

All public messages may be shared between USSs with user agreement, and USSs would be free to make agreements with one another for USS-to-USS data exchange. Remote ID messages are not distribution-sensitive (the Remote ID message is public, as it is subject to broadcast). Session IDs continue to provide a degree of anonymity as designed.

The FAA is the qualifying and governing organization for Remote ID USSs. In connection with a USS's qualification with the FAA, credentials would be issued for use in USS-to-FAA data exchanges. These credentials also serve as a basis for other parties (like other USSs or other types of service providers) to recognize the USS as a qualified, authoritative source of Remote ID information. This is shown in Figure 11 as the FAA providing authentication of Remote ID USSs.

5.7.3 FAA-to-Federal Partners Data Exchange

Various other federal government partners would need Remote ID data to fulfill their regulatory roles, such as local law enforcement, emergency services, and military personnel. To provide these partners with the information they need, the FAA would establish data exchange interfaces to pass along relevant Remote ID messages (and correlated registry, etc.) from USSs to authorized government recipients.

In addition to acting as a conduit for Remote ID information, the FAA can also perform additional information processing functions such as correlating to registration data and aggregating information across multiple USSs. This additional processing is only performed and used as appropriate and as authorized in the applicable System of Record Notice (SORN).

The figure below illustrates the data exchange with federal partners (and the extended connections to state and local partners):

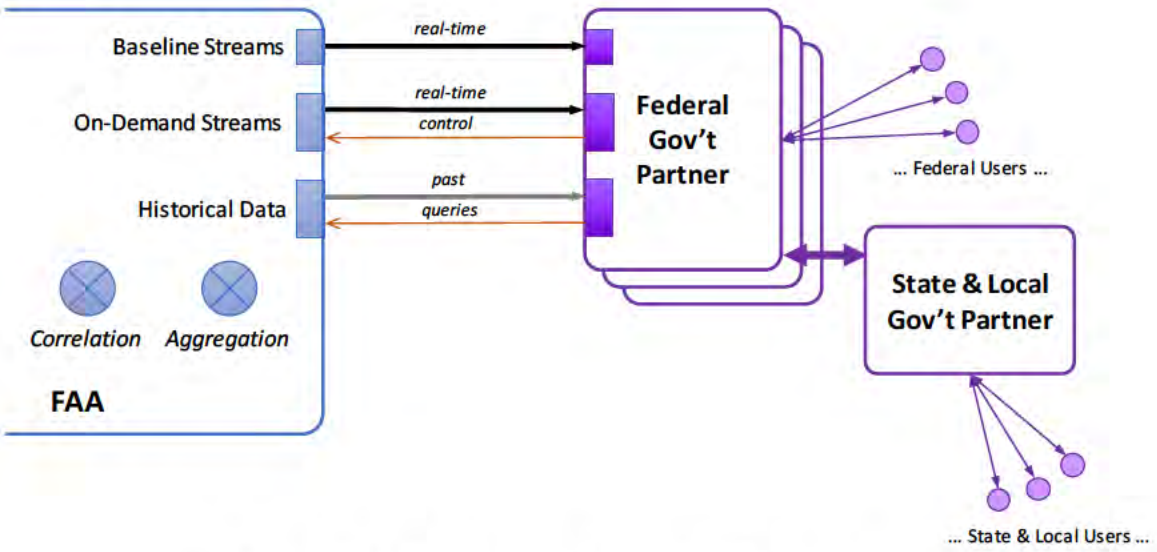


Figure 12: FAA-to-Agencies Information Mechanisms

FAA-to-Government interfaces are designed as system-to-system exchanges. Federal, State, and Local government partners would need to build suitable user interfaces and manage their own end users.

Note that end users in federal, state, and local government may have access to other sources besides the FAA to acquire the publicly available Remote ID information. For example, a local law enforcement (or emergency services) organization could subscribe to a service from a commercial provider that tailors information for such purposes. However, commercial providers would only have access to public Remote ID information. As described above, the FAA has the additional capability to correlate Remote ID information with registration information. This aspect is described in more detail in the next section.

5.8 Classes of Remote ID Information

5.8.1 Public Remote ID Information

Remote ID messages are inherently public information. Anyone may receive them including private citizens, corporations, and government representatives. Publicly sourced Remote ID information may be passed between USSs and other systems.

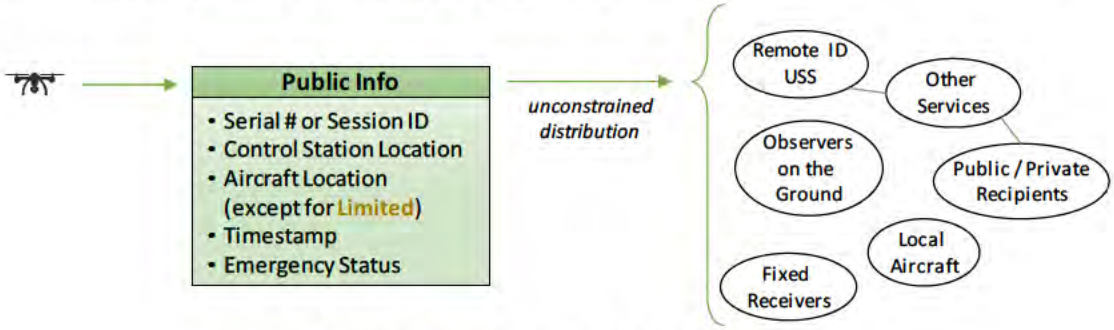


Figure 13: Public Remote ID Information

There may be some cases in which it is more expeditious for federal partners to acquire publicly available Remote ID information than to obtain it through the FAA. For example, local emergency services may utilize services in the short term by acquiring local Remote ID information from a commercial source. Commercial sources would normally be limited to public Remote ID information: session IDs would not be correlated with serial numbers, and no registration information would be correlated to the Remote ID messages.

5.8.2 Government Use Remote ID Information

For legitimate government uses described in the SORN, the FAA can act as a source for Remote ID information that includes non-public elements. As part of its interface to Remote ID USSs, the FAA would receive session IDs as well as serial numbers. The FAA would have the ability to make correlations to other aviation-related information: registration, certificates, waivers, authorizations, etc. Distribution of information would be governed by the appropriate SORN. Furthermore, the FAA and federal government partners are bound by the protections provided by Privacy Act.

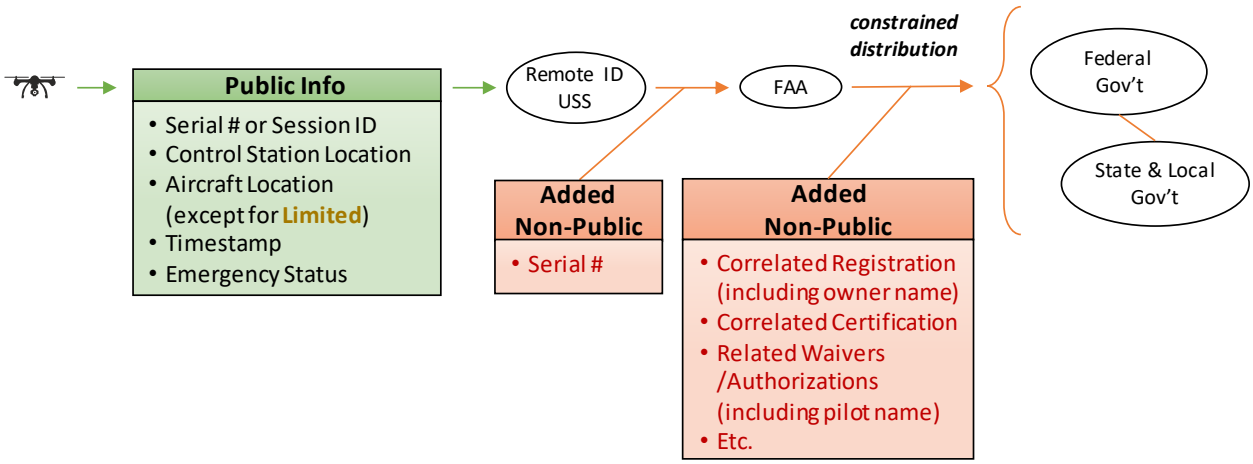


Figure 14: Government Use Remote ID Information

6 Combined Use Data Exchange Scenarios

The following scenarios build on the operational scenarios presented in the NPRM. Aspects added here illustrate the data exchanges occurring behind the scenes. These scenarios are not comprehensive.

6.1 Operation of Standard Remote ID UAS

See NPRM Section X.G.1 and X.I.

Patty purchases a standard Remote ID UAS for use in her photography business. The UAS is a "phone on a controller" configuration (see Section 5.4.1), and she already has a compatible smartphone with a mobile data plan from a major carrier. Patty subscribes to Alpha, Inc., an FAA-qualified Remote ID USS. Since she already has a compatible mobile networking plan, she does not need to procure anything besides her UAS and Alpha services to fly under Remote ID.

When Patty flies with internet coverage, her UAS automatically connects to the internet via her smartphone. Once connected to the internet, the UAS attempts to connect to Alpha's USS interface at a specific configured web address. This includes some credentialing that Alpha has provided to Patty (username and password, for example). When the connection is successful (which is most of the time), the UAS streams Remote ID messages once per second to Alpha. Per Patty's selection, these Remote ID messages include the UAS's serial number.

Alpha receives all the Remote ID messages from Patty's UAS and stores them per its data retention agreement with the FAA. By default, Alpha constructs a baseline stream from Patty's operation and sends it to the FAA. This involves Alpha connecting to the FAA's Remote ID interface on the internet, using credentials that the FAA has provided to Alpha. In Patty's case, no other streams have been configured that apply to her operations, so the baseline stream is the only data the USS is required to provide to the FAA (in addition to making the Remote ID messages available for later historical queries).

There are times when Patty is flying in rural areas and mobile internet coverage is lost. (Neither her mobile carrier nor any roaming-available mobile carriers have coverage.) Since Patty has a standard Remote ID UAS, she can continue to fly using only the broadcast remote ID capability, although network Remote ID is not functional during these periods.

If Alpha's servers on the internet have an outage and Patty's UAS still has a connection to the internet, her UAS will attempt to connect to an alternate Remote ID USS (for example, Bravo, Inc.). If the UAS makes a successful connection, Bravo will handle the operation.

As a photographer, Patty takes a job covering an outdoor concert. Sheriff's Deputy Lucy is working security at the concert. On her department-issued smartphone, Lucy can log into a mobile-friendly internal website provided by the Department of Justice. The website requires her credentials as a police officer. Through this web app on her phone, Deputy Lucy requests full streams on all network Remote ID messages before, during, and after the concert within a 5-mile radius.

DOJ's systems are connected to the FAA through the applicable Remote ID data exchange. DOJ forwards the full stream request to the FAA, which sends it to all Remote ID USSs (including Alpha). When Patty starts her UAS in the concert area, all her Remote ID messages (not just the

baseline stream) are sent to the FAA, which forwards it to DOJ and subsequently to Lucy's web app.

Patty flies her UAS in compliance with 14 CFR Part 107, so Deputy Lucy has no reason to approach her. Deputy Lucy is able to track and identify the flight on her DOJ-connected web app. A separate, publicly-available web app also allows Deputy Lucy to track the UAS via its broadcasts when the signal is within range in this environment[11].

However, Deputy Lucy observes another UAS operating over the crowd. The UAS is apparently connected via network Remote ID, because Deputy Lucy can see it on her web app. It shows as a standard Remote ID UAS with a controller location about 90 feet away. The FAA is receiving a stream on the UAS from USS Delta, Inc. As the stream is received, the FAA attempts to correlate the serial number to registration and determines that the UAS is unregistered. This is shown as a prominent flag on Deputy Lucy's web app display. The pilot name is not available. Deputy Lucy can also see the UAS based on its broadcast, but the broadcast app display cannot show that the UAS is unregistered (since the app only shows public information captured from the local transmission).

Deputy Lucy approaches the pilot and determines that the pilot is not certified and is not aware of applicable regulations. Deputy Lucy directs the pilot to land safely and immediately.

6.2 Operation of a Limited Remote ID UAS

See NPRM Section X.G.2 and X.I.

Charlie buys a used limited Remote ID UAS. It has a controller that is designed to pair up with his smartphone (therefore, it is a "phone on a controller" type configuration – see Section 5.4.1). Charlie's mobile phone plan has adequate coverage to provide internet access for the purposes of Remote ID. Whenever Charlie's smartphone does not have coverage, his UAS will not take off. Furthermore, Charlie subscribes to Bravo, Inc., which offers USS services on the internet but does not provide mobile data coverage.

Charlie likes to fly his UAS in a large field near his home which is municipal property and open to use by the community. Adjacent to this large field is a national security facility operated by the Department of Defense (DOD).

Officer Schroeder works as a law enforcement officer at the DOD facility. In his office, Officer Schroeder has a DOD computer through which he can log into a Remote ID monitoring application using his DOD credentials. He also has a DOD-issued tablet with the same capability, which he can carry around the facility. In the DOD Remote ID web application, he configures a default view to show the vicinity around the facility with all baseline streams shown in near-real-time. The facility also has several fixed receivers around the perimeter for Remote ID broadcasts. These are wired to a dedicated display unit in Officer Schroeder's office which he can observe in addition to his web app for network Remote ID.

Officer Schroeder frequently observes Charlie operating in the area of the large field next to the DOD facility (on the web app, not on the broadcast map, since Charlie operates a limited Remote

[11] Note that unlicensed spectrum congestion may be a factor in this case, given the show infrastructure and many devices carried by attendees.

ID UAS). He never has reason to investigate or report potential violations concerning Charlie's flights. In the baseline stream from the FAA, registration correlation is included, showing that the UAS is properly registered.

Officer Schroeder also sees flights by Schultz Inspection Services on the grounds of the facility itself. The serial numbers for Schultz Inspection Services UASs correlate to that company through registration data. Officer Schroeder receives notices in advance of when and where Schultz Inspection Services will be conducting authorized operations.

As a part of his duties, Officer Schroeder frequently visually checks the area for unauthorized UAS operations. He brings his DOD tablet with Remote ID information with him during these checks. If he sees a UAS operation, the presence or absence of corresponding Remote ID information is critical information for him. If the operation can be identified and correlated to expected and acceptable activity, there is no need for intervention. This allows nearly all UAS operations to be conducted without unnecessary constraints. In the rare case that an operation is not identifiable, Officer Schroeder knows to follow applicable procedures.

PARTNERSHIP FOR REMOTE IDENTIFICATION COLLABORATION

A

MEMORANDUM OF UNDERSTANDING

Between

Federal Aviation Administration

and

AirMap, Inc.

Date: January 7, 2020

1. PARTIES

The Federal Aviation Administration (FAA) and AirMap, Inc. , also known as (aka) the "Parties".

2. PURPOSE

The purpose of this Memorandum of Understanding (MOU) is to establish a working relationship between (FAA) and AirMap, Inc. that will facilitate a collaborative working environment for the development of a technical and legal framework for initial prototyping and testing that will inform a national capability for Remote ID Unmanned Aircraft System (UAS) Service Suppliers (UAS) future of Remote Identification (Remote ID).

The result of this collaboration will be the creation of Remote ID Unmanned Aircraft Service Supplier (USS), via a Memorandum of Agreement (MOA) between the FAA and FAA-qualified organizations. Please be advised that participation in the Remote ID cohort collaboration sessions, as detailed and contemplated in this MOU, does not guarantee that an organization will be qualified as a Remote ID USS for a future USS MOA.

The purpose of this MOU is to establish a relationship between the FAA and AirMap, Inc. to pursue mutual goals and to leverage resources, expertise and information, to enable innovation, development and maturation of Remote ID technology. Equally important, this partnership will facilitate the sharing of experience and best practice in fostering a culture of innovation across the FAA and industry partners.

3. BACKGROUND

In 2016, as the FAA promulgated and implemented 14 CFR Part 107 – Small Unmanned Aircraft Systems (sUAS), the FAA recognized a need to create a streamlined and scalable authorization process to address operations of small unmanned aircraft in controlled airspace.

To address the need for timely responses to authorization requests, the FAA determined that automation was necessary and decided to test the Unmanned Aircraft Traffic Management (UTM) principles of data exchange with third parties. To that end, the FAA developed the Low Altitude Authorization and Notification Capability (LAANC). LAANC automates the application and approval process for airspace authorizations. For remote pilots, LAANC provides near real-time access to controlled airspace below FAA approved altitudes. For FAA Air Traffic, LAANC provides awareness of planned drone operations at low altitudes and quick access to the drone operators.

To develop and implement LAANC, the FAA surveyed industry's interest and ability to provide near term solutions through a Request for Information (RFI), which was issued in August of 2016. From industry's responses to the RFI, FAA established a cohort of approximately a dozen potential partners in December 2016. By September 2018, LAANC was rolled out to nearly all FAA Air Traffic Facilities in a national beta evaluation with five FAA qualified LAANC USS partners. The FAA will continue to open onboarding periods for interested third parties to participate in the initiative. Onboarding includes signing an MOA outlining the legal framework under which services can be provided, proving they can meet the LAANC USS Performance Rules, and testing the end-to-end system and connections. LAANC serves as a "proof point" for the FAA-USS model, as it demonstrates that a fully automated solution offered by industry and enabled by data sharing with the Air Navigation Service Provider is viable.

The FAA believes that the use of a rules-based governance structure with USS have been an effective mechanism to implement the requirements, also known as USS Operating Rules, for airspace authorizations. The FAA anticipates using the same concepts for additional UTM capabilities, such as UAS Remote ID. The FAA emphasizes that it views LAANC USS as independent of and separate from Remote ID USS. Nothing in this framework requires or precludes (i) a LAANC USS from also operating as a Remote ID USS or (ii) a Remote ID USS from conducting only Remote ID USS activities.

The FAA anticipates continuing this philosophy in future uses of USS. As USS roles and the services provided expand, the FAA anticipates that some USS may choose to offer an entire suite of services, while others may choose to specialize in one service. The FAA is agnostic to the USS business models.

