FLIGHT SAFETY FOUNDATION

GLOBAL SAFETY INFORMATION PROJECT

Information Protection Toolkit

MARCH 2017

FLIGHT SAFETY FOUNDATION

GLOBAL SAFETY INFORMATION PROJECT

Information Protection Toolkit

Welcome

Thank you for your interest in enhancing aviation safety information protection (SIP). The protection of safety data and safety information is critical to ensure that they remain available to your safety data collection and processing system (SDCPS), helping your organization to identify known and potential risks to flight operations and to effectively mitigate the risks.

This toolkit is a product of Flight Safety Foundation's Global Safety Information Project (GSIP) and primarily aims at providing all SDCPS stakeholders — at the regional, state, government agency and corporate levels — guidance on complying with existing and upcoming International Civil Aviation Organization (ICAO) standards and recommended practices (SARPs) for SIP.

The toolkit's website-based content <flightsafety.org/gsip> will also contain Foundation-developed best practices for SIP that are suitable for various service providers — such as aircraft operators in domestic and international commercial air transportation, approved maintenance and repair organizations providing services to operators, approved training organizations, organizations responsible for type design or manufacture of aircraft, air traffic service providers, and airport operators.

To briefly summarize our primary scope, ICAO's existing and upcoming SARPs provide stakeholders (i.e., service providers and civil aviation authorities [CAAs]) with principles of protection and principles of exception. They also require stakeholders to protect against the public disclosure of safety information; to have a competent authority that balances the interests of safety and the need for the proper administration of justice; and to apply appropriate safeguards to ensure safety information is protected.

With these requirements in mind, and with advice from international experts in the legal aspects of safety, the Foundation has analyzed SIP in the ICAO-defined Asia and Pacific Region and in the Pan America Region. Our analysis included studying the differences between current SIP practices and the ICAO SARPs, and developing this toolkit to assist stakeholders around the world with required and recommended SIP-implementation methods.

We believe that SIP should be implemented by the appropriate government organizations in your country and by the aviation organizations for which the government conducts regulatory oversight or has another type of authority. At the national level, the Foundation agrees with ICAO's recommendation that states must implement rules to provide a protection framework not only for CAAs and service providers but also for a very broad range of aviation stakeholders — including, for example, law

enforcement agencies and accident investigation authorities. Within organizations, policies should be in place to protect programs such as employee voluntary safety reporting and flight data monitoring.

Similar to the three SDCPS-focused toolkits on our website, our plan for this *Information Protection Toolkit* calls for increasingly advanced guidance and recommendations to states and service providers; capability to capture your feedback and to share feedback from other toolkit users with you; and a repository of stakeholders' de-identified SIP experiences and best practices.

Note that this toolkit, like the other GSIP toolkits, distinguishes the term *safety data* from the term safety information in a manner similar to the typical distinction in ICAO documents (i.e., aviation organizations typically collect safety data comprising discrete or irreducible elements such as numerical values and, by analytical processes, transform these data into valuable safety information). This toolkit addresses not only the protection of both safety data and safety information but also protection for the related sources, as provided in ICAO's principles of protection.

Based on international research and promotion by our experts in legal aspects of aviation safety — and on discussions and participant surveys in the two regions during FSF GSIP focus groups and toolkit-development workshops in 2015 and 2016, respectively — the Foundation became aware of various stakeholders' perspectives of SIP. Among these, we heard that information protection by CAAs, service providers and other aviation stakeholders remains a serious challenge today in many of the countries visited. We believe that addressing stakeholders' specific legal, regulatory, technical, cultural and practical impediments is essential because SIP is a key element of every SDCPS component: data collection, data analysis and information sharing.

Further updates to the *Information Protection Toolkit* are planned during 2017 to provide adaptable, interactive training modules that can help you — and can help fellow stakeholders who have different needs — to better understand and implement SIP. These modules will be able to be readily tailored to the whole range of potential users. This could extend from the smallest service provider responsible for implementing SIP as part of its safety management system (SMS) to a large CAA providing training and education to judicial and law enforcement authorities in the context of a state safety program (SSP).

