Seattle-Tacoma International Airport

SMS Data Collection and System Review

Prepared For: Federal Aviation Administration
Office of Airports
Airport Safety and Operations Division

Prepared By: Landry Consultants LLC, on behalf of Seattle-Tacoma International Airport and Operations Senior Manager, Mark Coates

Date: 11/25/2009

Revision History

Date	Version	Description
5/7/09	v.0.1	Initial draft
6/18/09	v.0.2	Draft updated following meeting with Warren Randolph, FAA ASIAS program
10/12/09	v.0.3	Updated draft
11/3/09	v .1.0	Version 1 complete for Sea-Tac review and approval
11/25/09	v.1.0	Final

Prepared in Support of Statement of Work Section A – Airport Safety Policy, Task 4:

Research third party data collection, collaboration, and reporting systems. *Under the Freedom of Information Action (FOIA), the public can request a variety of information from airports. To encourage reporting under the airport's SMS Program, research of a third party database to collect, store, and report on SMS events, trends, and activities will protect data from FOIA requests. Obviously, the level of detail and expanse of the reporting system will vary from airport to airport. Therefore, under this tasks, the airport will develop a list of requirements for third party hosting; collaborate with FAA/JPDO for best practices and possible joint development of a system; and, report out on the pros and cons of systems with a recommendation for Part 139 airports of similar size and operations.*

Table of Contents

List of Figures

List of Tables

1. Introduction

As part of the FAA-sponsored Safety Management System (SMS) follow-on pilot study conducted at Seattle-Tacoma International Airport (SEA or Sea-Tac) and as required under Policy, Task 4 the team has performed an assessment of third party data collection, collaboration, and reporting systems. As referenced in the SMS follow-on Statement of Work (SOW), the task was driven by a fundamental interest in determining an individual airport's most effective strategy to protect SMS and, in particular, Safety Risk Management (SRM) data from Freedom of Information Act (FOIA) requests:

> *Under the Freedom of Information Act, the public can request a variety of information from airports. To encourage reporting under the airport's SMS Program, research of a third party database to collect, store, and report on SMS events, trends, and activities will protect the data from FOIA requests.*

Inherent in this task (though not specifically highlighted within the SOW) were 3 core assumptions:

1. Airport SMS data (in particular, SRM data) must be protected from FOIA requests.
2. Implementing a third party data collection system will enable airports to protect SMS data.
3. Protecting SMS data will encourage air carriers and other airport tenants to report.

During the course of the detailed assessment, the team discovered that the assumptions outlined above do not constitute a solid foundation on which to build a data collection and protection strategy. Therefore, the assumptions themselves merited further examination. Therefore, this document is not limited to a presentation of third party systems but is, rather, a holistic discussion of data collection, collaboration, and reporting strategies that we feel will add important context to SMS rulemaking and implementation. This document includes:

1. Assessment of the initial set of data collection and protection assumptions
2. Recommended approach to data collection and reporting
3. Detailed functional requirements for SRM and SMS data collection and reporting applications, as modeled at Sea-Tac

2. Initial Assumption Assessment

As outlined in Section 1, the task of researching data collection, collaboration and reporting systems for the follow-on airport proof of concept study was founded on several inherent assumptions. This section includes a discussion of the team's findings relevant to each assumption.

2.1 SMS Data Must Be Protected Against FOIA Requests

The assumption that data must be protected against FOIA requests in order for a SMS to be most effective has been prevalent in writings and discussions and additionally served as the basis for Policy, Task 4 in the SMS follow-on study SOW. To discuss this assumption, it is important to note that "SMS data" is a broad concept that includes a variety of information. For the purposes of this document, and as the reader will note in future sections, "SMS data" can be discussed in 2 general categories:

1. Safety Risk Management (SRM) data
2. Other SMS data

The primary discussion and concern surrounding public disclosure has historically been focused on SRM data. It is the information related to hazards, accidents, incidents, and near misses that is generally regarded as the area of most concern. The concern has been articulated that public availability of airport SRM data may result in increased liability for both airports and air carriers. However, airports have not voiced as significant a concern regarding other types of SMS data (to include training records, inspection results, etc). Bearing this in mind, the assessment of this assumption is focused primarily on ***the need to protect SRM data*** from public disclosure.

In exploring this assumption, the team discovered that airports (Sea-Tac in particular) are already capturing, documenting, and retaining large amounts of SRM data. This information is related to hazards, accidents, incidents, personal injury, near misses, and other significant operational activities, all of which is currently available for public release. As of this writing, there have been 207 FOIA requests to the Port of Seattle (Sea-Tac's governing body) in 2009. A brief review of FOIA requests found that 16 were related to the airfield (4-construction bidding process), airport operations (3-noise), or linked to personal accident/injury at Sea-Tac (9).

There is discussion and question among airports about whether formalizing and documenting the SRM processes and having that information disclosed publicly will increase an airport's liability. It is currently unknown whether SMS program implementation will result in an increase in FOIA requests but it is conceivable that, if members of the public have knowledge about the program, they will request more safety related information. With the implementation of tracking and trending databases, the information will be easier to locate and the public may thereby receive more detailed information than is available to them today.

However, in the team's research, we have discovered that for airports with a willingness and drive to implement SMS, FOIA requests do not, at least anecdotally, appear to be a significant cause for concern, either for SRM or other SMS data. The team believes that implementing SMS and associated tracking databases will simply not present a significant departure from the current state. Airports already collect much, if not all, of

the data necessary for SRM (as well as the other SMS elements) and this information is currently available for public release. In fact, airport advocates of SMS voice a counter argument that there may be decreased liability due to the demonstrated due diligence, rigor, and documentation that a SMS will bring to airport SRM efforts.

Regardless of the arguments for or against, it is highly unlikely that a definitive answer to the question of SMS impact on FOIA requests (and any downstream impact to airport liability) will be available until SMS has been operational for several years. Because of this, the team does not believe that the potential for FOIA requests should impact the functional requirements for developing and implementing a data collection system. Nor does the team believe that airports should abstain from implementing SMS until such time as SRM data protection can be guaranteed.

2.2 Third Party Hosting will Provide Data Protection

It has been assumed that utilizing a third party, hosted data collection system to anonymously capture and de-identify data, and provide "scrubbed" reports, will enable airports to protect both its data and its tenant's data from potential public disclosure.

The team agrees that protecting SMS data from public disclosure would be beneficial to airports but, as detailed in the Foley & Lardner legal brief (insert below), does not believe that third party hosting will necessarily meet this objective.