Remote ID USS would provide remote identification services to UAS operating in the national airspace system (NAS) in coordination with the FAA. The FAA expects that the initial Remote ID USS business models may transform to include other services related to UTM. FAA also expects that Remote ID USS services will be provided at no cost to the FAA. As long as a single Remote ID USS is available to provide services, the data exchange model is viable. The FAA does not intend on becoming a Remote ID USS. FAA believes certain Federal agencies (e.g. DoD, DOI) will consider creating their own Remote ID USS to manage and control their own assets and flights.

Under this arrangement, the FAA would establish the operational framework (requirements and criteria) for Remote ID USS and provide supporting data to airspace users as necessary for collaboration and safe operations.

One critical element of implementing remote identification will be establishing a cooperative data exchange mechanism between the FAA and the Remote ID USS. The FAA is proposing to implement the remote identification requirements in a way that will allow the marketplace to grow in collaboration with the FAA. The FAA, working with the selected industry cohort, intends to build out a feature set and hold a prototype evaluation. The FAA also intends to evaluate the features in the prototype, address findings, and then roll the features out in a larger evaluation.

USS would be allowed to provide remote identification services if they enter into an agreement with the FAA to provide those specific services and demonstrate they can meet a set of technical requirements applicable specifically to Remote ID USS (Remote ID USS Performance Rules). The relationship between Remote ID USS and the FAA would be governed by a legal framework signed by both parties called a memorandum of agreement (MOA), which will be generated in parallel with the operational framework.

4. OBJECTIVES

The MOU establishes a framework for cooperation and collaboration between the FAA and AirMap, Inc. , in developing a technical and legal framework for initial Remote ID prototyping and testing that will inform a national capability. This collaboration is anticipated to accomplish the following activities:

- Form a cohort of industry participants to collaboratively solve the challenges (technical/legal) with the FAA around establishing Remote ID capability using the UAS Service Supplier Model. Develop demonstrations of information sharing capabilities that

offer “proofs-of-concept” for supporting sUAS Remote ID operations in a “live” environment;
- Deploy one or more systems or services to support sUAS Remote ID capabilities, with an evolution path to adding functionality, capacity and users over time; and,
- Apply collaborative problem solving among FAA and USS (e.g., virtual and in-person workshops) to identify sUAS information sharing needs, assess experience data collected from demonstrations, and recommend system enhancements

A key objective of this cohort collaboration is the establishment of an initial sUAS Remote ID capability accomplishing the following four objectives:

1) Market research and initial collaboration phase: Gather information from industry regarding appropriate Remote ID technologies and issues. Information will be gathered as a result of the Remote ID request for information previously posted, one-on-one discussions, and UAS Remote ID demonstration planning workshops. Outputs from this phase will shape the initial demonstrations framework.

2) Demonstration phase: Deploy working demonstrations of information exchange capabilities between FAA and commercial providers that address Remote ID requirements as determined through the market research and initial collaboration activities. FAA anticipates that one or more Remote ID demonstration systems will be fielded.

3) Demonstration collaboration phase: Establish collaborative problem-solving among FAA, other government entities, and industry cohort to address sUAS Remote ID information and data sharing needs, assess experience data collected from demonstrations, and recommend system enhancements. Data collection requirements and strategies will be developed as part of the workshop collaborations.

4) Expanded capability phase: Building on experience gained from the initial demonstrations, expand Remote ID and data exchange capabilities, taking into consideration the following:

    - Alternative approaches, technology solutions, development models, business models, evolution paths, scaling strategies, etc., for information sharing;
    - Assuring UAS Remote ID capabilities fulfill the complete set of requirements for the greatest number of potential sUAS operators;
    - How to collect, integrate, and display sUAS Remote ID operational information, government agencies, and local and regional authorized users of the capability.

5. EXPECTED BENEFITS

a) Establish the operational framework (requirements and criteria) for Remote ID USS and provide supporting data to airspace users as necessary for collaboration and safe operations.
b) Pursue the establishment of a practical approach to information and data sharing for the purpose of implementing an enterprise Remote ID capability.
c) Development of technical and legal framework for initial prototyping and testing that will inform a national capability.

6. RESPONSIBILITIES OF THE PARTIES

a. Both parties will:
   i. Engage collaboratively with Remote ID cohort members to develop demonstrations of information sharing capabilities that offer "proof of concept" for supporting sUAS Remote ID operations in an operational or field environment.
   ii. Apply collaborative problem solving amongst FAA and Remote ID cohort.
   iii. Work toward a goal of building prototype network Remote ID capabilities by December 2020.

b. The FAA will:
   i. Provide access to data sets, ConUse document, draft Performance Rules and ICD.
   ii. Provide subject matter expert review and advice to proposed technology products, concepts, equipment, software, and other related activities.

c. AirMap, Inc. will:
   .. Participate in monthly meetings (nominally 2 days in duration) in person in the Washington, D.C. area.
   ii. Send 2-3 representatives from its organization to each meeting referenced in Section 6(c)(i) of this MOU. Representatives that AirMap, Inc. provides for these meetings must possess the demonstrated capability to cover strategic, technical, and/or legal aspects of Remote ID.

d. Products. If applicable: All data and information produced as a result of AirMap, Inc. performing, managing and administering its responsibilities under this MOU shall be made available to the FAA for use in connection with its ongoing programs. This includes publication of results where appropriate, except in cases prohibited by proprietary and security considerations.

e. Public information. Subject to the terms set forth under Section 7 of this MOU, any press releases or published information resulting from AirMap, Inc. performing, managing and administering its responsibilities under this MOU must be coordinated with the FAA's POC, who will act as liaison with the FAA's Office of Communications. The FAA Program POC must be copied on all requests.

7. USE OF NAME, ENDORSEMENT AND PUBLICITY

a. Use of FAA Name Prohibited

AirMap, Inc. must not use the name of the FAA on any product or service, which is directly or indirectly related to either this MOU or any patent license or assignment, which implements this MOU without the prior approval of the FAA.

b. No Endorsement by the FAA

By entering into this MOU, the FAA does not directly or indirectly endorse any product or service provided, or to be provided, by AirMap, Inc., its successors, assignees, or licensees AirMap, Inc. must not in any way imply that this MOU is an endorsement by the FAA of any such product or service.

c. Publicity

Nothing in paragraphs a and b of Section 7 shall prevent AirMap, Inc. or the FAA from publicizing this MOU or activities taken pursuant to this MOU; provided that: (A) except as otherwise required by law, neither AirMap, Inc. nor the FAA shall publicize statements from the other Party's employees or the other Party's positions (regardless of whether such statements and/or positions were presented orally, visually or in writing) without the prior written approval of such Party, which may be withheld in its sole discretion; and (B) prior to any public announcements being released, AirMap, Inc. and the FAA each agree to provide such announcements in writing to the other Party for review.

8. POINTS OF CONTACT

For the Federal Aviation Administration:
Casey Nair
FAA UAS Services; Program Manager
[redacted]

For the AirMap, Inc.
NAME: Jacob Ruytenbeek
TITLE: Director of Government Affair
Phone: [redacted]
Email:

9. FUNDING

No funds are obligated under this MOU. Each party shall bear the full cost it incurs in performing, managing and administering its responsibilities under this MOU.

10. WARRANTIES

Neither the FAA nor the AirMap, Inc. makes any express or implied warranty as to any matter arising under this MOU.

11. EFFECTIVE DATE/TERM/TERMINATION

This MOU will take effect upon the date of the last signature of the Parties.

12. This MOU will remain in effect for a period of eighteen (18) months from its effective date. Any Party may terminate its participation in this MOU unilaterally by providing written notice to the other Parties at least thirty (30) calendar days in advance of the effective date of termination, or by mutual agreement.

13. CHANGES AND MODIFICATIONS

This MOU may be amended, including the inclusion of additional agencies and partners, at any time during the term by mutual agreement of the Parties and signed by the original signatories to the MOU or their designees or successors.

The Parties shall document the details of any such amendment in a writing signed by both parties.

14. CONSTRUCTION

The parties understand and agree that this MOU does not confer any legal rights, duties or obligations on either party and is not subject to dispute in any forum. Neither party is authorized or empowered to act on behalf of the other with regard to any matter. Neither party shall be bound by the acts or conduct of the other in connection with any activity under this MOU. This provision shall survive termination of this MOU.

Nothing in this MOU shall be interpreted as limiting, superseding, or otherwise affecting a Party from conducting normal operations or making decisions in carrying out its mission and duties. This MOU does not limit or restrict the Parties from participating in similar activities or arrangements with other entities.

15. PROTECTION OF CONFIDENTIAL/PRIVILEGED INFORMATION

Each party shall take appropriate measures to protect proprietary, privileged or otherwise confidential information obtained as a result of its activities under this MOU.

16. LEGAL AUTHORITY

The authority for this MOU is 49 U.S.C 106 (f)(2)(A) and 106(*l*) and (m).

17. SIGNATURES

The FAA and AirMap, Inc. agree to the provisions of this MOU as indicated by the signatures of their duly authorized representatives:

COMPANY SIGNATURE  INSERT DATE David Hose, CEO	
Casey Nair UAS Services Program Manager Federal Aviation Administration	
Stephen Jenniss Contracting Officer Federal Aviation Administration	

From: Harrison, Tenisha (FAA)
Sent: Friday, January 24, 2020 7:53 AM
Cc: Gullan, Nina CTR (FAA); LePage, Allison (FAA); Nair, Casey (FAA)
Subject: Remote ID Cohort_Communication, Marketing and Outreach Info

Good Morning and Happy Friday All!

My name is Tenisha Harrison and I have recently taken over as the CO (thank you Stephen Jenniss!) on this Remote ID Cohort effort. I look forward with meeting and working with you all!

The Office of Communications (AOC) is developing an outreach strategy and announcement plan for the Remote Id Cohort, and would like to connect with your communication team to coordinate external messaging and press releases as well as provide guidance on shared key messages. Please connect with my colleagues *Alison LePage and Nina Gullan (cc'd)* so that they may coordinate with you directly, answer any marketing/outreach questions you may have and ensure message consistency. They are also developing art work for remote ID that you will be able to use in your own marketing materials. (Note: Please do not use the FAA logo on your website or remote ID materials.)

Thanks and have a wonderful weekend ☺

Tenisha Harrison
Contracting Officer
SE2020/2025 Team AAQ-350
Federal Aviation Administration
Phone: [redacted]

ACQ
WE GET IT

From: Harrison, Tenisha (FAA)
Sent: Friday, February 07, 2020 10:12 AM
Cc: Nair, Casey (FAA)
Subject: 1st Remote ID Technical Interchange Meeting (2/26 - 2/27)
Attachments: TIM1 HL Agenda Draft 20200205.docx

Good Morning Cohort Members!

We know everyone is eager to make travel plans for our first upcoming meeting. Here are the detail.

The first Remote ID Technical Interchange Meeting (TIM) will be held on February 26-27, 2020. The location will be the AMA Conference Center in Arlington, VA (see https://www.amaconferencecenters.org/washington/). Meetings will convene each day from 9:00am to 3:00pm with a break for lunch. The agenda is attached.

To maximize the effectiveness of these meetings, there will be no teleconference attendance (in person only). The FAA recommends each participating industry organization send 2-3 representatives to cover the areas of technology, operations, and program management (this first TIM will not require legal expertise, although future TIMs will). The TIM location is particularly convenient to Washington National Airport (DCA), but in any case participants are free to arrange travel and accommodations as they see fit. There are numerous hotels and restaurants in the Crystal City area; all costs must be borne by attendees independently. Please confirm a list of your organization's attendees to Tenisha.Harrison@faa.gov by COB February 20 so that the FAA knows who to expect and can prepare appropriately.

We look forward to meeting with you. Have a wonderful weekend ☺

Tenisha Harrison
Contracting Officer
SE2020/2025 Team AAQ-350
Federal Aviation Administration
Phone: [redacted]

ACQ
WE GET IT

Agenda

DAY 1

1. Welcome and Agenda Overview
    - Introductions of all participants
    - Expectations and Ground Rules
    - Meeting Schedule
    - Scope

    Introduce all TIM participants, including participating FAA organizations and their roles. Discuss the planned organization and ground rules of the meeting (such as expectation that everyone will participate). Lay out the planned scope of the TIMs.

2. RID Minimum Viable Product (MVP)
    - Objective
    - Desired Outcomes
    - Schedule
    - Major Elements of MVP

    Define the concept and objective of the RID MVP capability. Define the planned outcomes that the group seeks in developing and deploying the MVP. Discuss the planned schedule for achieving an operational MVP by December 2020.

3. RID Concept of Use (ConUse)
    - High-Level Walkthrough
    - Focus on RID Networking (5.4)
    - Focus on Data Exchanges (5.7)

    Level-set concerning fundamental approach to network-based RID.

4. MVP System Architecture
    - Data Links and Performance
    - Interfaces (protocols, security, etc.)
    - Data Standards
    - Authentication Framework

    Discuss broad technical options. It is important cover these thoroughly early in the program.

Agenda

DAY 2

5. MVP USS Performance Rules
    - Baseline Streams
    - High Availability
    - Degradation & Protection
    - Quality Assurance (O&M)

    Introduce an outline of the Rules. Discuss starting points on key topics such as those listed above.

6. USS-FAA RID Interface Control Document
    - Operational Endpoints / Messages
    - Operations and Maintenance (O&M) Endpoints / Messages
    - Supporting Endpoints / Messages for Overhead (security, etc.)

    Introduce an outline of the ICD. Start framing and filling in details as possible in light of architecture and protocol open decisions.

7. RID USS MOA
    - General Scope & Topics
    - Anticipated Activities and Milestones

    Establish role of RID USS MOA, its general characteristics, and plan moving forward.

From: Harrison, Tenisha (FAA)
Sent: Tuesday, March 10, 2020 10:24 AM
Cc: Nair, Casey (FAA); Zachary Desmond (Evans Incorporated); Rinehart, David CTR (FAA); msanders@aurora-innovations.com; Jim Little; Larrow, Jarrett (FAA); jillian mcknight
Subject: RID TIM Notes + Slides_from February 26th and 27th
Attachments: FAA RID TIM Slides_Feb_2020_FINAL.pptx; RID USS TIM 01 Notes Feb_2020_Final.docx

Hello Cohort Members,

Thank you for your participation in the initial Remote ID Cohort kick-off meeting held in Arlington, VA February 26th and 27th. Enclosed you will find the Technical Interchange Meeting (TIM) slides, notes and actions from that meeting. Please note that there are a set of actions posted within the notes and some of those actions are due by the cohort in advance of the next TIM scheduled for March 24th and 25th.

Please note that the next meeting will be planned as a video teleconference and will be remote only. The FAA will provide additional details on that meeting as the time approaches. The FAA is currently planning for the next TIM using the outcomes from the initial meeting. If you additional topics you would like to discuss, please forward them to my attention by March 15, 2020.

Thank You,
Tenisha Harrison
Contracting Officer
SE2020/2025 Team AAQ-350
Federal Aviation Administration
Phone: [redacted]

ACQ
WE GET IT

Remote ID Cohort

Technical Interchange Meeting #1

February 26-27, 2020

Proprietary

Remote ID TIM Agenda – Day 1

Welcome & Agenda Overview • Introduction of all participants • Expectations and Ground Rules • Meeting Schedule • Scope
Concept of Use Review
Overview of Remote ID Data Exchange (RIDEx)
12:00 – 1:00 PM : Lunch
Topic: Baseline Streams

Remote ID TIM Agenda – Day 2

Topic: Authorizations & Authentication
Topic: Service Monitoring & Analytics
Topic: Public Data Sharing
12:00 – 1:00 PM: Lunch
Topic: Reliability
Other USS Rules
Wrap Up

Program Introduction

Intro and Welcome

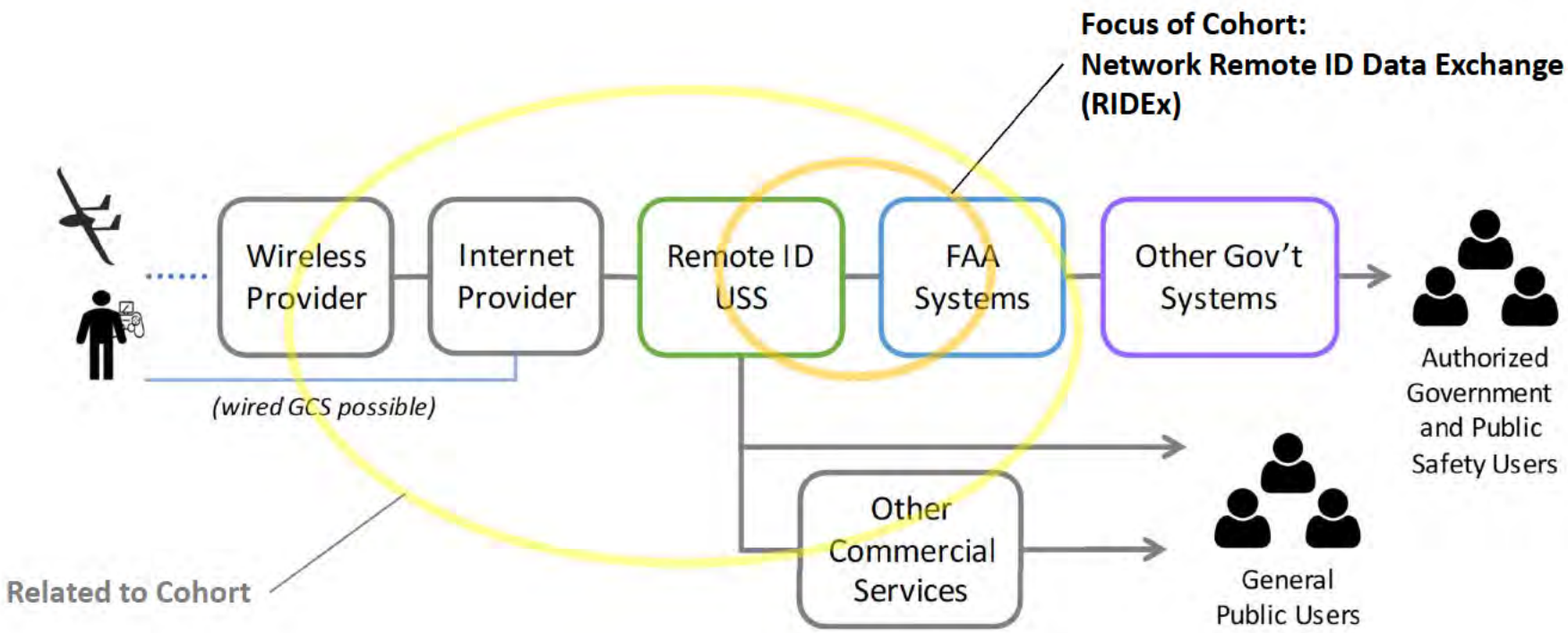
- **Welcome**
- **Why are we here?**
  - Context for Cohort and TIM
  - What we know and don't know
- **How will this work?**
  - What you can expect to hear from us
  - How you can participate – expectation of connected system later in the year
  - Rules that govern the USS will be issued in May timeframe with the expectation of design onboarding in late Fall CY20
- **Operating Norms**
  - Guidelines for the Cohort – Not Federal Advisory Committee Meeting (FACA);
  - Not consensus making body – All ideas will be considered
  - Operating norm – Express design and architecture ideas in the cohort and we will address as needed
- **Operating Tempo**
  - Monthly meetings
  - Locations
  - Overall Schedule and expectations to participate

Cohort Members – Please Introduce Yourselves!

