



## FOURTEENTH AIR NAVIGATION CONFERENCE

Montréal, Canada, 26 August to 6 September 2024

- Agenda Item 1: Update on the ICAO 2023-2025 Business Plan and long-term strategic planning**  
**1.1: Reprioritization of the ICAO 2023-2025 Business Plan**

### GLOBAL SAFETY INFORMATION MANAGEMENT EXCHANGE - PLAYBOOK

(Presented by the United States and co-sponsored by Australia)

#### EXECUTIVE SUMMARY

The United States, in collaboration with Australia, led the Global Safety Information Management Exchange (GSIME) initiative and conducted a proof-of-concept study to validate the mutual benefits of a global safety information exchange using Annex 8 — *Airworthiness of Aircraft* safety data as a use-case. This Playbook, a result of this study, serves as a practical guide to assist States in identifying opportunities and working through potential challenges to establish a safety information exchange.

## 1. INTRODUCTION

1.1 The Federal Aviation Administration's (FAA) Global Safety Information Management Exchange (GSIME) initiative aims to enhance safety management by improving and facilitating safety intelligence through safety data exchange and information sharing with international aviation organizations and authorities<sup>1</sup>. The GSIME initiative's scope is focused on identifying and documenting relevant considerations required for regulatory organizations to establish an exchange for data, information, and intelligence with other authorities.

1.2 The objective of a GSIME type exchange is to enhance safety management by sharing data and information to directly support safety decision-making and risk mitigation (safety intelligence<sup>2</sup>). Aviation safety in the digital age may leverage data, information, and intelligence to identify emerging safety issues and improve operational hazard identification, with the goal of achieving proactive and predictive safety management in today's fast-changing environment.

<sup>1</sup> *Organizations* refers to a product or service provider, operator, as well as aviation industry organizations; and *authorities* refers to the regulator authority and any other relevant government agency or entity with oversight responsibility.

<sup>2</sup> ICAO Nineth Meeting of Africa-Indian Ocean Regional Aviation Safety Group (RASG-AFI/9), Safety Intelligence to support decision-making. November 2023. <https://www.icao.int/WACAF/Documents/RASG%20AFI/RASG-AFI-9/ENG/WPs-ENG/RASG-AFI9%20-%20WP04C3%20-%20Safety%20Intelligence%20to%20support%20decision%20making.pdf>

1.3 Global cooperation in the exchange and management of safety information is critical to achieving enhanced safety outcomes, both domestically and internationally. ICAO's *Global Aviation Safety Plan* (GASP, Doc 10004) and Annexes 8 and 19 – *Safety Management* strongly emphasize the importance of exchanging safety information globally and regionally<sup>3</sup>.

## 2. DISCUSSION

2.1 The collection and analysis of safety data is the cornerstone of a robust safety management system. Sharing of safety data, information and intelligence between States can help to better identify existing and emerging risks in the aviation system, allowing for a more holistic analysis and aligned safety outcomes.

2.2 Establishing an international data and information exchange requires significant commitment from all stakeholders, including the provision of resources to collect, analyse and protect the data and information shared. This commitment is also necessary to ensure the continued availability of data and to align on common safety outcomes. Apart from the technical, organizational and governance aspects, legal, financial, cultural and communication aspects must also be addressed to ensure effectiveness.

2.3 Safety-related data and information exchange between authorities can lead to enhanced safety in aircraft operations across territories and facilitate the mutual recognition of standards in alignment with ICAO's Standards and Recommended Practices (SARPs).

2.4 This paper introduces the GSIME Playbook, which serves as a practical reference to successfully engage with an international organization and/or authority to exchange data and information, including the analytic approach and methods, to promote alignment and confidence in safety outcomes. The intent of this Playbook is to provide a practical, real-world guide that addresses policy/process, operational, economic, data governance, legal and technical considerations. In addition, this Playbook leverages lessons learned by building upon previous efforts and challenges encountered. The goal is to provide civil aviation authorities (CAAs) with the knowledge and help identify best practices and tools required to successfully exchange data and information by defining a process focused on four key activities:

- a) Identify the data and information exchange scope, opportunity, analytical approach and methods, and value proposition.
- b) Identify the relevant data protections with a particular focus on confidentiality to enable a positive safety culture.
- c) Identify and establish the pertinent legal and governance requirements that may be formalized through agreements or memoranda of understanding.
- d) Execute, learn and refine the exchange process.

2.5 For a successful safety data and information exchange, it is important that CAAs focus on establishing certain foundational elements within their State, such as:

- a) a robust system for safety data collection from operators and other aviation stakeholders;

---

<sup>3</sup> Annex 19, International Civil Aviation Organization, Second Edition, July 2016.

- b) a positive safety culture that promotes voluntary safety reporting and establishes a community of learning; and
- c) a strong partnership between regulators and industry to improve safety management, including the implementation of data protections and confidentiality policies.