> *Such third party hosting of information is often performed for health care institutions, not because of FOIA concerns, but to maximize efficiency. In the airport context, however, if data is provided directly to a third party not subject to FOIA, in certain cases it may be possible to prevent the disclosure of that information under FOIA. There are several drawbacks to this approach, however. The first is that the federal FOIA was recently amended to include information gathered on behalf of a federal agency by a third party as information subject to FOIA.[45] It is likely that many, if not all, state FOIAs will follow this lead at some point, thereby mooting this potential means for avoiding disclosure. Second, once the airport accesses the third party's database, the information that is delivered to the airport becomes subject to applicable FOIA.*

As discussed in the Foley & Lardner brief (prepared in support of Policy, Task 3), the team believes that enacting federal legislation to maintain the confidentiality of SMS data would be the most effective method of ensuring data protection. Though this approach would clearly enable airports to protect such information, recent developments with the national bird strike database lead the team to believe that this type of protection is not forthcoming, at least not in the very near-term.

---

45 *See* 5 U.S.C. § 552(f)(2) (" 'record' and any other term used in this section in reference to information includes – (A) any information that would be an agency record subject to the requirements of this section when maintained by an agency in any format, including an electronic format; and (B) any information described under subparagraph (A) that is maintained for an agency by an entity under Government contract, for the purposes of records management.") added by Pub. L. 110-175, Sec. 9 (Dec. 31, 2007).

In light of this, the data collection and protection strategy must be effective without a guarantee of maintaining confidentiality. Further, the determination to implement a third party-hosted solution should be made based on features, functionality, and cost, rather than an assumption of data protection.

2.3 If You Protect It, They Will Come

A driving assumption in SMS airport implementations has historically been that protecting safety risk management data (hazards, accidents, incidents and near misses) from public disclosure will encourage air carriers and other airport tenants to report into an airport's SMS.

It is undisputed that the more data collected, the better tracking on safety hazards, risks, and trends will be. The bottom line is that an airport can't improve what it can't track. The team noted that "data" can take many forms and that the term should not be used to loosely categorize all items on which airport or airline may report. When applied to airport reporting, the distinction between hazards and incident/accident/near misses is a meaningful one. The ICAO distinction has also been referenced in the Foley & Lardner legal brief:

> *ICAO has clearly noted the distinction between what it terms "error reporting" and "hazard reporting", stating that "error reporting is self-incriminatory and may thus lead to blame and punishment, while hazard reporting is objective and neutral.*[25]

The type of data must be considered when designing a collection and reporting strategy. In meeting and discussing data collection with airlines, the team heard repeatedly that air carriers are very willing to report hazards into an airport and, in fact, do so outside of a formal SMS program at Sea-Tac and at many other airports today. But because of liability concerns, there is a significant reluctance among air carriers to share information regarding accidents, incidents, or near misses with airports.

These concerns and issues are not new and have been the focus of much discussion since the inception of airport SMS programs in the United States. What the team further examined, however, was the feasibility of airlines reporting to an airport's SMS in the event that the confidentiality of the data could be maintained. Through our research, the team discovered that even if the data were protected, airlines would be unlikely to report accidents, incidents, and near misses to airports. Airlines are similarly reluctant to report hazards for which the airport will play no role or have no accountability in risk mitigation. Airlines, however, appear to be willing to report hazards for which the airport is responsible for corrective measures.

[25] ICAO Safety Management Manual ("SMM"), 2d ed. (draft), § 2.8.23.

Air carriers have communicated the following reasons (other than confidentiality) for their reluctance to report into an airport's SMS:

1. Duplication of Effort
   Air carriers report safety risk data into their own SMS program. Those that have not voluntarily implemented SMS will soon be required to so. Reporting both into an airline and an airport SMS would create redundancy.

2. Risk Assessment Discrepancies
   Hazards reported into multiple systems would be subject to disparate SRM processes and risk assessments. It is possible that an air carrier and airport would utilize different risk matrices and that the same hazard could be categorized differently, thereby affecting prioritization and planning for mitigation.

3. Ownership and Accountability
   Hazards, accidents, and incidents reported into multiple systems may not have clear lines of ownership and accountability resulting in confusion and inefficiency in mitigation and corrective actions.

For these reasons, the team does not believe that solving the data protection issue will in itself result in airlines sharing all safety-related data with airports. Therefore the strategy must:

- Acknowledge that airline data may not be feasibly protected.
- Consider the simultaneous operation of multiple SMS programs at an airport.
- Clearly define scope, boundaries and processes for airport data collection and reporting.

2.4 Application of Assumption Findings to Assessment

Upon review of the initial core assumptions above, the team believes an assessment and strategy based solely on data protection overlooks current realities faced by airports. Although we agree that maintaining the confidentiality of SMS data would be ideal, it would not resolve all issues related to collecting relevant safety information. And because the most direct path to fully protect SMS data lies in federal legislation that could be years in the making, the team recommends that airports invest resources and efforts in developing a strategy and process that is practical and effective given today's known constraints.

Therefore, the team recommends that the data collection program should be geared toward:

- Collecting the most data possible
- Implementing manual methods to de-identify as necessary
- Encouraging collaboration and discussion
- Assigning clear lines of responsibility and accountability

The data collection approach and functional requirement recommendations outlined in the remainder of this document were developed for Sea-Tac and other Class 1 airports based the following updated set of 4 assumptions:

1. Data will not be protected and, if it is, it is likely that protection will occur after Sea-Tac has begun its SMS and SRM implementation.
2. Selection or development of a risk management application should be based on an assessment of features, functionality, and cost, rather than in-house vs. external hosting.
3. Air carriers will have an operational SMS program.
4. Air carrier participation and contributions to data collection efforts with the airport SMS program will be a largely manual process, requiring focused efforts on collaboration and communication. Collection of important safety data will be a function of culture and relationships rather than a product of protected data and technological functionality.

3. Recommended Approach for Data Collection and Reporting

In order to present a comprehensive approach for SMS data collection and reporting, the team considered both individual airport and national strategies, focused on the manner in which airports can collect the most safety data and how that information may be utilized most effectively for tracking and trending. Our recommendations for each are discussed in detail in the following section and specific functional requirements for an airport SMS application are outlined, in detail, in Section 4.

3.1 Airport Data Collection and Reporting Strategy

The heart of an airport's SMS strategy is not necessarily the technical specifications of the data repository but, rather, in developing a process or methodology by which the most data can be collected given today's operational constraints (data protection and liability concerns, over-allocated resources, and limited time).

Because SMS is founded on proactively identifying safety hazards and mitigating risks to an acceptable level before accidents or incidents occur, the primary focus of an airport's data collection and reporting strategy should be to ***capture every hazard that the airport has responsibility for addressing***. These hazards may be identified by airport personnel, tenants, or even the travelling public.

The ability to perform tracking and trending is also a major component of a successful SMS program. Without information relative to the number of hazards, incidents, accidents and other events on and around the airfield, it is not possible to effectively perform necessary safety assurance functions and quantitatively assess the effectiveness of the SMS. Therefore, the secondary focus of an airport's data collection and reporting strategy should be to ***capture data on as many accidents, incidents, near misses and other events as is possible and, from this, determine root cause and identify additional potential hazards.***

As discussed at length, there are numerous challenges that airports will face when collecting safety information. Given these obstacles and knowing that data is a vital piece of the SMS puzzle, the following strategic approaches are recommended to facilitate the amount and quality of safety data collected by the airport:

<u>Airport Internal</u>

1. Create of an airport hazard, incident, accident, and near miss reporting process that allows anonymous reporting or de-identification of tenant (air carrier, ground service providers [GSP], etc.) data. Ideally, this will include an online portal (see Section 4 for full details regarding recommended specifications), but may also include drop boxes and telephone hotlines, particularly in the short-term during portal development.
2. Continue to collect information on hazards, incidents, accidents or near misses that airports are already identifying during daily operations. These are the same events that airports are currently involved with and, thusly, present no difference from a FOIA perspective than airports currently face.

