January 2013

AIRPORT COOPERATIVE RESEARCH PROGRAM
Sponsored by the Federal Aviation Administration

Responsible Senior Program Officer: Marci A. Greenberger

Legal Research Digest 19

LEGAL ISSUES RELATED TO DEVELOPING SAFETY MANAGEMENT SYSTEMS AND SAFETY RISK MANAGEMENT AT U.S. AIRPORTS

This report was prepared under ACRP Project 11-01, "Legal Aspects of Airport Programs," for which the Transportation Research Board (TRB) is the agency coordinating the research. The report was prepared by David Y. Bannard, Foley and Lardner LLP, the principal investigator.

Background

There are over 4,000 airports in the country and most of these airports are owned by governments. A 2003 survey conducted by Airports Council International–North America concluded that city ownership accounts for 38 percent, followed by regional airports at 25 percent, single county at 17 percent, and multi-jurisdictional at 9 percent. Primary legal services to these airports are, in most cases, provided by municipal, county, and state attorneys.

Reports and summaries produced by the Airport Continuing Legal Studies Project and published as ACRP Legal Research Digests are developed to assist these attorneys seeking to deal with the myriad of legal problems encountered during airport development and operations. Such substantive areas as eminent domain, environmental concerns, leasing, contracting, security, insurance, civil rights, and tort liability present cutting-edge legal issues where research is useful and indeed needed. Airport legal research, when conducted through the TRB's legal studies process, either collects primary data that usually are not available elsewhere or performs analysis of existing literature.

Applications

Safety Management System (SMS) has been defined as a systematic approach to managing safety not only by proactively conducting safety assessments before there is an incident or accident, but also by having the necessary policies, procedures, organization structure, and accountabilities in place. SMS has four key elements: 1) Safety Policy, which defines the methods and tools for achieving safety goals, including management accountability for such goals; 2) Safety Risk Management (SRM), which requires a proactive approach to identifying risks, quantitatively and qualitatively categorizing risks, and establishing mitigation for identified risks; 3) Safety Assurance, which includes a method for establishing processes to monitor an organization's performance in identifying risks and establishing preventive or corrective actions to maintain safety; and 4) Safety Promotion, which involves the establishment of procedures and processes that change the safety culture and environment, including the establishment of confidential reporting systems, to encourage employee reporting and feedback as well as employee training.

The identification of risks and the creation of such records could increase airports' liability as entities subject to their individual state sunshine laws. The result could be less data obtained as confidentiality of data is crucial to those reporting information. Since SMS has been in effect at airports around the world, experiences from Europe, Canada, and Australia are discussed. SMS has been implemented in other industries in the United States, including the maritime, oil, and gas industries, as well as in the area of patient safety. These are examined in the context of U.S. airport implementation.

While this digest does not evaluate the FAA's Notice of Proposed Rulemaking, it does provide an evaluation of SMS and the issues that airport operators must consider and address when establishing SMS.

CONTENTS

I. Introduction, 3

II. Basics of SMS, 4

A. Description of SMS and SRM, 4

B. ICAO Requirements, 5

C. FAA Actions Concerning SMS, 6

III. Just Culture and SMS, 9

A. The Case for Implementing Just Culture, 10

B. Legal Impediments to Just Culture, 11

IV. Aviation SMS in Selected Jurisdictions, 11

A. Canada: Canadian Aviation Regulations and SMS, 11

B. Europe, 12

C. Australia, 14

V. SMS in Other Fields, 14

A. Patient Safety, 15

B. Maritime SMS, 16

C. Oil and Gas Industry, 19

VI. Liability and SMS, 21

A. The Effect of SMS on the Elements of a Negligence Claim, 21

B. Qualified Immunities for Governmental Entities, 25

VII. Data Protection and SMS, 28

A. FOIA and State Sunshine Laws, 30

B. Qualified Privileges, 34

C. Attorney-Client Privilege, 36

VIII. Strategies for Managing Legal Risks Due to SMS, 39

A. Review of State and Local Law, 40

B. Audit of Applicable Regulatory Documents, 40

C. Organizational Review, 41

D. Audit of FAA Approvals, 41

E. Assembly of SMS Review Team, 41

F. Outline of Development of Initial SMS, 41

G. Data Gathering and Data Protection, 42

H. Gap Analysis, 42

I. Hazard Identification and Analysis, 42

J. Risk Mitigation and the Predictive Risk Matrix, 42

K. FAA Approval of SMS, 44

IX. Conclusion, 44

LEGAL ISSUES RELATED TO DEVELOPING SAFETY MANAGEMENT SYSTEMS AND SAFETY RISK MANAGEMENT AT U.S. AIRPORTS

By David Y. Bannard, Foley and Lardner LLP*

I. INTRODUCTION

Implementation of Safety Management Systems (SMS) by U.S. airport sponsors and operators (collectively, "airport operators") has the potential to increase safety at airports in the United States. However, implementation of SMS may also increase legal exposure for airport operators and the "accountable executives" required to implement SMS. Perhaps more importantly, SMS at U.S. airports is not likely to realize its full potential unless and until state sunshine laws are modified or other steps are taken to protect SMS data from disclosure.

The Federal Aviation Administration (FAA) has noted that the International Civil Aviation Organization (ICAO) has adopted a standard that all member states establish SMS requirements for airport operators.[1] The FAA has further stated that it supports conforming U.S. aviation safety regulations with ICAO standards.[2] As of the date of this *Legal Research Digest*, the FAA has issued a Notice of Proposed Rulemaking (Proposed Rule) that, when finally promulgated, will require U.S. airports certificated by the FAA under Part 139 of Chapter 14 of the Code of Federal Regulations (C.F.R.) to adopt SMS.[3]

SMS is a proactive approach to safety that is expected to increase the likelihood that airport operators will detect and correct safety problems before those problems result in an incident or accident,[4] rather than relying on analyses of accidents after the fact to draw conclusions regarding improvements that should be made to enhance safety. The FAA defines SMS as a safety program that allows an airport operator "to strike a realistic and efficient balance between safety and operations."[5]

* The author is a partner with Foley and Lardner LLP, resident in the Boston office. He would like to thank partner Lawrence M. Kraus for his assistance with this LRD. He would also like to acknowledge Kevin A. Martin, Jaclyn V. Piltch, Torrey K. Young, JennyBess Dulac, Katherine Kraschel, and Jasmine D. Pierce, associates with Foley and Lardner LLP, for their assistance in researching these issues.

The essence of SMS is the safety risk management (SRM) process, pursuant to which data regarding potential hazards and means to mitigate those hazards are gathered and regularly updated; the potential for harm is evaluated, and risks are objectively ranked pursuant to a predictive risk matrix as being acceptable, acceptable with mitigation,[6] or unacceptable; and methods to mitigate hazards are developed and evaluated. According to the FAA, SMS is "[t]he formal, top-down business-like approach to managing safety risk. It includes systematic procedures, practices, and policies for the management of safety…."[7] SMS is to be overseen by an accountable executive designated by the airport operator who has both "ultimate responsibility and accountability" for the implementation and maintenance of the airport's SMS and "full control of the human and financial resources required to implement and maintain" it.

SMS will require airport operators to identify hazards, evaluate and rank risks, and mitigate unacceptable risks, in part through the development of a database or other records of hazards and the predictive risk matrix recommended by the FAA in Advisory Circular (AC) 150/5200-37.

Implementation of SMS could result in increased liability exposure for airport operators because SMS may identify otherwise unknown hazards and quantify the potential impact of such incidents. An airport operator put on notice of these risks through an SRM analysis arguably has a duty to persons lawfully at the airport (including, for example, airport tenants, those doing business at the airport, and travelers) to take all reasonable steps to mitigate the identified risk. If the SMS analysis had not been performed, the lack of knowledge of a risk could itself be a defense in some jurisdictions. Depending upon the scope of the SMS adopted by an airport operator, SMS could also expand the scope of persons to whom the airport operator arguably owes a duty of care to include persons lawfully within areas of the airport subject to SMS but under the control of a third party, such as portions of the nonmovement area leased to an air carrier.

The accountable executive may also run the risk of personal liability for decisions made or actions taken in his or her oversight of the airport's SMS program. However, the law in most jurisdictions protects a public officer from personal liability for his or her decisions or actions if they are within the scope of the person's authority and made in good faith.

[1] Safety Management Systems for Certificated Airports, Notice of Proposed Rulemaking, 75 Fed. Reg. 62,008, 62,009 (Oct. 7, 2010) (the "Proposed Rule").

[2] *Id*.

[3] *Id*.

[4] FAA Advisory Circular (AC) No. AC 150/5200-37, Introduction to Safety Management Systems (SMS) for Airport Operators, Feb. 28, 2007 (AC 150/5200-37). *See* FAA Web site: http://www.faa.gov/airports/airport_safety/safety_management_systems/. Note that on June 29, 2012, the FAA issued a draft revision of AC 150/5200-37 (AC 150/5200-37A).

[5] *Id.*

[6] *Id*.

[7] *Id.*

The most difficult problem confronting airport operators that undertake an SMS will likely be the gathering and protection of data. Nearly all of the approximately 570 commercial service airports in the United States that are certificated by the FAA (Part 139 airports) are owned and operated by governmental entities. These entities take many forms, including state departments of aviation, city or county enterprise funds, and quasi-governmental authorities. All these public entities are subject to applicable state and local public records laws, also known as "sunshine laws," governing records maintained by public entities.[8] These laws, which are modeled on the Federal Freedom of Information Act (FOIA),[9] generally broadly define what constitutes a public record and then require that, with certain very limited and enumerated exceptions, public records must be made available to any person requesting them. Sunshine laws create a presumption that information in the hands of a public entity will be made available to the public. Thus, without further legislative or regulatory action, the huge amount of safety data that will be generated by the SRM process that is central to SMS may all be subject to disclosure under state sunshine laws. The dissemination of SMS data in accordance with state and local sunshine laws could result in unwanted publicity, provide evidence in tort claims cases, and, as a result, could create disincentives for reporting safety information.

SMS is founded on the principle that by collecting and analyzing safety data, trends can be spotted and accidents avoided. For this process to work as envisioned, however, there must be a regular and robust flow of data into the system. Studies and experience in comparable settings have amply demonstrated that the less protection there is from disclosure of safety data, the less likely it is that persons will report that data. As noted by the Flight Safety Foundation with respect to safety data gathered under certain aviation safety programs described below, the majority of information on which safety enhancements now depend would not have surfaced at all if not voluntarily disclosed. Airport operators will need to become familiar with the law regarding disclosure of public records and they would be wise to develop their SMS programs, to the greatest extent possible, to prevent disclosure of such data. Because the vast majority of Part 139 airport operators are governmental entities, and therefore subject to state sunshine laws, SMS safety data will not be likely to be maintained confidentially. Nevertheless, airport operators could take steps, such as de-identifying safety data, implementing elements of just culture, and providing for anonymous reporting, that will encourage reporting of safety data.

As will be discussed herein, one of the hallmarks of effective safety systems in comparable contexts is that safety data are not only kept confidential, but such data are subject to a privilege preventing disclosure in litigation. The recently adopted FAA reauthorization act includes protection from disclosure of SMS data provided to the FAA,[10] but this protection does not expressly apply to protecting data from disclosure under state sunshine laws.

This digest begins with a summary of the basics of SMS in Section II. It then discusses the concept of "just culture" (a regime that encourages reporting by not punishing individuals in most circumstances) with respect to SMS in Section III. It then summarizes certain recent efforts to implement SMS at airports in other jurisdictions and in other fields, including maritime, patient safety, and the oil and gas industry in Sections IV and V. The theories under which SMS could lead to increased liability for airports are then examined, along with certain immunities from liability that may be available to airports, in Section VI. Section VII provides a review of sunshine laws from three selected jurisdictions as well as Federal FOIA, and a discussion of certain available means of protecting SMS data from disclosure or discovery. The digest concludes with Section VIII, which suggests potential strategies for managing the legal issues that may arise due to implementation of SMS.

II. BASICS OF SMS

A. Description of SMS and SRM

SMS is predicated upon the belief that a proactive analysis of data concerning hazards and their potential severity can be applied to identify the causes that may lead to accidents and, thus, to mitigate the personal injury and property damage resulting from such accidents by avoiding these causes. SMS comprises the following four elements:

- Development and adoption of *safety policy and objectives* by senior management, including staff responsibilities, and dissemination of the safety policy throughout the organization.
- Development of an *SRM* process, which describes each such system or activity at an airport, identifies hazards associated with such system or activity, determines and analyzes the risk associated with each such hazard, and treats or mitigates and monitors the risk. SRM is also a continuous process so that the effectiveness of mitigation strategies and the classification of risks are regularly reviewed.
- *Safety assurance*, through oversight and auditing to ensure that the safety programs are implemented and effective.

[8] *See, e.g.*, California Public Records Act, CAL. GOV'T CODE §§ 6250–6276.48 (West 2012), Florida Public Records Act, FLA. STAT. §§ 119.01–119.15 (2012), Massachusetts Public Records Law, MASS. GEN. LAWS ch. 66, § 10 (hereinafter, state public records laws are referred to as "sunshine laws").

[9] 5 U.S.C. § 552.

[10] FAA Modernization and Reform Act of 2012, § 310, Pub. L. No. 112-95, 126 Stat. 11 (Feb. 14, 2012) (adding new § 44735 to Title 49 of the U.S. Code).