With these foundational elements in place, creating a global opportunity and perspective to identify hazards, trends, and potential risk mitigations is achievable through a common approach that enables safety data exchange.

### 3. CONCLUSION

3.1 The GSIME objective is to enhance safety management by exchanging data and information with international aviation organizations and authorities to directly support safety decision-making and proactive risk mitigation.

3.2 In light of the above, the Conference is invited to review AN-Conf/14-WP/101 entitled, *Facilitating Safety Intelligence Through Global Safety Information Management Exchange* and consider the proposed recommendations therein, as well as study the Playbook in the appendix.

-----

## **APPENDIX**

### **GLOBAL SAFETY INFORMATION MANAGEMENT EXCHANGE – PLAYBOOK**

#### **1. Introduction**

The intent of this Playbook is to provide a practical, real-world guide that addresses policy/process, operational, economic, data governance, legal and technical considerations for establishing a safety data and information exchange. In addition, this Playbook leverages lessons learned by building upon previous similar efforts and challenges encountered.

The playbook incorporates lessons learned from an actual (vs. hypothetical) case study where the FAA has exchanged data with another authority. The case study is described in Attachment A to this Playbook including specific examples illustrating how key playbook concepts were applied.

##### **1.1 How to Use the Playbook**

This playbook will not focus on specific project objectives, needs and legal determinations for the exchange and protection of safety data and information from international stakeholders beyond a general address. Rather, the focus of this document is to address the key elements of establishing a successful data and information exchange, trust and mutual benefits, including the underlying considerations, and the core principles, responsibilities, and data confidentiality for the parties.

The playbook is structured with 4 major activities, each with a set of questions and potential supporting documentation.

1. Identify Scope, Opportunity, and Mutual Benefits
2. Data Protection and Confidentiality
3. Legal and Governance Requirements
4. Finalize Documents, Execute Exchange, and Refine Process



This Playbook is focused on exchanging safety data and information with CAAs, who are responsible for serving as a regulator, and ICAO, which is responsible for establishing international standards and recommended practices, as well as procedures. State(s), within this document, is specifically focused on the regulator role and the duty Governments assume with respect to aviation safety.

## **2. Identify Scope, Opportunity, and Mutual Benefits**

The initial step in a successful international information exchange is clearly articulating both the problem being addressed, and why exchanging information with an international stakeholder will help to better address that problem. This section of the playbook provides guidance on three steps to successfully define the need for an international information exchange and the potential opportunity space for regulators.

### **2.1 Develop Scope and Use Case**

The objective of a GSIME type exchange is to enhance safety management by sharing data and information to directly support safety decision-making. It creates an opportunity for international collaboration to identify hazards, emerging trends, and potential risk mitigations, and enables States to meet ICAO SARP requirements and align on safety outcomes. It is best to begin by clearly defining the problem the data and information exchange is intended to address. Not defining the scope of the problem can lead to an inability to target the proper data and eventually a lack of usable data.

In some instances, defining a use case for the data and information exchange may be helpful to define, develop and deploy a safety information sharing system. Similar to the process used to develop this playbook, a Use Case is a methodology used in system analysis to identify, clarify and organize system

requirements. The method creates a document that describes all the steps taken by a user to complete an activity. A use case may establish the success scenarios, the failure scenarios, and any critical variations or exceptions.

To begin defining the focus of the data and information exchange and initial work scope, consider answering the following questions internally:

1. What is the specific safety question being addressed?
2. What data and information would help answer the safety question and inform the actionable safety intelligence?
3. What limitations exist in addressing this question today?
4. Can data from additional and diverse sources, such as international operations improve our answer to the safety question? How would a GSIME help address any limitations and further enhance safety in a way that directly supports decision-making? What is the value proposition to each of the stakeholders?
5. How would each of the stakeholders benefit? Why would they want to participate?
6. What are the relevant strategy and policy documents from the respective CAAs that could inform the exchange?
7. What are the relevant ICAO documents that could inform the exchange?
8. What are some potential risks (legal and technical) that would prevent the exchange?
9. How could these risks be mitigated?

At the conclusion of this step, documentation may include:

- Descriptions of the scope of the data and information exchange.
- Descriptions of the decided highest priority problems and related work scope.
- High level outline of a potential use case, including stakeholders, data, and potential benefits.
- Description of specific data and sources that would answer the safety question and inform the actionable intelligence.
- List of identified primary CAA and ICAO documents used to inform and prioritize the safety focus areas for the exchange.
- Any risks or barriers to the exchange of identified data and information.

## **2.2 Identify and Engage with International Stakeholders**

After the scope of the information and data exchange is defined, the next step is to identify potential stakeholders who would be willing and able to participate, and the resulting mutual benefits. In this version of the playbook, stakeholders are assumed to be other CAAs. Once candidate stakeholders have been identified, analyzed, and prioritized, initial outreach activities can begin.