3. Create a formalized method of conducting investigations, standardized data elements for collection (weather conditions, time of day, location, photographs, measurements, etc.) and implementation of a centralized location for recording and storing the data. In the short-term, this may be as simple as an Excel spreadsheet; see Section 4 for full details regarding requirements for creation of a full database.

Collaboration with Air Carriers

1. Development of relationships with tenants to encourage reporting of hazards, accidents and incidents:
    a. Create (or expand) of an Airport Safety Action Committee (see SMS Roles & Responsibilities document for full details).
    b. Attend individual tenant safety meetings.
    c. Conduct an Airport Safety Fair.
    d. Walk around, introduce, and discuss.
    e. Personally assess and participate when hazards, accidents, or incidents are identified.
    f. Formally rollout and train on airport Safety Policy and/or online portal.

2. Facilitate and encourage collaboration between the airport and tenants. Fostering an atmosphere of cooperation and mutual interest in proactive safety measures for creation of trust and enhanced willingness to share information.
3. Demonstrate the airport's willingness to manually de-identify specific pieces of verbally shared air carrier accident and incident information when recording into the data collection system. Depending on the nature, location, etc. of the event, de-identification may result in complete anonymity for the air carrier, but it may also be feasible to determine the air carrier based on other pieces of information (gate number, time of day, etc.). For this approach to be successful, development of positive relationships and safety culture is critical.
4. Participate in and encourage root cause analysis for hazard identification. In the event that an air carrier or GSP is unwilling to share specific accident or incident information, the airport can assist with or encourage root cause analysis to identify the hazard leading to the event.
5. Provide a consistent and timely response, feedback, and mitigation. Airports must provide tenants with information and, wherever possible, enlist participation from the tenants in the risk assessment and mitigation processes. Tenant involvement will increase if concerns are being addressed and, conversely, will drop significantly if no action is taken, or if communication regarding the action is lacking.
6. Recognize participation in airport safety programs.
7. Create and communicate clear lines of ownership, accountability, and responsibility as related to the airport's Safety Policy, its scope, and its boundaries. In general, the airport's SMS program and, in particular, SRM should focus on hazards for which the airport bears responsibility. The airline SMS program should be focused on hazards for which it bears responsibility.
8. Recognize that some safety issues may not have clear lines of ownership and accountability and collaboration leveraging the Airport Safety Action Committee to determine responsibility for mitigation, where necessary. Because air carriers will have independent SMS programs, they may receive reports that fall outside of their SMS scope. Likewise, airports may receive reports that fall within the

boundaries of an airline's SMS program. Due to the fluid and changing nature of airports and air carrier operations, it is unlikely that a perfectly clear line of demarcation will ever exist between an airport and airline SMS. Therefore, the ability to communicate and collaborate where gray areas are identified will be vital to the success of both programs.

3.2 National Safety Management System Reporting Strategy

As discussed in Section 2, it is unlikely that airport SMS programs will soon be in a position to collect all relevant safety data from air carriers and other tenants that operate in/on the facility (even in the event that it becomes protected from public disclosure). Even were airports in a position to collect all pertinent data, housing it in an airport-centric repository would allow for reporting only on the specific facility, its safety metrics, and its trends. An airport would not have the benefit of access to other local, regional, or system-wide SMS data for use in identifying large-scale trends, safety issues, or improvements.

In order to provide such system-wide safety information, the team recommends implementation of a national data repository to collect and report on SMS data. In this model, both airports and air carriers would maintain disparate SMS data collection and reporting systems. Data from the individual repositories would be interfaced and uploaded to a shared platform from which reports could be produced at a local, regional, and national level. In lieu of individual airports identifying and implementing methods to provide data protection for air carriers (which would need to comply with local, state, and federal laws), air carrier data would be either de-identified or protected (or both) in a single, federally-managed location. It is assumed that airport data, as we have already discussed, would be available for public disclosure as it is today.

A national-level discussion and program development, called Aviation Safety Information Analysis and Sharing (ASIAS), is currently in process, under the direction of the Joint Planning and Development Office (JPDO), and white papers (specifically 08-007 and 08-008) have been reviewed and referenced in light of national (and potentially international) standards. These documents set out an agenda, goals, and information that is well-considered and establishes the beginning of the dialogue and development of a national approach to safety management and – in particular – reporting. They identify pertinent issues and challenges, recognize the barriers to adoption and participation, and have presented, in the opinion of the team, a good start.

Given the early stage of this effort, the ASIAS and JPDO papers do not yet present technical standards for the systems, nor do they identify the information to be gathered, though they recognize the goals that must drive these standards (data format, interoperability and data exchange, for example). The JPDO documents specifically identify the challenges here, given that

> "…*various agencies with aviation operations or regulatory roles have disparate policies, rules, standards, taxonomies, architectures, and systems to analyze safety information, assess findings, and create corrective actions."*[1]

[1] JPDO Paper 08-008, p. 1

Because SMS-specific data collection and reporting do not currently exist within the ASIAS platform, this would need to be developed in partnership with airports and air carriers during SMS implementation. The team has developed and presents in this document, high-level functional requirements and data elements that we hope may contribute to an understanding of airport data collection needs and a foundation on which to begin building a national SMS data warehouse. Figure 1 below illustrates the team's recommended data collection and reporting path, based on an extension of and integration with the existing ASIAS warehouse and reporting platform.