To sum up, as noted in the *GSIP Toolkits Introduction,* our set of toolkits serves as an architecture to facilitate further communication. That is our first goal. This means the website enables us to link you to other programs and resources to help you gather practical concepts and implementation methods suitable for your organization such as guides for handling sensitive data, model regulations and legislation.

Our second goal is to interact appropriately with toolkit users as a trusted independent organization, capturing your experiences and questions for the benefit of a network of people facing common SIP issues. Your input about putting structures in place to protect safety data and safety information — and sharing your documented outcomes — holds promise of being extremely valuable.

Getting to Know ICAO SARPs for SIP

The *Information Protection Toolkit* will be refreshed as needed to help your aviation safety specialists, whether at a CAA, service provider or other concerned organization, to better understand which SIP practices fall under Annex 13, *Aircraft Accident and Incident Investigation,* and which fall under *Annex 19, Safety Management.* Each annex provides a separate, yet complementary, framework to protect safety data and safety information.

Annex 13 contains the SIP-related SARPs most relevant to aircraft accident and incident investigations, while Annex 19 contains the protection-related SARPs for a service provider's SDCPS and the specific SARP provisions related to the SSP of a country.

Specifically, as we add them, you will find synopses of the definition of SIP and the key elements of SIP, as well as SIP laws and regulations; policies; model advance arrangements and information safeguards; and education and training programs for CAAs, service providers, judicial authorities, government leaders and the global legal community. Our plans for 2017 also call for a periodically

updated SIP timeline, highlighting milestones such as ICAO's recognition of the need for SIP, and the development of the basic SIP framework as initially published in Annex 13 and Annex 19.

SIP Intensity Levels

In the *GSIP Toolkits Introduction* and in the three other GSIP toolkits, Flight Safety Foundation proposed intensity levels as a highly useful concept and terminology for every stakeholder to self-identify and to improve its SDCPS capabilities over time. We hope to settle by early 2017 on a similarly clear and simple way to categorize a stakeholder's capacity to employ SIP, to self-assess the differences among organizations in SIP-related sophistication and initiatives, and to openly discuss what is happening in the local, national, regional or global SIP domains over time.

Currently, we envision a set of SIP intensity levels requiring different descriptive narratives compared with those related to SDCPS. Based on FSF research and analysis of ICAO's SARPs, the observations of our collaborating experts in the legal aspects of aviation safety and discussions of the current SIP implementations in Asia Pacific and Pan America, we are proposing four intensity levels as follows:

- At the first intensity level, the typical service provider or CAA characterizes its sophistication and performance only in relation to adhering to all the SIP-related standards of Annex 19. This essentially means taking steps that help to protect aviation professionals against inappropriate uses of safety data and safety information that lead to disciplinary action by the employer, criminal prosecution, CAA certificate action or related punitive actions outside internationally recognized principles of just culture.
- At the second intensity level, the typical service provider or CAA characterizes itself as adhering to the same requirements as in the first intensity level, but additionally implements a policy and procedures that shield aviation professionals, such as protection from punitive actions based upon certain types of mandatory occurrence reporting of safety issues. The strongest argument for protection of some mandatory occurrence reports is that of resolution advisories from traffic-alert and collision avoidance systems (TCAS RAs) and warnings from terrain awareness and warning systems (including Enhanced Ground-Proximity Warning Systems [EGPWS]). There may be other comparable safety issues that are not always monitored, detected or recorded from outside the flight deck. Protection of safety information recorded automatically and consistent reporting by aviation professionals can encourage full reporting and lead to everyone's greater awareness of the existence of these events. Historically, the world's airlines have found underreported levels of TCAS RAs and EGPWS warnings in both their employee voluntary reporting programs and their mandatory occurrence reporting. SIP measures exceeding those at the first level may promote the awareness made possible by flight data monitoring programs. Information protection inherent in those programs typically has not extended to all the types of mandatory occurrence reporting where high volumes of reports are received and CAA investigations may lead to punitive action. (For SSPs, Annex 19 recommends similar protection of certain required safety reports.)
- If we reach a consensus about the need for a third intensity level, the typical CAA, and potentially a service provider, would characterize itself as adhering to the same requirements as in the first two intensity levels. In addition, the protections would apply to specific cases that would encourage global adoption of just culture principles. This would facilitate a CAA's recognition of situations in which the need to know about all safety events that occur, the need to maximize the benefits of SIP to fully understand the risks, and that safety outweighs any benefit of taking punitive action against aviation professionals based on this safety information.
- If we reach a consensus about the need for a fourth intensity level, the CAA would characterize itself as adhering to the same requirements and to similar recommendations as in the first three intensity levels. In addition, information protections would be designed to facilitate advance