• *Safety promotion*, through the development of a positive safety culture, including training, within the organization.[11]

SMS, through the SRM function, at a minimum should 1) establish a system to identify actual and potential safety hazards; 2) establish a systematic process to analyze hazards and their associated risks; 3) provide for regular assessment to ensure that safety objectives are being met; and 4) establish and maintain records that document the Part 139 airport's SMS processes.[12] SMS should clearly define the lines of safety accountability throughout the airport operator's organization, including a direct accountability for safety on the part of senior management.[13]

ICAO has provided guidance on SMS in the *ICAO Safety Management Manual*[14] (SMM) and in the *Manual on Certification of Aerodromes* (Doc. 9774).[15] Other guidance on SMS for airports is available on the FAA's Web site.[16] These materials include the Airport Cooperative Research Program's (ACRP) two-volume *Report 1: Safety Management Systems for Airports* and links to the FAA's Proposed Rule regarding SMS for airports and the docket, including comments and results of pilot SMS studies commissioned by the FAA.

ICAO recommends that a single, identified individual, known as the "accountable executive," oversee and be responsible for implementation and maintenance of the SMS at each airport.[17] He or she should have final authority over operations conducted at an airport and have final responsibility for all safety issues.[18] The accountable executive must also be given extraordinarily broad powers, including full control of the human and financial resources required to implement and maintain the SMS.[19]

In implementing SMS, airport operators will need to gather and analyze a great deal of data. Following the initial identification of airport hazards and risks as part of the SRM process, as part of the safety assurance process airport operators will continue to gather data on risks associated with new activities, newly identified hazards, changes in the degree of risk assigned to hazards, and the results of mitigation activities. Airport operators are also required to audit the SMS program to ensure that the airport operator is complying with its SMS.

Many airports will develop a "Predictive Risk Matrix," a database system that records the identified hazards, the means of mitigating certain hazards, and a table of the risks following such mitigation. The FAA recommends that airports categorize the acceptability of risks through development of a Predictive Risk Matrix, which will categorize risk based upon the severity and likelihood of identified hazards.[20] Theoretically, the more data that can be included in an SMS analysis, the better the likelihood that hazards can be identified and mitigated and accidents avoided. As a practical matter, however, it is this critical matrix of risk information that presents many of the legal issues that are associated with SMS.

B. ICAO Requirements

The ICAO adopted an amendment to its International Standards and Recommended Practices that requires member states, which include the United States and Canada, to require that operators of international airports implement an SMS.[21] ICAO has adopted similar requirements applicable to operators of commercial aircraft, aircraft maintenance organizations, and air traffic services.[22] According to ICAO, SMS is "a systematic approach to managing safety, including the necessary organizational structure, accountabilities, policies and procedures."[23]

ICAO's SMM defines "safety" as "[t]he state in which the possibility of harm to persons or of property damage is reduced to, and maintained at or below, an acceptable level through a continuing process of hazard identification and safety risk management."[24] ICAO has taken the position that elimination of all accidents and serious incidents, while desirable, is not possible.[25] Thus, the SMM states, "safety risks and operational errors that are controlled to a reasonable degree are acceptable in an inherently safe system."[26]

The SMM and *ACRP Report 1: Safety Management Systems for Airports* both provide valuable guidance regarding the development and implementation of SMS at airports, but neither addresses the legal issues that the development of SMS may raise at U.S. airports.

---

[11] *See* AC 150/5200-37, ch. 2 (Elements of a Safety Management System).

[12] *Id.*

[13] *See* ICAO SAFETY MANAGEMENT MANUAL, 2d ed., 2009 (SMM), Doc. 9859 (a third edition of the SMM was issued in advance draft form in May 2012).

[14] *Id*.

[15] *See* Annex 14 to the Convention on International Civil Aviation (CICA), § 1.4 (Certification of aerodromes).

[16] http://www.faa.gov/airports/airport_safety/safety_ _management_systems/.

[17] *See* SMM. *See also* Annex 14 to CICA, § 1.5.4 ("an approved safety management system shall clearly define lines of safety accountability throughout a certified aerodrome operator, including a direct accountability for safety on the part of senior management").

[18] *See* SMM.

[19] *Id*.

[20] *See* AC 150/5200-37, § 3.3, at 11–12.

[21] *See* Annex 14 to CICA, § 1.4 (Certification of aerodromes).

[22] *See* Annex 6, pt. I, ch. 3 (aircraft), ch. 8 (aeroplane maintenance), pt. III, ch. 1 (commercial air transport), and Annex 11 (air traffic services) to the CICA.

[23] CICA, Annex 14, vol. I, § 1.1.

[24] SMM, § 2.2.4.

[25] *Id*. § 2.2.2.

[26] *Id*. § 2.2.3.

C. FAA Actions Concerning SMS

As discussed below, the FAA has undertaken safety programs and rulemakings relating to SMS for several discrete sectors of the aviation industry, including Part 139 airports. FAA has established separate SMS programs for its air traffic control function[27] and the FAA's Office of Airports, as well as a separate SRM process for review of changes to airport standards or certain project-specific approvals.[28] The FAA is also undertaking a separate SMS rulemaking process for air carriers.[29] In addition, for many years prior to its more recent focus on SMS, the FAA, in partnership with the National Aeronautics and Space Agency (NASA), developed and has maintained safety reporting programs that incorporate data gathering and analytical elements that are now central to SMS. As a result, there is a diversity of FAA-mandated standards, terminology, and approaches applicable to SMS programs operating or to be operated within the U.S. aviation system.

FAA has stated that it will synchronize its SMS efforts both internally and externally to the extent practicable.[30] Notwithstanding the separate approach to SMS rulemaking it has undertaken, the FAA has also stated that it is committed to an integrated approach to SMS, including common definitions and understanding of risk, consistent methods for analyzing and assessing safety risks, common safety risk management techniques, consistent safety assurance procedures, and common approaches to defining acceptable levels of risk.[31]

1. Airport SMS

In part to comply with the ICAO requirements, the FAA issued a Proposed Rule on October 7, 2010, regarding implementation of SMS at commercial airports.[32] The Proposed Rule would amend the FAA's primary regulatory guidance applicable to commercial airports, 14 C.F.R. Part 139 (Part 139), to require all Part 139 airports to develop and maintain an SMS that is approved by the FAA.[33]

Part 139 regulates the certification and operation of all airports within the United States that have scheduled or unscheduled passenger service, other than airports served by very small aircraft.[34] Part 139 does not, however, currently require Part 139 airports to implement an SMS program. The Proposed Rule follows the ICAO model and emphasizes the four critical elements of SMS described above.

As described above, the Proposed Rule places accountability for the implementation and maintenance of each airport operator's SMS in the hands of an identified accountable executive. The commentary to the Proposed Rule states that the accountable executive must be a high-level manager who can influence safety-related decisions and who has authority to approve operational decisions and changes.[35] In general, the accountable executive will be the highest approving authority at the airport for operational decisions and changes.[36]

Unlike the ICAO and other FAA models, the Proposed Rule is applicable only to Part 139 airports and not to other participants in the national aviation system. Unlike other FAA SMS guidance,[37] the Proposed Rule does not address either confidentiality and protection of safety data or just culture. This can be contrasted with the proposed guidance applicable to air carriers that relies on the existing confidential reporting programs, including the Aviation Safety Action Program and the Aviation Safety Reporting System (ASRS), discussed below, which are not applicable to Part 139 airports.

In addition to the Proposed Rule, the FAA has already implemented a policy regarding SMS that affects airports. Order 5200-11 became effective August 30, 2010, and is applicable to the FAA's Office of Airports (ARP). Effective on June 1, 2011, for large hub airports,[38] Order 5200-11 requires that an SMS review be undertaken in connection with FAA's review of revisions to Airport Layout Plans, construction project coordination, noise compatibility program measures that could affect safety (such as noise-abatement departure procedures), approval of requests for project-specific modifications of standards, certain nonconstruction changes (such as runway or taxiway designations), material changes from a previous SRM assessment, or development of or updates to FAA standards published in ACs.[39]

Although Order 5200.11 initially was to apply on a phased basis to all airport within the National Plan of Integrated Airport Systems, due to a lack of resources, the FAA has postponed full implementation of Order 5200.11 to airports other than large hub airports until further notice.[40] For the majority of the matters reviewed under Order 5200.11, the airport operator will

---

[27] *See* FAA Air Traffic Order JO 1000.37, *Air Traffic Organization Safety Management System* (Mar. 19, 2007), and Air Traffic Organization SMS Manual, Version 2.1 (May 2008).

[28] *See* FAA Order 5200.11, FAA Airports (ARP) Safety Management System, Aug. 30, 2010.

[29] *See* Safety Management Systems for Part 121 Certificate Holders, 75 Fed. Reg. 68, 224 (Nov. 5, 2010) (to be codified at 14 C.F.R., pts. 5 and 119).

[30] FAA Order 5200.11, § 1-6.

[31] *Id*., § 2-2.

[32] Proposed Rule, 75 Fed. Reg. 62,008.

[33] *Id*. at 62,022.

[34] 14 C.F.R. § 139.1 (applicability). There are approximately 570 Part 139 certificated airports in the United States.

[35] Proposed Rule, 75 Fed. Reg. 62.008, 62011.

[36] *Id*.

[37] *See, e.g.*, 75 Fed. Reg. 68224, 68233 (referencing the data protection of ASRS, ASAP, and FOQA with respect to the proposed SMS regulations applicable to certificated air carriers).

[38] Order 5200.11, § 1-4(b).

[39] *Id*., § 4-3.

[40] *See* FAA Order 5200.11, Change 1, effective May 31, 2011.

be a part of the safety review process overseen by the ARP, along with other subject matter experts. To undertake a project, the airport operator will be required to accept and undertake any mitigation determined by a review panel established by the ARP to be necessary to achieve an acceptable level of risk.[41]

In preparation for the Part 139 SMS rulemaking process, the FAA has sponsored several pilot SMS programs, summaries of which are available in the docket for the Proposed Rule and through the FAA's Web site.[42] In addition, the ACRP of the Transportation Research Board has produced a report containing an overview of SMS,[43] and has issued an SMS user guidebook for airport operators.[44] The initial airport SMS pilot studies concluded that, although Part 139 addresses safety at airports in many areas, the existing safety regulations at Part 139 are not a comprehensive SMS.[45] Part 139 does not cover all areas of a commercial airport, or even all airside areas of the movement or non-movement areas, nor does it address all aspects of safety management.

2. Air Carrier SMS

On October 29, 2010, the FAA issued a Notice of Proposed Rulemaking (NPRM) that would amend 14 C.F.R. by adding a new Part 5 (Part 121 SMS NPRM).[46] The Part 121 SMS NPRM would require all air carriers certificated under Part 121 to implement an SMS that meets the requirements of the new regulations and is acceptable to the FAA within 3 years of the effective date of the final rule. The Part 121 SMS NPRM contrasts in several notable ways with the Proposed Rule.

Like the Proposed Rule, the Part 121 SMS NPRM requires that a Part 121 certificate holder's SMS follow the familiar four-prong approach of the ICAO guidance: 1) safety policy, 2) SRM, 3) safety assurance, and 4) safety promotion.[47] Unlike the Proposed Rule, however, the commentary to the Part 121 SMS NPRM addresses the concerns raised about protecting data submitted through the SMS. Like the Proposed Rule, the Part 121 SMS NPRM would not require SMS data to be provided to the FAA; instead, the FAA may inspect the carrier's records, and existing protections for voluntary programs such as the Aviation Safety Action Program (ASAP) would still apply.[48] One critical difference is apparent, however; unlike the vast majority of Part 139 airport operators, the carriers holding Part 121 certificates are private entities not subject to the disclosure requirements of state or federal sunshine laws. Only by providing safety data to the FAA (or another governmental entity) would such data become public under such laws.

The Part 121 SMS NPRM also provides that a designated accountable executive must be responsible for the certificated carrier's SMS, but the proposed regulations provide much more detail regarding that person's responsibilities and duties for a Part 121 carrier.[49] In addition, the accountable executive must designate a management representative to manage the SMS on a day-to-day basis, including facilitating hazard identification and safety risk analysis, monitoring the effectiveness of safety risk controls, ensuring safety promotion is carried out, and reporting to the accountable executive.[50] The accountable executive and management representative would also be tasked with developing an emergency response plan for the carrier.[51] The Proposed Rule does not provide for a management representative, although airports with larger and more complex SMS programs may choose to adopt this model.

3. NASA/FAA Programs

Although the U.S. government has not yet required that SMS be adopted by most participants in the U.S. aviation system, two programs that anticipate elements of SMS have been operated successfully by NASA and the FAA for many years: the ASRS and the ASAP. In the Part 121 SMS NPRM, the FAA notes that these programs can be incorporated as elements of an air carrier's SMS.

ASRS and ASAP have generated significant amounts of safety data that have led to improvements in the national aviation system. As an independent review team examining ASAP concluded, "the majority of the infor-

---

[41] *Id.*, §§ 4-8, 4-9.

[42] *See* FAA Web site: http://www.faa.gov/airports/airport_safety/safety_management_systems/.

[43] *See* AIRPORT COOPERATIVE RESEARCH PROGRAM, REPORT 1: SAFETY MANAGEMENT SYSTEMS FOR AIRPORTS, Vol. 1: OVERVIEW OF SAFETY MANAGEMENT SYSTEMS FOR AIRPORTS (2007), http://onlinepubs.trb.org/onlinepubs/acrp/acrp_rpt_001a.pdf.