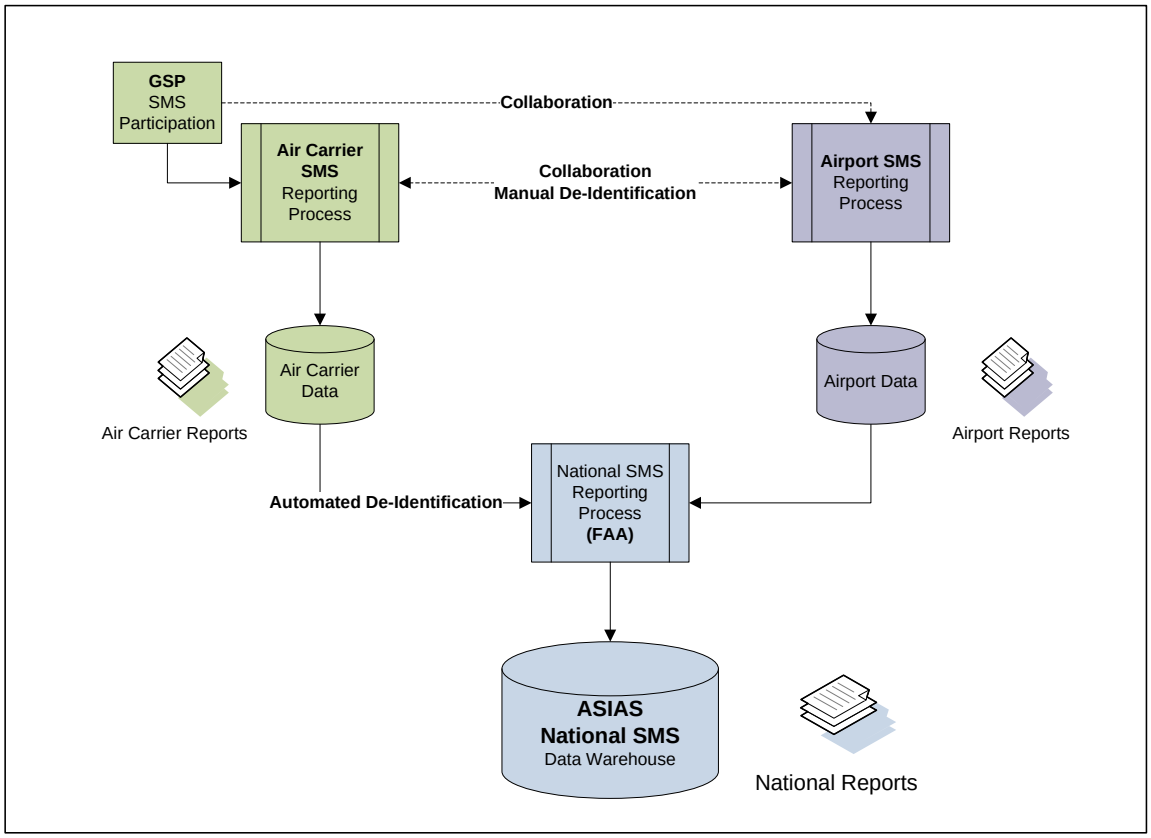

Figure 1 - Recommended National Data Collection and Reporting Path

4. SMS Data Collection Functional Requirements

4.1 Overview

Of critical importance in the discussion of systems and technology at Sea-Tac is an understanding of the balance between defining and developing or otherwise acquiring a tool that meets the needs of the airport in the near-term with the development of a national tool, as introduced in Section 3. While the focus in this document is on Sea-Tac, the eventual existence of a national reporting system with a data repository cannot be ignored. In fact, it raises three valid options in terms of the local program:

1. Develop or acquire a system or tool that is specific to Sea-Tac, but provides a coordinated interface to the eventual national standard. This implies some informed guesswork on the part of the system design or configuration, and requires a heavy focus on documented standards for data exchange. Of less certainty are the details of the information taxonomy to be used, meaning that some conversion, data transformation, or future modification is likely. ***This is the recommended approach.***
2. Develop or acquire a system independent of national standards, and accept that it will either require modification or wholesale replacement at some point in the future. This approach is not recommended for operational or financial reasons.
3. Delay any development or acquisition of a SMS system until such time as the national standard is finalized, and then deploy a commercial or federally-procured solution. This approach, while valid at several levels, does not address the need or desire to proceed with a system development or acquisition, and is not considered in this document.

The primary focus of SMS data collection is SRM. Likewise, this document primarily considers functional requirements for collecting and reporting on SRM data elements, referred to as the “Risk Database” throughout this document. However, the team recognizes that, just as SRM does not in itself constitute a Safety Management System, the Risk Database does not represent the entirety of a comprehensive SMS data collection strategy. Functional requirements, therefore, have been broken into a detailed discussion of SRM followed by a high-level discussion of additional SMS data collection, systems, and reporting considerations.

4.2 Risk Database Functional Requirements

The Sea-Tac SRM system, referred to as the "Risk Database," is in fact a larger, more comprehensive tool than the general name implies. It requires a database system, but several more elements are necessary to implement it successfully. These additional items include:

- A reporting system and structure that includes both manual and automatic data entry.
- A system and structure that allow for the warehousing of data from multiple reporting systems and/or sources.
- Firewalls and protective software to prevent unauthorized access, use, or tainting of data.
- Redundant servers, supporting the storing and archiving of data, the generation of reports and trends, and numerous tools and sub-elements (such as standard operating procedures, policies and guidelines).
- Software tools to provide reports, trending, analysis, and notification or publishing of reports, notices, and data to individuals or other systems.
- The ability, in the future, to interface with a national, centralized database or repository. The ability to export data (using standard methods such as flat files, XML, etc.) may not be required for the initial implementation, but the system should not be developed in any way that would preclude this type of interface, pending the definition of standardized national reporting requirements, procedures and systems configuration.

Bearing the preceding information and discussion in mind, the base assumptions driving the Risk Database development for Sea-Tac include:

- The solution(s) described herein shall be specific to Sea-Tac.
- The development will take into account and allow for a generic case that can be customized and adapted to other airports or transportation facilities and modes, and can interface with a national system, as required by the JPDO – see paper 08-007.
- The solution(s) shall, to the greatest extent possible, rely on commercial, off-the-shelf (COTS) software and components that may be provided by more than one vendor and support a non-proprietary solution.
- The solution(s) may be of a custom nature, using COTS products, to deliver the required product.
- The solution shall be flexible, to allow for changing requirements, situations, and scenarios, such that it may be modified, updated, and augmented to suit the Safety Management environment.
- The solution must be able to store, cross-reference and retrieve multiple data types, including photographs, maps, video files, audio files, spreadsheets, forms, and other file types as needed.
- The solution shall be consistent with Sea-Tac's infrastructure, architecture, data retention, quality control and quality assurance policies.

By far the most significant effort and expense related to the Risk Database will be in the software development and tools, particularly adapting the system to meet specific needs. Based on JPDO and other recommendations, as well as the specific issues identified by this team, the general, basic requirements are discussed in the following sections.

4.2.1 General Requirements

- Windows-based operating system (OS)
- SQL Server-based product
- Primary database for active and on-going work
- Archive database for closed and archived/inactive items

4.2.2 Reporting Portal

The system must have a reporting portal that allows for multiple means of reporting hazards and risks. The set of inputs may include telephone calls, email, written documents and reports, verbally delivered items, and electronically generated hazards. Essentially, all of these can be broken down into one of two categories of input:

1. Manual Entry

   Manual entry cases include any event or report that would require the data to be entered into the Risk Database manually, by a system operator. This includes telephone calls, email, written documents, etc. At this time, the expectation is that the majority of the reports will be handled this way, using the Airport Communication Center (ACC) as the focal point for data collection.

2. Remote Entry (Web-based)

   Automatic entry of data would be provided through a web-based portal, in which a reporting form is made available to the remote user to populate information. The system should allow for users outside the Owner's domain/firewall to access the tool and make reports.

