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

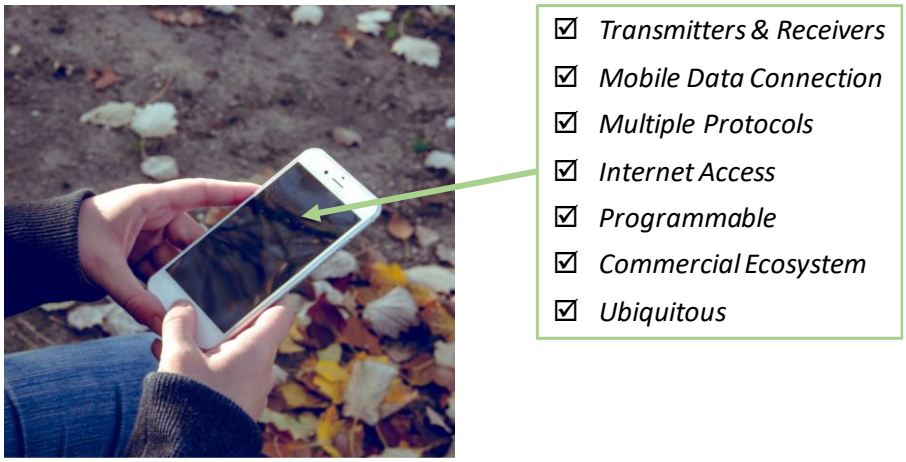

Figure 2: Existing technology offers foundation for Remote ID

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

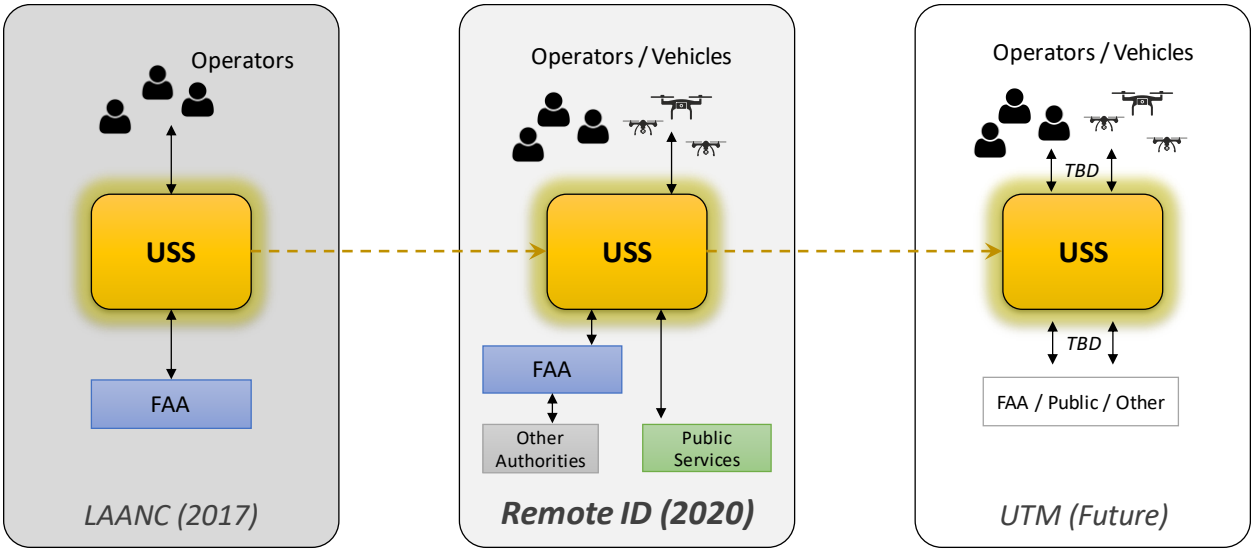

Figure 3: The UAS Service Supplier (USS) is central to recent capability architectures