- What does your organization do?
- Who are your representatives?
- What is your anticipated role in Remote ID?
- What does your organization expect to get out of cohort involvement?

Concept of Use
Review for the Cohort

Remote ID Intermediaries (ConUse)



Scenarios (Section 6)

- **Parts of the scenarios involve RIDEx capabilities:**
  - Network Remote ID via USS
  - Remote ID capability in the near term
  - Failover / roaming
- **Not all points relate to RIDEx:**
  - Broadcast
  - Public access
  - Government use of data
- **Scenario 6.1 applies through "Bravo"**
- **Scenario 6.2 only the first paragraph is relevant to RIDEx**
- **(Read through relevant parts of scenarios & discuss)**

RID Networking (5.4)

Network Remote ID is Internet-Based

- USS must offer services on the internet
- FAA is flexible on other details of UAS networking
  (Use existing mobile data plan? Special hardware/plans? etc.)

"Phone on a controller" seems like the likely first configuration

"Phone on a drone" could also work within RIDEx v1

Data Exchanges (5.7): USS-FAA

RIDEx 2020 = Baseline Streams and minimal monitoring *only*

Major USS-FAA characteristics:

- FAA cloud infrastructure hosting Remote ID services
- Online USS systems
- Industry-standard, secure interfaces
- 24/7 availability with backups and redundancies
- Automation of nominal processes
- Authentication and credentials administered by the FAA

Baseline Streams rationale:

- The FAA (and other government users) may not need every message, especially not redundant ones.
- Excessive bandwidth use is inefficient for systems on both sides.
- The USS can store messages for later retrieval if needed.
- A certain degree of near-real-time data is necessary for situational awareness.
- Data transfer requirements will be driven not only by the FAA, but also by other government stakeholders downstream of the FAA.

Data Exchanges (5.7): USS-USS

- FAA does not have a direct need for USS-USS communication
- However, RIDEx could provide USS-USS authentication
- Is this useful to USSs?

Key Take-Aways from ConUse

- The purpose of Remote ID is supplying necessary data to security partners...
  not Air Traffic, different from LAANC
- FAA is designated regulator for airspace...
  needs appropriate systems, data, and processes to conduct its mandated role
- Network Remote ID is a foundational mechanism in the Remote ID concept

Network Remote ID Data Exchange (RIDEx) 2020: Introduction for the Cohort

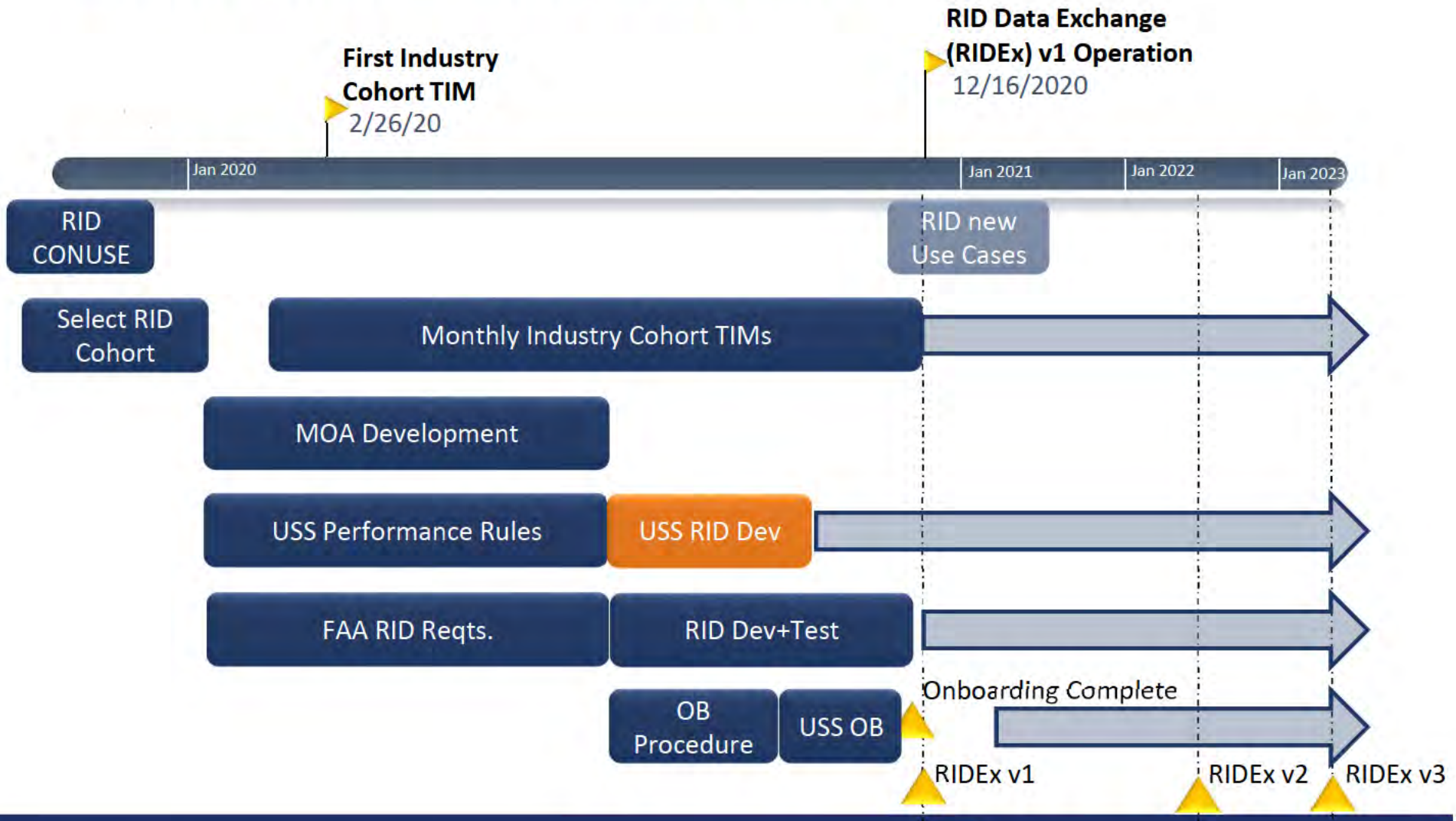
RIDEx 2020 Objectives & Outcomes

- Establish minimum level of common operational picture over the Remote ID network capability.
- Complete by end of 2020.
- Establish Remote ID USSs.

  Fundamentals such as:

  - operator access
  - data logging
  - service monitoring
- Support service availability to UAS of 99.9%.

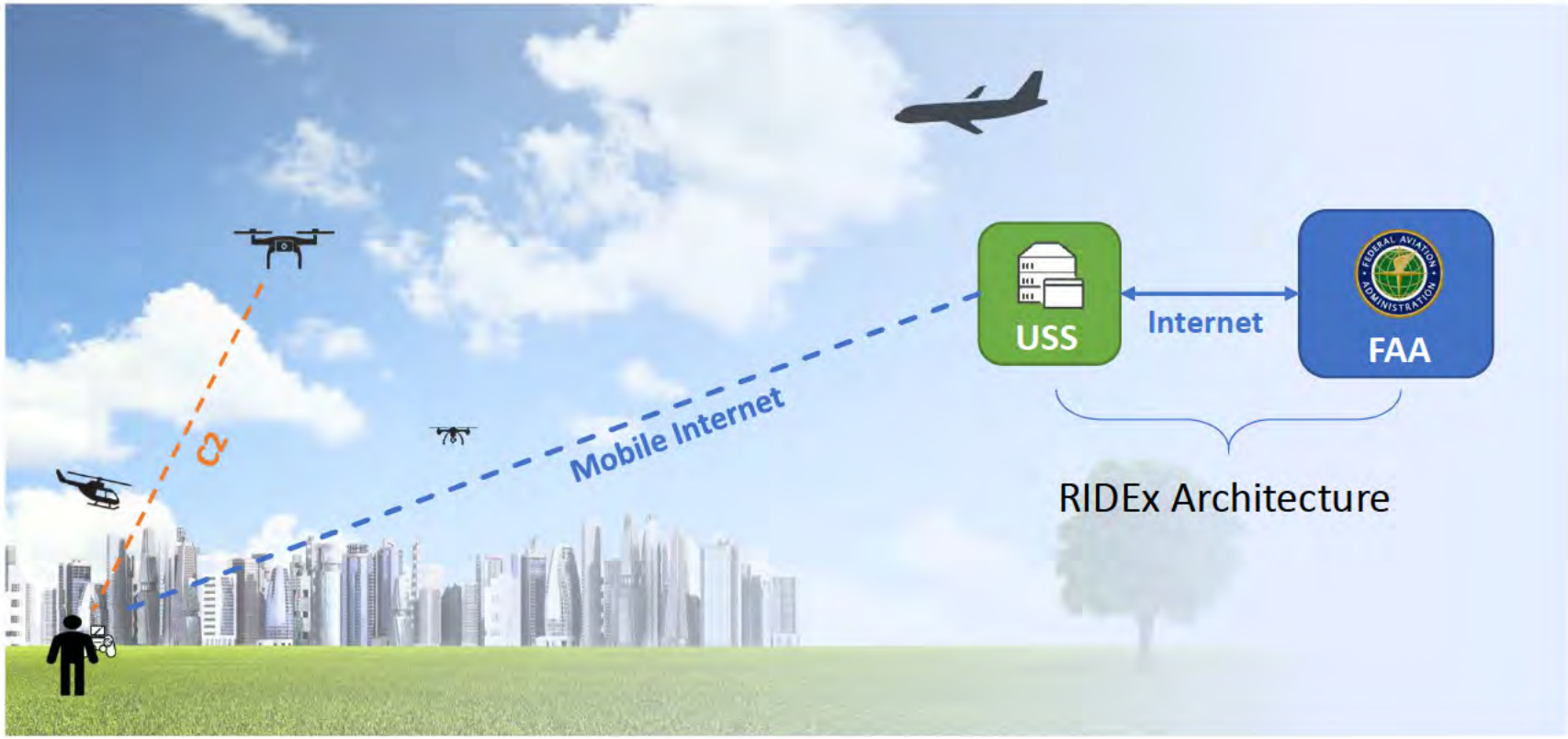
Overall RIDEx 2020 Schedule



RIDEx 2020 Scope

1. Basic Secure Connections between USS and FAA (A&A)
2. Initial Data Models
3. Baseline Streams
4. Basic Monitoring & Analytics between USS and FAA

Operational Context



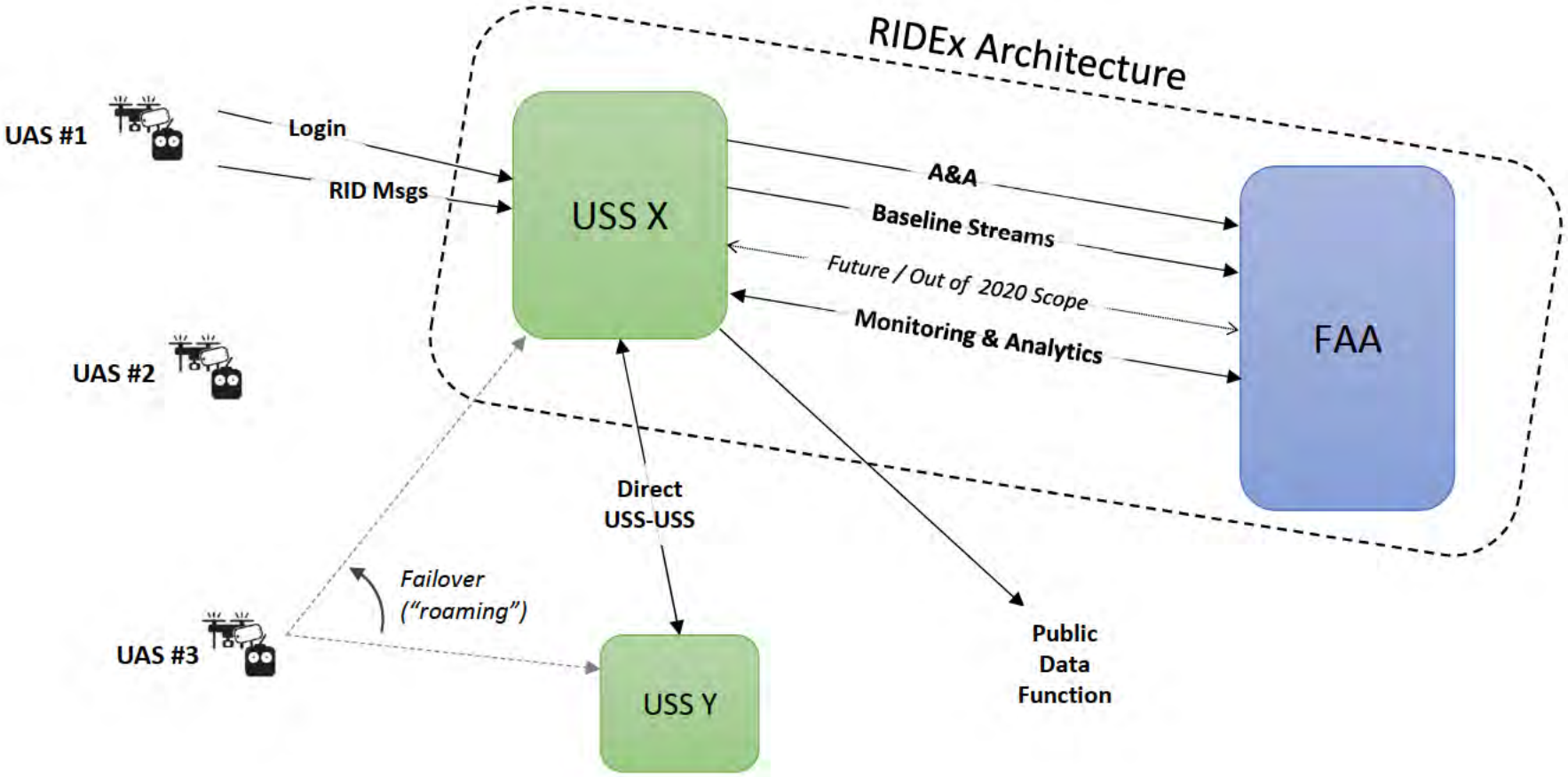
RIDEx Architecture Foundational Pillars

Pillar	Objective/Reason	How
Operational Excellence	To run and monitor systems to deliver business value and to continually improve supporting processes and procedures	• Logging capabilities • Monitoring capabilities • Change management processes
Security	To protect information, systems, and assets while delivering business value through risk assessments and mitigation strategies	• Network security measures • Application access (MFA AuthN/AuthZ/) • Data security(data in-transit and data at-rest)
Reliability	To be able to recover from infrastructure or service disruptions, dynamically acquire computing resources to meet demand, and mitigate any disruptions (i.e. misconfigurations or transient network issues)	• USS Failover • Soft dependency on FAA
Performance Efficiency	To use computing resources efficiently to meet system requirements and to maintain that efficiency as demand changes and technologies evolve	• Efficient, simple protocols • Modern computing design

RIDEx Architecture Application Pillars

Pillar	Objective/Reason	How
Composability	To allow ease of composing and connecting application components in order building higher-level services.	• Employing modern API-driven, standard-based integration protocol between USS and FAA
Flexibility	To decouple USS and FAA (system-to-system) and to allow configuration driven design and agnostic implementation	• Establishing loose coupled design with standard based design of the Contract/Interface
Programmability	To utilize API-first approach to provisioning, deployment, and management	• Central focus is on USS-FAA API
Frictionlessness	To hide the complexity and detail of infrastructure and operations from the application layer	• Containerizing application components and achieving ease of portability, scalability and deployment

Data Exchanges (with Context)



Elements of RIDEx Data Model

Topic: Baseline Streams

Baseline Messages

- Controller location
- Drone Location (if available)
- Serial Number
- Date/Timestamp
- Emergency Status

Topic: Service Monitoring & Analytics

Status

- Up/Down
- Status Codes

Analytics

- # Unique UAS (for example)
- ...

Application of Scenario to RIDEx

- Alpha USS connects to FAA (A&A)
- Patty Pilot powers up drone – connects to Alpha
- Patty takes off – first RID message to FAA (Baseline Stream)
- Patty continues to fly, generating messages (Baseline Stream)
- Patty lands – last RID message to FAA (Baseline Stream)
- Patty powers down drone – disconnects from Alpha
- FAA checks Alpha's system (Service Monitoring & Analytics)
- Alpha checks FAA's system (Service Monitoring & Analytics)
- Alpha renews connection to FAA (A&A)

Additional Functions

Standard for Public Data Function

- Part of 2020 objectives
- As regulator, FAA needs comprehensive and dedicated information streams (RIDEx)
- FAA is supportive of standards as a means of public network Remote ID information sharing

Additional Functions

FAA Correlation Functions

- In parallel with Cohort activities, FAA has a role correlating Remote ID information with other government-held information (registrations, authorizations)
- Correlation functions will be bounded by regulations for use of information
- Correlated information is not intended for distribution outside approved government uses

Baseline Streams

Baseline Streams

The concept of the baseline stream is to give the FAA initial minimal information on each operation.