[44] AIRPORT COOPERATIVE RESEARCH PROGRAM, REPORT 1: SAFETY MANAGEMENT SYSTEMS FOR AIRPORTS, Vol. 2: GUIDEBOOK (2009), http://onlinepubs.trb.org/onlinepubs/acrp/acrp_rpt_001b.pdf.

[45] *See* FAA summary of initial pilot SMS studies, concluding that it is

> [a]pparent that [Part] 139 is not SMS in and of itself.... Evidence that SMS is something larger, more comprehensive, than is currently found in the act of complying with 139 requirements. Evidence that 139 compliance may eventually become part of airport SMS program…contrary to the idea that SMS would eventually become part of 139. Reference made to the idea that SMS could be used to ensure 139 compliance…but that 139 by itself could not ensure that SMS was functioning.

Presentation at joint FAA/Airports Council International–North America/American Association of Airport Executives SMS Conference, Baltimore, Md., Oct. 2008, available by membership at http://events.aaae.org/sites/080703/index.cfm.

[46] *See Safety Management Systems for Part 121 Certificate Holders*, 75 Fed Reg. 68,224 (proposed Nov. 5, 2010), Docket No. FAA-2009-0671; Notice No. 10-15 (the "Part 121 SMS NPRM").

[47] 75 Fed. Reg. 68,224, 68242 (§ 5.3(a)).

[48] *Id*. at 68,233.

[49] *Id*. at 68,243 (§ 5.25).

[50] *Id*. (§ 5.25(c)).

[51] *Id*. (§ 5.27).

mation on which [safety] enhancements now depend would not surface at all if not voluntarily disclosed."[52]

a. Aviation Safety Reporting System.—ASRS has been operated by NASA since 1975 and gathers data from multiple sources, including pilots, air traffic controllers, flight attendants, and maintenance personnel, that is intended to identify actual or potential discrepancies and deficiencies involving the safety of aviation operations that are the precursors of accidents and fatalities in the airline industry.[53] As a result of information generated by ASRS, the FAA takes corrective action to remedy defects or deficiencies in the national airspace system. The data is also used to both improve the current system and assist in planning for the future national airspace system.[54] By all accounts, ASRS has been a significant success, generating thousands of reports leading to many improvements in aviation safety.[55]

Notably, ASRS incorporates significant confidentiality provisions and restrictions on the use of reports. ASRS reports are de-identified—that is, they are stripped of data identifying the person reporting as well as data that could identify other parties.[56] ASRS reports may not be used in any disciplinary action, except for information concerning criminal offenses or accidents (which are promptly referred to appropriate federal authorities by NASA before the identifying information is removed).[57] In the more than 34 years of the ASRS program under NASA's management, there has not been a single breach of confidentiality.[58]

The ASRS was originally undertaken by the FAA. The FAA quickly determined, however, that the effectiveness of ASRS would be greatly enhanced if NASA processed the data, ensuring the anonymity of the reporter and all parties involved.[59] The FAA believed that such confidentiality protections would increase the flow of information necessary for the effective evaluation of the safety and efficiency of the national airspace system.[60]

As an additional incentive to encourage the reporting of incidents, the FAA has stated that it considers the filing of an ASRS report with NASA concerning an incident or occurrence involving a violation of the law or regulations applicable to air operations "to be indicative of a constructive attitude."[61] Accordingly, if the reported violation 1) was inadvertent and not deliberate, 2) did not involve a criminal offense or accident, 3) involved a violator who has not previously violated federal aviation law within the preceding 5 years, and 4) if the ASRS report was filed promptly after the violation or awareness of such violation, the FAA will not impose a civil penalty or suspend certification.[62]

b. Aviation Safety Action Program.—Under an ASAP, "safety issues are resolved through corrective action rather than through punishment or discipline."[63] The ASAP is administered by the FAA and provides a means for individual certificate holders (both air carriers and repair stations) to voluntarily report safety information that may be critical to identifying potential precursors to accidents.[64] An ASAP typically involves three parties: the FAA, the certificate holder, and a third party, often a labor organization, representing the group of employees involved in the ASAP.[65] These parties enter into a memorandum of agreement (MOA) setting forth the terms and conditions of the ASAP.[66]

ASAP provides for the collection, analysis, and retention of safety data concerning a specific air carrier or repair station, much of which would otherwise be unobtainable.[67] In a report issued in 2008, an independent review team examining ASAP concluded that "the majority of the information on which [safety] enhancements now depend would not surface at all if not volun-

---

[52] Linda Werfelman, *Rebuilding ASAP*, 4 AEROSAFETY WORLD, 40, 42 (Feb. 2009), quoting Independent Review Team, *Managing Risks in Civil Aviation: A Review of the FAA's Approach to Safety*, Sept. 2, 2008.

[53] *See* FAA, AC No. 00-46E, Aviation Safety Reporting Program, Dec. 16, 2011, at ¶ 1, link available at http://www.faa.gov/regulations_policies/advisory_circulars/index.cfm/go/document.information/documentID/1019713.

[54] *Id*.

[55] *See, e.g*., Brian Raymond & Robert Crane, *Design Considerations for a Patient Safety Improvement Reporting System*, Institute for Health Policy, Kaiser Permanente, Apr. 2001, at 6 (hereinafter, the "Kaiser Report") ("Members of the aviation community have visible evidence that they are helping to improve aviation safety by reporting to ASRS. The ability of ASRS to convert aviation incident reports into constructive output is demonstrated by the variety of products made available to the aviation community."), http://www.kpinstitute forhealthpolicy.com/kpihp/CMS/Files/safety_improvement.pdf.

[56] FAA, AC No. 00-46E, at ¶ 8, Dec. 16, 2011.

[57] *Id*. at ¶ 5(b); 14 C.F.R. § 91.25.

[58] *Id*. at ¶ 5(a).

[59] *Id*. at ¶ 3.

[60] *Id*.

[61] *Id*. at ¶ 9(c).

[62] *Id*.

[63] *See* FAA, AC No. 120-66B, ¶ 1, Aviation Safety Action Program, Nov. 15, 2002, link available at http://www.faa.gov/regulations_policies/advisory_circulars/index.cfm/go/document.information/documentID/23207.

[64] *Id*.

[65] *Id*. at ¶ 1.

[66] *Id*. at ¶ 1(c).

[67] Werfelman, *supra* note 52. The U.S. Government Accountability Office (GAO) has noted that

> the data that FAA obtains through voluntary reporting programs afford insights into safety events that are not available from other sources and are critical to improving aviation safety, but participation in these programs has been limited by concerns about the impact of disclosure and, especially in the case of smaller carriers, by cost considerations.

GOVERNMENT ACCOUNTABILITY OFFICE, AVIATION SAFETY–IMPROVED DATA QUALITY AND ANALYSIS CAPABILITIES ARE NEEDED AS FAA PLANS A RISK-BASED APPROACH TO SAFETY OVERSIGHT, Report 10-414, at 31–32 (May 2010), http://www.gao.gov/new.items/d10414.pdf.

tarily disclosed."[68] The Flight Safety Foundation estimates that 98 percent of the safety information obtained from voluntary disclosure programs would not have been available if participants were subject to prosecution and penalties.[69]

Under an ASAP MOA, neither the FAA nor the company holding the certificate may use information gathered to take disciplinary action, unless (as with ASRS), the reported action involves criminal activity, substance abuse, controlled substances, alcohol, or intentional falsification of reports.[70] Otherwise, if the ASAP report is the only source of the information with respect to the reported incident, the FAA will not take legal action.[71] If an ASAP report is not the only source of information regarding an incident, the potential sanction for violation of federal aviation regulations will be reduced.[72]

Under ASAP, education and corrective action are intended to take the place of FAA penalties or company disciplinary measures.[73] Nevertheless, the use of ASAP data to initiate retraining is sometimes considered by employees to be a punitive action, and the availability of ASAP data for use in civil and criminal proceedings is of concern to participants in ASAPs. In addition, alleged use of ASAP data to penalize pilots and others reporting mistakes has led to interruptions in ASAPs at certain carriers.[74] Moreover, ASAP remains a program that may be terminated by any of the three parties to the MOA.

ASAP reports are not de-identified, but they are protected from public disclosure. Congress recognized the importance of protecting the confidentiality of safety data and the persons who supply such data by enacting 49 U.S.C. § 40123 (Section 40123), which provides for protection of voluntarily provided aviation safety data under ASAP. In Section 40123, Congress exempted from disclosure under FOIA[75] voluntarily-provided safety or security information where the FAA finds that the disclosure of that information would inhibit the voluntary provision of that type of information.[76]

Section 40123 therefore recognizes that protecting the confidentiality of data leads to more honest and complete reporting of hazards and analysis of risks and how to mitigate them. It should be noted that it is only the act of reporting the safety data to the FAA, a federal agency, that makes such data subject to disclosure under FOIA. As private corporate entities, the air carriers themselves are not subject to the disclosure obligations imposed under FOIA. Notably, in the now withdrawn notice of an earlier proposed rulemaking for an SMS program for air carriers, the FAA went to great lengths to retain the benefits of confidentiality available under Section 40123 for safety data generated pursuant to an SMS implemented by an air carrier.[77]

> The [Aviation Rulemaking Committee ("ARC")] was also concerned with the protection of SMS safety information and proprietary data. …According to the ARC, protecting safety information from use in litigation (discovery), Freedom of Information Act (FOIA) requests, and FAA enforcement action is necessary to ensure the availability of this information, which is essential to SMS.78

Under Section 40123, Congress required the FAA to find that

> (1) the disclosure of the information would inhibit the voluntary provision of that type of information and that the receipt of that type of information aids in fulfilling the Administrator's safety and security responsibilities; and (2) withholding such information from disclosure would be consistent with the Administrator's safety and security responsibilities.[79]

The FAA has issued regulations pursuant to Section 40123 that provide for the protection of certain voluntarily-disclosed aviation safety information.[80] Part 193 protects such information from disclosure under FOIA as well as in other contexts, including litigation, unless disclosed pursuant to a court order.[81]

III. JUST CULTURE AND SMS

As previously described with respect to ASAP, there is a tension between the desire to obtain safety data from one of the persons most likely to be aware of a specific incident—the person who made a mistake—and the desire to penalize such persons for their mistakes. A critical element of successful safety reporting programs is implementation of "just culture." Just culture is generally considered to be a corporate culture where persons reporting errors that do not constitute criminal behavior, gross negligence, or willful misconduct are actively protected from punishment for their errors. As the author of a recent article describing the tension between safety reporting and European national laws regarding civil and criminal liabilities and the importance of just culture to aviation safety noted,

> [t]he fear of legal proceedings…can have an impact on the level of reporting of safety incidents. With respect to aviation, failure to gather all available safety data may have serious consequences, as one of the most valuable tools for

[68] *Id*. at 42, quoting Independent Review Team, *Managing Risks in Civil Aviation: A Review of the FAA's Approach to Safety*, Sept. 2, 2008.

[69] *Id*. at 43.

[70] FAA AC No. 120-66B, at ¶ 1(b).

[71] *Id*. at ¶ 11(b)(2).

[72] *Id*. at ¶ 11(b)(1).

[73] Werfelman, *supra* note 52, at 41.

[74] *See, e.g*., *id.* at 40.

[75] 5 U.S.C. § 552.

[76] 49 U.S.C. § 40123.

[77] *See* Safety Management Systems for Part 121 Certificate Holders, 75 Fed. Reg. 68224, 68231, Nov. 5, 2010 (to be codified at 14 C.F.R. pts. 5 and 119).

[78] *Id.*

[79] 49 U.S.C. § 40123(a).

[80] *See* 14 C.F.R. pt. 193 ("Part 193").

[81] *Id*. at § 193.7(f) ("…the FAA will not release information designated as protected under this part unless ordered to do so by a court of competent jurisdiction.").

the promotion of safety is the ability to learn from previous mistakes.[82]

This element of safety management is one of the most difficult issues confronting entities that implement SMS, as it runs counter to the need in many cultures to find fault and fix blame. Just culture can also be in opposition to general standards of tort law, where a factfinder seeks to determine the proximate cause of an injury to a party. Nevertheless, it has been clearly demonstrated that the absence of a just culture will lead to under-reporting of safety data, while careful adherence to just culture principles leads to robust reporting of such data.