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

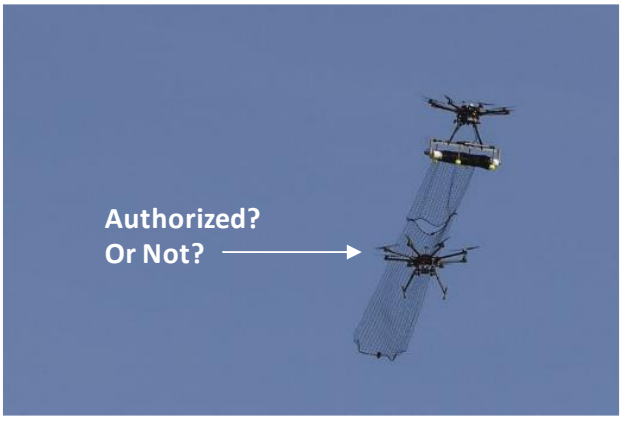

Figure 4: UAS enforcement faces unique difficulties

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.

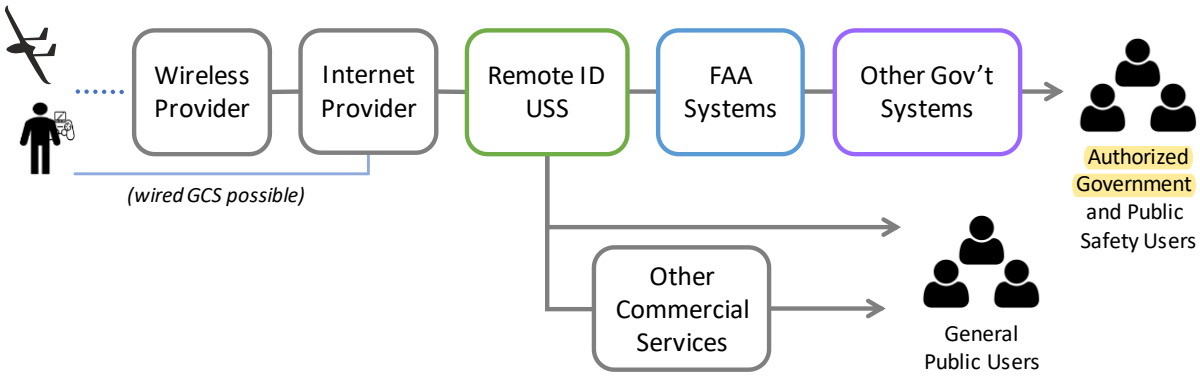

Figure 6: Remote ID Intermediaries

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.

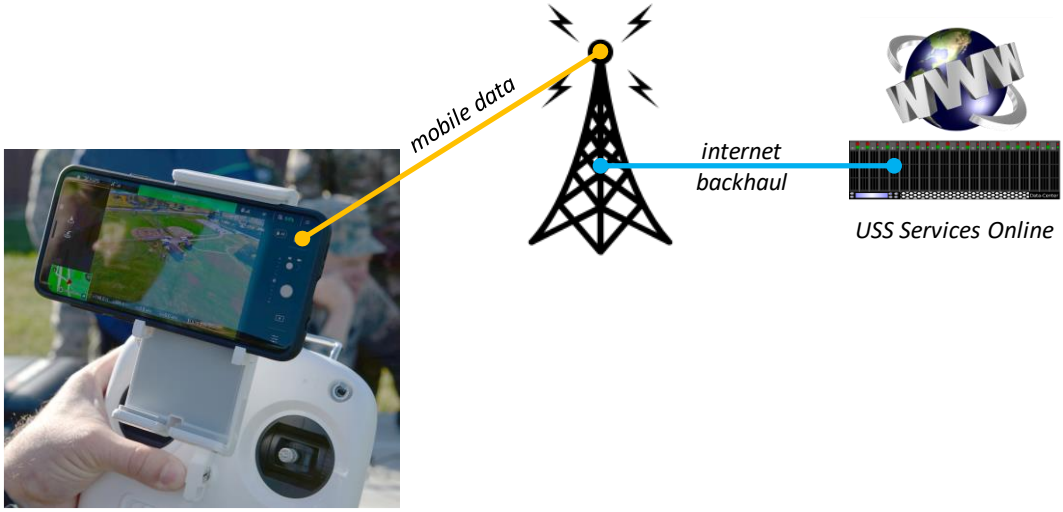

Figure 7: Remote ID Network – Early Configuration (Integrated Smart Device)

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.)