- This is the simplest way to provide a common operational picture between USS and FAA
- FAA is single point of aggregation *for government uses*
- The baseline stream will be *much* smaller than the full stream of messages from the UAS to the USS

Baseline Stream: Scenario Summary

- Patty's UAS takes off. Immediately upon detecting takeoff, the UAS begins transmitting Remote ID messages to Alpha.
- Upon receiving the first report, Alpha begins a baseline stream of messages to the FAA. The first message is immediately forwarded to the FAA.
- At times, Patty flies quickly from place to place, and other times, hovers. When moving quickly, Alpha forwards a message to the baseline stream every time the position (since the last message) has changed more than 100' (configurable). When Patty hovers for long periods, the baseline stream rate slows to once per minute.
- When Patty lands, Alpha gets an indication of it, and sends the FAA the last baseline stream message. Alpha also indicates to the FAA that the flight has landed.

Baseline Stream: High-Level Requirements

- USSs send a reduced set of UAS Remote ID messages to the FAA.
- Baseline stream happens by default any time a UAS operation occurs.
- Baseline stream is configurable (at the program level).
  E.g. USSs could be asked to change the period between baseline stream messages.
- The USS may or may not get confirmation of receipt.
- Remote ID messages must be secured to ensure that they come from an authorized USS and are not tampered in transit.
  Note: see A&A section.

Baseline Stream: USS Rules

- Applicability
  - Reports shall be provided for every connected UAS being serviced by the USS between takeoff and landing
- Frequency
  - USS shall provide at least 1 report / minute to the FAA for every connected UAS
- Latency
  - Time of Applicability of RID reports sent to FAA must not exceed 3 sec (includes maximum latency of RID message and latency of RID report creation and transmission)
- Encryption
  - Use of industry standard encryption method
- Messages must be valid per ICD
  - USS must generate message, and FAA may verify correctness

Baseline Stream: USS Rules (Data Retention)

- Retention
  - USS must retain UAS data transmitted to FAA for all operations for a period of 6 months
  - USS must make RID records available to FAA upon request

Baseline Streams: Data Model

Data Item	Description
Serial Number	Unique Identifier for the UAS
Control Station Location	Latitude, Longitude, Barometric Altitude
Aircraft Location (if available)	Latitude, Longitude, Barometric Altitude
Date/Timestamp	UTC, corresponding to location data
Emergency Status	Identifies special flight situations

Data Exchange Architecture: Baseline Stream

- Who is communicating with whom?
- Who initiates?
- Does the sender need confirmation of receipt?
- Does the data need guaranteed delivery?
- Does lost data need to be recovered?
- How much data (bandwidth)?
- Frequency?
- Reliability, availability, security?

Authorization & Authentication

Authentication & Authorization

- Leverage best practices
- Basis for trusted Remote ID messages from USSs
- Also could provide basis for USS-USS communication
- Notionally FAA can provide high-reliability A&A services (within constraints)

A&A: Scenario Summary

- Patty's USS, "Alpha Inc.", must authenticate and authorize to connect to the FAA.
- Alpha provides credentials and is given access to the FAA side of RIDEx.
- Access is not indefinite – credentials need to be re-submitted periodically.

For consideration:

Since Alpha must provide baseline streams at any time with no prior warning, it should maintain a continuous connection to the FAA?

A&A: High-Level Requirements

- The FAA must authenticate a USS before accepting RID messages.
- Authentication must be renewed periodically.

A&A: USS Rules

- USS must follow A&A specification in ICD.
- Discussion: USSs may use FAA to authenticate (verify identity of) other USSs?

A&A: Data Exchange Architecture

- Who is communicating with whom?
- Who initiates?
- Does the sender need confirmation of receipt?
- Does the data need guaranteed delivery?
- Does lost data need to be recovered?
- How much data (bandwidth)?
- Frequency?
- Reliability, availability, security?

Service Monitoring & Analytics

Service Monitoring & Analytics (SM&A)

- Resilient capability calls for shared system awareness.
- Automated status and analytics are bi-directional between USS and FAA.
- Data logging and access is required for process monitoring.
  Note: automated SM&A only touches a small portion of logged data.

SM&A: Scenario Summary

- Both the FAA and the USS could have concerns that the other side is functioning and healthy.
- The FAA calls the USS periodically to check for operational status (determined automatically) and basic operational statistics. In this case, the FAA calls Alpha for health status every minute (configurable) and operational statistics every hour (configurable).
- Alpha does the same checks on the FAA.

SM&A: High-Level Requirements

- The FAA can determine if the USS is functioning normally.
- The USS can determine if the FAA is functioning normally.
- The FAA can retrieve analytics from the USS for comparison to its own records.
- The USS can retrieve analytics from the FAA for comparison to its own records.

SM&A: USS Rules

- **Service Status**
  - USS must expose a system monitoring API to the FAA that provides service status indicators
- **Data Logging**
  - USS must log all RID data *(policy, only status/analytics in API)*
- **Analytics**
  - USS must expose an operations analytics API to the FAA that provides operations information for the requested time period
- **Reporting**
  - USS must report service outages (planned and unplanned) to the FAA

SM&A: Data Model

Status

Data Item	Description
System Status	Up/Down
Error Codes / Descriptions	Diagnostic information

Analytics

Data Item	Description
UAS Counts	Number of UAS exchanged in past 24hrs (for example)
Message Counts	Number of messages in the past 24hrs (for example)

SM&A: Data Exchange Architecture

- Who is communicating with whom?
- Who initiates?
- Does the sender need confirmation of receipt?
- Does lost data need to be recovered?
- How much data (bandwidth)?
- Frequency?
- Reliability, availability, security?

RIDEx v1 Reliability

Reliability (Intermittent Connection): Scenario Summary

- Charlie loses connection while flying in a rural area due to limited mobile internet coverage.
- Bravo identifies a lost connection.
- Charlie realizes he has lost connection and must land his UAS safely as soon as practicable (limited drone / no broadcast).
- If the connection is restored before Charlie's UAS lands, the operation can continue.

Reliability (USS Outage): Scenario Summary

- Patty loses connection while flying because Alpha's servers have an outage.
- Patty's UAS attempts to login and connect to an alternate USS, Bravo, after determining that Alpha out of service.
- If the connection to Bravo is successful, the operation continues without interruption (If the connection to Bravo is unsuccessful, Patty can continue to fly based on broadcast).

Reliability (Anti-spoofing): Scenario Summary

- A hacker pretends to be a drone and fools Alpha's servers and injects false RID messages into Alpha
- Alpha identifies spoofed targets and does not process them as valid UAS RID information

Reliability: High-Level Requirements

- The Network Remote ID capability must be tolerant to intermittent connections.
- The Network Remote ID capability must be tolerant to individual USS outages.
- The Network Remote ID capability must be tolerant to FAA system outages.
- The Network Remote ID capability must protect against false UAS reports.

Reliability: USS Rules

- **Intermittent Connections**
  - If a RID connection is restored with for the same UAS before landing (i.e. RID messages are received according to required performance tolerances), the USS must resume sending RID reports to the FAA
- **USS/FAA Outages *(for discussion)***
  - USS availability must align with RID availability > 0.999
  - If USS experiences an outage, the USS must provide an automatic failover to another RID USS
  - If USS does not receive a response from the FAA (i.e. FAA outage), the USS may continue to send RID reports for connected UAS.

Reliability: USS Rules

- **Anti-spoofing**
  - USS must incorporate a mechanism to detect and mitigated against false targets (i.e. some level of UAS / user validation)
  - USS must ensure that no unique UAS serial number is being received by more than one connected UAS
  - Serial number of a connected drone should not change during a connected session
  - USS must send validated RID messages to the FAA

Public RID Information

Public RID Information: Scenario Summary

- Joe sees a UAS flying near his house and would like to learn more information on it
- He opens a commercial service on his smartphone and sees general operating information for the UAS, which is updated regularly as the aircraft moves
- He also sees information for other UAS in the vicinity through the same service

Public RID Information: High-Level Requirements

- The public needs a mechanism for obtaining RID messages for situational awareness of drone activity.

Public RID Information: USS Rules

- USSs must make RID information available to the public for situational awareness and commercial services

Public RID Information: Data Model

Note: FAA is not involved in sending or receiving this data.

Data Item	Description
Serial Number	Unique Identifier for the UAS
Control Station Location	Latitude, Longitude, Barometric Altitude
Aircraft Location (if available)	Latitude, Longitude, Barometric Altitude
Date/Timestamp	UTC, corresponding to location data
Emergency Status	Identifies special flight situations

Other RID USS Performance Rules

Other – Access/Accounts & Data Sources

- **Accounts & Identification**
  - USSs must manage operator accounts using reasonably secure identification methods
  - USSs must make a capability statement availability to operators upon account creation and login
  - USSs must notify operators that of the FAA privacy statement

Wrap Up

TIM Schedule

- March 24-25
- April 28-29
- May 27-28
- June 23-24
- July 28-29
- August 25-26
- September 29-30
- October 27-28
- November 23-24
- December 16-17

Remote ID TIM Meeting #1

Notes and Action Items Day 1 and 2: 2/26/20 – 2/27/20

FAA Attendees: PMO, AGC, AUS, AIT, ASH

Industry Attendees: Airbus, AirMap, Amazon, Intel, OneSky, Skyward, T-Mobile, Wing

[Bullets indicate points the FAA made in connection with the TIM presentation and discussion topics. Points made by cohort participants are labelled "Industry".]

Actions:

Action	Assigned	Due Date
Be prepared to present/discuss ASTM standard in depth, focusing on those areas that map to the concepts presented by the FAA.	Cohort	March TIM
Bring questions about the ASTM standard	FAA	March TIM
Investigate how LAANC Rules and RID Rules overlap.	FAA	March TIM
Discuss public dating sharing and the standard.	Cohort	March TIM
Better define the government use cases of the baseline stream.	FAA	March TIM
Define what is the need for emergency status field in the baseline stream?	FAA	March TIM
Send implementation ideas for the baseline stream.	Cohort	March TIM
Consider using the same OAuth that is used in LAANC (Non-VPN, OAuth based, non-SWIM).	FAA	March TIM
Consider automated onboarding and continuous verification	FAA	March TIM
Consider RID and LAANC onboarding simultaneously	FAA	March TIM

Framing the TIM and "Ground Rules"

- Any comments on the proposed rule need to go to the docket, these TIMs will not discuss the NPRM. Basis of discussion will be RID ConUse document.
- The goal for this year is to figure out the first version of network Remote ID, not strategic deconfliction or other UTM efforts
- The FAA aiming for draft USS Rules early May and onboarding period will be in late Fall CY20
- Plan for monthly meetings (TIMs) until December

Topic: ConUse Overview

- FAA views Remote ID USSs as independent from LAANC USSs. An organization may be both.
- The TIMs will build on the ConUse. The ConUse is the source reference document for the cohort's work this year. Note that the ConUse is separate from the NPRM.
- Cohort will discuss how data is protected and shared in this concept.
- Presented and discussed ConUse scenarios as they relate to network Remote ID, specifically the link between USS and FAA.

Industry: Recommend that there is a consideration that government pays for some historical data requests. There are examples of this in other telecom areas.

Industry: Does the FAA see the role they play in data sharing between USSs?
FAA Response: The FAA does not expect to be an intermediary for data between USSs. The FAA may provide authentication and authorization services to support the exchange.

Industry: Why a group this size and why these players?
FAA Response: The cohort was selected based on their RFI responses and various considerations, including a workable group size and composition.

Industry: Why are there no government security partners here?
FAA Response: ASH is here representing the government security partners.

- An underlying concept is that the source Remote ID information is public information. Everything happening on the FAA back-end is addressed in public SORN documentation. Most everything will go to federal security partners and law enforcement if they ask for it. By virtue of operating in U.S. airspace, data can be shared with government security partners.
- Assume that FAA will do correlation to other information it holds.

Industry: What can be subject to FOIA by the public?
FAA Response: All the Systems Of Records Notice (SORN) address what can be provide to the public.

Industry: What will future versions of RID look like?
FAA Response: The immediate focus is on functionality for 2020. Likely need a few years with iterations for additional capabilities (i.e. queries, subscriptions, session IDs).

Industry: Concern about the burden of onboarding checkout for USSs.
Industry: Recent LAANC checkout has been far less painful (getting better).
FAA Response: Unlike LAANC, Remote ID does not fundamentally include a UI. This should make onboarding less difficult and potentially more automated.

Industry: Where does the ConUse end? The network concept demands some level of interface between the USS and the vehicle, and we don't have any manufacturers. Which governing body

will address this? Move to industry or not. Concern that there is a need for standardization and control on this side.

Industry: What happens when there is an FAA outage? How will the operator still have Remote ID services?
FAA Response: The USS only needs to attempt to send baseline data to the FAA; if the FAA is unresponsive, it's not the USS or operator responsibility and the operator can continue to operate.

Industry: Recommend session IDs this year as a feature from the start, believe that this is a huge benefit to provide to operators and manufacturers.
Industry: Cohort agreement.
FAA Response: Policies would have to be put in place. Need to make sure there is bandwidth to do it.

Industry: Do you see the FAA recognize a commercial standard as an MOC between vehicle and USS in the UTM standard?

Industry: Why is baseline stream useful to FAA and law enforcement, especially if law enforcement in scenario really wants the higher fidelity data.
FAA Response: The FAA determined to start with a low bar for entry (baseline stream should require less resources than high-fidelity data). The capability could evolve in either direction after this initial start. Regarding use of baseline stream, interagency partners and inspectors ask for general awareness information all the time (who is flying, where, etc.). Unlikely that this is where we land as a permanent data delivery. Understood that Counter-UAS will need a higher fidelity feed one way or another.

Industry: Why does the FAA care about the connection between the phone on the drone?
FAA Response: The specific implementation is not important but need to make sure there is some viable concept for drone to share data with the USS.
Industry: Suggests other ways i.e. wireless networks.

Industry: Suggest having some interface that can be used to simulate vehicles in the onboarding test process. The FAA can simulate the data to USS systems. But it's also important to have actual vehicles in operation for 2020 in order to achieve success.

Industry: Does there need to be a validation of the drone data?
FAA Response: Not in general, it's assumed it's accurate, but some protection against spoofing etc. is needed.

- Government users want baseline stream and need information like this constantly. If we don't have baseline stream and awareness, how does FAA or government security partners know what to ask for?

Industry: Wants FAA to help authenticate USS to USS communication.

Industry: Where does law enforcement fit in to connection? If USSs aren't in communication with one another, does the public feed fall apart. All USSs need to be able to exchange information.

Industry: What value is public data to law enforcement; they want a smartphone app that they can open and go right away.
FAA Response: Public data has some value but yes, they want more. FAA doing this work separately from the initial work of the cohort.

Topic: RID Exchange (RIDEx) Overview

Industry: RID trial demonstrated some type of knowledge function for local law enforcement.
FAA Response: FAA concerned about any discussion of operator education and law enforcement education. FAA working on it but doesn't want to address it here. Baseline assumption is all operators know and follow rules, as does law enforcement.

- FAA would get a constant baseline stream by default from each USS as a push-type data exchange.
- Supply Remote ID info to the public is separate from the baseline stream and does not go through FAA.
- This is where we are going to start the network Remote ID work.
- Expect options for future capabilities – but for now we are trying to get capabilities to Remote ID users by early next year.

Industry: Concerned that a USS cannot achieve an availability of 99.9%.
FAA Response: The 99.9% is for the overall operator access to Remote ID, it could be achieved via the failover (roaming) mechanism.
Industry: Recommends achieving this availability and ignoring fail-over. Concern that USS can or cannot meet 99.9% availability – does it matter? Some USSs plan to manage private fleets, they can handle it internally if they are down.

Industry: Concerned about planning for data integrity.

Industry: [Concerning application principles presented] Are these principles to be imposed on USS architecture as well, or does FAA care?
FAA Response: FAA doesn't care as long as applicable contracts are followed. These principles are presented for collaboration and shared objectives.

Industry: Why is the baseline stream needed? Why not use InterUSS – have the FAA be a node like other USSs – and not have a standing data feed? Why get all license plates when you can selectively get the ones you need?
FAA Response: InterUSS appears promising for UTM and certain use cases, but it's not sufficient for anticipated government Remote ID uses. Baseline stream is planned for initial 2020 work.

Industry: No discussion of what the operator needs. In order to get a baseline stream, we need someone to opt in so how does the schedule line up for this? FAA dancing around topic of Rule finalization. USSs don't want to invest if this is only a technical paper exercise or something that doesn't go live.
FAA Response: Need to work out details, and FAA is considering ways to encourage early adoption. Even if adoption is limited, nothing prevents willing volunteers from doing a task.

Industry: There is a DAC tasker to look at some incentivization for willing volunteers.

- Session ID could be added this year, per earlier feedback – FAA will consider
- Supplemental information presented (such as connection status), at least discuss

Industry: Suggests examining the ASTM standard for data formats and don't make new ones unnecessarily. Copy the same JSON formats and follow API spec in published standard.
Use RESTful APIs.
FAA Response: Want to use that standard for the public data sharing, perhaps other aspects – will take back and consider.

Industry: What about intent information?
FAA Response: Not in scope for this work, but maybe in the future.

- USSs will need to be able to do both functions (baseline stream and general public information) to be approved.

Industry: Can we charge for public data sharing? Will this be in the rule or the MOA?
FAA Response: FAA will define requirements in RID USS Performance Rules.

Industry: Clearly define what RID data is so we don't have problems (like on LAANC) in the future. Be clear with terminology, make sure that RID service doesn't hinder from promoting other services.

ACTION: Cohort – be prepared to present/discuss ASTM standard in depth, focusing on those areas that map to the concepts presented by the FAA.
FAA to bring questions about the ASTM standard.

Topic: Baseline Streams

Industry: Recommend correlating session IDs to serial numbers.