Consider answering the following questions to help identify specific CAAs:

1. What CAAs may have the specific data identified in 2.1?
2. Would safety intelligence be gleaned from this data to enhance safety in the other State?
3. Why might CAAs be reluctant to participate? And how might these barriers be addressed?
4. Are there existing data and information exchanges that can be leveraged and expanded?
5. What specific offices and staff at the candidate CAA would be relevant and potentially interested in an exchange?

At the conclusion of this step, documentation may include:

- List of potential CAA partners, with specific contact information.
- Description of potential mutual benefits for all stakeholders.
- Description of data and related data protections that may be required.
- Any risks or barriers to the exchange of identified data and information.

Once candidate CAAs have been identified, prioritized, and appropriate Points of Contact (POCs) identified, preliminary discussions can occur to understand if there is any mutual interest in the potential exchange. Following these initial discussions, and once approvals are granted, the parties can work collaboratively to understand the problem space, data and information exchange scope, initial data types, value proposition, and existing international agreements. If these preliminary discussions are positive, further work towards documenting the scope and additional details of the exchange can take place.

Consider answering the following questions when engaging with specific CAAs:

1. What are the high-level goals of the safety information exchange partnership (be as specific as possible)?
2. What data types and level of detail are being considered for the exchange?
3. Are the schedules and timing expectations aligned?
4. How can the scope or schedule change to improve alignment?
5. How will the safety culture of partnering authorities influence the safety data and information exchange?
6. Is there mutual interest in proceeding?
7. Has something like this been tried before? If so, what happened, and what can/was to be learned/applied here?
8. Is there an existing agreement between the CAAs?

At the conclusion of this step, documentation may include:

- Description of collaborative understanding of problem space, value proposition and mutual benefit, data and information that could be exchanged and partnership models.
- Description of initial scope, schedule and proofs of concepts or prototypes that are mutually beneficial to all stakeholders based the use case.
- Documentation of existing agreements between the CAAs.
- Any risks or barriers to the exchange of identified data and information.

### **2.3 Determine Data and Information Needs**

Once preliminary agreement on the purpose and scope of a data and information exchange has been reached, further discussions can proceed on potentially relevant data and information sources, including analytic methods. As stated in the introduction, the purpose of a data and information exchange is to enhance safety outcomes. An initial strategy can prioritize leveraging publicly available data to build a foundation for authorities to exchange data on safety issues. This approach allows CAAs to establish the value of safety data exchange while mitigating initial challenges. This offers several key advantages:

- **Reduced Cost:** Utilizing readily available public data allows for cost-effective initiation of GSIME.

- **Reduced Risks:** Testing the playbook with public data minimized potential risks associated with sharing sensitive information.
- **Building Trust:** The initial phases focus on demonstrating value and building trust among stakeholders, paving the way for future collaboration.
- **Scalability:** The initial strategy establishes a clear path towards progressively evolving the playbook to include more comprehensive safety data sets.

This version of the playbook is focused on government-to-government exchanges of more comprehensive safety data and information.

The following terms will apply to this playbook:

- The term “Data” is defined in FAA Order 1375.1 as:  
Representation of fact, concept, or instruction in a form suitable for communication, interpretation, or processing either by humans and/or by automated systems. This is the lowest level of abstraction, compared to information and knowledge.
- The term “Information” is defined in FAA Order 1375.1 as:  
Data in context. The meaning given to data or the interpretation of data based on its context. The finished product as a result of the interpretation of data. Data that is processed in such a way that it can increase the knowledge of the person who receives it. Data that (1) has been verified to be accurate and timely, (2) is specific and organized for a purpose, (3) is presented within a context that gives it meaning and relevance, and (4) leads to an increase in understanding and decrease in uncertainty. The value of information lies solely in its ability to affect a behavior, decision, or outcome.
- The term “Intelligence” is defined by ICAO as:  
Safety intelligence refers to a more systematic structured approach for collection, analysis, and use of safety-related data and information to identify, understand, and proactively manage safety risks. Safety intelligence is an outcome of analyzing safety data and information, which provides the knowledge and skills to support decision-making process.

Data that is collected by CAAs can be categorized into two groups:

- **Mandatory data** is required to be submitted to a CAA due to a regulatory mandate, and is characterized by:
  - Typically structured in format.
  - May not be protected by legislation, and thus is subject to public disclosure.
- **Voluntary data** is submitted to a CAA on a voluntary basis, and is characterized by:
  - Typically unstructured in format.
  - May be protected from disclosure, depending on the specific statutes of the State. For example, in the U.S, voluntary data is protected if submitted as a part of Title 49 U.S. Code Section 44735 – Limitation on Disclosure of Safety Information. Five specific programs are identified in § 44735. However, this section may apply to other voluntary information.