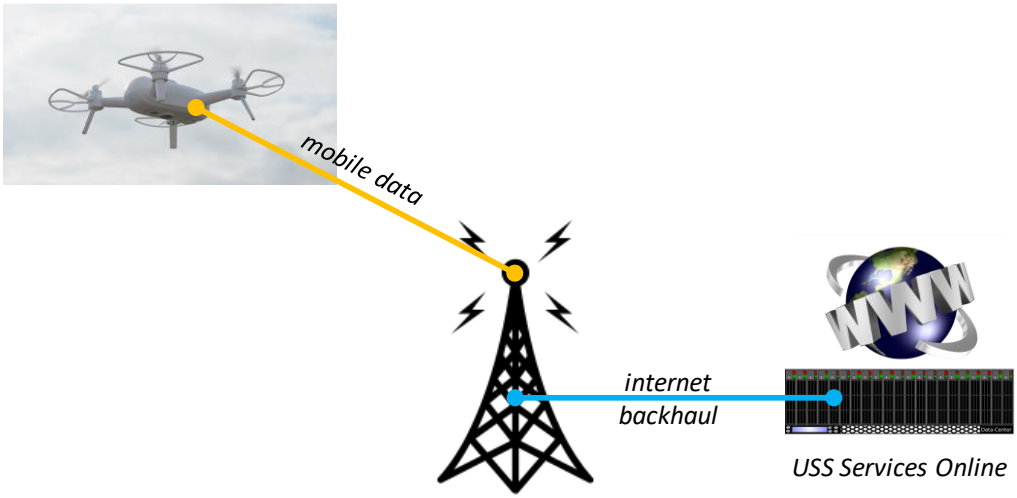

Figure 8: Remote ID Network – Mid-term Configuration (Mobile Data on Vehicle)

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.

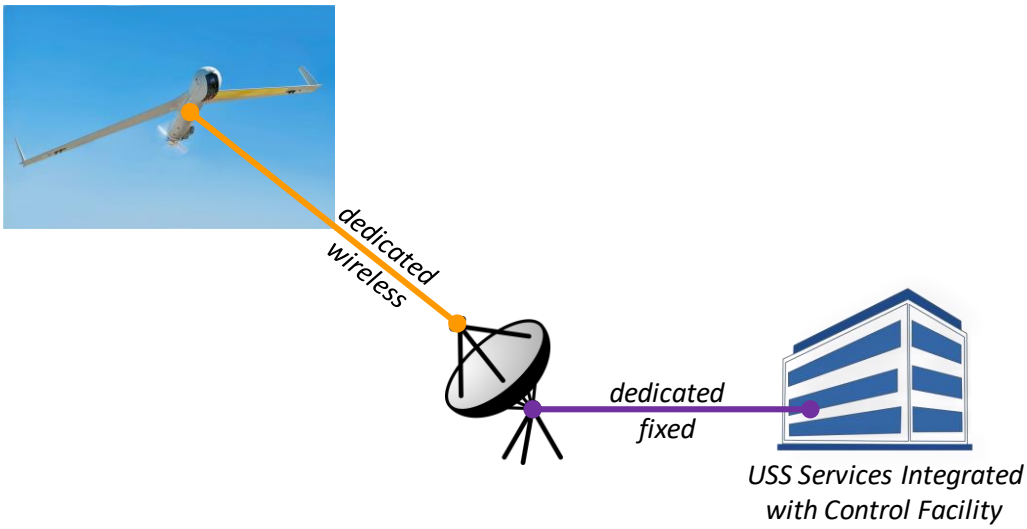

Figure 9: Remote ID Network – Long-Term Configuration (with BVLOS)

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.