arrangements and other agreements across state or regional boundaries. For example, assume that several states are collaborating on safety information sharing. They likely would characterize themselves as engaged in SIP activities at the fourth intensity level at a time when the knowledge gained from sharing rates of specific events drives them to adopt SIP practices that prohibit corporate disciplinary action, criminal prosecution or CAA certificate action by one state against individuals or organizations in other states.

A summary of all of these intensity levels along with the other SDCPS activities is provided on page 6 of this document.

Looking Forward

Potential sources of new toolkit content include feedback from FSF GSIP focus groups, workshops, webinars, and public and private discussions during our planning phase. Also valuable will be insights collected from SIP experts; participants in other related conferences and meetings; our extensive SIP research; our experts' 2015 review and analysis of Asia Pacific and Pan American states' level of SIP implementation; examples of the use of safety data and safety information in civil, criminal, administrative and disciplinary proceedings; and the FSF Legal Advisory Committee's (LAC's) efforts on SIP issues.

The LAC is a voluntary FSF committee established in June 2013 and is composed of globally diverse experts in the legal aspects of aviation safety, including representatives from manufacturers, labor unions, airlines, regulators, plaintiffs' and defense lawyers, and international organizations. The LAC will be an ongoing resource for potential future GSIP efforts.

Local SIP Best Practices

Complementing the main sections of the *Information Protection Toolkit* that cover ICAO-endorsed international practices, Flight Safety Foundation aims to address several "soft" aspects of SIP (i.e., best practices that service providers and CAAs find valuable, separately from state laws, ICAO SARPs and official guidance). We want to publicize relatively unknown, SIP-relevant best practices that have come to GSIP researchers' attention. We are motivated by the belief that strong safety culture (including strong employee voluntary safety reporting, for example) and the just culture principles noted above will be essential elements of SIP success.

Participants in GSIP focus groups and workshops told us that many effective practices in information protection are not based solely on state laws, CAA regulations, company policy or formal commitments among service providers. They come from other practices established over long periods with favorable results. The following examples of such practices, typically carried out to support a formal policy, would be worth covering in more detail:

- **De-identification —** Whether you process safety data with an advanced computer system or a rudimentary, non-technical method, it is worth the time of everyone involved to discuss exactly how each specific process must be performed. Knowing this level of detail can prevent protected information from inadvertently surfacing (i.e., causing harm by being revealed internally or to the public) at some time long after the initial employee voluntary safety report was received or the routine flight data were extracted from a flight data–recording system. Usually, the SIP process is straightforward and routine, a matter of checking that the content of key data fields has been de-identified. Other times, however, data that must be manually de-identified by the analyst are buried in dense or voluminous text, and you may need to perform additional extraction or summarization of raw data to ensure that the de-identification occurred.
- **Non-disclosure agreements —** Service providers routinely use these agreements to reduce the risk of disclosure to third parties of sensitive information. Often, the protected materials may be a program status or results that have been shared within internal discussions that are speculative/inconclusive in nature, or within preliminary group "brainstorming" about how to improve safety

performance when something in a policy or process fails to achieve the target rate of occurrence, for example.

- **Summarized information —** Recognize the characteristics of your audience and the implications of conducting a summary-type presentation of safety data or safety information for that audience. Stakeholders may inadvertently communicate information that immediately implies that some aspect of your organization's safety performance is the "worst ever," and thus obviously "unsafe," when in fact that conclusion is neither intended nor accurate. Ask yourself how special provisions, such as a clear introduction with caveats, and clear documentation of accurate conclusions, can prevent the audience from jumping to the wrong conclusion and misinforming others.
- **Handling identifiable information —** In some situations, a case can be made for an exception to the typical rule that all aviation safety-event information must be de-identified prior to disclosure outside a very small group of authorized data analysts. This could be seen as quite a "progressive decision" — but one made only when safety leaders, directors of safety, high level administrators and groups of aviation safety specialists make a strong commitment to focus solely on achieving a critical safety benefit and prohibiting disclosure of the identities of flights, flight crews, etc., and the assignment of blame to identified people. The importance of everyone adhering to such a commitment cannot be overstated because breaches can destroy an entire safety program that has been built upon a high degree of employee-management trust.