Potential data sources and types are described in the Global Safety Information Project<sup>4</sup>. These include outcome-based data from automated/system-based data sources (such as flight data monitoring, air traffic control radar data), as well as observational data (such as line operations safety audit (LOSA) and normal operations safety survey (NOSS)) to advance a comprehensive understanding of causal and contributory factors.

Data and information sharing covers a broad spectrum and ranges from raw data sets to qualitative, de-identified and aggregated information. Significant value (safety intelligence that directly supports decision-making) can be derived from various forms of data and information. While de-identification offers a layer of data protection, whenever possible identified data acquisition should be considered. Identified data offers the richest analytical environment, enabling partners to extract the most nuanced and actionable safety intelligence. However, the GSIME initiative recognizes the importance of data confidentiality. Therefore, implementing safeguards like de-identification at publication or staged de-identification<sup>5</sup> is still very valuable to gain broader safety trend insights while maintaining a robust dataset for analysis.

Consider answering the following questions when determining data and information needs with a CAA (recognizing more detailed information will be gathered as part of the Data Protection and Confidentiality Requirements in Section 3):

1. What specific data or information will be exchanged? Identify specific safety intelligence needs for all parties to ensure mutual benefits.
2. For what time period?
3. What risks are associated with the data types, and what protections might be necessary to mitigate the risks with each data type?
4. Are there alternative approaches to scope the data exchange that would reduce risk, ensure confidentiality, and accelerate initial progress?
5. Is a common data taxonomy definition required to facilitate a seamless exchange?
6. What data-driven products or services (in lieu of raw data) could be offered to stakeholders?
7. Logistically, where is the data to be shared/exchanged, currently held/stored?
8. Logistically, how will the data to be shared/exchanged, to be transferred?
9. Where will the data to be shared/exchanged, once received, promote enterprise level sharing and analysis?

At the conclusion of this step, documentation may include:

- Description of final data and information requirements mutually agreed upon by the stakeholders.
- Description of data system compatibility and interface requirements between the stakeholders.
- Any risks or barriers to the proposed exchange of data and information.

### **3. Data Protection and Confidentiality**

A key step in a successful data and information exchange is to define and document the data protection and confidentiality requirements to ensure their continued availability and use for improving aviation safety.

---

<sup>4</sup> Global Safety Information Project; Level 3 Intensity Toolkit; Flight Safety Foundation. <https://flightsafety.org/gsip/gsip-toolkits/>

<sup>5</sup> De-identification at publication requires GSIME participants (e.g., authorities) to establish agreements that mandate de-identification upon publication or release from a CAA; staged de-identification considers redacting specific details such as flight, tail, and date at an earlier stage in the data pipeline.

The integrity of any data and information exchange rests upon the identification and protection of the supplied safety data and information from unauthorized access and disclosure. Any disclosure for purposes other than safety management can compromise the voluntary provision of safety data. Annex 19 suggests that States establish voluntary safety reporting systems to compliment mandatory reporting systems. ICAO encourages States to implement data protections in their legal frameworks to promote safety reporting. Data confidentiality plays a crucial role in enabling safety reporting and fostering a positive safety culture. Therefore, the safety data protection procedures must be clearly identified, documented, and agreed to by all parties and documented in any agreements or governance documents.

### **3.1 Conduct Required Data and Information Assessments**

Begin by conducting a data and information feasibility assessment, that may include identifying any restrictions and limitations regarding access and sharing of the required data and information. Additionally, the applicable laws and regulations of both parties should be identified, and their impact assessed. The results of this assessment should be documented as part of the governance agreement. As part of this process, work closely with stakeholders to adjust the exchange scope as necessary while still ensuring mutually beneficial results.

One potential option to enhance mutual trust between the stakeholder with regard to data protection and confidentiality is to utilize the services of an independent third party to hold and analyze the data. The third party would be the only entity to have access and visibility across all the data and information shared among stakeholders. The roles and responsibilities of the third party would need to be clearly documented in the governance agreement and not result in the loss of critical safety data being shared with all parties.

The data protection and confidentiality portion of the governance agreement may also include data principles, that define how the data may be used. Examples of data principles include:

- Stakeholders shall not use any information presented by another participating organization for commercial, competitive, punitive, or litigation purposes.
- Stakeholders shall not share or disclose the proprietary information provided by participants with external parties, without the written consent of the owner.
- Stakeholders shall not record (audio or video), take photographs of presentations, discussions or expositions, and share discussion proceedings or outcomes with external parties.