- Baseline stream report could be triggered by a maximum time since last report (nominally 1min) or maximum distance (nominally 100ft).

Industry: What is the fidelity of position report for baseline stream because the use case isn't clear. What does the special feed gain for the added complexity? Why does FAA not adopt a tile model and possibly offer much less fidelity and precision.

Industry: The maximum distance idea adds complexity by adding state information in generating the baseline stream. That's an undesirable resource (computing) load.

Industry: Prefers a standing 1 min, preferred over 1 sec, without variations.

- FAA also want to help maintain the value added of USS. The 1-minute update was decided by FAA to provide some awareness of who's flying but not going to answer all questions.

Industry: Why not just address the start and stop time of a flight, not any of the position reports?

Industry: Is there a possibility of starting with on-demand stream rather than baseline stream and moving to baseline later?

Industry: If the operator has a UAS that's less than .5 lbs flying Part 107 in a controlled airspace they need authorization, does USS need to mention that they need to comply with Remote ID rule? Need to think about how things overlap between RID and LAANC. Need to understand the use case to put in the rules.

Industry: Overall requirements for latency – best way to test is from into USS to out of USS. Brings it back to question of UAS-USS interface.

ACTION: FAA to investigate how LAANC Rules and RID Rules overlap.

ACTION: Next meeting discuss public dating sharing and the standard.

Industry: Need to clarify if baseline stream must be retained in a separate way from the high-fidelity source data. Once the FAA has data, why do USSs need to retain it?

- One of the drivers for 6 month planned retention requirement is connection to the enforcement period

ACTION: FAA to better define the government use cases of the baseline stream.

Day 2: 2-27-20

DAC Meeting Incentivizing RID equipage and USSs

- Period 1: NPRM to Final Rule and industry consensus standard exists
- Period 2: Final Rule to having an MOC, starts with USSs (December 2020) and Final Rule (date TBD)

- Period 3: FAA accepted standard to comply and NPRM compliance date with the rule – after publication

Topic: Baseline Streams cont'd

Industry: Emergency status? What's your roadmap?
FAA Response: The goal is to include emergency status in the first year. Open to industry input on format/contents.
Industry: Suggests making it like the safety justification field as like LAANC.

ACTION: FAA to define what is the need for emergency status field in the baseline stream?

- Initial FAA estimates for baseline stream, USS to FAA, are not excessive – ballpark less than 1Mbps.

Industry: Bandwidth may be higher because some recommend doing everything at the 1 min mark (a NAS-wide snapshot). So, much higher bandwidth during a few seconds out of the minute.
Industry: Need to consider. Some suggest best effort on USSs to make 1 min or more often, depending on their processing loads and make the FAA ready to accept.
Industry: Recommends fault tolerance to ensure that we receive messages or are prepared for bursts. What is the risk analysis for the system, risk of lost data, what is tolerance to data loss? FAA system needs to be prepared for data bursts and may get same message multiple times, depending on how USS systems are distributed and made redundant.
FAA Response: For this data exchange, tolerance for lost data is relatively high. Delivery does not need to be guaranteed.

Action: The cohort to send implementation ideas for the baseline stream.

Industry: Cohort consensus that keeping implementation lightweight is a priority for this year. Since it's not clear how it will evolve and who will adopt early, keep the investment required minimal. Even if simplified first iteration is replaced in the future.

Industry: USSs don't expect to make money off RID. It can be bundled with things that can be charged for, but generally don't think that this will be revenue-generating. Expectation is that manufacturers will be incentivized to be USSs, not create a market competition for the USS arena. Concern is that either user can pay or that manufacturer can pay, and therefore little expectation that anyone will go to a standalone USS.

Industry: Major concern: the USS concept proposed in rule will not work for business reasons. USSs see a need to realize revenue within 1-2 yrs to be viable. If operators want to become USSs, their model makes sense just for their own flights. Many see high volume of flight hours as key metric for revenue generation. When will that occur in Remote ID?

Industry: Investment perspectives on this include:

- global market view (create alternative to all-government approach)
- supporting other services like air taxi
- RID as a pillar for UTM and C-UAS
- services to end users like operators and public safety personnel

FAA: Encourage all to comment on the rule as appropriate.

Topic: Authorization & Authentication

- FAA will be provider of authentication services (HA), and USS to USS authentication can occur within some constraints (services not overloaded).

Industry: Recommends using the same OAuth service as LAANC, don't want new authentication providers. Cohort generally agreed.

ACTION: FAA to consider using the same OAuth that is used in LAANC (Non-VPN, OAuth based, non-SWIM).

Topic: Service Monitoring & Analytics

Industry: Generally, dislikes the statistics exchange that exists on LAANC. No LAANC USSs are using FAA O&M endpoints right now, except for FAA health and versions endpoints.
Industry: What do you need and why? (Use cases) FAA needs to do discuss what the need is for service monitoring and analytics

Industry: Proposed validation of a data injected into USS for testing. This can be an opportunity to improve onboarding.

ACTION: The FAA to consider automated onboarding and continuous verification.
ACTION: The FAA to consider RID and LAANC onboarding simultaneously.

- The goal is to log any data concerning the Remote ID function

FAA: Will you get raw data from UAS? Do you see that depending on what manufacturer does? That it would not be raw data but rather be a specifically Remote ID feed?

Industry: Note that often a USS might get raw data from the UAS and convert the data into different data sets, one of which is Remote ID data.

Industry: USS are already collecting data; would like all data to be on the same level of precision for all services. Generally want manufacturer to send the data once.

Industry: Example – DJI has SDK [software development kit] to access UAS data. Subscribe then convert SDK to support for RID.

Industry: If you ask us to save all data from RID: (telemetry); having clear boundary for what is needed and what is not is important.

Industry: There are a other functions USS can support, if the USS is already sending RID formatted data then FAA should receive it; standardization of the data format is a good USS function; it is one of the main points for having USS.

Topic: Reliability RIDEx

- Interoperability complexities with UAS types

Subtopic: Intermittent Service

Industry: Value interoperability but perhaps not advocate for 2020, support roaming approach. Could be taken into ASTM standard but not currently there. Currently, roaming in the telecom world is a contract between carriers and likely even no indicator to operator.

Industry: Recommends offering a high reliability and a low reliability service. Recommend using this as a business opportunity rather than as an FAA requirement.

Industry: Security operators need a high availability connection.

Industry: Also, should consider cross-border operations – failover could support international harmonization.

Subtopic: Anti-Spoofing

Industry: ASTM standard has validation, but it assumed that USS would have pilot information, such as license, registration, and serial number. Without access to that data, USSs cannot do those checks. Possible that it could be done on a large scale but not on a small scale.

FAA: Start with simple approaches to deliver anti-spoofing. Look for large flooding, repeated serial numbers, behavior not acting like a drone, etc.

Industry: Wants validation of registration information and pilot certification, not FAA giving data, just USS checking with FAA.

Industry: Can also do a pilot ID verification from the FAA.

FAA Response: Willing to consider but may not be in v1.

Industry: Cellular layer validation could accomplish this but generally don't want to tie this concept to cellular, which is not intended or desired.

Industry: Advocates for future sharing of registration data from FAA to USSs, which is what other governments are doing.

Discussed including in March Meeting:

- Baseline Stream Implementation
- F38 Standard – what can be applied to 2020 work

From: Harrison, Tenisha (FAA)
Sent: Friday, March 20, 2020 5:24 PM
Cc: Nair, Casey (FAA); 'Zachary Desmond (Evans Incorporated)'; Rinehart, David CTR (FAA); [redacted]; 'Jim Little'; Larrow, Jarrett (FAA); 'jillian mcknight'
Subject: 2nd Remote ID Technical Interchange Meeting (3/24 - 3/25)
Attachments: F3411.34559 (003).pdf

Hello Cohort Members,

Please see dates/times and video conference info for day 1 and 2 of our meeting next week. Please take care.

Meeting: Remote ID Data Exchange

TIM #2, Day 1 Date & Time: 24 March 2020, 11:00am-1:00pm EDT

TIM #2, Day 2 Date & Time: 25 March 2020, 11:00am-1:00pm and 2:00pm-4:00pm EDT

This meeting will be held by videoconference. Please note the following recommendations:

- For voice, participants can join with either phone or computer audio.
- Connect from your computer to view shared presentation materials and webcam video from other participants.
- Enable your webcam for better engagement among participants.
- Conferencing services and networks are under higher demand than usual. If a connection is stalled or malfunctioning, close it, and reconnect.
- If there is a significant disruption, the CO (Tenisha Harrison) will send an email with alternate arrangements.
- Zoom will be used. If you haven't used Zoom before, please visit the Zoom test site prior to the meeting to ensure you will be able to connect without problem.

Detailed connection steps:

1. Join the meeting 10-15 minutes ahead of time to allow for possible setup required.
2. Zoom link [redacted]
    a. Telephone Number: [redacted]
    b. Meeting ID: [redacted]
    c. Participant ID will be provided individually
3. You may need to download and install Zoom. A web client (little or no download) is probably also available.
4. You will be prompted for the meeting password. Enter "RemoteID".
5. Please sign in with your name and organization so that other participants can effectively identify you – for example: "Pat Smith (ABC Inc)". After connecting, you can edit your name by (1) Clicking on "Participants" in the Zoom task bar or hitting "Alt + U". (2) The Participant Bar will appear, hover the mouse over your name, and select "Rename" (3) Change your name and click OK
6. Audio: Default audio is through the computer. If you choose to use phone audio, please follow the below steps:
    a. The phone number, Meeting ID, and Participant ID can be found at any time by clicking the arrow next to the microphone on the Zoom task bar. Select "Switch to Phone Audio" and the phone number, Meeting ID, and Participant ID will be shown.

b. Please remember to enter your Participant ID (after the Meeting ID) so that your web/video connection is associated with your phone connection. This is important so that every caller is easily identified (there are no unknown participants) and others can tell who you are when you are talking. Unidentified callers may be removed by the organizer.
c. If, for whatever reason, you do not enter your Participant ID when prompted, you can enter it at any time later in the call. For example, if your Participant ID is 25, enter "#25#" at any time to associate your call with your web/video connection.

7. Please use webcams. You may need to enable browser or application access to your webcam. Webcam video can be turned on or off using the camera icon. Please use the Zoom test site ahead of time to test your connection.
8. The microphone icon can be used to mute yourself. Please mute yourself when you are not talking.
9. Chat system will be enabled during the meeting and can be accessed from the Zoom task bar.

Here is a link to some useful tips on videoconferencing: https://www.pcmag.com/how-to/8-tips-for-better-video-conference-calls

Tenisha Harrison
Contracting Officer
SE2020/2025 Team AAQ-350
Federal Aviation Administration
Phone: [redacted]

From: Harrison, Tenisha (FAA)
Sent: Thursday, April 23, 2020 1:06 PM
Cc: Nair, Casey (FAA); Gallagher, Victoria (FAA)
Subject: 3nd Remote ID Technical Interchange Meeting (4/28 - 4/29)
Attachments: TIM3-WebConf.docx; FAA RID TIM Apr 2020 Agenda DRAFT.pptx

Hello Cohort Members,

Please see dates/times, video conference info and agenda for day 1 and 2 of our meeting next week.

The Remote ID Data Exchange TIM #3 will be held on Tuesday April 28th and Wednesday April 29th. This TIM will consist of three 2-hour sessions held by webconference, two on the 28th and one on the 29th. Please see attached instructions for the webconference.

With regard to the cohort action item from TIM #2, cohort members are requested to send their onboarding input to the CO (Tenisha Harrison) before the 28th or bring their input to the TIM. Please be prepared to present and discuss onboarding input. With regard to the FAA action item from TIM #2, the FAA did not identify any questions on the ASTM standard requiring follow-up. The FAA has considered the ASTM standard extensively, which is a major topic of TIM #3. Please see attached draft agenda. Each cohort member organization is requested to participate with nominally two representatives. The FAA Program Office looks forward to a productive dialog with you on the 28th and 29th.

Take care and stay safe,

Tenisha Harrison
Contracting Officer
SE2020/2025 Team AAQ-350
Remote ID
LAANC
Federal Aviation Administration
Phone: [redacted]

ACQ
WE GET IT

Meeting: **Remote ID Data Exchange TIM #3**

Dates & Times: **28 April 2020, 11:00am-1:00pm and 2:00pm-4:00pm EDT**
29 April 2020, 11:00am-1:00pm EDT

This meeting will be held by videoconference. Please note the following recommendations:

- For voice, participants can join with either phone or computer audio.
- Connect from your computer to view shared presentation materials and webcam video from other participants.
- Enable your webcam for better engagement among participants.
- Conferencing services and networks are under higher demand than usual. If a connection is stalled or malfunctioning, close it, and reconnect.
- If there is a significant disruption, the CO (Tenisha Harrison) will send an email with alternate arrangements.

Detailed connection steps:

1. Join the meeting 10-15 minutes ahead of time to allow for possible setup required.
2. URL: [redacted]
3. This meeting is locked with a password: [redacted]
4. You can also dial in using your phone.
   United States: [redacted]
   One-touch [redacted]
   Access Code: [redacted]
   When joining by phone, Participant ID will be provided individually. Please enter it so that all callers are identified. Unidentified callers may be removed by the organizer.
5. Please sign in with your name and organization so that other participants can effectively identify you – for example: “Pat Smith (ABC Inc)”. After connecting, you can edit your name by in the participants list.
6. Please use webcams. You may need to enable browser or application access to your webcam. Webcam video can be turned on or off using the camera icon.
7. The microphone icon can be used to mute yourself. Please mute yourself when you are not talking.
8. Chat system will be enabled during the meeting.

Agenda Day 1 (4/28) – FAA & Industry Actions

Session 1 & 2: 11am-1pm & 2pm-4pm ET	
Welcome & Overview Program Update, Schedule, etc.	
FAA Action: Consider Leveraging ASTM Standard	Replanning MVP to Leverage ASTM Standard • Critical Goal for MVP: 1+ Qualified USSs Providing Public Service
	Revised MVP Architecture • High-Level Diagrams
	ASTM Requirements in FAA Qualification • Rules that are / are not incorporated into USS Rules
Industry Action: Onboarding Input	Onboarding & Test • Cohort Input • Testbed • End-to-End Automated Testing

Agenda Day 2 (4/29) – Other Topics

Session 3: 11am-1pm ET
Architecture of Authentication and Authorization (A&A) • Overall Design of FAA USS A&A Service • Credentialing processes in Onboarding, Continuous Monitoring, Upgrades, etc.
Interfaces (beyond ASTM Standard) • USS → PMO • USS → General Public • Session ID management

Miscellaneous
• Update on Federal Partner Use Cases
• Upcoming ConUse changes
  • Use of ASTM Standard in architecture
  • Changes to Limited Category
• Schedule and format of remote TIMs
• (additional topics as needed)

From: Harrison, Tenisha (FAA)
Sent: Tuesday, April 28, 2020 2:17 PM
Cc: Nair, Casey (FAA); Gallagher, Victoria (FAA)
Subject: Slides_3rd Remote ID Technical Interchange Meeting (4/28 - 4/29)
Attachments: FAA RID Data Ex TIM 3 - April 2020.pptx

Per the Cohorts request.. please see slides attached.

Best,

Tenisha Harrison
Contracting Officer
SE2020/2025 Team AAQ-350
Remote ID
LAANC
Federal Aviation Administration
Phone: [redacted]

ACQ
WE GET IT

Remote ID Data Exchange

Technical Interchange Meeting #3

April 28-29, 2020

Agenda Day 1 (4/28) – FAA & Industry Actions

Session 1 & 2: 11am-1pm & 2pm-4pm ET	
Welcome & Overview Program Update, Schedule, etc.	
FAA Action: Consider Leveraging ASTM Standard	Replanning Year 1 to Leverage ASTM Standard • Critical Goal: 1+ Qualified USSs Providing Public Service
	Revised RIDEx Architecture • High-Level Diagrams
	ASTM Requirements in FAA Qualification • Rules that are / are not incorporated into USS Rules
Industry Action: Onboarding Input	Onboarding & Test • Cohort Input • Testbed • End-to-End Automated Testing

Agenda Day 2 (4/29) – Other Topics

Session 3: 11am-1pm ET
Architecture of Authentication and Authorization (A&A) • Overall Design of FAA USS A&A Service • Credentialing processes in Onboarding, Continuous Monitoring, Upgrades, etc.