4.2.3 Hardware

The exact hardware required cannot be specified at this time, pending the further definition of the system. In general, the following components define the general hardware requirements:

- Primary Server

  This is the dedicated server used as the primary operating system to run the Risk Database and supporting tools. It may include a built-in storage system, or make use of a separate file storage area, within the security requirements for the system.

- Redundant Server

  A secondary server, located remotely from the Primary Server is required for data integrity and continuity of operations in the event of a failure or outage of the Primary Server.

- Web-Server

  Unless there are specific objections or operational issues preventing the use of existing airport web portals, the web server will utilize existing systems and services.

- User Consoles

  User consoles for data entry and other functions are assumed to exist within the Sea-Tac systems. The primary issue associated with them will be ensuring the proper software installation, configuration, and security, and adequate system capacity to handle the work load.

- Supporting Infrastructure

  This will include connectivity of the Risk Database to the hardware and Internet, presumably using the existing Sea-Tac Network, on a virtual private network (VPN) for greater security and control.

Regarding the servers and hosting arrangements for the system, one option is to establish a hosting arrangement with a third party for all data. Alternately, one of the servers – preferably the primary – may be located on-site or within the Airport's facilities, and a secondary mirrored server may be located off-site or hosted by a third party to serve as a back-up system.

This approach, to use an outside organization and/or to locate the servers at some location other than Airport facilities, is reflected in the JPDO's thinking regarding a repository integrator; however, that is clearly a requirement in a nationally integrated data warehouse, and not necessarily the best solution in a local, airport-specific solution.

Relative to this last item, the JPDO has defined the role of Repository Integrator[2] as follows:

- Advocate for the updating, expanding, and/or normalizing of data standards, event classification system, and data dictionaries as needed to permit the sharing of safety-relevant information.
- Integrate safety information from multiple, disparate, decentralized sources[3].
- Continuously improve ASIAS tools, methods, and processes.
- Manage role-based access to aviation safety information.
- Develop and maintain standard operating procedures including data management, quality, security, strategy, and access plans.

[2] At this time Mitre has been identified as the organization serving this function.
[3] While the JPDO clearly recognizes the need to work with many disparate organizations, we do not believe the intent of this statement was to require the Repository Integrator to manipulate disparate data, only to work with the different contributing agencies to effectively communicate the data.

Remote hosting provides many benefits to information technology (IT) systems, including the security of data storage away from the primary business premises, and the reduced capital investment by avoiding the development of space, systems, and infrastructure, and the recurring maintenance costs. Also, if the hosting company is a party specializing or possessing expert knowledge of SMS software, there can be a reduction in maintenance and administrative costs.

The determination of the best hosting environment needs to take into account several issues, and should be addressed directly with Sea-Tac:

- The choice of software selected.
- The capability of Sea-Tac to provide space and staff to support one or more servers within suitable IT space with access to the airport's network.
- Sea-Tac's general policy and approach to internal systems versus hosted systems.

Initially, the team views the existing Repository Integrator to be focused on a national solution. Should a national reporting solution be pursued, it is likely that Sea-Tac IT personnel and/or any vendors with whom Sea-Tac partners for the Risk Database, will work directly with the Repository Integrator on integration standards, protocols, and testing.

4.2.4 Security Functions

- Firewall: Any remote, indirect access to the system (i.e., web-based or remote access) must be run through a firewall to protect the system from unauthorized and malicious access attempts.
- Security Rights Access Control: The system must be equipped with a multi-layer security access program, including:
    - Security access for general administrative rights and functions
    - Security access based on the type of files and rights to files (read, write, read-write, etc)
    - Security access to bar access to certain files (e.g., names and information of persons and organizations making reports, etc.)

4.2.5 Tools

The following represent a general set of tools needed for input of and analysis of data into and within the Risk Database, based on the approach developed for Sea-Tac.

<u>Data Input Tools</u>

- Hazard Report (Initial and Updated)
- Root Cause Analysis Report
- Risk Assessment and Reporting Standards, Definitions, Terminology
- Hazard Criteria Definitions
- Prioritization Protocols
- Risk Matrix
- Risk Tolerance Guidelines

- Airport Risk Responsibilities
- Non-airport Risk Definitions
- Airport Standard Operating Procedures, Policies, and Guidelines, including:
    - Safety policies
    - Safety objectives
    - SMS requirements
    - Safety procedures and processes
    - Responsibilities and authorities for safety procedures and processes
    - Interaction/interfaces between safety procedures and processes

Data Analysis Tools

- GIS Interface (for tracking locations and tendencies for risks in specific locations)
- Trending and Analysis Tools
- Risk Event Status Tool
- Risk Assessment Tools
- Audit Tools
    - Self-audit functions
    - External audit functions
    - Auditing
    - Follow-up
    - Flagging of over-due or unresolved items, actions, or elements
- Notification Tools (Automatic and Manual, preferably using a standard email tool):
    - Initial Report
    - Report Status
    - Report Closed
    - Open item past shelf date
    - Follow-up to originator
- Custom Reports/Custom Query Tool(s)

4.2.6 Archiving Tools

- The System must have archiving and retrieval tools. In support of this, Sea-Tac or Ruling Regulatory Entity:
    - Must establish an archiving period, and a policy regarding on-line “live” archives and stored (CD, tape, other) archives. As a reference, the FAA requires Part 139 inspection records to be stored for a period of one year, and Sea-Tac requires a two-year retention. ICAO requires five years generally, but stores accident information indefinitely. Because safety trending and accident details are important and useful, a longer retention period (five years minimum) is recommended.
    - Must establish an archiving protocol.

4.3 Commercial Solutions vs. Custom Solution

Several different commercial products have been identified as potential SRM solutions. Some of these products have been reviewed by other parties, and the results of those reviews have been considered, allowing for a different set of review criteria unique to the parties involved. The review conducted herein is general, based on the goals and guidelines defined in this document, rather than vendor-specific or product-specific.

The nature of the offerings is highly diverse. Some of them are SMS- and risk management-specific solutions focused on an aviation environment (though not exclusively on Part 139 airports), and others are modifications to or augmentations of maintenance and asset management tools. The organizations that offer these tools tend to fall into one of two categories of providers: small, niche (SMS- and aviation-specific) product suppliers, or larger companies with a more generalized product focusing on asset and risk management, with SMS being an add-on or enhancement of a known product. In the latter case, these add-ons are typically related to tools common in large airport environments (such as Maximo), which is a benefit due to a familiarity with the software and an installed base system.

As with the vendors, the types of systems available at this time cover a range of approaches and solutions, using different models and software and database tools as their foundations. The variables encountered include:

- Different hosting environments (local, remote/web-hosted, and remote)
- Different database solutions (Access, SQL, etc.)
- Different levels of customer customization
- Different target markets and focus (safety management versus risk/hazard management
- Regulatory focus (OSHA versus FAA/JPDO)

While many of these products appear to be well-positioned to support an SMS program, the very nature of the regulatory environment does not allow for there to be a clear, favored best solution. Further, it is far more likely that multiple products and approaches will be suitable to varying degrees of success, and choices will need to be balanced against cost, existing systems, airport size, procurement policies, and the operations and functions of the safety organization.