To begin conducting the required data and information assessments, consider answering the following questions:

1. Who are the data stewards for the required information and data, and related data repositories?
2. What format is the data stored in?
3. What taxonomies exist that define the different data fields?
4. What is the data type for each field (e.g., integer, real, character, string, Boolean, ...)
5. Are any metrics used? How are these metrics calculated? What is their intent?
6. What is the size of the data that will be shared?
7. How will the data be stored?
8. What processes are in place to ensure that overall security and integrity of the data?
9. How will the data be transferred?

10. Who has access to the data?
11. Would an independent third-party data steward improve the mutual trust among the stakeholders?
12. Are there any restrictions on using the data?
13. How often is the data updated?
14. What are the steps to follow to update the data?
15. How will the data be deleted at the end of the exchange partnership?

At the conclusion of this step, documentation may include:

- Summary of data assessment conclusions.
- Description of changes in information and data exchange scope to reflect data protection and confidentiality requirements.
- Mutually agreed upon data protection and confidentiality portion of the governance agreement.
- Descriptions of meta-data (i.e. description, purpose, structure, source, quality, known issues) and related data models.
- Description of required security measures that must be implemented.
- Any risks or barriers to the exchange of identified data and information.

#### **4. Legal and Governance Requirements**

This section of the playbook provides guidance on identifying, defining, and documenting any legal agreements and related governance documents required to successfully conduct a data and information exchange between CAAs. Formally documenting and describing how the data and information exchange will be governed is an important step in ensuring a successful exchange.

##### **4.1 Identify Existing and/or Required International Agreements**

With a mutual understanding of the scope, potential safety benefits, data protection and confidentiality requirements, CAAs can begin by identifying and reviewing any existing agreements that address information exchanges and related topics. The results of this review process should be shared with relevant stakeholders, so the exchange scope and schedule can be adjusted to reflect the review findings. Alternatively, existing agreements can be amended, or new agreements executed.

To begin identifying existing and/or required international agreements, consider answering the following questions:

1. What agreements are currently in place between the CAAs?
2. Are they relevant to the proposed exchange?
3. How will the agreements need to be amended, or will new agreements be required?
4. How will the scope of work and schedule need to be modified based on the status of the international agreements?

At the conclusion of this step, documentation may include:

- Summary of existing, relevant agreements and analysis of any required changes.
- Descriptions of potential changes in scope or schedule.
- Draft of new international agreement.
- Any risks or barriers to the exchange of identified data and information.

#### 4.2 Develop Data and Information Exchange Governance Process and Related Documentation

While the required legal documents are being developed, work can also proceed on defining the governance process for the data and information exchange. Key aspects of a governance document include core principles, responsibilities of parties, and data protection and confidentiality requirements.

- **Core principles** set out the high-level objectives and policies in relation to the exchange. Examples include: using exchanged data to advance safety goals only; exchanging data in alignment with the principles of protection in ICAO's Annex 19 on Safety Management; conforming to the roles, responsibilities and accountabilities as defined in the governance document.
- **Responsibilities of the parties** may include: following the core principles; defining and supporting how decisions are made; defining roles and responsibilities of each stakeholder and the independent third party (if applicable).
- **Data protection and confidentiality requirements** are described in section 3 but should be included in the governance document.

As described in section 2, defining a successfully exchange is an iterative process, and the scope of the data and information exchange may need to be adjusted based on legal and governance restrictions identified as part of this step.

To begin developing the data and information exchange governance process and related documentation, consider answering the following questions:

1. What are the core principles all stakeholders are expected to abide by?
2. What is the current level of trust among stakeholders? Do they have pre-existing working relationships (and if so, how are they)?
3. How will decisions be made between the stakeholders?
4. What level of formality is required to document decisions?
5. Are there previous examples of governance documents that can be leveraged?

At the conclusion of this step, documentation may include:

- Draft data and information exchange governance agreement, including core principles, roles and responsibilities, and data confidentiality requirements.
- Descriptions of potential changes in scope or schedule due to data protection procedures to meet confidentiality requirements.
- Any risks or barriers to the exchange of identified data and information.

#### 5. Finalize Documents, Execute Exchange, and Refine Process

The final step in the exchange process is to finalize the documentation, execute the agreed upon plan, conduct a limited data exchange test, then conduct the initial exchange and refine the process based on feedback from the stakeholders.

##### 5.1 Finalize Required Documents

Before conducting the initial exchange, ensure all the relevant documents, including required international agreements and governance documents prepared as described in Section 4, have been finalized to reflect any required changes and executed as appropriate.

To obtain approval of the agreements, consider answering the following questions:

1. Who needs to sign-off on each of the documents?
2. How long will it take to obtain the required approvals from all stakeholders?

At the conclusion of this step, documentation may include:

- Executed international agreements.
- Finalized governance document, include any data protection and confidentiality requirements.
- Any risks or barriers to the exchange of identified data and information.