A. The Case for Implementing Just Culture

A critical and fundamental component of any SMS is the expectation that errors will be reported so that the organization undertaking the SMS can compile information, analyze data, communicate trends, develop tools for resolving events, and ultimately implement procedural and systematic change to mitigate or eliminate hazards. The success of an SMS is in part dependent upon ensuring that there are no impediments, including reprisals, to information flowing freely to management and leadership.[83] Reporting is unlikely to occur if staff believe they will be punished for doing so. The international aviation community has recognized the importance of just culture to SMS.[84]

ICAO has clearly noted the distinction between what it terms "error reporting" and "hazard reporting," stating that "error reporting is reactive and may incriminate the reporter or the reported, which may lead to blame and punishment" while "hazard reporting is predictive and should be objective and neutral."[85] ICAO goes on to note that the protection of reporters and sources of safety information was, and is, a key and often contentious issue in establishing reporting systems and could be a significant obstacle to the success of safety management.[86] ICAO distinguishes between records relating to accidents and serious incidents, where there may be overriding considerations that require disclosure of the records for judicial investigations, and records related to voluntary hazard reporting, where there is strong justification for protection.[87]

ICAO also notes, however, the difficulty of harmonizing just culture principles with a sovereign state's legal structure, which may provide for the "criminalization of error."[88] ICAO notes that there should be a means to distinguish between, and protect, voluntary hazard reports, which relate to latent deficiencies of a system or its performance, and those reports concerning an accident and serious incident investigations.[89]

Punishing employees for making a mistake emanates from the perception that the individual is to "blame" for his or her mistake and that punishment will lead to improved performance by that individual and serve as a deterrent to error in others. However, research has shown that most human errors are symptoms of underlying system failures, not personal failures, undercutting that fundamental rationale for punitive action.[90]

According to the ICAO, an effective SMS requires that organizations attain a "just culture," an atmosphere of trust where people are encouraged and even rewarded for providing safety-related information, but which also clearly delineates the difference between acceptable and unacceptable behavior.[91] The threshold for discipline is generally determined to be incidents where the individual had no conscious disregard of a known risk. As stated in ICAO's SMM, a "safety policy should actively encourage effective safety reporting and, by defining the line between acceptable performance (often unintended errors) and unacceptable performance (such as negligence, recklessness, violations or sabotage), provide fair protection to reporters."[92]

---

[82] Roderick D. van Dam, *Preserving Safety in Aviation: "Just Culture" and the Administration of Justice*, 22:2 AIR & SPACE LAW 6 (2009), http://aci-na.org/static/entransit/airspace_lawyer_vol22no2%201.pdf.

[83] *See, e.g.*, Mark E. Meaney, *Error Reduction, Patient Safety and Institutional Ethics Committees*, 32 J.L. MED. & ETHICS 358–62, American Society of Law, Medicine & Ethics (2004) (contrasting "Safety Culture" with a "Culture of Blame").

[84] *See, e.g.*, SMM, § 1.5 (contrasting "errors" with "violations"); guidance on SMS provided by Transport Canada that states that among the essential elements of a safety culture is "just culture" that establishes an "atmosphere of trust where reporting is encouraged and where a line is drawn between acceptable and unacceptable behaviours." AC No. 107-001, § 3.6; and FAA's Part 121 SMS NPRM, requiring certificated carriers to implement a confidential safety reporting program (Safety Management Systems for Part 121 Certificate Holders, 75 Fed. Reg. 68224, 68234, 68243 (§ 5.21)), and in the Proposed Rule by requiring that Part 139 Airports "establish and maintain a hazard reporting system that maintains a means for reporter confidentiality." (Proposed Rule, 75 Fed. Reg. at 62022). The Part 121 SMS NPRM requires that a carrier's safety reporting policy "allow employees to report unsafe working conditions or equipment for correction without fear of reprisal by either management or labor groups within the organization." (75 Fed. Reg. 68224, 68234).

[85] SMM, § 2.8.19.

[86] *Id*. at 2.8.20.

[87] *Id*. at 2.8.22.

[88] *Id*. at 2.8.23.

[89] *Id*.

[90] *See, e.g.*, Robert M. Wachter, *Balancing "No Blame" with Accountability in Patient Safety*, 14 N. ENG. J. MED. 1401 (Oct. 1. 2009) ("the traditional focus on identifying who is at fault is a distraction. It is far more productive to identify error-prone situations and settings and to implement systems that prevent caregivers from committing errors, catch errors before they cause harm, or mitigate harm from errors that do reach patients."), http://www.mayorswellnesscampaign.org/wp-content/uploads/2010/04/Balancing-No-Blame.pdf.

[91] SMM at 2.8.22.

[92] *Id*.

An organization that adopts a just culture does not eliminate individual or organizational accountability. Organizations promulgating a just culture model should adopt disciplinary policies that center on accountability and integrate the notions of individual and organizational culpability with the type of error. Each safety event should be assessed individually.

B. Legal Impediments to Just Culture

As described in the ICAO SMM, and noted below in connection with the difficulties associated with creating a European safety reporting system, the criminalization of error is "legally, ethically and morally within the sovereign rights of any State."[93] Thus, civil and criminal laws may run directly counter to the precepts of just culture, by permitting punishment of persons for their errors even where such errors are unintentional. ICAO accurately states that "a judicial investigation, and consequences of some form, may be expected following an accident or serious incident especially if a system failure resulted in lives lost or property damaged, even if no negligence or ill-intent existed."[94] Thus, an organization seeking to establish a just culture will only be able to protect reporters and those persons named in such reports to the extent permitted by applicable laws. In addition, many such organizations will also have a unionized workforce, and the provisions of applicable collective bargaining agreements may also limit the ability of an organization to protect reporters who have committed errors from punishment.

Notwithstanding these legal issues, the benefits to safety of a shift to just culture are apparent. Robust SMS relies on the free flow of information; therefore, removing impediments to that flow is not only consistent with SMS goals, but is critical to its success.

IV. AVIATION SMS IN SELECTED JURISDICTIONS

International experience suggests that the success of implementing SMS for airports has depended in large part upon the existing law in the respective jurisdiction. In Canada, for example, where the country's international airports are operated by private entities not subject to federal or provincial sunshine laws, and preexisting laws impose liability for failure to seek and correct defects, the establishment of SMS appears to have resulted in few if any legal issues. In contrast, the European Union (EU) has sought to require its Member States to implement SMS, but the varying legal requirements of these States regarding protection of data and civil or criminal liability for injury has led to much less uniform and less widespread adoption. In a third model, Australia has provided data protection at the federal level through legislation and an interagency agreement. Although there are documented concerns regarding the liability of an accountable executive in Australia, it appears that prior to the adoption of SMS legislation, senior airport officers had been held accountable for safety-related issues under Australian common law.

Following is a brief overview of these three international approaches to implementation of SMS at airports.

A. Canada: Canadian Aviation Regulations and SMS

In 2005, Transport Canada (TC), the Canadian federal regulatory body overseeing aviation, required that SMS be implemented by all aviation certificate holders, including air carriers and operators of certain large airports.[95] TC's SMS regulations are modeled on the ICAO standards and include the familiar four components of an SMS. TC has implemented SMS for aviation in an integrated and coordinated manner. TC has issued unified regulations regarding SMS applicable to all of the primary participants in the Canadian aviation system: air carriers, international airports, aircraft maintenance providers, and air traffic service providers.[96]

The Canadian Aviation Regulations (CARs) require that international airports certificated by TC must "establish, maintain and adhere to a safety management system."[97] Among the required elements is a safety management plan that includes "a process for identifying hazards to aviation safety and for evaluating and managing the associated risks…and a process for the internal reporting and analyzing of hazards, incidents and accidents and for taking corrective actions to prevent their recurrence…."[98] The CARs also require a "policy for the internal reporting of hazards, incidents and accidents, including the conditions under which immunity from disciplinary action will be granted…."[99]

TC's SMS regulations and related guidance clearly outline a program where confidentiality of reported safety information is respected and a just culture is encouraged. Unlike the United States, where the vast majority of Part 139 airports are owned and operated by governmental entities, the Canadian federal or provincial governments have leased the major commercial service airports to private not-for-profit corporations. These entities are not subject to federal or provincial freedom of information or "sunshine" laws and, therefore, may protect safety-related data from disclosure, similar to commercial air carriers in both the United States and Canada.

Consistent with ICAO's SMM, the CARs also require that each certificated international airport designate an

[93] *Id*.

[94] *Id*.

[95] *See* Canadian Aviation Regulations (CAR) pt. I, subpt. 7 (Safety Management System Requirements), § 107.01 (SMS required of certificated approved maintenance organizations, air operators, international airports, and air traffic service (ATS) providers).

[96] *Id.*

[97] *Id*. § 107.01(2)(a).

[98] *Id*. § 107.03(c), (e).

[99] CAR pt. III, § 302.502(a)(iv).

"accountable executive" responsible for operations or activities authorized under the airport certificate and accountable for meeting the requirements of the CARs regarding SMS.[100] The accountable executive must submit a signed statement accepting the responsibilities of the position to the Minister of Transportation.[101] The accountable executive must have control of the financial and human resources necessary for the activities and operations authorized under the airport's certificate issued by TC.[102]

Canadian law, like that of the United States, is generally based upon English common law and includes liability for the tort of negligence. Thus, as is discussed in more detail below, implementation of SMS would ordinarily heighten the potential for liability for negligence by making identified hazards more likely to be foreseeable. However, airports in Canada are also subject to Canadian law that imposes a duty to ensure that persons may use the airport in a safe manner, similar to some U.S. premises liability statutes. Canadian airport operators are therefore under some preexisting duty to seek out hazards at the airport and to mitigate them. Thus, implementation of SMS does not appear to significantly increase Canadian airport operators' potential liability for negligence, as Canadian airport operators already are under a duty to identify and mitigate hazards,[103] in contrast to U.S. airport operators.[104]

Guidance on SMS published by TC states that among the essential elements of a safety culture are a "reporting culture" where "people are prepared and encouraged to report their errors and near misses" and "just culture" that establishes an "atmosphere of trust where reporting is encouraged and where a line is drawn between acceptable and unacceptable behaviours."[105] To encourage reporting, TC's guidance states that "[a]n essential element of any SMS is the safety reporting policy. To the extent possible, it should be non-punitive and implemented with all affected parties."[106] TC's guidance continues, stating that

> …employees are more likely to report events and cooperate in an investigation when some level of immunity from disciplinary action is offered. When considering the application of a safety reporting policy, the organization should consider whether the event was willful, deliberate or negligent on the part of the individual involved and the attendant circumstances.[107]

TC's unified approach to the implementation of SMS for all Canadian aviation certificate holders also strongly encourages the various participants in the Canadian aviation system, including air carriers, airport operators, and ground handlers, to share safety-related data. The Canadian approach, which permits such data to be held in confidence and which encourages—if not requires—implementation of just culture, makes it far more likely that critical safety data will be reported and shared widely.

B. Europe

The EU has opted to take a comprehensive approach to aviation safety and, more specifically, SMS implementation. To achieve the goal of pan-European aviation safety, the European Parliament and Council (EPC) promulgated a regulation in 2008 (the 2008 EU Regulation)[108] that substantially incorporates the provisions of the ICAO Chicago Convention, pursuant to which all countries that are members of the EU are legally bound.[109] In furtherance of the goal of a comprehensive EU aviation safety policy, the 2008 EU Regulation created the European Aviation Safety Agency to regulate aviation safety in the EU, as well as provide technical specifications, opinions, and guidance to Member States with regards to implementation of the 2008 EU Regulation and SMS.

The EPC adopted a second regulation in 2009 (2009 EU Regulation; together with the 2008 EU Regulation, the "EU Regulations") that expanded the SMS requirements and safety initiatives under EU governance to include airports and air traffic control.[110] As discussed below, the EU Regulations substantially incorporate ICAO's SMS requirements to clarify the objectives of the legislation.

The EPC has taken steps to mirror ICAO's SMS language to improve safety and create uniformity in aviation safety laws and regulations across the EU. Specifically, the stated objectives of the 2008 EU Regulation are to provide a basis for common interpretation and uniform interpretation of the provisions of the Chicago Convention and to promote the EU's safety standards throughout the world by establishing methods of cooperation with outside countries and organizations.[111] The EU has implemented the EU Regulations in the manner that the ICAO intended, with the objective of fostering safety and uniformity within the aviation industry, not drastically altering legal standards in the aviation industry that could have unintended legal consequences.

---

[100] CAR pt. I, § 106.01(a) (applicability to international airports).

[101] *Id*. § 106.02(1)(a).

[102] *Id*. § 106.02(2).

[103] Telephone interview with Peter Humele of the Greater Toronto Airport Authority General Counsel's office.

[104] *See* pt. VI.A below for an analysis of the effect of SMS on negligence claims in the United States.

[105] Transport Canada AC No. 107-001, § 3.6, http://www.tc.gc.ca/media/documents/ca-opssvs/107-001-e.pdf.

[106] *Id*. § 4.6(1). Thus, based upon telephone interviews, airport operators routinely require tenants, including air carriers, to share safety data with the airport operator.

[107] *Id*. § 4.6(2).

[108] Commission Regulation 216/2008, 2008 O.J. (L 79).

[109] *Commission Staff Working Paper on The European Safety Programme*, at 10 COM (2011) 670 final (Oct. 25, 2011).

[110] Commission Regulation 1108/2009, 2009 O.J. (L 309).

[111] Commission Regulation 216/2008, art. II, 2008 O.J. (L 79).

Despite the measures taken by the EU, the EPC has acknowledged that the implementation of the EU Regulations may either conflict with existing Member State legislation or have other unintended consequences that may adversely affect safety. With this in mind, the preamble to the EU Regulations provides for flexibility and exemptions from the requirements of the EU Regulations where Member States already have laws in place to reach an equivalent safety level.[112] By allowing such exemptions and flexibility, the EU Regulations allow for the achievement of the necessary levels of safety while allowing Member States to deviate as necessary to make the system work. Such deviations have been necessary based on various Member State laws, in particular freedom of information laws.

One of the most beneficial aspects of the SMS, the identification of potential risks and hazards through reporting accidents and incidents at airports, has resulted in the greatest legal impediment to the successful implementation of SMS in the EU. One goal of the EU Regulations is to collect information and reports at the individual airport and Member State levels, and compile the information at the EU level to analyze the information and identify EU-wide issues and patterns. Unfortunately, due to legal issues at both the EU and Member State level, such compilation and analysis of safety information is not yet taking place.