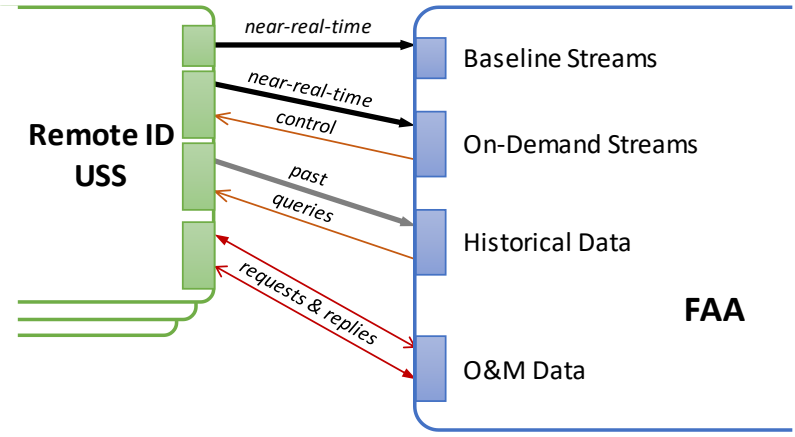

Figure 10: UAS-FAA Data Exchange Interface (General Design)

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.

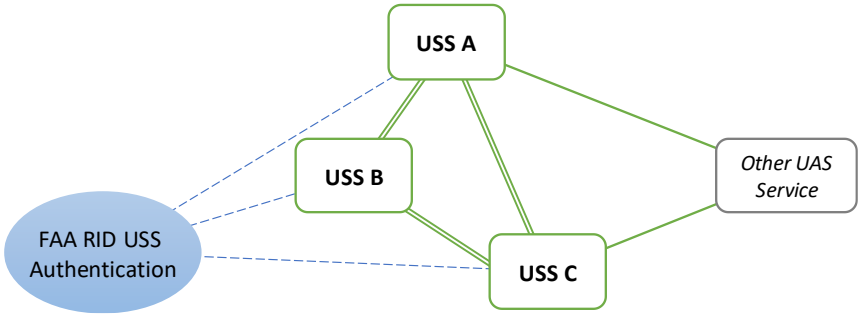

Figure 11: USS-to-USS and Related Data Exchanges

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):