## **5.2 Data and Information Exchange Test**

It is recommended that CAAs conduct a limited data exchange test based on data volume, complexity, confidentiality, and protection requirements. Technical solutions may range from email exchange of spreadsheets to direct access to systems. Based on stakeholder requirements, agree upon and test the data exchange technical solution with sample data as a proof of concept.

To define and the data and information exchange technical solution, consider answering the following questions:

1. What are potential technical solutions based on data volume, complexity, confidentiality, and protection requirements?
2. What are the validation criteria for finalizing the technical solution to exchange data?
3. How will the solution be documented?
4. How can the solution be tested and validated?
5. If required, what is the specific role of the independent third-party data steward?

At the conclusion of this step, documentation may include:

- Summary of the technical solution and proof of concept alternatives.
- Descriptions of selected solution.
- Description of test plan and validation criteria.
- Any risks or barriers to the exchange of identified data and information.

## **5.3 Conduct Initial Data and Information Exchange**

With all the plans in place and approved, a successful data and information exchange test, the initial data and information exchange can be conducted. Based on global best practices, adopting a progressive and incremental approach to the exchange will help to build trust among the stakeholders and reduce the information security risks.

To conduct the initial data and information exchange, consider answering the following questions:

1. What initial data and information will be exchanged?
2. How will the stakeholders validate the data was properly received?
3. What criteria will be used to evaluate the success of the exchange?

At the conclusion of this step, documentation may include:

- Validated list of information and data exchanged between the CAAs.

#### **5.4 Generate and Share Safety Intelligence**

The next step is to utilize analytic capabilities to uncover patterns, trends and insights using the new data and information that was exchanged. To achieve the goals of building a mutually beneficial partnership, the results of analysis and the safety intelligence analytical approach should be shared with stakeholders to the greatest extent possible.

To begin generating and share insights, consider answering the following questions:

1. What insights have we gained?
2. What other organizations in each respective CAA might be interested in these results?
3. How can the results be shared with the broader aviation community?
4. How might we work with stakeholders to develop mitigation strategies?

At the conclusion of this step, documentation may include:

- Reports documenting safety intelligence resulting from the data and information exchanged.
- Any risks or barriers to the exchange of identified data and information.

#### **5.5 Identify Value and Plan Subsequent Exchanges**

After completing the initial set of exchanges and analyses, the stakeholders should mutually determine scope of additional data and information exchanges (if any). As part of this process, stakeholders should articulate the value and mutual benefits gained from the exchange.

As subsequent exchanges are planned, the stakeholders should modify the international agreements and governance documents as necessary to reflect changes in the scope and focus, as well as lessons learned from the initial exchange. If concluding the exchange, delete data and information as defined in agreements.

To identify the initial exchange value and plan subsequent exchanges, consider answering the following questions:

1. What have the stakeholders learned that would not be possible without the exchange?
2. What changes in the exchange process would improve the efficiency and/or effectiveness of the exchange?
3. How do we need to change the governance documents to reflect those improvements?

At the conclusion of this step, documentation may include:

- Summary of value and mutual benefits of exchange to all stakeholders.
- Documented lessons learned from conducting the exchange (both positive and challenge areas).
- Updated international agreements and/or exchange governance documents.
- How to process safety issues and steps to mitigate (see example in Attachment A).
- Any risks or barriers to the exchange of identified data and information.

#### **5.6 Feedback Loop: Address any Discrepancies that Emerge During the Exchange**

Implementation of the data exchange could reveal previously unknown deficiency areas of either regulatory, technical, or bilateral nature. Engage with the appropriate organizations within each CAA to address any issues revealed during the exchange.

## 6. Future Revisions to This Playbook

As stated in the introduction, the GSIME initiative is leveraging a Proof-of-Concept approach focused on identifying and documenting relevant considerations required for regulatory organizations to establish an exchange for data, information, and intelligence with other authorities. As a result, this playbook is meant to be a dynamic document that is continuously updated as more information and data exchanges are conducted.

The focus of this playbook version is on safety-centered data and information exchanges between CAAs. Over time, exchanges could expand to address operational and other issues, and thus involve other stakeholders such as air navigation service providers (ANSPs), airports and aircraft operators, which will likely have different sets of risks.

Lessons learned from these ongoing exchanges may also assist in the Identification and evaluation of legislative gaps, including gaps that would be necessary to enhance the protection of Annex 8 data or data recommended by ICAO and provided by foreign entities for the purpose of improving aviation safety.

## 7. References

The following references were used in preparing this playbook.