Your Opportunity to Share

From the outset of GSIP, Flight Safety Foundation has requested permission to curate and publish de-identified narratives about SIP, drawing from experiences of aviation safety organizations and professionals. We welcome you and fellow *Information Protection Toolkit* website visitors to take advantage of this chance to advance and enrich the knowledge of your counterparts worldwide.

Others want to learn, for example, how you implement SIP in flight operations — such as ensuring the protection of de-identified, aggregated and other forms of shared information from flight data monitoring of routine operations, air traffic management safety data, aircraft maintenance and repair irregularities, internal accident/incident studies, audits/assessments, employee voluntary safety reporting systems and other confidential sources. Hundreds of GSIP participants and other individual stakeholders will appreciate the chance to learn from you and to share with you in return. GSIP will follow U.S. Federal Aviation Administration and Flight Safety Foundation confidentiality standards on vetting information and protecting your privacy.

To demonstrate the value and importance of SIP, this toolkit will present SIP success stories. For example, this toolkit will discuss a legal example where safety information had been protected.

Ultimately, the *Information Protection Toolkit* will address all the issues that states, their CAAs and service providers should consider when implementing SIP. We welcome your feedback about this toolkit to help achieve one of the core objectives of GSIP — to improve the sharing and harmonization of safety information. Members of the GSIP team will respond and consider SIP ideas, best practices, lessons learned and applications in flight operations.

Global Safety Information Project (GSIP)

Overview Matrix Of Intensity Levels

Risk management is a tool for decision making and improving safety performance. As it is executed, additional learning continues to take place, which expands our knowledge on hazards and our horizons of influence. GSIP recognizes this ever-expanding growth of risk management and therefore incorporates a level of intensity across our toolkits. The following chart includes a simplified version of the different levels of intensity across all risk management safety activities.

	SMS Core Level	Expanded Level	Advanced Level	Industry Level
Data Collection	Data are collected to adequately monitor the normal hazards an organization may encounter and to support a functioning SMS.	Data are collected to understand both the hazards and exposure to operations with those hazards (e.g., *flight data acquisition systems).*	Data are collected to advance understanding of primary causes and contributing factors (e.g., *monitored data through LOSA).*	Data are collected to utilize and contribute to a larger industry understanding through bow tie organization of events (e.g., *data collection with industry partners).*
Data Analysis	Data are analyzed to determine acceptable risks. Safety performance indicators with current status against objectives.	Data are analyzed to understand all direct hazards and their impact on undesired outcomes. Multiple hazards are each examined for their influence on risk.	Data are analyzed to understand all potential direct and indirect hazards and their impact on undesired outcomes.	Data are analyzed to understand all industry impacts on safety. The math behind paths leading to and from an undesired state are well understood.
Information Sharing	Information sharing of performance results is comprehensive within an organization (e.g., within one organization).	Information sharing of performance and key areas of linked performance is performed among divisions or industry peers at detailed levels (e.g., ANSP to ANSP).	Information sharing is across the industry for key risks and mitigations. Generally this is through presenting detailed independent investigative work in the data (e.g., ANSP to airline).	Information is shared and managed across the industry for benchmarking capabilities and emerging conditions. Cooperative analysis is conducted (e.g., pooled data).
Information Protection	Individuals and organizations are protected against disciplinary, civil, administrative and criminal proceedings, except in case of gross negligence, willful misconduct or criminal intent.	The protection extends to certain mandatory safety reporting systems. In Annex 13, the protection extends to final reports and investigation personnel.	Further protection mechanisms may be in place to implement just culture principles and cross-industry support for strong safety reporting cultures.	Protection is formalized at the highest level between countries through memorandums of understanding or similar agreements.

ANSP = air navigation service provider; LOSA = line operations quality assurance; SMS = safety management system