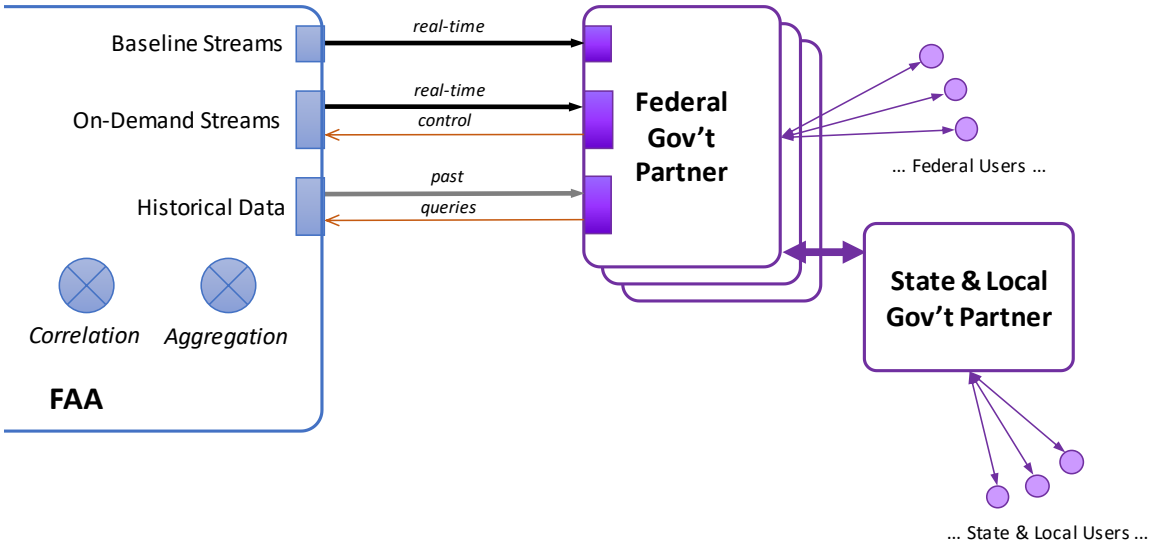

Figure 12: FAA-to-Agencies Information Mechanisms

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.

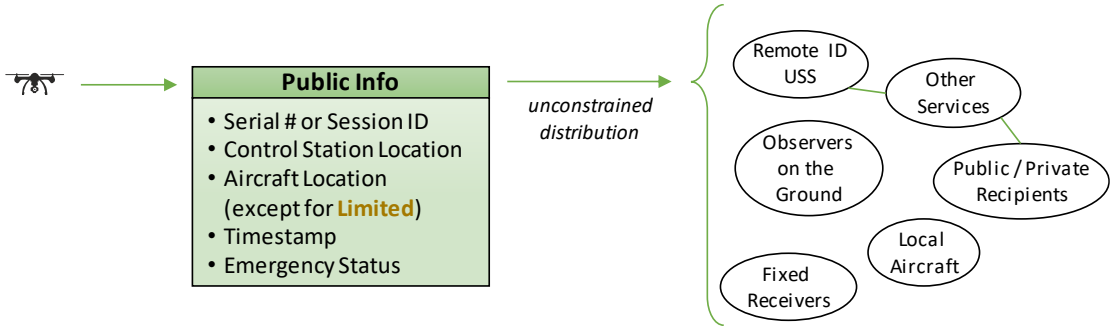

Figure 13: Public Remote ID Information

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.

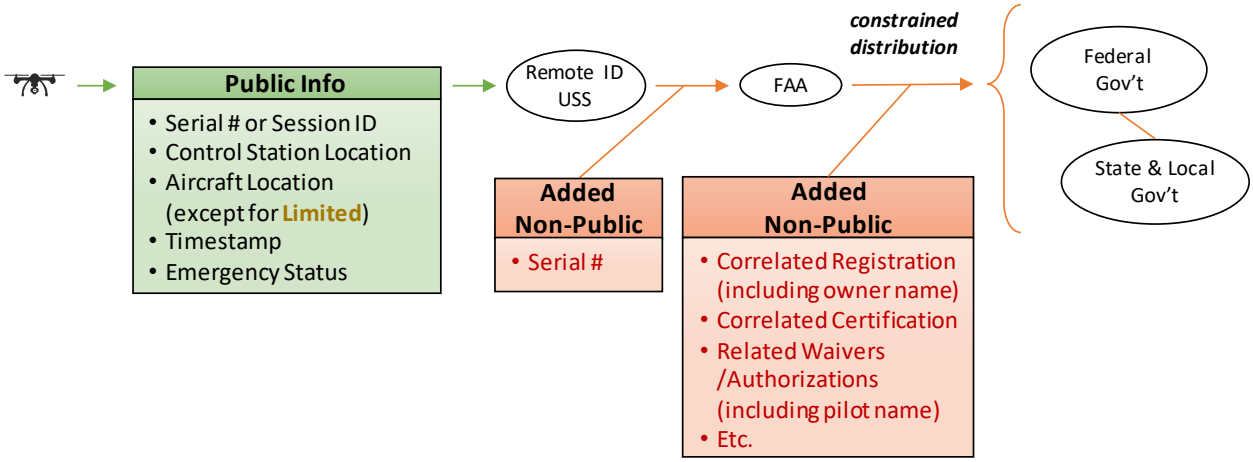

Figure 14: Government Use Remote ID Information

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.