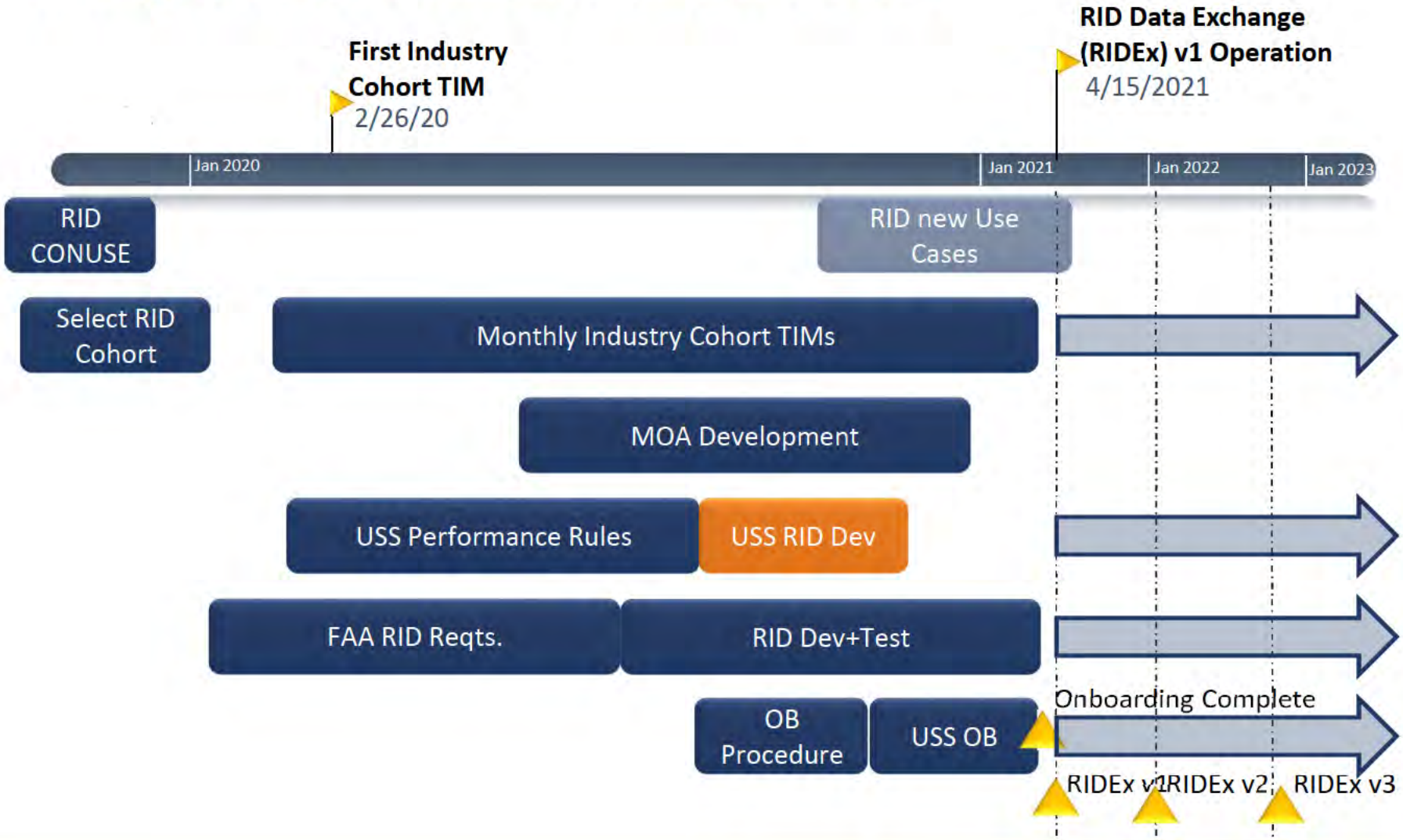
Miscellaneous
• Session IDs
• Update on Federal Partner Use Cases
• Upcoming ConUse changes
  • Use of ASTM Standard in architecture
  • Changes to Limited Category
• Schedule and format of remote TIMs
• (additional topics as needed)

Sessions 1 & 2

Welcome & Overview

- Introduction of all participants
- Expectations and Ground Rules
- Scope
- Program Schedule

Program Schedule: RIDEx Year 1

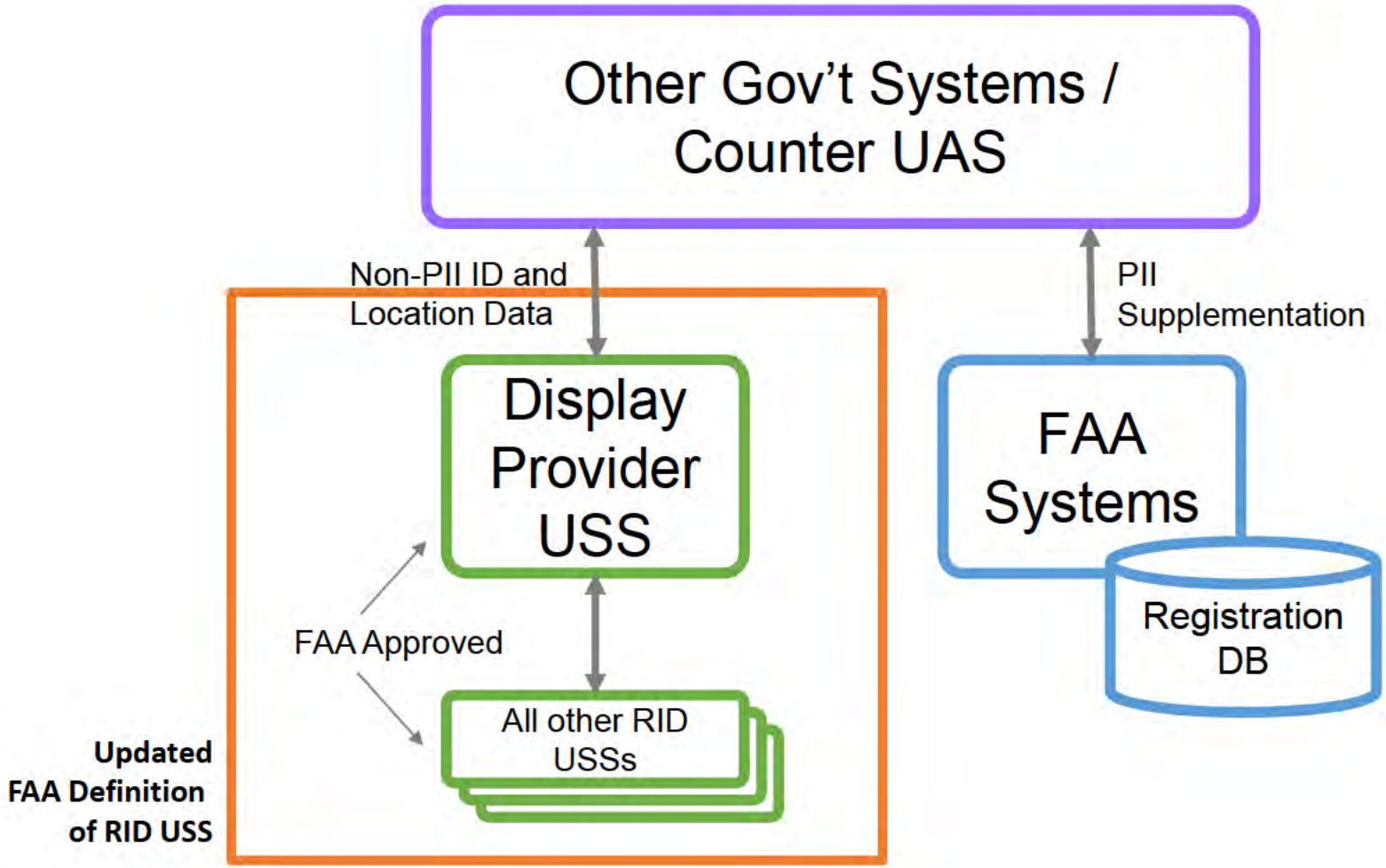


Replanning Year 1 to Leverage ASTM Standard

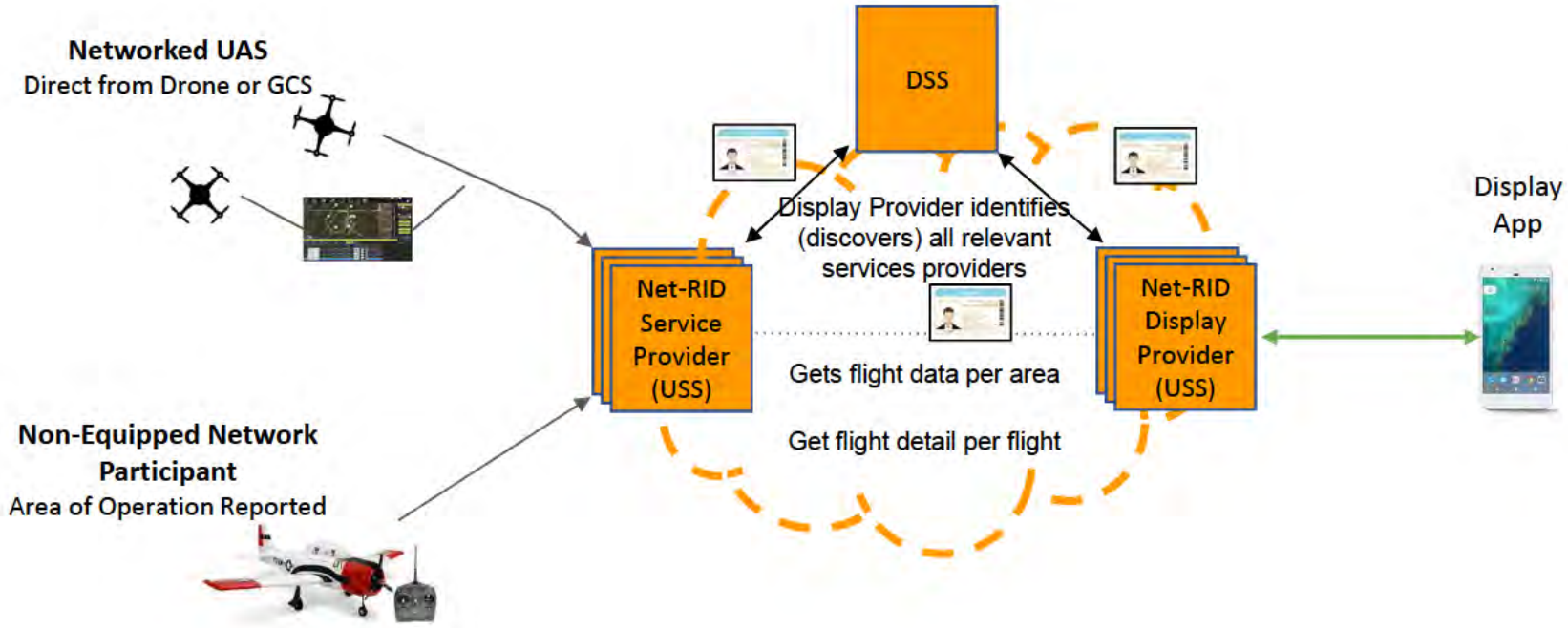
FAA Perspective

- **FAA supportive of leveraging standard**
- **Baseline stream is not planned for Year 1**
- **FAA cares about a certain subset of functions in the standard:**
  - UAS Connectivity
  - Discovery (across USSs)
  - Aggregation (across USSs)
- **FAA looks at "RID USS" holistically**
- **Recognize interest in UTM but FAA needs to maintain short-term focus on Remote ID**
- **Critical Goal for Year 1: 1+ qualified USSs providing public service**

Cohort Request from Last TIM



Cohort Request from Last TIM (Cont'd)



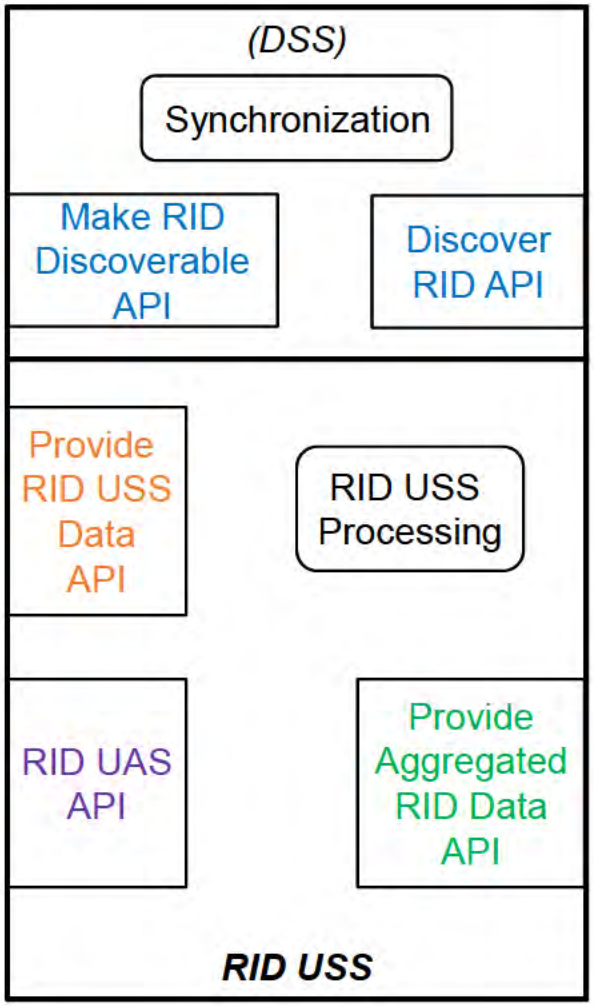
FAA Definition of RID USS

- **RID USS is qualified as a whole**
- **Key data exchange functions are shown as APIs:**

  All RID USS…
  - UAS Connection API
  - Provide Data to Other USS API*
  - Provide Aggregated Data to Requesters API

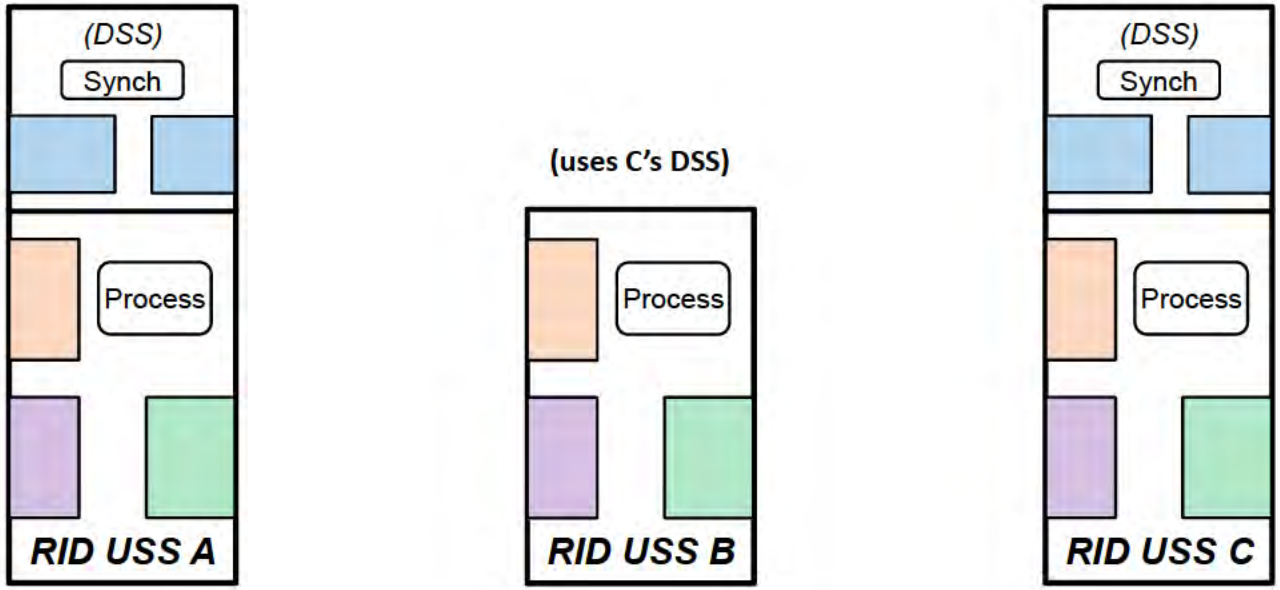
  RID USS with a DSS also have…
  - Make Data Discoverable API*
  - Discover Data API*

** = API is specified by ASTM Std*

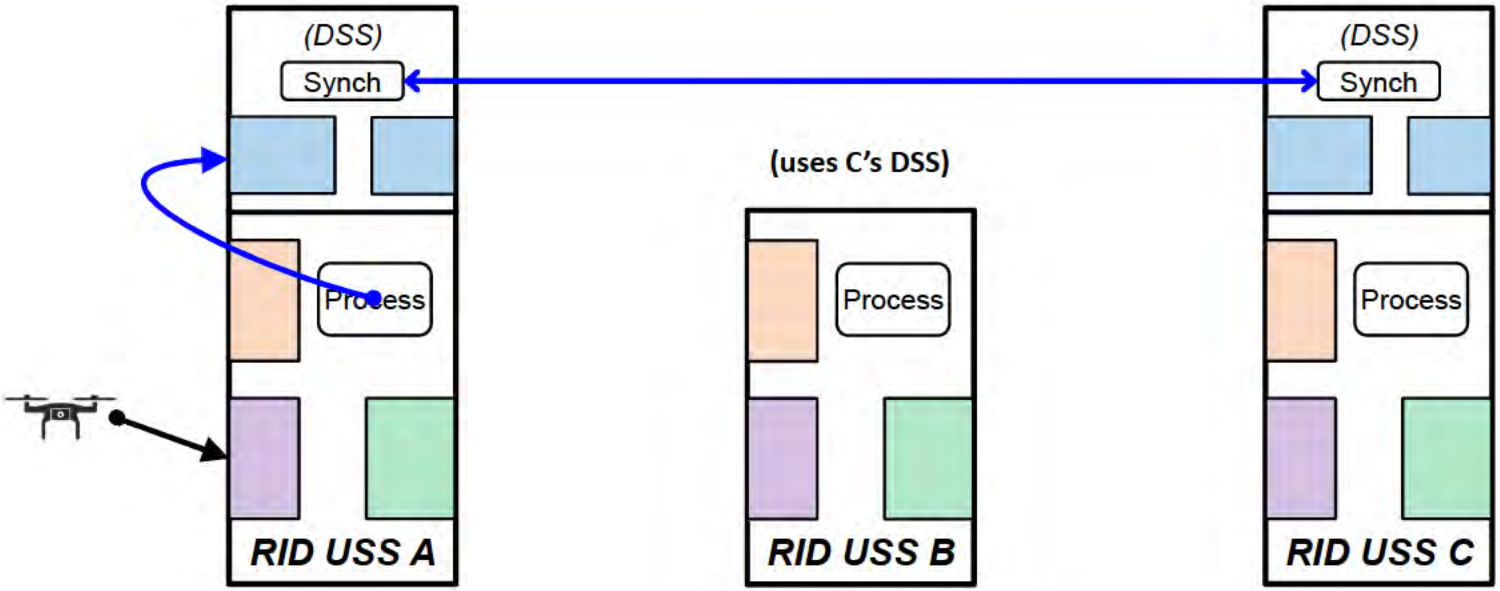


Revised RIDEx Architecture

RIDEx Architecture – Example w/ 3 RID USS



RID USS A gets new data

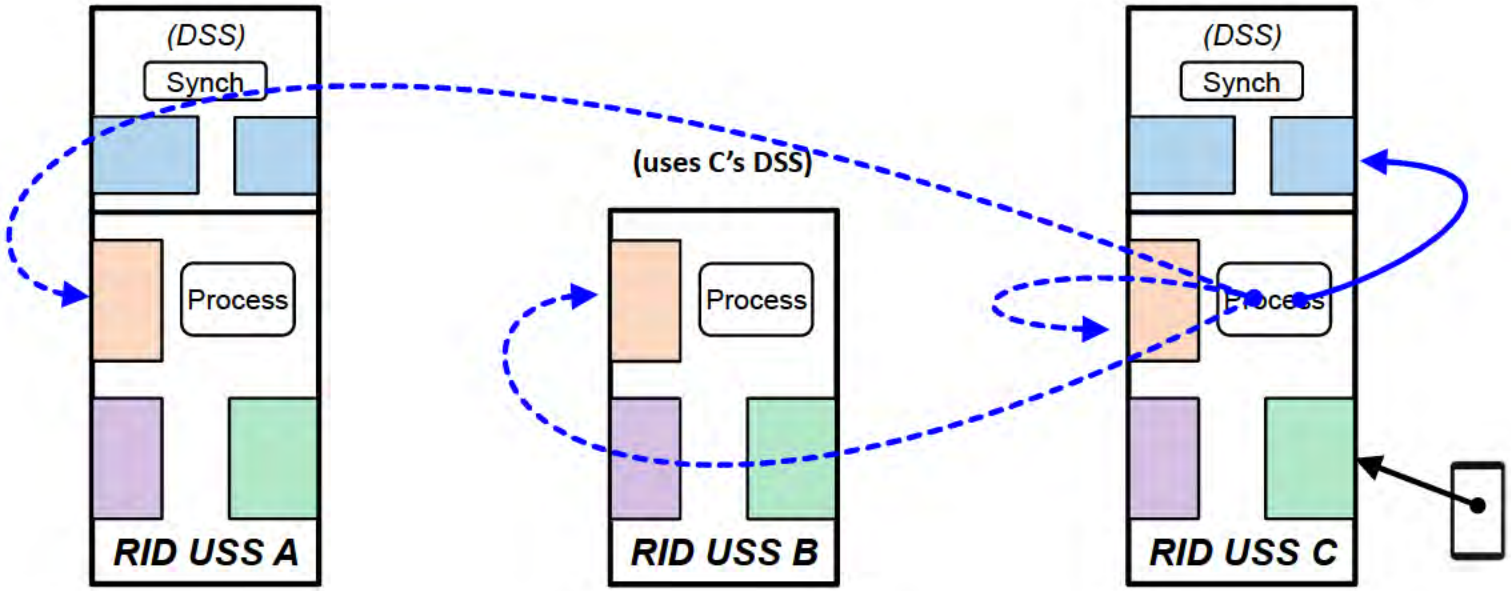


- **DSS "make discoverable" function must be part of qualification**
- **DSS synchronization must be part of qualification**
- **A's credentials used to sync with other DSSs**