1. 49 U.S. Code Section 44735 – Limitation on Disclosure of Safety Information
2. ICAO Annex 8: Airworthiness of Aircraft, Part II, Chapter 4, Thirteenth Edition, July 2022
3. ICAO Annex 19, Safety Management, Second Edition, July 2016
4. Global Safety Information Project; Level 3 Intensity Toolkit; Flight Safety Foundation.  
<https://flightsafety.org/gsip/gsip-toolkits/>
5. ICAO Ninth Meeting of Africa-Indian Ocean Regional Aviation Safety Group (RASG-AFI/9), Safety Intelligence to support decision-making. November 2023.  
<https://www.icao.int/WACAF/Documents/RASG%20AFI/RASG-AFI-9/ENG/WPs-ENG/RASG-AFI9%20-%20WP04C3%20-%20Safety%20Intelligence%20to%20support%20decision%20making.pdf>

## Attachment A: FAA-CASA Case Study

The playbook incorporates lessons learned based on historical case studies where the U.S. Federal Aviation Administration (FAA) exchanged data with international stakeholders. This appendix describes how the FAA's Compliance and Airworthiness Division (AIR-700) of the Aircraft Certification Service (AIR) used Analyze Safety – Performance Insight – Results Environment (ASPIRE) initiative in partnership with the Australian Civil Aviation Safety Authority (CASA). Specific examples describing how each of the steps defined in the playbook were applied in the CASA case study are documented below.

### 1. Identify Scope and Opportunity

#### • Develop Scope and Use Case

- After launching a data analytics operating system (“data OS”) called ASPIRE in June 2021, FAA discovered potential gaps in the international safety reporting of failures, malfunctions, and defects (FMD) related to U.S. products operating overseas. By identifying a partner Civil Aviation Authority (CAA) with U.S. products in their fleet, the

FAA could test its ability to aggregate and analyze product-level safety data in ASPIRE, highlighting potential safety hazards in the worldwide fleet.

- **Identify and Engage with International Stakeholders**
  - The FAA reached out to several CAAs in the Asia-Pacific region after the launch of ASPIRE to discuss the potential benefits of increased access into the operational performance of U.S. products overseas. This included providing an overview of FAA's new data analytics capabilities to CAAs participating in the Asia Pacific Continued Operational Safety (COS) forum, a periodic meeting of FAA safety experts with counterparts from this region to discuss regional safety issues. From this engagement, the Civil Aviation Safety Authority of Australia (CASA) emerged as a potential safety partner with a wide range of U.S. products on its registry.
  - Estimated benefits of conducting a proof-of-concept with CASA included: a similar regulatory framework, established bilateral agreements for airworthiness with strong collaborative history, ease of communication, penetration of U.S. product operating in the Australia environment, and the unique operational profile of certain US products not observable in our own domestic fleet (for example, Robinson helicopters' extensive use in the in the harsh interiors of Australia)
- **Determine Data and Information Needs**
  - The first step included an internal FAA assessment of FMD submittals, in accordance with both, the bilateral Agreement and ICAO framework as codified in Annex 8, Airworthiness of Aircraft, as well as associated guidance such as ICAO Circular 95.
  - Following FAA potential safety gap determination, FAA and CASA met to discuss how each side collects data for FMDs (i.e., voluntary, regulatorily mandated, or both), the extent of and how operators report safety events, the extent of and how maintenance facilities report service difficulties, availability of ANSP data, access and use of outside sources of data to complement safety investigations, and maturity of data analytics capabilities.

## 2. Data Protection and Confidentiality

### • **Conduct Required Data and Information Assessments**

- Before initiating the case study, the FAA procured a commercially available, off-the-shelf data operating system. This acquisition was aimed at enhancing the FAA's capabilities in safety data analytics. The procurement process involved comprehensive data protection analyses and data governance reviews to ensure the security of the data stored within the system.
- The data identified for exchange in the proof-of-concept was thoroughly evaluated and classified as sensitive unclassified information (SUI). The guidelines for safeguarding and disseminating SUI are detailed in FAA Order 1600.75, titled "Protecting Sensitive Unclassified Information (SUI)".
- The FAA also verified that U.S. regulations offer protection against the disclosure of voluntarily shared safety data by Civil Aviation Authorities (CAAs).

## 3. Legal and Governance Requirements

- **Identify Existing and/or Required International Agreements**

- The FAA benefits from mature State-State Bilateral Aviation Safety Agreements (BASA) that include validation, airworthiness, and exchange of aerospace products, post certification support and continued operational safety of these products, communication and conflict resolution protocols, and high-level provisional language for the exchange of data.
- FAA and CASA collaborate in a variety of aviation areas in accordance with the U.S.-Australia BASA. Provisions specific to the certification and COS of products can be found in the Implementation Procedures for Airworthiness (IPA). Both agreements can be found here:  
[https://www.faa.gov/aircraft/air\\_cert/international/bilateral\\_agreements/baa\\_basa\\_listing](https://www.faa.gov/aircraft/air_cert/international/bilateral_agreements/baa_basa_listing).
- While these Agreements provide process-like detailed coverage on the validation, airworthiness, and exchange of products with other CAAs, coverage for post certification activities (such as COS and data submittal) is top level and not as specific as in the certification stage.
- **Develop Information Exchange Governance Process and Related Documentation**
  - FAA and CASA determined that in relation to FMD data, the IPA provides sufficient coverage for the submittal of such data in a PoC environment aligned with ICAO Circular 95 notification of FMDs.
  - FAA and CASA agreed that subject matter experts on both sides would communicate directly via email once Australian Defect Report Service (DRS) data was integrated in ASPIRE, analyzing Australian safety events as prioritized by CASA and agreed upon by FAA. Any findings would be verified by engineering subject matter experts working in conjunction with data scientists.