The framework for reporting, collecting, and sharing safety information and reports across the EU was in place well before the EU Regulations were promulgated. Prior to their issuance, the EPC promulgated various directives, pursuant to which Member States are required to adopt laws meeting EU standards, setting forth EU reporting requirements and standards. The first such directive, issued in 2003, required aviation authorities in Member States to collect, evaluate, process, and store reports of occurrences that endanger, or, if not corrected, would endanger an aircraft, its occupants, or any other person.[113] To foster a reporting culture, this directive clearly stated that the Member States must take all necessary steps to ensure confidentiality of such reports. Furthermore, Member States were directed to avoid instituting proceedings as a result of the reports except in extreme cases and to avoid any retributive actions to the parties reporting.

The EPC created a central repository for safety reports and, pursuant to a 2007 regulation, required all Member States to submit reports to the central repository, thus allowing all Member States to access reports from across the EU.[114] The EPC set forth the parameters for controlling access to such information, balancing the public's need for safety information with the benefits of confidentiality to foster a culture within which parties are willing to report and share information with other Member States. However, due to the disparity among Member States in freedom of information laws and protection of safety information, Member States have been reluctant to fully comply with the EPC's reporting requirements.

A commission of Eurocontrol undertook a study to determine impediments to reporting and sharing information across Member States in the EU.[115] The study found that legal issues, such as national laws allowing for prosecution of individuals in the aviation industry, as well as freedom of information-related laws, directly led to underreporting.

The commission found that the most striking example of legal impediments to candid reporting occurred in the Netherlands, where there was a well-publicized case of air traffic controllers being prosecuted for violations of a national air traffic control law.[116] Rather than protecting incident reports and safety data, as is the case in many Member States, the Dutch Parliament provides prosecutors with access to all information within government-certified safety management systems. The combination of fear of prosecution and the fear that information generated pursuant to SMS through incident reporting could be potentially incriminating evidence has greatly deincentivized SMS reporting in the Netherlands.

Freedom of information laws in many other Member States provide the public with access to any reports or information held by a state entity, which would include SMS information and reports. For example, the Swedish Constitution protects the public's access to government documents, and implementing the EPC's regulatory approach to protect SMS information from disclosures would therefore require a constitutional amendment.[117] Although freedom of information laws do not yet appear to have affected safety reporting in Sweden, Eurocontrol predicts that it is only a matter of time before SMS information is used in a lawsuit, resulting in a reporting climate similar to that of the Netherlands.

Other Member States such as Finland, Denmark, Norway, and the United Kingdom have attempted to strike a balance between protection of SMS data and public access to government information by enacting legislation to exempt safety information from freedom of information requests.[118] In the United Kingdom, legislation requiring incident reporting includes language explicitly requiring that the information be protected and only used for safety objectives. The first two provisions of the relevant article of the United Kingdom's Air Navigation Order pertaining to occurrence reporting state that the objective of the article is to contribute to the improvement of air safety, and that the sole objec-

[112] *Id.*

[113] Council Directive 2003/42/EC, art. 3, art. 5, 2003 O.J. (L 167).

[114] Commission Regulation 1321/2007, art. 2, 2007 O.J. (L 294).

[115] *Legal and Cultural Issues in Relation to ATM Safety Occurrence Reporting in Europe*, Performance Control Commission (Eurocontrol), Article 4.2.3–4.2.4 (Sept. 2006).

[116] *Id.* at 4.2.8–4.2.9.

[117] *Id.* at 4.4.6.

[118] *Id.* at 4.4.5.

tive of occurrence reporting is the prevention of accidents and incidents, and not to attribute blame or liability.[119] The United Kingdom's Air Navigation Order further establishes procedures for protecting confidentiality of reported SMS information.

The discrepancies within the EU with regard to protection of safety information and use of such information in legal proceedings have discouraged Member States from reporting and sharing such safety information with the EU central depository. Even if a Member State has national protections in place with regard to such information, the absence of similar protections in other jurisdictions could lead to damaging disclosure. At a recent EU safety conference, numerous experts and trade groups called upon the EU and individual Member States to enact legislation providing for confidentiality of safety information and the effective sharing of such information among Member States.[120] Without such protections and the establishment of just culture, the meaningful collection, analysis, and sharing of hazard and safety information necessary for the SMS to be effective are significantly reduced.

C. Australia

Australia, like Canada, has privatized the ownership and operation of many of its airports (overseen and regulated by the Australian federal government). Thus, safety data may be protected from disclosure by the individual private airport operators.

Unlike the EU, Australia has adopted a Civil Aviation Safety Regulation that requires all airports to have an SMS in place per the standards set forth in a Manual of Standards.[121] Similar to the EU, the Australian SMS requirements are largely in line with ICAO's requirements. However, the Australian Parliament has acknowledged that there are variations from the ICAO, on which the Australian regulations are controlling.[122]

In Australia, much as in the EU, the largest issue surrounding SMS legislation is the confidentiality and disclosure of hazards and safety information reported and collected pursuant to the SMS. There are three federal agencies involved with safety reporting and investigation: the Australian Transport Safety Bureau (ATSB), Airservices Australia, and Civil Aviation Safety Authority. Australia has established a confidential reporting system, allowing any person having an aviation-related concern to confidentially report the concern to the ATSB.[123] The stated purpose of the reporting system is to identify unsafe procedures and provide information to the aviation industry to facilitate safety awareness and safety action and improvement. The legislation specifically prohibits disclosure of information within the reports made to the ATSB, except in the instance of violations of the criminal code or where necessary to lessen or prevent serious and imminent threat to a person's health or life.[124]

While information disclosed to the ATSB pursuant to the confidential reporting system is protected by legislation, the ATSB, Airservices Australia, and the Civil Aviation Safety Authority are required to share information where necessary to carry out their mandated responsibilities. In recognition of the necessity to preserve the confidentiality and nondisclosure of information, each agency has executed a memorandum of understanding with the other entities with regard to the information to be shared and the use of that information in investigations and proceedings. Within each memorandum, the agencies largely incorporate the protections of the ICAO Chicago Convention and the ATSB regulations.[125]

In addition to confidentiality and disclosure of safety information concerns, there are documented concerns with regard to the concept of the accountable executive and the surrounding liability inherent in such a position. There is literature on this point, however, suggesting that the designation of an accountable executive does not present a novel issue with regard to liability for airport management. Prior to the SMS legislation, numerous officers had been held accountable for safety-related issues under Australian common law.[126] Furthermore, a preexisting statute concerning other aviation-related fields held the chief executive officer accountable for corporate-level safety decisions. In light of the state of the common law and analogous statutes in Australia, the designation of an accountable executive should not alter the level of liability to which a chief executive officer of an Australian airport may be exposed.

V. SMS IN OTHER FIELDS

Other fields have adopted practices and procedures that are either explicitly or implicitly modeled on SMS. Examined below are three different approaches to SMS in nonaviation contexts: patient safety, maritime SMS, and the safety and environmental management systems (SEMS) mandated for the U.S. off-shore oil and gas industry. In each case, there have been industry efforts to implement voluntary SMS programs and federal action

[119] Air Navigation Order, 2005, c.14, § 142 (U.K.).

[120] *See* various presentation materials from Jan. 26, 2011, EU Aviation Safety Conference, available at http://easa.europa.eu/conf2011/, under "Documents." (Last accessed Sept. 14, 2012).

[121] Civil Aviation Regulations 1998, reg. 139 (Austl.).

[122] *Id*.

[123] *Id.*

[124] Air Navigation (Confidential Reporting) Regulations 2006, reg. 13 (Austl.).

[125] *Memorandum of Understanding between the Australian Transport Safety Bureau and the Civil Aviation Safety Authority* (Feb. 2010), http://www.atsb.gov/au/media/1371655/mou_atsb-casa.pdf; *Memorandum of Understanding between the Australian Transport Safety Bureau and Airservices Australia* (Sept. 2010), http://www.atsb.gov.au/media/1543248/mou%20between%20atsb%20and%20airservices.pdf.

[126] *Safety Management and the CEO*, Australian Government Civil Aviation Safety Authority (2008), http://atcvantage.com/docs/CASA_sms-ceo.pdf.

that is either intended to assist in the implementation process, in the case of patient safety, or mandate implementation of SMS, in the cases of the maritime and oil and gas industries. It is also important to note that in each of these three fields, the required safety data and related documentation are not required to be provided to the Federal Government, but instead are maintained by the private entity subject to the regulation and, thus, are not subject to disclosure under FOIA. Further, both the maritime SMS and SEMS regulations provide for the audit of the programs by an independent third party, rather than direct federal audit and investigation.

A. Patient Safety

Following the publication in 1999 of the seminal Institute of Medicine report, *To Err Is Human: Building a Safer Health System*,[127] a number of health care providers determined that a more proactive patient safety system needed to be developed. The healthcare industry looked to aviation safety models to improve patient safety and found that aviation industry leaders "consider safety to be the dominant characteristic of organizational culture."[128]

Health care providers looked to established aviation safety programs, such as the Aviation Safety Reporting System undertaken by NASA, for guidance in enhancing patient safety. In a report generated by the Institute for Health Policy (the Kaiser Report), after a pair of roundtable forums that included participation by both health care and aviation safety experts, the authors from Kaiser Permanente® concluded that a reporting system for voluntary patient safety improvement would be a valuable tool to identify errors and vulnerabilities in the health care system and to learn from those errors to prevent future adverse events.[129] The Kaiser Report recommended building on design elements of ASRS and a prototype patient safety reporting system program of the Department of Veterans Affairs.[130] Among the key design elements of such a program were the following:

- Voluntary reporting of adverse events, close calls, and hazardous conditions to a nonregulatory, national entity.[131]
- Strong confidentiality protections, including an evidentiary privilege protecting data against disclosure and discovery in litigation.[132] Reports will be confidential but not anonymous to allow for follow-up.[133]
- Public access to a de-identified database.[134]
- Expert analysis of reports.[135]
- Separate reporting to appropriate authorities of criminal activity, gross negligence, or professional misconduct.[136]

The Kaiser Report noted that federal action would likely be required to protect such data and to establish such a system. It noted the lack of success by the Joint Commission on Accreditation of Healthcare Organizations (Joint Commission), discussed below, with establishing a sentinel event-reporting system, stemming from concerns regarding confidentiality and protection of data.[137] The Kaiser Report also stated that "any potential increased exposure to fines, law suits, or reprisals will discourage health care professionals from voluntarily reporting close calls and adverse events."[138]

In 1996, the Joint Commission, an independent, nonprofit organization that evaluates and accredits the majority of U.S. health care organizations and programs, initiated a "sentinel event" reporting system for hospitals accredited by it.[139] A sentinel event is defined as one that results in an unanticipated death or major permanent loss of function not related to the natural course of the patient's illness or underlying condition.[140] However, certain other events and near misses were not required to be reported.[141] The Joint Commission's Sentinel Event Policy required that an accredited hospital report each sentinel event and, in addition, within 45 days after the event, submit a thorough "root cause analysis" intended to identify the fundamental systemic elements that underlie the event.[142] The assessment is required to include a detailed review of the circumstances surrounding the event and a proposed action plan.[143] The action plan must include potential strategies and systems changes the organization intends to implement to improve quality and reduce the risk of future comparable errors.[144]

Commentators have noted that few hospitals report sentinel events, and one noted that hospitals "are concerned about the confidentiality of the information and fear that public disclosure of reports may damage their reputation and lead to a decline in business, a loss of

---

[127] National Academy Press 2000, available at http://www.nap.edu/openbook.php?isbn=0309068371.

[128] Wachter, *supra* note 90.

[129] *See* Brian Raymond & Robert Crane, *Design Considerations for a Patient Safety Improvement Reporting System*, Institute for Health Policy, Kaiser Permanente, Apr. 2001.

[130] *Id*. at 10.

[131] *Id*.

[132] *Id*. at 11.

[133] *Id*. at 16.

[134] *Id*. at 14.

[135] *Id*. at 15.

[136] *Id*. at 16.

[137] *Id*. at 1.

[138] *Id*. at 18.

[139] C. Stephen Redhead, *Health Care Quality: Improving Patient Safety by Promoting Medical Errors Reporting*, CRS, RL 31983, updated Mar. 24, 2005, at 12.

[140] *Id.*

[141] Bryan A. Liang & Kristopher Storti, *Creating Problems as Part of the "Solution": The JCAHO Sentinel Event Policy, Legal Issues, and Patient Safety*, 33 JOUR. HEALTH CARE L. 263 (2000).