Interfaces described by ASTM Std

Other Interfaces

RID USS C gets request for data

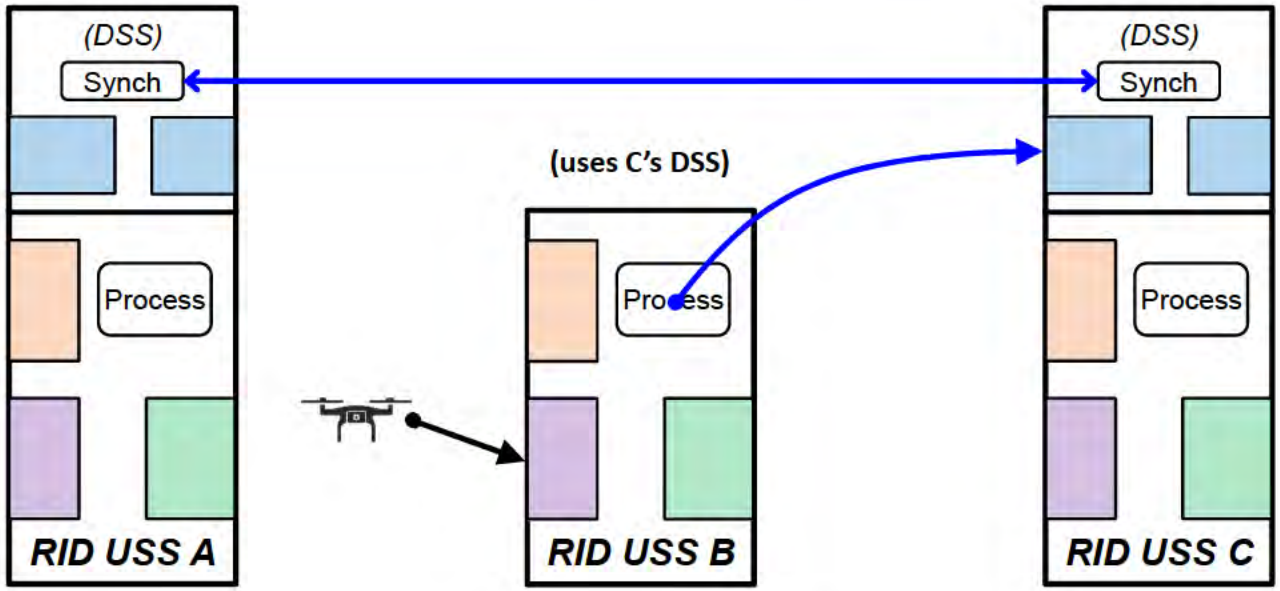


- DSS "discover" function must be part of qualification
- RID USS query of other RID USSs must be part of qualification
- C's credentials used to query other RID USSs

Interfaces described by ASTM Std

Other Interfaces

RID USS B gets new data

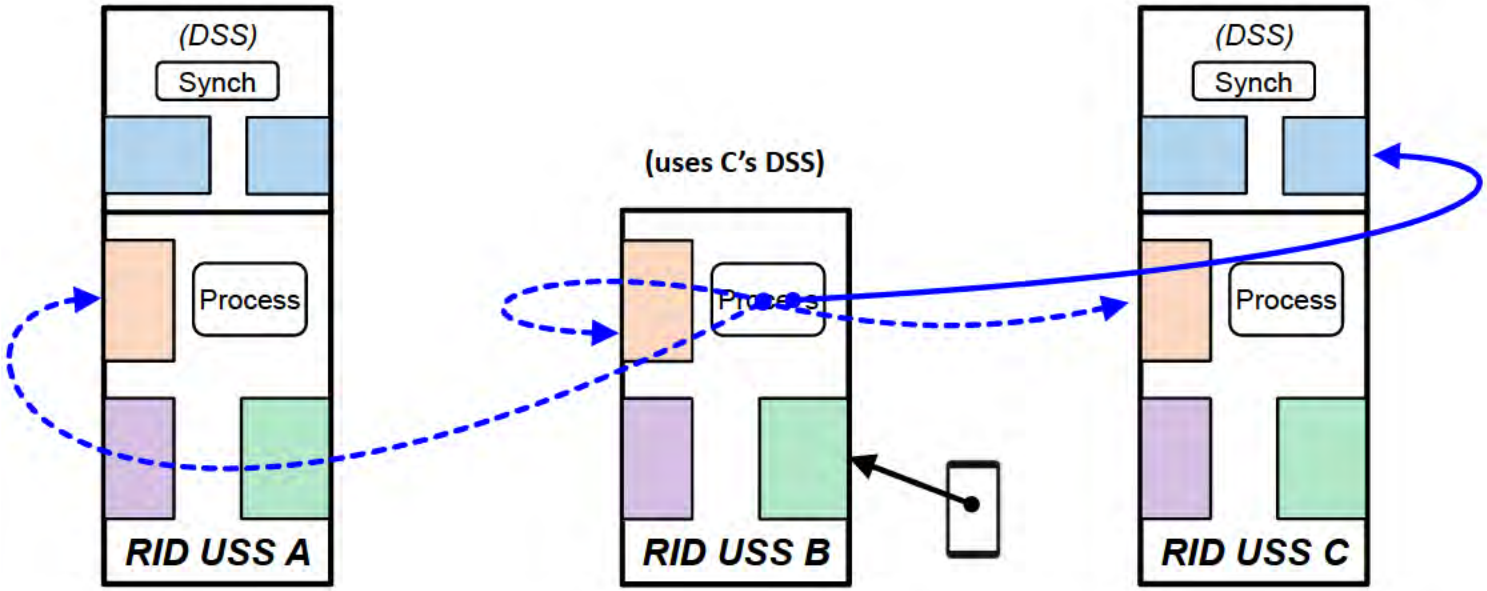


- **B's credentials used to "make discoverable" using C** (not by scope, but by agreement between C & B)
- **C's credentials used to sync with other DSSs** (by scope as a qualified DSS)

Interfaces described by ASTM Std

Other Interfaces

RID USS B gets request for data

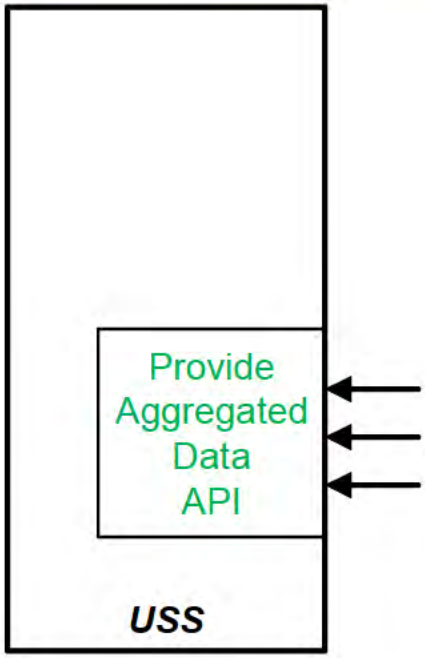


- **B's credentials used to "discover" using C**
  (not by scope, but by agreement between C & B)

Interfaces described by ASTM Std

Other Interfaces

RIDEx Architecture: Requesters



Requesters include:

- **Display Apps**
- **Government Systems**
- **General Public Display Apps?**

FAA can credential government systems, but not display apps or general public.

To discuss:

- *Can connection to display apps be managed as a business between USS and app provider?*
- *What counts as providing data to the General Public?*

Review of Applicable Requirements in ASTM Standard

Introduction

- **The ASTM standard includes numerous requirements on USSs, DSS instances, etc.**
- **As part of the FAA's use of the standard in the RIDEx architecture, some of these requirements would be adopted as USS Rules.**
- **Compliance with these rules would become part of USS qualification (subject to FAA verification in onboarding and continuous monitoring).**
- **Not all standard requirements will be adopted, and some may be modified.**
- **Rules derived from the standard would only be a *subset* of the full USS Rules.**
- **The following categorizations are preliminary and not comprehensive.**

UAS API Requirements

RID UAS API

Requirements to consider including in Rules:

- **Authentication and encryption between the drone and the USS. [5.5.2.4: NET0010, NET0020]**
- **Operator notification of failure to provide data. [5.5.2.4: NET0030, NET0040]**

Unclear for inclusion in Rules:

- **Requirements associated with "Non-Equipped Network Participants" are TBD. [5.5.3]**

USS Data API Requirements

Provide RID USS Data API

Requirements to consider including in Rules:

- **Authentication and encryption. [5.5.4.4: NET0210, NET0220]**
- **Make data discoverable. [A2.3.2.1: NET0610]**
- **Rules for responsiveness to valid data requests from Display Provider USS. [5.5.4.4: NET0260]**
  Nominally 1s 95% of the time.
- **Scope of data & vehicles included in responses to requests. [5.5.4.4: NET0270]**
- **Error responses. [5.5.4.4: NET0250]**
- **Specific interfaces (P2P OpenAPI). [A2.4.1.1: NET0710]**

Unclear for inclusion in Rules:

- **Rules for blocking requests larger than a tile. [5.5.4.4: NET0250]**
- **Rules for extrapolation. [5.5.4.4: NET0280-NET0320]**

Aggregated Data API Requirements

Provide Aggregated RID Data API

Requirements to consider including in Rules:

- **Authentication and encryption. [5.5.4.4: NET0210, NET0220]**
- **Rules for responsiveness to valid data requests. [5.5.5.9: NET0440] Nominally 6s 95% initially (to allow for discovery) and then 1s 95%.**
- **Scope of data & vehicles included in responses to requests. [5.5.5.9: NET0450]**
- **Specific interfaces (P2P OpenAPI). [A2.4.1.3: NET0730]**

Unclear for inclusion in Rules:

- **Requesting data only where requested by end users. [5.5.4.4: NET0430], [A2.3.2.1: NET0630]**
- **Rules for blocking requests larger than a tile. [5.5.5.9: NET0460]**

Requirements likely not included in Rules:

- **Rules for not retaining (deleting) data. [5.5.4.4: NET0330] Nominally 24hrs.**

DSS Requirements

Make RID Discoverable API

Discover RID API

Requirements to consider including in Rules:

- **Authentication and encryption. [A2.3.1.1]**
- **Supporting specific subscription interface. [A2.3.1.1]**
- **Limiting the number of subscriptions per USS for a given area. [A2.3.1.1]**
  Nominally 10 per USS per Display Provider USS.
- **Limiting the duration of subscriptions. [A2.3.1.1]**
  Nominally 24 hours.
- **All instances must be active (synchronized). [A2.3.1.1]**
- **Authentication and encryption between DSS instances. [A.2.5.5]**

Other Rules

Aside from Rules derived from the ASTM standard, there are other categories of anticipated Rules including (but not limited to):

- **Availability**
- **Reliability (see TIM #1)**
- **Data Retention**
- **Data Protection**

Onboarding & Test

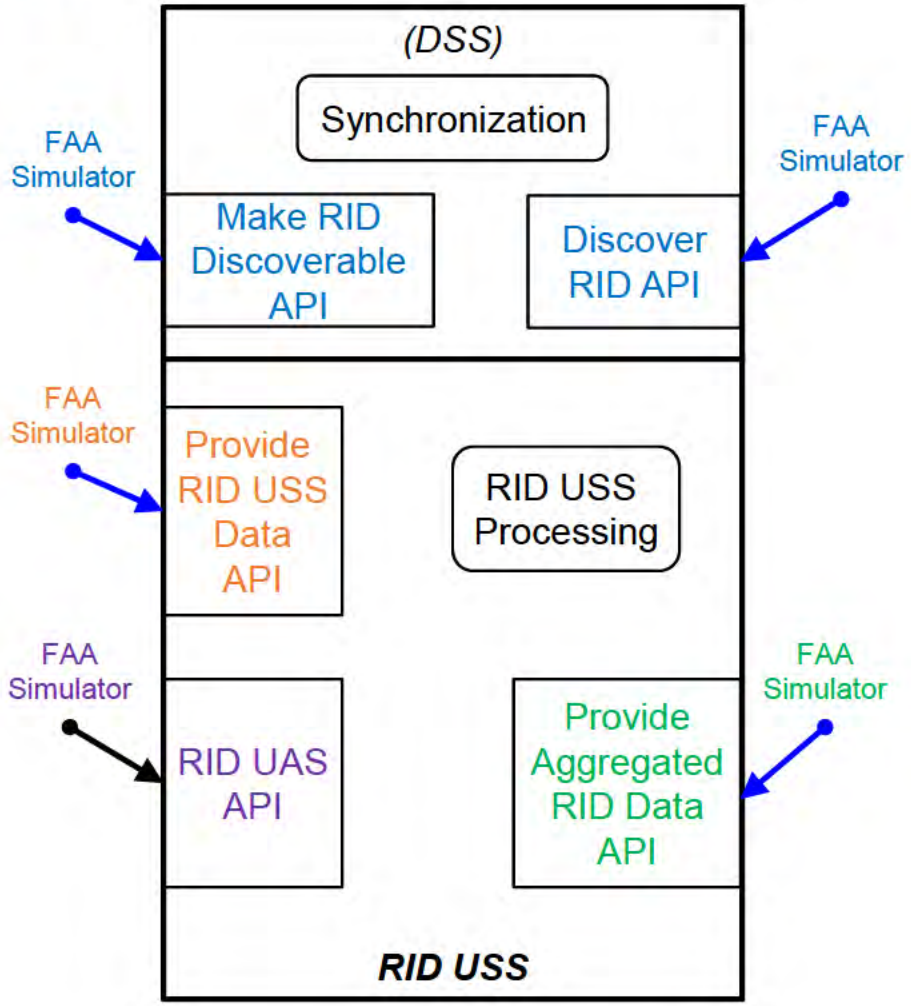
Cohort Input: Action

FAA Onboarding Approach

- **The FAA will onboard the following RID configuration**
  - RID USS + Aggregation + DSS (single entity) (e.g. RID *USS A*)
  - RID USS + Aggregation + external DSS (e.g. RID *USS B*)
- **Testing approach described in ASTM Standard A2 is applicable**
  - Note that DSS is nominally tested in conjunction with a USS
  - In Year 1, FAA is planning to test a USS with DSS integrated (or partnering with a USS+DSS)
  - Input?