Given the varied nature of the offerings and the unsettled requirements for airport safety management, as well as the on-going development by the JPDO of guides and standards, a best solution cannot be defined at this time. The fundamental choices are to:

1. Develop a custom solution.
2. Purchase and customize a commercial product.
3. Wait for further development and refinement of the SMS software requirements and re-examine the options at a later date in a more mature product environment.

In all three cases, a careful and thorough examination of the available options and products, including presentations, specific requirements definition, and examination of the solution in both the context of Sea-Tac and the FAA/JPDO guidelines needs to be completed. This also needs to take into account existing software available either at Sea-Tac or from the FAA, and to allow for the specific operational approach used at Sea-Tac for safety management.

4.4 Data Elements

The following table lists recommended data elements for consideration and inclusion in the development of any SMS program. This list is by no means comprehensive, nor does it define elements in the sense of identifiers, format, or any of the other criteria associated with the specific and detailed development of a database. Instead, this list is intended to define the required information, in general categories and specific cases, explained in layperson's terms.

Element	Usage	Comments
General Information		
• Event Identifier	Unique event identification	Used to track, trace, and identify an event and for cross-referencing to other events
• Report Date	Initial Report Creation	
• Report Time	Initial Report Creation	
Reporting Party		
• Person/Organization	Used for follow-up or interviews for further information	Provide for option of anonymity
• Contact Information	Used for follow-up or interviews for further information	Include telephone number(s) and email
Reporting Method		
	Web, Email, Telephone, Verbal, Written	Allows for evaluation of the reporting methodologies
Event Details		
Event Type		Tracks type of event that has been identified: Hazard Incident Accident Near Miss
Event Date(s)		Allow for reporting of multiple occurrences of an event
Event Time(s)		
Type of Incident		Based on Standard Definitions
Classification of Incident	Incident, accident, safety issue, hazards, other	Based on Standard Definitions; would include sub-categories.
• Incident Type		
• Accident Type		
• Hazard Type		
• Safety Issue Type		
Person(s) Involved		
• Contact Information		Include contact and organization as appropriate
Witness(es)		
• Contact Information		
Location of Event	To define the specific location	Define specific location event

	within the airport, including GIS location if applicable.	occurred, including any details such as elevators, escalators, drive lanes, jet bridges, etc.
Equipment Involved		Include any and all items involved, including fixed machinery, lifts, elevators, etc.
• Vehicle		
• Aircraft		
• Tools and/or Machinery		
• Other		
Conditions		
• Weather		Describe physical conditions (sun, rain, snow, ice, etc.)
• Visibility		Such as fog, mist, heavy rain, heavy snow
• Surface Conditions		
Risk Assessment		
• Severity		
• Likelihood		
• Classification		Based on risk matrix
• Requires mitigation?		Y/N
Damage Assessment		
• Nature and Extent of Damage		
• Value/Cost of Damage		
• Assessment by:		
• Contact Information:		
Injury Assessment		Provide information on degree of injury, medical response, fatalities
• Nature and Extent of Injury		
• Financial Costs Associated with Injury		
• Medical Evaluation by:		
• Contact Information:		
• Hospital transport required?		Y/N
Investigation		
• Assigned Person/Organization		
• Contact Information		
• Issue Owner	Sea-Tac, tenant, or other	Determine if the event is the responsibility of Sea-Tac, or needs to be forwarded to another party for response.
• Main Behavior, Root Cause or Condition		
• Contributing Factors		

• Recurring/Repeated Incident		Links to Related Events/Occurrences
• Incident Priority		
• Relevant Policy Item		
Related Events/Occurrences		
Corrective Action(s)		
• Type of Action Taken/Required		
• Owner of Corrective Action		
• Mitigation/Corrective Action Plan Approval Date/Authority		Allows upload of mitigation/corrective action plan
• Amendments to Safety Policies		
• Amendments to Safety Procedures		
• Notification		
• Work Order Number		
Audit/Follow-Up		
• Auditing Person/Organization		
• Contact Information		
• Audit Date(s)		
• Reporting Person Contacted		If applicable
Spot Check of Condition		
• Person Performing Check		
• Contact Information		
• Date of Check		
• Status of Check		

Table 1 - Recommended Risk Database Data Elements

4.5 Taxonomies

One of the key elements mentioned both in this document and in other, related discussions is the matter of a common taxonomy. For this discussion, taxonomy is defined as a pre-defined classification of key words, terminologies, acronyms, and the agreed-upon and understood definition of each of these terms.

A common taxonomy is required as it forms the base language from which the communications about a particular area, industry, activity, or event draws its terminology. In an international industry such as aviation, where there are national and international standards and ruling organizations involved, it is necessary to have a clear and understood set of terms from which to work.

Further, with the growth in international travel and the number of persons who are not native English speakers and are involved in using a reporting system, the risk of a mis-use of or mis-understanding of a term increases. By contrast, a defined set of terms reduces the risks associated with this condition dramatically.

The value of this approach has been shown repeatedly in the aviation industry as well as in other industries and organizations.

The benefits of a common taxonomy are apparent:

- Improved quality of communication between parties (human-based communication)
- Improved data sharing between information systems (machine-based communication)
- Improved data analysis

In 1997, government and industry came together to establish the Commercial Aviation Safety Team (CAST), with the intent to reduce accidents and improve aviation safety world-wide. CAST determined that a necessary part of their activities was the analysis of data, directing this at accidents and known safety risks, and at emerging risks.

This focus has led to the understanding that a common taxonomy for safety was necessary to gain the maximum value from the information available. In 1999, ICAO and CAST formed the CAST/ICAO Common Taxonomy Team (CICTT).

Examples of the formalization of taxonomies exist throughout the safety community, and to a lesser extent in the aviation industry both in the government/regulatory and the private/operator sub-groups. CICTT has published four primary and one secondary common taxonomy to date, including:

- Aircraft Make/Model/Series
- Engine Make/Model
- Phases of Flight
- Occurrence Categories
- Engine Occurrence Sub-category

Similarly, the Federal Aviation Administration and the JPDO understand the importance of a commonly understood taxonomy, and have addressed elements of the process through the development of IMEX, which by its very nature will require a common terminology or means to baseline different terms and taxonomies to a common base.

Another example of efforts undertaken in this area includes the program undertaken by the airline industry and FAA as the Voluntary Aviation Safety Information-sharing Process (VASIP). Funded by NASA and the FAA, the University of Texas was asked to study, develop, and demonstrate a Distributed National ASAP Archive (ASAP meaning the Aviations Safety Action Program), as a means of supporting the sharing of safety information at a national level. The study considered hardware, software, infrastructure, and other elements.