[142] *Id.*

[143] *Id.*

[144] *Id.*

licensure or accreditation, and litigation."[145] Because there is no privilege protecting the materials provided to the Joint Commission from discovery, organizations fear that they will be required to produce sentinel event documents to an opposing party at trial. As one article put it, "by reporting a sentinel event to the [Joint Commission] and performing a [root cause analysis], a provider effectively could be compiling and delivering the equivalent of a signed admission of liability to the opposing legal counsel."[146] As a result, between January 1995 and March 2000, some 800 sentinel events were reported, compared to approximately 13,000 to 30,000 annual ASRS reports being filed.[147]

Partially in response to the Joint Commission's failure to establish a robust reporting program, and building on the recommendations of the Kaiser Report, Congress enacted the Patient Safety and Quality Improvement Act of 2005 (PSQIA),[148] providing for creation of certified patient safety organizations that may receive and analyze patient safety data.[149] "Patient safety work product" that is either reported to a patient safety organization or "identifies or constitutes the deliberation or analysis of a patient safety evaluation system" is confidential and subject to a strong privilege against disclosure that preempts all inconsistent federal, state, or local law.[150] In an article examining PSQIA and the regulations promulgated in 2008 to effectuate certain of its provisions, a commentator stated that "effective confidentiality, privilege, and other protection of patient safety information is essential to the promotion of medical error reporting. The PSQIA privilege…and the incentives for participation have real value for [health care] providers."[151]

There is evidence that as many as 50 percent to 96 percent of adverse medical incidents are not reported.[152] One study published in 2007 concluded that it is possible to improve reporting rates and diversify the types of incidents reported through various techniques, including education, creation of simplified systems for reporting, and use of an anonymous and de-identified reporting system.[153] As another article noted, nonpunitive, protected, voluntary incident reporting systems in high-risk, nonmedical domains have grown to produce large amounts of essential process information unobtainable by other means.[154] This reporting has led to moving "beyond traditional linear thinking about human error, to analyses of multiple causation at the level of systems."[155]

Another recent commentator has noted, however, that a just culture does not mean a "blame-free culture."[156] He argues that health care providers must balance accountability with fairness. Certain standards are now so widely recognized and efficacious, the commentator argues, that failure to adhere to them should subject violators to some sort of sanctions.[157] To be established as fair and enforceable, however, such standards must be widely accepted, and punishment must be proportional and fair.[158]

B. Maritime SMS

International maritime SMS dates to 1994, when the International Maritime Organization adopted the International Safety Management Code (ISM) as Chapter IX of the International Convention for the Safety of Life at Sea (SOLAS). The United States adopted Chapter IX of SOLAS in 1996.[159]

In May 1997, the U.S. Coast Guard issued an NPRM on implementation standards for SMS.[160] Many trade organizations and other industry participants submitted comments regarding the legal effects of the ISM, including comments concerning the effects that the discoverability of reports and documents generated by the SMS would have in litigation, as well as general comments on the effect of the proposed rules on principles of negligence and liability. Commenting parties specifically requested that the Coast Guard protect any reports or documents resulting from internal audits pursuant to SMS requirements against public disclosure in civil proceedings.[161]

The Coast Guard promulgated the final rule on December 24, 1997, which is codified at 33 C.F.R. Part 96 (Part 96).[162] In the notice accompanying the final rule, the Coast Guard conceded that protecting reports or other documents generated in compliance with the maritime SMS requirements is necessary for the successful implementation of the SMS, but concluded that

[145] Redhead, *supra* note 139, at 12–13.

[146] Liang & Storti, *supra* note 141, at 244.

[147] *Id.*

[148] 42 U.S.C. §§ 299b-21–299b-26.

[149] *See* Charles M. Key, *The Role of PSQIA Privilege in Medical Error Reduction*, 21 HEALTH LAWYER 24 (Oct. 2008).

[150] *Id*. at 25.

[151] *Id*. at 27.

[152] Paul Barach & Stephen D. Small, *Reporting and Preventing Medical Mishaps: Lesson from Non-Medical Near Miss Reporting Systems*, 320 BMJ 320 (Mar. 18, 2000).

[153] Sue M. Evans et al., *Evaluation of an Intervention Aimed at Improving Voluntary Incident Reporting in Hospitals*, 16 QUAL. SAF. HEALTH CARE, 169, 170 (Mar. 4, 2007).

[154] Barach & Small, *supra* note 152, at 763.

[155] *Id*.

[156] Wachter, *supra* note 90.

[157] *Id*. at 1402.

[158] *Id*. at 1403.

[159] 46 U.S.C. ch. 32 (2011).

[160] U.S. Coast Guard, International Management Code for the Safe Operation of Ships and for Pollution Prevention (International Safety Management (ISM) Code), 62 Fed. Reg. 23,705 (proposed May 1, 1997).

[161] *See* U.S. Coast Guard, International Management Code for the Safe Operation of Ships and for Pollution Prevention (International Safety Management (ISM) Code), 62 Fed. Reg. 67492, 67496 (Dec. 24, 1997) ("The comments request that the regulations be amended to prohibit use of these [SMS] records in civil or administrative proceedings.").

[162] *Id*. (now codified at 33 C.F.R. pt. 96 (2011)).

it did not have the authority to afford such protection from disclosure as requested by the commenting parties.[163] The Coast Guard did, however, modify the final rule by adding a footnote to the SMS requirements, which states in part, "[t]he documents and reports required by this part are for the purpose of promoting safety of life and property at sea, as well as protection of the environment."[164] In the "discussion of comments and changes" published in connection with the issuance of Part 96, the Coast Guard stated that the purpose of the footnote is to clarify the Coast Guard's intent with regard to the reporting requirement.[165] As discussed below, courts have looked to this footnote and statement of intent in determining whether reports generated per the requirements of the SMS must be disclosed in litigation.

1. Requirements of Part 96

Part 96 applies to the "Responsible Person," defined as the owner of a vessel, or any other person who has assumed the responsibility for operation of the vessel or has agreed to assume the responsibility for complying with Part 96 with respect to the vessel.[166] The Responsible Person must hold a valid "Document of Compliance," defined as a certificate issued to a company or Responsible Person that complies with the requirements of Part 96 and the ISM.[167] The Coast Guard will issue the Document of Compliance upon the completion of an initial audit.[168] The Document of Compliance is valid for 60 months, subject to an annual verification audit within 3 months of its annual anniversary date.[169]

The Coast Guard may board any vessel operating within waters under the jurisdiction of the United States to determine that valid copies of the Document of Compliance and SMS certificate are on board and that the vessel's crew or shore-based personnel are following the procedures and policies of the SMS while operating the vessel or transferring cargo.[170] The Coast Guard is the only authority that can revoke a Document of Compliance. It may only do so, however, if the annual SMS audit is not completed by the Responsible Person; if major nonconformities are found in the company's SMS during an audit or other inspection; or if the Coast Guard is denied or restricted access to any vessel, record, or personnel of the company at any time necessary to evaluate the SMS.[171]

Part 96 requires that the maritime SMS document include the following for the Responsible Person: 1) safety and pollution prevention policy, 2) functional safety and operational requirements, 3) recordkeeping responsibilities, and 4) reporting responsibilities. Part 96 also requires the SMS to be consistent with the functional standards and performance elements of International Maritime Organization Resolution A.741(18), which includes 1) instructions and procedures to ensure safe operation of ships and protection of the environment in compliance with relevant international and flag state legislation; 2) procedures for internal audits; and 3) designation of a designated person on shore having direct access to the highest levels of management whose responsibility includes monitoring the safety and pollution-prevention aspects of the operation of each ship and ensuring that adequate resources and shore-based support are applied, as required.[172]

Under Part 96, a maritime SMS must include the following functional requirements: 1) a written statement from the Responsible Person stating the company's safety and environmental protection policy; 2) instructions and procedures to provide direction for the safe operation of the vessel and protection of the environment in compliance with the Regulation and applicable international conventions; 3) documents showing the levels of authority between shoreside and shipboard personnel; 4) procedures for reporting accidents, near accidents, and nonconformities with the provisions of the company and vessel's SMS and the ISM; 5) procedures to prepare for and respond to emergency situations by shoreside and shipboard personnel; 6) procedures for internal audits on the operation of the company and vessel's SMS; and 7) procedures and process for management review of company internal audit reports and correction of nonconformities reported.[173]

Part 96 requires that a number of documents and reports be maintained, including 1) safety and environmental policy statements; 2) company responsibilities and authority statements; 3) designation in writing of the person to monitor the SMS for the company and vessel; 4) vessel safety and pollution prevention operation plans and instructions for key shipboard operations; 5) emergency preparedness procedures; 6) reporting procedures on required actions, including nonconformities of the SMS, accidents, and hazardous situations, to the Responsible Person and investigation of reported items with the objective of improving safety and pollution prevention; 7) vessel maintenance procedures verifying that the vessel is maintained in conformity with the rules and regulations and additional requirements established by the company; 8) SMS

[163] *See id*. at 67496,

> The Coast Guard agrees that for a safety management system to work correctly and to be continuously self-improving, it requires the proactive actions of the responsible person to have reported completed on non-conformities and hazardous situations no matter how minor or major, so that management reviews can be completed and corrections made to the safety management system accordingly. However, the Coast Guard cannot provide any protection for these records because to do so would exceed its authority granted in 46 U.S.C. Chapter 32.

[164] 33 C.F.R. § 96.250 (2011).

[165] 62 Fed. Reg. 67492, 67496.

[166] 33 C.F.R. § 96.110, § 96.120.

[167] 33 C.F.R. § 96.120.

[168] 33 C.F.R. § 96.330(c).

[169] 33 C.F.R. § 96.330(f).

[170] 33 C.F.R. § 96.380(a).

[171] 33 C.F.R. § 96.330(g).

[172] 33 C.F.R. § 96.250, tbl. 96.250.

[173] *Id.*

document and data maintenance; and 9) SMS internal audits verifying pollution prevention activities.[174]

2. Legal Issues Regarding Maritime SMS

The major legal issues surrounding the implementation of maritime SMS in the United States include the effect of SMS reporting and audits in creating discoverable records and the effect of Part 96 on negligence and standards of care. These two areas are further addressed below.

a. Discoverability of SMS Documents.—The first major legal issue confronting the maritime industry post-implementation of Part 96 was the discovery in litigation of reports, audits, or other documents produced pursuant to the SMS requirements of Part 96. In recognition of this concern, the Coast Guard issued a circular in March of 1998 addressed to officials enforcing Part 96 that instructs investigating officers only to seek evidence that the certifications required by Part 96 are in force.[175]

In recognition of industry concerns regarding the auditing and recording requirements under Part 96, the Coast Guard proposed a study of the implementation and enforcement of SMS regulations and complying with Part 96 in April of 1999.[176] In the Notice of Meeting, the Coast Guard solicited comments on the legal effects of SMS and answers to specific questions regarding disclosure of reports generated pursuant to the requirements of Part 96.[177]

The notice of meeting and request for comments included references by the Coast Guard to existing protections against discovery and disclosure to third parties, including laws, such as the Privacy Act, protecting certain personal or business information and intellectual property protections for a company's SMS.[178] However, the Coast Guard conceded that the records produced as part of the SMS "…to improve safety may also demonstrate the omission or commission of an act that could be construed as negligent…" and that legal actions could occur as a result of this documentation.[179] The Coast Guard reiterated that legal actions stemming from documentation developed as part of SMS is not the intention of the ISM.[180]

Various courts have pointed to the Coast Guard's declarations of intent and the legislative history behind the ISM and SMS in protecting companies against disclosure and more stringent negligence standards as a result of adoption of Part 96. The principal case in the United States with regard to discovery and disclosure of maritime SMS data is *Eisenberg v. Carnival Corp.*[181] In *Eisenberg*, the plaintiff sued the corporate ship owner for a slip and fall aboard the ship. During the litigation, plaintiff sought production of the accident investigation reports prepared by defendant, claiming that Part 96 vitiates the work-product privilege protecting the defendant from disclosing the reports. The court held that the plain language of Part 96, together with the background and purpose of the ISM Code, reveal that Part 96 "does not require reports to be filed with any particular governmental agency."[182] Rather, Part 96 only requires the defendant to establish a safety management system that meets certain objectives and provides a minimum level of documentation.[183] The key point in *Eisenberg* was whether or not the statute or regulation pursuant to which the accident reports were generated required the party to submit the reports to a governmental agency. Under Part 96, there is no requirement that a ship owner submit accident reports to any governmental agency; instead, Part 96 clearly states that the production of such reports to the ship owner's shore-based and vessel-based personnel is sufficient to meet the requirements of Part 96.[184] The court contrasted the requirements of Part 96 with other statutes or regulations that required submission of the reports to a governmental agency; in that case, the reports were not protected by the work-product privilege and were discoverable.[185]

b. Negligence.—The second major legal issue confronting the U.S. maritime industry post-implementation of Part 96 is the effect that adoption of Part 96 may have on standards of negligence in the maritime industry. The specific industry concerns, as noted in both the federal notices and comments thereto as well as numerous treatises, are that 1) Part 96 may establish a heightened duty of care; and 2) any nonconformity with Part 96 resulting in harm to a party protected by Part 96 may result in negligence *per se*.

When presented with this issue, federal courts have generally held that Part 96 does not alter the long-standing negligence standards under federal law in the maritime industry, pointing again to the legislative history and declarations of intent by the Coast Guard.[186] (As discussed below, however, some *state* courts have found that maritime SMS created a new

---

[174] *Id.*

[175] *Id*. at § 6.B.(2).

[176] U.S. Coast Guard, Study of the Implementation and Enforcement of Safety Management System (SMS) regulations, Complying with the International Safety Management (ISM) Code, Meeting Notice, 64 Fed. Reg. 19,850 (Apr. 22, 1999).

[177] *Id*. at 19852 ("Should the information contained in an SMS be restricted to direct users of the system…and no others?").

[178] *Id*. at 19851.

[179] *Id*.

[180] *Id*.

[181] Eisenberg v. Carnival Corp., No. 07-22058-CIV-Jordan/Torres, 2008 U.S. Dist. LEXIS 56573 (S.D. Fla., July 7, 2008).

[182] *Id*. at 3.

[183] *Id*.

[184] *See* 33 C.F.R. 96.250 and tbl. 96.250 (Safety Management System Documents and Reports), (i)(2) (required to report accidents).

[185] *Eisenberg*, 2008 U.S. Dist. Lexis 56573, at 10, *citing* Goosman v. A. Duie Pyle, Inc., 320 F.2d 45, 53 (4th Cir. 1963).