#### 4. **Finalize Documents, Execute Exchange and Refine Process**

- **Finalize Required Documents**
  - As discussed, FAA and CASA specialists in consultation with their respective international support staff agreed that the data exchange provisions in the IPA would be sufficient to commence a data exchange PoC.
- **Data and Information Exchange Test**
  - FAA's regulatory responsibilities center on products' performance in the NAS, spanning from original certification to the operational safety of these products once in service. Upon consulting with CASA, a joint determination was made that the Australian DRS data for U.S. products operating in Australia would be best suited for a PoC on data integration. DRS data is considered equivalent to Service Difficulty Reporting (SDR) data in the FAA system, i.e. service difficulty reporting by operators covered in the Code of Federal Regulations (14 CFR) part 91, 125, 135, 121, as well as repair stations under part 145.
  - CASA uses Power BI to interpret safety data. The process is not automated and data is loaded monthly. Since the scope of the merged data sets covers both FAA and CASA U.S. registered product, integration of the data would take place in the ASIRE data OS. Findings would then be shared with CASA for their own analyses and evaluation.
  - FAA and CASA determined that actual data transmittal would occur via email from CASA to FAA in MS Excel file format. This data would then be transformed, integrated,

and commingled in the ASPIRE data OS to analyze safety events on Australian registered U.S. products vis-a-vis the U.S. fleet. This would include fleet trending, comparative analyses and other advance machine learning statistical approaches.

- **Conduct Initial Information Exchange**

- FAA imported CASA's DRS .csv file using basic transformation techniques with python code. FAA was able to achieve a high rate of joining, but short of 100% and noted that having additional information, such as the registration, would increase fidelity of the merge, better mapping, and simplify the joining steps even further.

- **Generate and Share Safety Intelligence**

- During regular monthly steering meetings, FAA and CASA evaluated US products safety events in the Australian fleet, prioritizing events to serve as use cases for testing data integration and advanced analytics.
- Over the course of 12 months, FAA and CASA analyzed several product-related potential safety issues, including:
  - Boeing 737 NG thrust reversers failure to deploy.
  - Honeywell multi-function displays DU-1080 failure on AW189 and AW139 helicopters.
  - Rate of reply issue for Traffic Avoidance System Avidyne TAS600 on Diamond DA-40 and DA-42 aircraft.
  - Bell 206-L1 defective MR grip nut.
  - Beech 200 cargo door z clip cracking.
- A proof-of-concept portal was created and its use was demonstrated as an alternative and preferred method to exchange documents in a secure manner.

- **Identify Value and Plan Subsequent Exchanges**

- Through the integration of data, FAA and CASA were able to demonstrate how commingled data from different sources can help spot potential safety issues, determine the statistical validity of observed trends in the data, and/or verify if a safety issue is repeated in other data streams or other fleets.
- The data exchange also demonstrated the value of the enrichment of data for both entities, the FAA acting as a State of Design and CASA acting as State of Registry for U.S. products. The PoC was able to demonstrate that data integration expedites analysis of safety events and reduces the potential for human errors.

- **Feedback Loop: Address any Discrepancies that Emerge During the Exchange**

- FAA has an established COS reporting process to disposition safety issues and take appropriate action, up to the issuance of airworthiness directives (ADs). The PoC did not indicate the need to modify this process.
- However, through this PoC the FAA concluded that:
  - Establishment of a portal where CAAs can directly submit safety data would provide further efficiency in the exchange of product-related safety data.
  - The furtherance of data exchange needs enablement at the top level (such as bilateral agreements or other legal instruments) and a strong data governance framework so that sensitive data is protected from disclosure.
  - Commingling of data allows greater precision and insight into safety issues but this can only occur if the supporting Information Technology (IT) environment

can easily segregate information based on use case needs and the entity accessing the data (i.e., a CAA or outside organization given access to parts of the data lake).

- Barriers to integration of data are often internal to an organization (complex layers of approval, data stewards' resistance, unclear data exchange provisions, etc.), rather than due to technological limitations.

Safety data exchange must present a value proposition for all the parties sharing the data. In this use case, the enablement of CASA specialists through a data findings feedback loop created incentivization for greater collaboration and a more nuanced understanding of potential safety issues.

— END —