An initial set of published documents, available at the University of Texas website[4], show considerable thought and definition placed on the requirements for the common fields as required by a national database; however, as with much of the effort reviewed to date, the emphasis continues to be on flight operations, with little attention to airports. The primary exception to this is a set of fields contained in the data set called *DNAA Contributing Factors: External Issues List*. Within this section are three sets of fields, identified as *Airport Condition, Adverse Weather Conditions/Environmental,* and *Security Issue or Concern.*

These three subsets contain data elements that represent a starting point for an airfield-centric taxonomy, and have been developed with the intent of a national approach, rather than a local or airport-specific solution.

Some examples of the fields defined within the DNAA subsets include:

Airport Conditions		Complications resulting from airport conditions
8.1	Inaccurate/confusing airport diagram	Complications due to inaccurate or confusing airport diagrams
8.2	Ground/Satellite malfunction	Complications due to ground or satellite malfunctions
8.7	Buildings/structures	Complications due to buildings or structures at or surrounding an airport
8.8	Surfaces conditions/contamination	Complications due to airport runway, taxiway or ramp surface conditions or contamination
8.9	Special airport procedures	Complications due to special airport procedures
8.11	Construction	Complications due to construction at airport site

[4]http://homepage.psy.utexas.edu/homepage/group/HelmreichLAB/DNAA%20folder/Aviation/web-content/Welcome.html

8.12	Other Airport Conditions	Any other complications with an airports conditions, facilities, surrounding area or procedures
Adverse weather Conditions/Environmental issue		Complications due to adverse weather conditions or environmental issues
10.1	Temperature related issue	Complications due to temperature related issues or concerns
10.2	Ceiling/overcast	Complications due to the presence of overcast or clouding sky conditions
10.5	Visibility restrictions/Fog	Complications due to the presence of fog or other visibility restrictions
10.6	Precipitation related issue	Complications due to the precipitation related issues
10.7	Frontal storm passage	Complications due to the presence of a frontal storm or passage through a frontal storm
10.8	Icing	Complications due to the presence of ice on the aircraft or airport surfaces
10.10	Thunderstorms	Complications due to the presence of a thunderstorm
10.12	Other Adverse weather Conditions/Environmental issue	Any other complications due to adverse weather conditions or environmental issues
Security issue or concern		
12.2	Suspected unauthorized object aboard aircraft	Complications involving a security concern due to a suspected unauthorized object aboard the aircraft
12.3	Passenger misconduct	Complications involving a security concern due to a passenger's misconduct aboard the aircraft
12.4	Security concern in terminal/TSA	Complications involving a security concern in the terminal or involving TSA
12.5	Security concern on ramp	Complications involving a security concern on the ramp
12.6	Other Security Concern	Any other complications involving a security concern or issue

Table 2 - Recommended Initial Risk Database Taxonomy

To date, all of these developments have tended to focus on aircraft and flight operations. None of the CICTT Categories is specific to airports, though a review of the Occurrence Category documents does reveal some preliminary recognition of the issues and elements related to airport safety, specifically those related to security and to aerodrome. The DNAA program, like CICTT, has developed a good process and has made a start which cannot and should not be ignored.

(It should be noted that the DNAA has been accepted and approved by the ASIAS Executive Board as the ASAP element of the ASIAS program. The DNAA should be reviewed by the CICTT as a potential starting place for their taxonomy.)

For purposes of the discussion and development of SMS specifically emphasizing airport safety, three primary steps must be undertaken:

1. Develop a taxonomy that is appropriate to the airport safety and risk environment.
2. Coordinate the taxonomy to support, at minimum, a national approach, and preferably an international approach.
3. Coordinate the taxonomy with others in use for related aviation activities and systems to avoid conflicts and confusion, and to support the ultimate capacity of integrating terminology and taxonomy from the local airport operation to national and international systems.

In support of these three steps, an active process of identification of parallel and/or complimentary efforts, such as CICTT and DNAA must be undertaken in order to eliminate duplication of effort and to coordinate with programs that can contribute to and support the taxonomy definition and development.

4.6 Safety Management System High Level Requirements

SRM, though critical to SMS, is merely one of four elements that comprise a comprehensive SMS. In order to truly gauge the ongoing effectiveness of the program in its entirety, attention must be also paid to the remaining 3 elements:

- Safety Policy
- Safety Promotion
- Safety Assurance

Performing tracking and trending on these elements, particularly as they relate to the trajectory of hazards and risk mitigation effectiveness, will likely require airports to either integrate multiple, disparate systems for a comprehensive SMS reporting warehouse, or necessitate an additional level of manual analysis to determine the impact of each element on the others (or a little of both). For example, an airport may identify a correlation between increased foreign object debris/damage (FOD) promotional activities and decreased FOD discrepancies, but only if this information is available for tracking and review.

The following is a high-level summary of tracking and data collection considerations for airports with regard to the remaining 3 SMS elements.

4.6.1 Safety Policy

At a minimum, an airport's Safety Policy should be closely managed, available internally to airport employees, and made available for public and tenant review. In light of this, an airport should consider implementing and/or utilizing the following types of solutions:

- Document Management
  A document management system can assist the airport with versioning, approvals, managing permission and access parameters, revision history, and archiving past and related policy documents. If the airport does not implement a specific document management application or while an implementation is forthcoming, the Safety Policy and correlating documents can be managed using a standard file structure. In this instance, the airport should create policies and procedures for naming conventions, version control and tracking revision history (can be performed by notations within the document itself) and applying security directly to the document to ensure only appropriate personnel can make updates.

- Public Website
  Airports should ensure that their Safety Policy is posted, either in document or as online content, on their publically-available website. The policy should be posted on the website in a format that enables updates to be made quickly and efficiently, without requiring development effort. The best method for posting and updating the Safety Policy will depend on the infrastructure and architecture on which the airport's existing website is built but care should be taken that the process by which the policy is updated does not prevent or constrain the release or availability of the most current version. The Safety Policy should also be indexed so that it can be located in a search.

- Internal Availability
  Like with the public website, airports should ensure that the Safety Policy is easily accessible to its internal community and personnel. If the airport does have a document management system in place, this can be leveraged and personnel can access the document where it resides. For airports with an Intranet (similar to the public website approach above), the Safety Policy should be posted in a format where it is easy to locate and easy to maintain.

4.6.2 Safety Promotion

- Learning Management System
  Airports will need to track training in order to ensure that all SMS training and orientation is completed (both for tenants and airport personnel). In addition to recording initial completion, tracking of recurrence requirements, course scheduling and offerings, and overdue training should be performed by the airport. Due to the number of airport employees that will require SMS training and the potential complexity of initial and recurrent training requirements, it is highly recommended that airports implement a true learning management system or, at a minimum, a database that can store course completion, training requirements, due dates, and produce reports on upcoming and overdue training.

- Participation
  A major factor in the success of SMS is safety culture. One of the primary mechanisms for promoting and fostering a positive safety culture will be an Airport Safety Action Committee which should include at a minimum members of the airport, air carrier, and GSP communities. Airports will likely conduct other events as well, including safety fairs, FOD walks, etc. In order to track attendance and participation from the greater airport community, attendance should be taken at all events and recorded into a database, spreadsheet or other similar application.