[186] Johnson v. Horizon Lines, 520 F. Supp. 2d 524 (S.D. N.Y. 2007).

duty on behalf of those injured on board a ship.) It seems that the Coast Guard's declaration of intent has provided some guidance to courts in interpreting the effect of Part 96 on negligence law.

In *Johnson v. Horizon Lines*, a ship's crew member sued the ship and ship owner after falling into an open hatch on the ship's deck. Among other claims, the plaintiff asserted that his injuries were caused by the defendants' violation of the specific provision of Part 96 setting forth the requirements of an SMS.[187] In the decision, the federal court noted that it had not discovered any prior federal decisions on this issue.[188] State cases on the topic generally held that violations of Part 96 require the plaintiff to demonstrate that the defendant violated specific provisions of Part 96 and that those violations caused the plaintiff's injury.[189] The court in *Johnson* held that Part 96 cannot form the basis for negligence *per se* or preclude comparative fault.[190] The court reasoned that Part 96 is cast in general terms that restate well-established principles in American case law and was not meant to change long-established rules governing liability.[191] Rather, the court found that Part 96 was adopted to achieve the goals of international bodies regulating maritime law.[192]

The reasoning behind *Johnson* was affirmed in a subsequent case in which a plaintiff claimed Part 96 created a heightened duty of care and supervision under stevedoring laws.[193] The plaintiff in *Calderon v. Reederei Claus-Peter Offen* was an employee of a stevedore and was injured while loading cargo into the defendant's ship.[194] The plaintiff claimed that Part 96 obligates the ship's crew to supervise loading and unloading of the ship's cargo by a stevedore.[195] The federal court reaffirmed that Part 96 and the defendant's corporate safety manual adopted pursuant to Part 96 do not change the general negligence standard.[196] The court cited *Johnson* in agreeing that the intention of Congress in adopting the ISM Code was to participate with other maritime nations in achieving safety goals, not to change long-established liability law and its allocation in general maritime law.[197]

Contrary to the findings and reasoning of the various federal courts, however, in *Kyles v. E. Car Liners*, the Georgia Court of Appeals held that Part 96 did change the custom and practice in the maritime industry and increased the burden on ship owners to ensure the safety of laborers on ship decks and in ships' holds.[198] In *Kyles*, the plaintiff, an employee of a stevedoring company, was injured while loading cargo aboard the defendant ship owner's ship. The *Kyles* court found that the defendant's knowledge of an unsafe condition and failure to take actions to remedy those conditions gave rise to a factual issue as to whether Part 96 was breached.[199] The case was therefore reversed and remanded to the trial court to determine whether the defendant violated Part 96 and whether the violation proximately caused the defendant's injuries.[200]

Various federal and state courts have provided clarity as to what a plaintiff must prove to state a negligence claim under Part 96. In *Rinker v. Carnival Corp.*, a plaintiff became ill and was treated aboard defendant's ship.[201] The plaintiff alleged that the defendant violated Part 96, which violation caused the plaintiff's injury. In granting the defendant's motion to dismiss, the court reasoned that the plaintiff did not show any authority establishing that Part 96 creates a duty owed to the plaintiff by the defendant and that the plaintiff did not show a proximate causal link between an alleged violation of Part 96 and the injury to the plaintiff.[202] In *Dumitrescu v. General Maritime Management, Inc.*, the court denied plaintiff ship owner's motion for judgment as a matter of law where plaintiff crew member was injured aboard the ship.[203] The court reasoned, based on expert testimony, that the defendant's actions violated Part 96 and that the injuries sustained by plaintiff were foreseeable because they resulted from violations of Part 96.[204]

C. Oil and Gas Industry

The off-shore oil and gas industry has long been subject to voluntary SMS-like guidance, in the form of the American Petroleum Institute's (API) Recommended Practices 75 (RP 75).[205] In October 2010, the U.S. Bureau of Ocean Energy Management, Regulation and

---

[187] *Id*. at 528.

[188] *Id*. at 532.

[189] *See, e.g*., Caraska v. Dep't of Transp., No. 57814-6-I, 2007 Wash. App. LEXIS 2567 (Wash. Ct. App. Sept 4, 2007); Kyles v. E. Car Liners, 266 Ga. App. 784, 598 S.E.2d 353 (2004).

[190] *Johnson*, 520 F. Supp. at 533.

[191] *Id.*

> I do not find in [46 U.S.C. § 3201-3205] or [Part 96] a congressional intent to bring about a sea change in the long-established rules of law which govern liability and its allocation in cases tried under the Jones Act and the general maritime law in the federal courts.

[192] *Id.*

[193] Calderon v. Reederei Claus-Peter Offen, No. 07-61022-CIV-Cohn, 2009 U.S. Dist. LEXIS 97565 (S.D. Fla. Oct. 20, 2009).

[194] *Id.*

[195] *Id*. at 3.

[196] *Id*. at 4.

[197] *Id*.

[198] *Kyles*, 598 S.E.2d 353.

[199] *Id*.

[200] *Id*.

[201] Rinker v. Carnival Corp., 753 F. Supp. 2d 1237 (S.D. Fla. 2010).

[202] *Id*. at 1243.

[203] Dumitrescu v. Gen. Maritime Mgmt., Inc., No. 08 Civ. 5461 (PAC), 2009 U.S. Dist. LEXIS 116581 (S.D.N.Y. Dec. 15, 2009).

[204] *Id*. at 3-4.

[205] API Recommended Practice 75 (SEMP), Sutton Technical Books, *available at* http://www.stb07.com/sems/rp-75-semp.html.

Enforcement (BOEMRE) issued a new regulation requiring off-shore owners, operators, and contractors involved with oil, gas, and sulfur operations to implement a SEMS by November 15, 2011.[206] The SEMS Regulation is based largely on the RP 75 recommendations relating to the creation of a Safety Environmental Management Program (SEMP).

According to the API, RP 75 was organized to be performance based, with progress generally measured annually. RP 75 requires effective communications and a system for establishing continuous improvement. Rather than judging facilities on their direct compliance with a specific standard, facilities are expected to operate in a clean and safe manner. The scope of RP 75 is broad, addressing the identification and management of safety hazards in all stages of off-shore drilling—from design and construction to operation and maintenance. New, existing, or modified drilling and production facilities may be covered by the RP 75 standard. RP 75 requires management to implement a program that meets 12 specified principles.[207]

RP 75 also addresses the role of contractors and the importance they place in safe operations. While RP 75 does not require contractors to create a SEMP, the recommended practice is for contractors to become familiar with operators' SEMPs.

The SEMS Regulation explicitly requires oil, gas, and sulphur operators in the outer continental shelf to develop, implement, and maintain a SEMS by November 15, 2011. The goal of SEMS programs is to promote safety and environmental protection by ensuring that all personnel aboard a facility are complying with identified safety policies and procedures.[208] The SEMS Regulation requires all involved personnel to be trained and have the skills and knowledge to perform their assigned duties. Off-shore operations must have a properly documented SEMS program that meets certain minimum criteria and that is available upon request. The criteria are identical to the RP 75's 12 recommended categories, with the addition of a 13th general requirement and more detailed recordkeeping requirements, and the SEMS Regulation incorporates by reference RP 75.[209]

Management's general responsibilities for SEMS include developing, supporting, continuing to improve, and documenting the program. Management is responsible for the overall success of its SEMS program, and must:

1. Establish goals and performance measures, demand accountability for implementation, and provide necessary resources for carrying out an effective SEMS program.

2. Appoint management representatives who are responsible for establishing, implementing, and maintaining an effective SEMS program.

3. Designate specific management representatives who are responsible for reporting to management on the performance of the SEMS program.

4. At intervals specified in the SEMS program and at least annually, review the SEMS program to determine if it continues to be suitable, adequate, and effective (by addressing the possible need for change to policy, objectives, and other elements of the program in light of program audit results, changing circumstances, and the commitment to continual improvement) and document the observations, conclusions, and recommendations of that review.

5. Develop and endorse a written description of safety and environmental policies and organization structure that defines responsibilities, authorities, and lines of communication required to implement the SEMS program.

6. Utilize personnel with expertise in identifying safety hazards, environmental impacts, optimizing operations, developing safe work practices, developing training programs, and investigating incidents.

7. Ensure that facilities are designed, constructed, maintained, monitored, and operated in a manner compatible with applicable industry codes, consensus standards, and generally accepted practice as well as in compliance with all applicable governmental regulations.

8. Ensure that management of safety hazards and environmental impacts is an integral part of the design, construction, maintenance, operation, and monitoring of each facility.

9. Ensure that suitably trained and qualified personnel are employed to carry out all aspects of the SEMS program.

10. Ensure that the SEMS program is maintained and kept up to date by means of periodic audits to ensure effective performance.[210]

The SEMS Regulation requires that certain safety and environmental information be developed and maintained, such as the elements of a hazard analysis, process flow diagrams, and mechanical design information.[211] Hazard analyses must address hazards of the operation and previous incidents related to the operation. Previous incident information includes whether previous incidents led to civil or criminal penalties. Information regarding control technology and qualitative evaluations of the impact of failure of control systems are also required. The SEMS Regulation specifies that a Job Safety Analysis (JSA) must be developed and identified, describing the steps involved in performing a specific job, the existing or potential hazards associated

[206] 30 C.F.R. § 250.1900, *et seq*., (2012) (the "SEMS Regulations").

[207] API RP.

[208] 42 C.F.R. § 250.1901; *Id.* at § 250.1929. Operators must report the previous calendar year's data, broken down quarterly.

[209] 42 C.F.R. § 250.1904.

[210] *Id*. § 250.1909.

[211] *Id*. § 250.1910.

with each step, and recommendation for actions that will eliminate or reduce these hazards. The supervisor of each task must approve the JSA prior to someone performing the described job.[212]

Like aviation SMS, an important component of the SEMS program is having operators learn from incidents to help prevent similar incidents from happening. The SEMS Regulation requires the establishment of procedures for the investigation of all incidents with serious safety or environmental consequences or that possess the potential for serious safety or environmental consequences. Incident investigations must be initiated as promptly as possible under the circumstances. The incident investigators must be knowledgeable personnel, who in the course of their investigation address the nature of the incident and the contributing factors, and recommend changes. Findings of the investigation must lead to a corrective action program. Part of the corrective action program must include retaining the investigation findings for use in the next hazard analysis, determining and documenting the response to each finding to ensure that corrective actions are completed, and implementing a system that distributes conclusions to appropriate personnel.[213]

The SEMS also mandates that operators develop and implement written management of change procedures. These procedures address modifications associated with equipment, operating procedures, personnel changes, materials, and operating conditions. Contractors are included in the personnel change category. In addition, the operator must develop and implement written operating procedures for each operation addressed in the facility's SEMS program.

The SEMS Regulation addresses the integral role of contractors in off-shore operations. They specifically require safe work practices designed to minimize the risks involved with contractor selection. Operators must document contractor selection criteria, which must include evaluating information regarding the contractor's safety and environmental performance. Operators are tasked with ensuring that contractors have their own written safe work practices, and contractors may (although are not required to) adopt sections of the operator's SEMS program. The operator and contractor's agreement on safety and environmental policies and practices must be documented before the contractor begins working at the operator's facilities.[214]

Each operator's SEMS program must include a training program for all personnel that includes an initial training and requirements to ensure that changes made to procedures, practices, and emergency responses are communicated to personnel.

The SEMS regulations require auditing either by an independent third party or designated qualified personnel. The audit must occur within 2 years of the initial implementation of the SEMS program and at least once every 3 years thereafter. The comprehensive audit must evaluate compliance with all 13 elements of the SEMS Regulation and the RP 75 requirements. Audit plan and procedures must meet or exceed all of the recommendations included in RP 75, Section 12.

VI. LIABILITY AND SMS

Part 139 airports that implement SMS may heighten their risk of liability in several ways. Through the process of identifying hazards and ranking potential safety threats, airports may be increasing their risk of liability for negligence where a threat to safety is identified but not promptly or adequately mitigated. The scope of the SMS adopted by an airport operator may also lead to broadening an airport operator's potential liability. For example, an SMS that includes both the movement areas and the nonmovement areas of a Part 139 airport (which often include significant areas that are leased to third parties and therefore not subject to an airport operator's direct control), or that includes all of the landside operations of an airport, will likely lead to a greater range of persons to whom the airport operator arguably owes a duty of care. Finally, the accountable executive may find that a plaintiff may seek to hold him or her personally liable.

This section examines the potential that SMS could change the way in which airport operators and accountable executives could be held liable under negligence theories. It begins with a brief recap of the elements of the tort of negligence and a consideration of how SMS may affect those elements. It examines the law of three selected states as examples of typical state laws regarding premises liability to determine if, absent SMS, airport operators may already have some duty to seek out hazards and mitigate them.[215] It considers whether adoption of SMS may expand the scope of persons to whom an airport operator may owe a duty of care, and it also considers the impact of SMS on the potential liability of the accountable executive. The section concludes with an examination of several typical exceptions to liability that may be available to government entities, which includes most U.S. airport operators.

A. The Effect of SMS on the Elements of a Negligence Claim

Generally speaking, liability for negligence arises when a party owes others a duty to conform to a standard of conduct for the protection of others from unreasonable risk, and that party breaches that duty, resulting in injury or damage to another.[216] In addition,

[212] *Id.* § 250.1911.

[213] *Id.* § 250.1919.

[214] *Id.* § 250.1914.