FAA Onboarding Approach

- **FAA expects to build API simulators for each data exchange function**
- **FAA supports use of standardized, repeatable test cases to simplify onboarding and periodic updates**
- **Persistent test instance of each RID USS will be used**



Onboarding & Test: Continuous Monitoring

Continuous Monitoring

- **What are the major faults that must be monitored?**
  - Loss of service
  - Loss of synchronization with DSS

- **How much can be automated?**

UAS Connection (Test Approach)

- **Simulate a UAS using only minimum required RID data fields in ConUse**
- **Evaluate that RID data is provided, discovered, and made discoverable through each API**
- **Simulate operator notification of failure to provide data**
- **Simulate loss of data during flight(s)**
- **Confirm message response compliance**

Aggregated Data Requests (Test Approach)

- **Simulate valid user requests to determine responsiveness**
- **Simulate user requests for various geographic regions and area sizes**
- **Simulate user requests for a defined area with simulated UAS's entering and exited the area**
- **Confirm message response compliance**

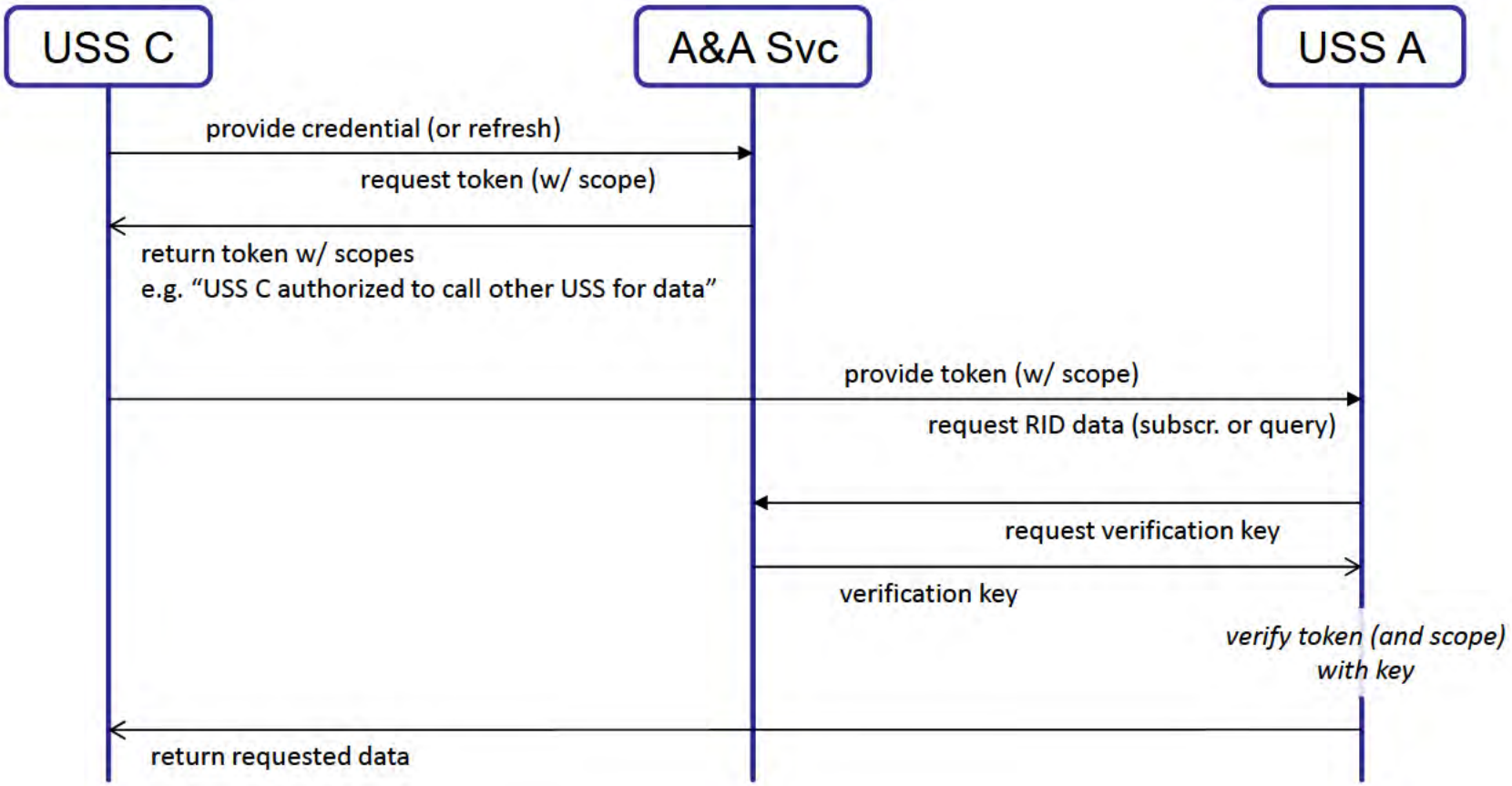
Testing/Handling Session ID

- **Perform API call to aggregation (or other) API for session ID management key (if applicable)**

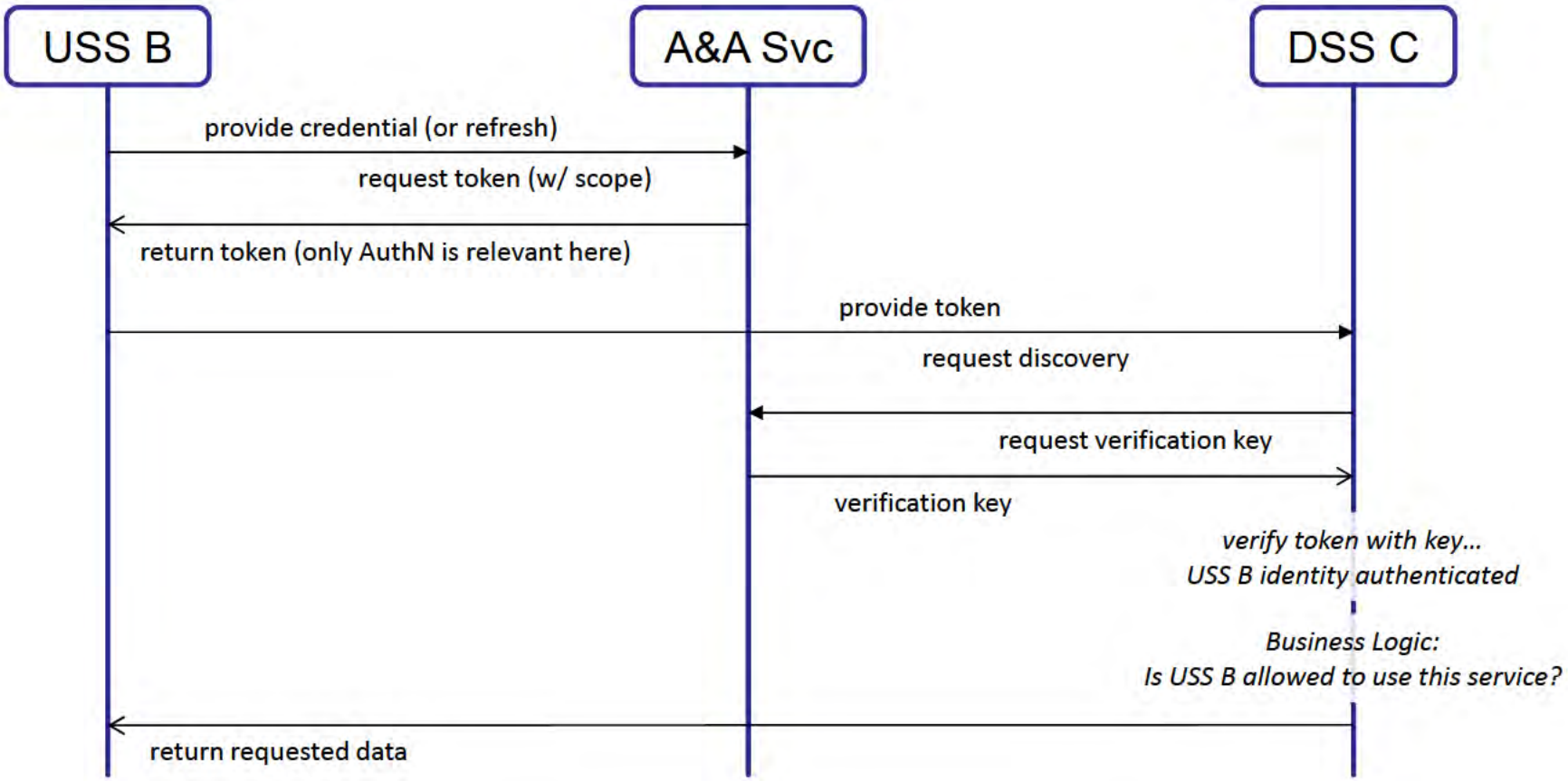
Session 3

Architecture of Authentication and Authorization (A&A)

A&A Example: USS C calls USS A for RID Data (in support of aggregation)



A&A Example: USS B "Discovers" via DSS C



Miscellaneous Topics

Topics

- Use Cases & Tiling
- Session IDs
- ConUse Changes Pending
- Participation Roadmap for FAA and Cohort
- Review TIM Action Items
- Format & Scheduling of Next Meetings

Use Cases & Tiling

From: Harrison, Tenisha (FAA)
Sent: Thursday, May 07, 2020 1:12 PM
Cc: Nair, Casey (FAA); Gallagher, Victoria (FAA)
Subject: Remote ID Cohort: FAA request for "Non Equipped Network Participants" Industry Presentation_May 13th 2-3pm

Importance: High

Hello Cohort Members,

I hope this email finds you all well. Industry has an action from the last TIM to provide the FAA with a 1 hour deep-dive on aspects of non-equipped operations within Remote ID that are incorporated into ASTM F3411-19. The PMO is looking to hold a dialog with the Remote ID Cohort next **Wednesday May 13, from 2 – 3pm** specifically on this topic.

Teleconference Info:

Remote ID Data Exchange: Non-Equipped Presentation

Please join my meeting from your computer, tablet or smartphone.
[redacted]
This meeting is locked with a password: RemoteID
You can also dial in using your phone.
(For supported devices, tap a one-touch number below to join instantly.)
United States: [redacted]
- One-touch: [redacted]
Access Code: [redacted] New to GoToMeeting? Get the app now and be ready when your first meeting starts: [redacted]

Take care and stay safe ☺

Tenisha Harrison
Contracting Officer
SE2020/2025 Team AAQ-350
Remote ID
LAANC
Federal Aviation Administration
Phone: [redacted]

ACQ
WE GET IT

From: Harrison, Tenisha (FAA)
Sent: Wednesday, May 20, 2020 11:09 AM
Cc: Rinehart, David CTR (FAA); Nair, Casey (FAA); 'Jim Little'; 'msanders@[redacted]'; Gallagher, Victoria (FAA)
Subject: 4th Remote ID Technical Interchange Meeting (5/27/20)
Attachments: WS4-WebConf.docx

Good Morning Cohort Members!

In place of a full May Technical Interchange Meeting (TIM), the FAA is holding a technical working session on the specific topic of **OAuth in Remote ID USS Data Exchanges**. This working session will be held by webconference on Wednesday, May 27th from 11am-1pm ET. Please see attached webconference instructions.

Cohort members are asked to bring representatives with subject matter knowledge of this topic, as well as any materials that can be shared during the working session. For example, similar prior implementations and/or recommended patterns are welcome. The FAA anticipates returning to the full monthly TIM format in June. At that time, a significant update to the Concept of Use document should be available for discussion. Aside from this OAuth working session, other topics and actions from the May TIM are deferred until the June TIM.

Take care and stay safe ☺

Tenisha Harrison
Contracting Officer
SE2020/2025 Team AAQ-350
Remote ID
LAANC
Federal Aviation Administration
Phone: [redacted]

ACQ
WE GET IT

Meeting: **Remote ID Data Exchange Working Session**

Dates & Times: **27 May 2020, 11:00am-1:00pm EDT**

This meeting will be held by videoconference. Please note the following recommendations:

- For voice, participants can join with either phone or computer audio.
- Connect from your computer to view shared presentation materials and webcam video from other participants.
- Enable your webcam for better engagement among participants.
- Conferencing services and networks are under higher demand than usual. If a connection is stalled or malfunctioning, close it, and reconnect.
- If there is a significant disruption, the CO (Tenisha Harrison) will send an email with alternate arrangements.

Detailed connection steps:

1. Join the meeting 10-15 minutes ahead of time to allow for possible setup required.
2. URL [redacted]
3. This meeting is locked with a password: [redacted]
4. You can also dial in using your phone.
   United States: [redacted]
   One-touch: [redacted]
   Access Code: [redacted]
   When joining by phone, Participant ID will be provided individually. Please enter it so that all callers are identified. Unidentified callers may be removed by the organizer.
5. Please sign in with your name and organization so that other participants can effectively identify you – for example: “Pat Smith (ABC Inc)”. After connecting, you can edit your name by in the participants list.
6. Please use webcams. You may need to enable browser or application access to your webcam. Webcam video can be turned on or off using the camera icon.
7. The microphone icon can be used to mute yourself. Please mute yourself when you are not talking.
8. Chat system will be enabled during the meeting.

From: Harrison, Tenisha (FAA)
Sent: Friday, May 08, 2020 12:45 PM
Cc: Gullan, Nina CTR (FAA); Nair, Casey (FAA); Duquette, Alison (FAA)
Subject: Recent Remote ID Cohort Press Release Announcement

Hello Remote ID Cohort Members:

We are writing to clarify the information provided in the recent Remote ID Cohort press release announcement. While the Remote ID Cohort was selected some time ago, approval was recently received to make the formal announcement. In the future, you can expect to receive information about external communications ahead of a release.

To address any confusion from the May 5 release, there are plans to publish social media content and send a clarifying email message to registered drone users.

Kind Regards,

Tenisha Harrison
Contracting Officer
SE2020/2025 Team AAQ-350
Remote ID
LAANC
Federal Aviation Administration
Phone: [redacted]

From: Harrison, Tenisha (FAA)
Sent: Friday, June 19, 2020 1:09 PM
Cc: Rinehart, David CTR (FAA); Nair, Casey (FAA); 'Jim Little'; [redacted]; Gallagher, Victoria (FAA)
Subject: 5th Remote ID Technical Interchange Meeting (6/29/20)
Attachments: Remote ID Cohort Meeting_June 2020_WebConf.docx

Importance: High

Happy Friday Cohort Members!

Instead of the previously planned 6/23-6/24 TIM, there will be a discussion and Q&A time with an FAA Executive concerning recent Remote ID strategic decisions. This session will be held via webconference on **Monday, June 29th from 1pm-2pm ET**. Please see attached webconference instructions.

I hope you all have a safe and wonderful weekend ☺

Tenisha Harrison
Contracting Officer
SE2020/2025 Team AAQ-350
Remote ID
LAANC
Federal Aviation Administration
Phone: [redacted]

ACQ
WE GET IT

Remote ID Cohort Meeting

When: June 29, 2020

Time: 1:00-2:00PM EDT

This meeting will be held by videoconference. Please note the following recommendations:

- For voice, participants can join with either phone or computer audio.
- Connect from your computer to view shared presentation materials and webcam video from other participants.
- Enable your webcam for better engagement among participants.
- Conferencing services and networks are under higher demand than usual. If a connection is stalled or malfunctioning, close it, and reconnect.
- If there is a significant disruption, the CO (Tenisha Harrison) will send an email with alternate arrangements.

Click to Join:
[redacted]
Password: [redacted]
• If prompted, accept the Zoom application as instructed
• For a camera enabled PC or laptop & Optimized for Google Chrome or Microsoft Edge

Web Browser:
[redacted]
• Click the JOIN button; enter Meeting ID: [redacted]
Password: [redacted]
• If prompted, accept the Zoom application as instructed
• For a camera enabled PC or laptop & Optimized for Google Chrome or Microsoft Edge

Mobile Device:
• Download the 'Zoom Cloud Meetings' App
• Select 'Join a Meeting' and enter Meeting ID [redacted]
Password: [redacted]

Phone Audio Only:
• Call [redacted] or [redacted]; enter Meeting ID: [redacted]
Password: [redacted]
• Please remember you can mute or unmute yourself by pressing *6.

Traditional VTC Room System (Via Polycom, Tandberg or Cisco):
• Dial/Call the following IP address [redacted] (No Spaces)
• If Applicable, with password: < [redacted] @ sip.zoomgov.com
• Press #1 to bring up the menu to unmute, mute, change the view and additional features
• There are many makes/models of traditional VTC room systems. For an easy 'how to connect' your system document, contact FAVES Customer Support.

From: Harrison, Tenisha (FAA)
Sent: Tuesday, July 21, 2020 10:01 AM
Cc: Nair, Casey (FAA); Gallagher, Victoria (FAA); Jim Little; david.rinehart [redacted]; Zachary Desmond (Evans Consulting); Sanders, Matt
Subject: Update on Remote ID Technical Interchange Meetings

Morning Cohort Members,

I hope this email finds you all well. The FAA is continuing to work on updates to the Remote ID ConUse and master schedule, as discussed during the June 29 executive meeting. The FAA does not plan to conduct further TIMs until these artifacts are completed. As a result, there will not be a TIM in July, and please stand by for future communication on the possibility of a TIM in August.

Take care and be safe ☺

Tenisha Harrison
Contracting Officer
SE2020/2025 Team AAQ-350
Remote ID
LAANC
Federal Aviation Administration
Phone: [redacted]

ACQ
WE GET IT

From: Sanders, Matt <msanders@[redacted]>
Sent: Monday, July 20, 2020 1:33 PM
To: Harrison, Tenisha (FAA) [redacted]
Cc: Nair, Casey (FAA) [redacted]; Gallagher, Victoria (FAA) [redacted]; Jim Little [redacted]; david.rinehart [redacted] Zachary Desmond (Evans Consulting) [redacted]
Subject: Cohort communication for upcoming RID TIMs

Tenisha – we have a lot of items in RID land swirling and will not be ready for a Cohort TIM next week, as originally scheduled. Below is some simple language to communicate to the group. Please feel free to tweak anything you like. We're not sure when these artifacts will be finished, pending various decisions, and therefore don't the August 25-26 dates will hold, either. Right now, it seems unlikely.

Thank you very much!

Cohort Members,
The FAA is continuing to work on updates to the RID ConUse and master schedule, as discussed during the June 29 executive discussion. The FAA does not plan to conduct further TIMs until these artifacts are completed. There will not be a TIM in July, and please stand by for future communication on the possibility of an August TIM.

Matt Sanders
Aurora Innovations
[redacted]
[redacted]com

From: Harrison, Tenisha (FAA)
Sent: Monday, August 17, 2020 12:23 PM
Cc: Nair, Casey (FAA); Gallagher, Victoria (FAA); Sanders, Matt
Subject: Update on Remote ID Technical Interchange Meetings_August and Future

Hello Cohort Members,

I hope this email finds you all well. The FAA is continuing to work with our interagency governmental security partners to refine the RID concept. Therefore, the planned August TIM and all future meetings are canceled until further notice. The FAA will share updates as they become available, and thank you for your continued participation in the Remote ID Cohort.

Kind Regards,
Tenisha Harrison
Contracting Officer
SE2020/2025 Team AAQ-350
Remote ID
LAANC
Federal Aviation Administration
Phone: [redacted]

ACQ
WE GET IT