- Promotional Campaigns
  To ascertain the effectiveness of and response to SMS promotional campaigns, the airport should track, at a minimum, start and end dates, campaign mission and goals and target audience in a spreadsheet or database. This will assist the airport in determining campaign success and in planning for future promotional activities.

4.6.3 Safety Assurance

Safety Assurance consists of both quality control (QC) and quality assurance (QA). This document does not aim to provide a detailed discussion of the differences and goals between QC and QA programs but the reader should consider the differentiation at a high level as it applies to data collection and systems. Quality control provides an airport with the mechanisms and processes to monitor and track the results of specifically targeted quality activities such as ramp safety or FOD inspections. Quality assurance utilizes data obtained from quality control activities to measure the larger effectiveness of such programs, and the effectiveness of SMS as a whole.

In the context of SMS, safety assurance and SRM should work hand-in-hand and to maximize the benefits of a quality program, airports should consider the following applications and data tracking measures:

Quality Control

- Inspection Results
  Inspections are an integral component of the Safety Assurance element and airports will likely develop a set of safety inspections specific to SMS during implementation. In order to track progress, identify trends, and potentially take corrective actions, the airport should develop a mechanism for tracking inspection results. This could take the form of an online checklist, assigning and recording qualitative scores and/or other assessment measurements, or merely tracking safety infractions/discrepancies. The specific solution, however, should not present an undue administrative burden, must be easy to use and easy to understand. If the application is time consuming or confusing, it is likely that inspection results will not be recorded, thereby diminishing the effort and minimizing their effectiveness.

- Integration of Inspection Results with Risk Database
  It is highly likely that inspections will often (though not always) result in the identification of a hazard. Therefore, it may be desirable to integrate (either automatically or via a manual process) inspection results with the airport's Risk Database. The most efficient solution would allow airport users to enter inspection results and indicate whether a discrepancy should be further treated as a hazard in the SRM process. If integrating or automating this process is not feasible, the airport should have a process in place that provides for secondary action to be taken on inspection results. Secondary actions may include creation of a new hazard in the risk database, follow-up communication with a tenant on their results, citation, updating minimum standards, etc.

Quality Assurance

- SMS Audit
  Upon implementing minimum standards, airports will need to perform regular audits to verify that tenants are meeting the standards as required. The manner in which airports perform the audit may differ substantially but airports should consider recording the results of the audit in a standardized database or format so that they can be tracked independently (last audit performed, next audit due, results, discrepancies, follow-up action, etc.), and also cross-referenced with other safety –related data.

- Claims Data Tracking
  One of the presumed benefits of an effective SMS program is a reduction in claims and, ultimately, a correlation in reduced insurance premiums. In order to monitor this, the airport should implement or utilize existing reports for claims filed. It is recommended that the airport develop a baseline of reported, airfield-centered claims prior to or at the beginning of implementation and correlate the number of claims to the rollout of specific SMS programs, including SRM, safety assurance and training. The integration of claims data with other safety data and the development of reporting requirements may be complex initially. An airport may be better served to track the correlation manually for a period of time until specific requirements for tracking and trending are more fully understood.

- Maintenance and Corrective Action Tracking
  Although ensuring that corrective action is completed and any mitigated risk is monitored will be handled via an airport's SRM program, maintenance and corrective action orders should be examined periodically to determine how effectively and efficiently actions are being taken and completed. Airports may choose to use an existing maintenance/work order application for SMS-related activities, if so, specific SMS data elements or categorization should be included. This will enable an airport to run reports on the number of SMS-related orders, average time to completion, cost metrics, general type of action, human resource impacts, and skilled labor required for mitigation.

- SMS Integrated Reporting Suggestions
  Quality assurance focuses on measuring the effectiveness of programs as a whole. In order to examine larger trends and correlate these to the success of programs and activities, airports may consider the creation of reports that pull data from disparate repositories. Depending on the airport's infrastructure and whether they have created a SMS data warehouse, this can be automated or performed manually. Some example reports for use in quality assurance may be:

    - Completed SMS orientation to inspection discrepancies by tenant or operator
    - Number/frequency of completed SMS inspections, by inspector, date range or location
    - Number and types of hazards identified by tenant, by location, by condition, by time, etc, cross-reference with audit/compliance status
    - Number/percentage of claims vs. number/percentage of hazard reports (in general, by tenant, by location)
    - Correlate results of minimum standards audit to known accidents, incidents and near misses
    - Measure participation in safety activities against inspection discrepancies and/or results of minimum standards audits.

5. Summary of Findings

As became quickly evident during the team's assessment, the selection and implementation of SMS and SRM data collection and reporting systems is not quite as straightforward as initially thought. However, the team believes that by developing an approach that is grounded in today's realities, that accepts rather than ignores current constraints, and that is founded upon collaboration and communication, airports can create effective and efficient programs that will improve the level of safety at their location and system-wide.

Below are the team's key findings:

1. The initial assessment approach was based on 3 key assumptions that, upon further review, the team believes are not wholly valid. Notably, the team does not agree that SMS and SRM data must be protected against FOIA requests, that a third party hosted solution will provide such protection, or that (even in the event data could be protected), air carriers will report directly into an airport solution.

2. Focusing purely on identifying and implementing SRM and other SMS data collection applications based on an assumption of data protection largely misses the mark where functional requirements are concerned. This should not be the single most important component when evaluating such systems.

3. Airports already collect much, if not all, of the data and information that would be recorded for an SRM and SMS program and, therefore, are not unduly or in any larger sense, more subject to FOIA and public disclosure ramifications than in today's environment.

4. There is no existing evidence that failure to protect airport SRM and SMS data will result in greater airport liability than airport's currently face today. Likewise, there is no evidence that a rigorous SRM and/or SMS will offer protection from the potential of increased liability. Until SMS has been operational for several years, it is extremely unlikely that this debate will be resolved.

5. The most effective mechanism for offering data protection would be through federal legislation, but this is unlikely to occur in the near-term and, as such, should not be considered a prerequisite for SRM or SMS implementation.

6. Regardless of an airport's ability to protect data, air carriers are extremely unlikely to formally report into an airport's SMS.

7. In order to collect and track a more substantive volume of SRM data, airports must find ways to collaborate with air carriers. There are mechanisms by which an airport can develop and enhance communication and collaboration and ultimately collect more safety data. However, this will require a substantial effort on the part of the airport. This is not a challenge that can be met simply with the "silver bullet" of data protection.

8. It is inefficient and cumbersome to rely on over 500 individual commercial airports to resolve data protection issues on behalf of air carriers. Rather, for true tracking and trending on a local, regional, and national level, data from airports and air carriers should be interfaced with a single national reporting platform, ASIAS, which could provide a single point for de-identifying proprietary air carrier data and produce system-wide tracking and trending information.