[215] It is beyond the scope of this *Legal Research Digest* to undertake a full 50 state survey of the law applicable to airports. Therefore, it was agreed that the laws of Massachusetts, California, and Florida would be surveyed as representative examples of state laws. The law of other jurisdictions may vary, in some cases materially.

[216] *See* PROSSER & KEETON ON TORTS 164–65, § 30 (5th ed. 1984).

negligence has been found where a risk has been identified and where there is an unreasonably great risk of causing damage or injury, and the identified risk is not mitigated.[217] In such cases, the general legal standard is whether a reasonable person would have mitigated the identified risk.[218] If a reasonable person, as determined by the fact finder (generally, a jury) would have undertaken steps to mitigate the identified risk, then the party that failed to mitigate such a risk (the defendant) will generally be found liable to the person injured (the plaintiff).

Implementation of SMS by Part 139 airport operators could lead to increased likelihood of liability for negligence for several reasons. First, SMS arguably creates a new duty to seek out hazards located within the portion of a Part 139 airport subject to the scope of the SMS and to take reasonable actions to mitigate unacceptable risks, thus identifying new dangerous conditions. The SRM process may change what risks are foreseeable because the SRM process is intended to identify otherwise unknown risks, quantify the potential impact of such risks, and seek to mitigate otherwise unacceptable risks. By being on notice of these risks through an SRM analysis, an airport operator arguably has a new or increased duty to persons lawfully at the airport (including, for example, airport tenants, those doing business at the airport, and travelers) to take all reasonable steps to mitigate the identified risk. If the SRM analysis had not been performed, the lack of knowledge of a risk, and thus failure to mitigate it, could be a defense. The scope of an adopted SMS may also expand the scope of persons to whom an airport operator owes a duty to include persons lawfully within portions of the airport that are within the scope of the SMS but leased or otherwise controlled by third parties other than the airport operator.

As noted above, SMS is not intended to lead to mitigation of all identified risks; it is intended to be used in a manner similar to a cost–benefit analysis. SMS is based on the premise that risk cannot be eliminated, only managed. Accordingly, ICAO defines "safety" as "…the state in which the possibility of harm to persons or of property damage is reduced to, and maintained at or below, an acceptable level through a continuing process of hazard identification and safety risk management."[219] However, airport operators are only too aware that where personal injury or significant property damage occurs, a plaintiff will seek to recover damages from all parties remotely related to that incident.

1. Duty to Seek Out Hazards

In states where a property owner must have actual or constructive notice of a defect to be held liable, SMS will likely heighten an airport operator's potential liability. The breadth of an SMS program may heighten the duty of an airport operator to seek out hazards and mitigate unacceptable risks.

To determine whether a property owner has a general duty to seek out and remedy hazards that may cause injury or property damage, the laws of four representative states, Massachusetts, California, Florida, and Wisconsin, were reviewed for this digest. In addition, the law of other jurisdictions was reviewed where there were notable differences from that of the foregoing four states. In all four of these states, property owners have an affirmative duty of reasonable or ordinary care to keep their premises in a reasonably safe condition for lawful visitors and a duty to warn of the unsafe condition. In California, this includes an affirmative duty to inspect or otherwise ascertain the condition of the premises. Both Massachusetts and Florida have adopted a "mode of operation" standard whereby in certain circumstances plaintiffs need not show that owners had actual or constructive knowledge of an unsafe condition, but rather that the owner's mode of operation made the unsafe condition reasonably foreseeable. This standard applies predominantly to supermarkets and restaurants in slip-and-fall cases. It is not strictly limited to those types of owners, however, so it could potentially be used in negligence claims against airport operators. In Wisconsin, however, the state's Safe-Place Statute has been interpreted to require that an employer or owner of a place of employment have actual or constructive notice of an unsafe condition to be liable for injuries resulting from such a condition. The SRM process required by SMS may assist plaintiffs in Wisconsin courts in meeting their obligation to demonstrate an employer's or property owner's actual knowledge of an unsafe condition.

a. Massachusetts.—Property owners in Massachusetts have an affirmative duty of reasonable care to maintain their property "in a reasonably safe condition in view of all the circumstances, including the likelihood of injury to others, the seriousness of the injury, and the burden of avoiding the risk."[220] This duty under this "premises liability" approach does not transform owners into insurers of their property, nor does it impose unreasonable maintenance burdens.[221] It simply

[217] *Id*. at 169, § 31.

[218] *Id*.

[219] *See* ICAO SMM, § 2.2.4.

[220] Sheehan v. Roche Bros. Supermarkets, Inc., 448 Mass. 780, 784, 863 N.E.2d 1276, 1281 (2007), quoting Mounsey v. Ellard, 363 Mass. 693, 297 N.E.2d 43, 52 (1973) (discarding traditional premises liability distinction between licensees and invitees); *see also* Oliveri v. MBTA, 363 Mass. 165, 166–167, 292 N.E.2d 863, 864 (1973),

> The obligation of one who controls business premises is to use due care to keep the premises provided for the use of its patrons in a reasonably safe condition, or at least to warn them of any dangers that might arise from such use, which are not likely to be known to them, and of which the defendant knows or ought to know.

[221] Reardon v. Parisi, 63 Mass. App. Ct. 39, 44, 822 N.E.2d 748, 752 (2005) (relating to an employee's slip and fall on ice on the path between the employee parking lot and the business where she worked), citing *Mounsey*, 297 N.E.2d at 52–53.

requires taking reasonable precautions for the safety of all persons lawfully on the premises.[222]

A recent opinion of the highest Massachusetts court affirmed using the general premises liability standard in cases of "snow or ice, or rust on a railing, or a discarded banana peel," and finding further that for snow and ice, a fact finder will determine what "removal efforts are reasonable in light of the expense they impose on the landowner and the probability and seriousness of the foreseeable harm to others."[223] It is therefore likely that in the SMS context, fact finders in Massachusetts will inquire into the reasonableness of an airport operator's efforts to mitigate risks ascertained via SMS, in light of the expense mitigation imposes and the probability and seriousness of the harm from each risk, when determining whether to impose negligence liability on airports. Thus, while the implementation of SMS may not alter an airport operator's duty, the likelihood that additional hazards will be identified through the SRM process may expand the scope of potential liability.

Massachusetts has also adopted the "mode of operation" approach for store owners, which removes the plaintiff's burden to show the owner's actual or constructive knowledge of an unsafe condition on the premises.[224] Where applicable, a plaintiff may prove knowledge of the unsafe condition by showing only that it was reasonably foreseeable based on the owner's mode of operation (e.g., a slip-and-fall case at a self-service grocery store where loose items can fall to the floor).[225] The trier of fact must still determine whether the owner could reasonably foresee or anticipate the unsafe condition and whether the owner took all necessary reasonable precautions to protect against those risks.[226] Though typically applied to slip-and-fall cases in supermarkets and restaurants, it is possible that the doctrine could be extended to holding airport operators liable for risks that are reasonably foreseeable based on the airport's mode of operation.

b. California.—Property owners in California have statutorily imposed responsibility for injuries sustained on their property due to the owner's negligence in managing the property.[227] The owner has an affirmative duty to exercise ordinary care to keep the premises in a reasonably safe condition, and therefore must inspect the premises or take other proper means to ascertain their condition.[228] If the owner would have discovered the dangerous condition by the exercise of reasonable care, he or she may be liable for injury arising from that condition.[229] Exceptions to this statutory rule require clear support in public policy.[230]

When determining whether such a duty exists in a particular instance, California courts balance 1) the foreseeability of the harm to the plaintiff; 2) the degree of certainty that the plaintiff suffered injury; 3) the closeness of the connection between the owner's conduct and the injury suffered; 4) the moral blame attached to the owner's conduct; 5) the policy of preventing future harm; 6) the extent of the burden on the owner and the consequences to the community of imposing the duty; and 7) the availability, cost, and prevalence of insurance for the risks involved.[231] Owners must warn of a dangerous condition unless it is obvious.[232] However, even if the obviousness obviates the need for a warning, the owner may have a duty to remedy that danger, if it is foreseeable that the danger will cause harm despite its obviousness.[233]

Like Massachusetts, it appears that the affirmative duty to maintain the premises in a safe condition may heighten an airport operator's liability after undertaking the SRM process if new hazards are identified and not mitigated. Adoption of SMS may heighten negligence liability under California law, both to warn of additional dangerous conditions that are identified through the SRM process and, consistent with SMS principles requiring mitigation of unacceptable risks, to remedy those dangers.

c. Florida.—In addition to the traditional elements of negligence, to sustain a claim of premises liability in Florida requires proof of the defendant's possession or control of the premises and notice of the dangerous condition.[234] "It is undisputed that under Florida law, all premises owners owe a duty to their invitees to exercise reasonable care to maintain their premises in a safe condition."[235] This duty is not limited to detecting dan-

---

[222] *Id.* The typical analysis involves a review of the "length of time the condition is present and the opportunity for discovery on the facts of the case." Deagle v. Great Atlantic and Pacific Tea Co., 343 Mass. 263, 265, 178 N.E.2d 286, 288 (1961).

[223] Papadopoulous v. Target Corp., 457 Mass. 368, 384, 930 N.E.2d 142, 154 (2010), citing *Mounsey*, 297 N.E.2d at 53.

[224] *Sheehan*, 863 N.E.2d at 1286.

[225] *Id.*

[226] Although the court in *Sheehan* did not limit its decision to store owners, *see id.* at 1286–87 (referring to "owner," not "store owner," when stating the new rule), the "mode of operation" test has not yet been applied to other businesses or property owners such that it is possible to identify, for example, the specific types of injuries that might result from an airport's "mode of operation."

[227] *See* CAL. CIV. CODE § 1714 (West 2012) ("Everyone is responsible…for an injury occasioned to another by his or her want of ordinary care or skill in the management of his or her property or person.").

[228] Salinas v. Martin, 166 Cal. App. 4th 404, 412, 82 Cal. Rptr. 3d 735, 740 (2008); Swanberg v. Mectin, 157 Cal. App. 3d 325, 330, 203 Cal. Rptr. 701, 704 (1984), citing 4 WITKIN, SUMMARY OF CAL. LAW, TORTS § 592, at 2860 (8th ed. 1974).

[229] *Id.*

[230] *Salinas*, 82 Cal. Rptr. 3d at 740.

[231] *Id.*

[232] *See* Martinez v. Chippewa Enters., Inc., 121 Cal. App. 4th 1179, 1184, 18 Cal. Rptr. 3d 152, 155 (2004).

[233] *Id.*

[234] Lisanti v. City of Port Richey, 787 So. 2d 36, 37 (Fla. Dist. Ct. App. 2001).

[235] Markowitz v. Helen Homes of Kendall Corp., 826 So. 2d 256, 259 (Fla. 2002), quoting Owens v. Publix Supermarkets, Inc., 802 So. 2d 315, 330 (Fla. 2001).

gerous conditions after they occur and then correcting them; it may extend to taking actions to reduce, minimize, or eliminate foreseeable risks before they manifest themselves as particular dangerous conditions.[236]

Thus, like Massachusetts, Florida has adopted a "negligent mode of operation" standard for premises liability.[237] If the evidence establishes a specific negligent mode of operation such that dangerous conditions would arise as a result of the owner's mode of operation, then whether the owner had actual or constructive knowledge of the specific unsafe condition is not an issue.[238] The mode of operation theory of negligence is not unique to a particular business,[239] so it is possible that airport operators could face liability under this theory.

In addition to maintaining the premises in a safe condition, landowners have an affirmative duty to warn invitees of concealed perils.[240] Giving this warning does not absolve the landowner of the obligation to maintain the premises in a safe condition.[241] Thus, like Massachusetts and California, the affirmative duty to maintain the premises in a safe condition may heighten an airport operator's liability after undertaking the SRM process if new hazards are identified and not mitigated.

d. Wisconsin.—Wisconsin's safe-place statute requires that every employer and every owner of a place of employment or public building must construct, repair, or maintain such place of employment or public building as to render the same safe.[242] This duty extends to both employees and "frequenters," defined as others permissibly within the place of employment or public building, and requires that applicable places of employment and public buildings be free from danger to the life, health, safety, or welfare of such persons "…as the nature of the employment, place of employment or public building will reasonably permit."[243] Wisconsin courts have interpreted this requirement to require that "…in order to make an employer [or owner] liable for defects in the nature of repair or maintenance, he should have actual or constructive notice of such defects."[244] Further, the plaintiff bears the burden of proving that the employer or owner had actual or constructive knowledge of the defect,[245] and constructive notice can be found only where the hazard has existed for a sufficient length of time to allow the vigilant owner or employer the opportunity to discover and remedy the situation.[246]

Thus, the implementation of SMS by Wisconsin airport operators may heighten their potential liability under the state's safe-place statute. Unlike states where a property owner has an affirmative duty to seek out and remedy hazards in at least some situations, Wisconsin law does not appear to require such an affirmative act by employers or owners of public buildings. The SRM process of seeking out hazards and developing the predictive risk matrix is likely to assist plaintiffs in meeting their burden of proving that the airport operator had actual knowledge of a defect or other hazard that allegedly caused the injury or damage for which recourse is sought.

2. Scope of Persons Owed a Duty Under SMS

The scope of an adopted SMS may lead to changes in the common-law rule regarding the scope of the persons to whom a landlord owes a duty. The common-law rule is that a lease of real property transfers the rights of the landlord to the tenant for the term of the lease, except as may be expressly set forth in the lease. Thus, absent SMS, the general rule would make the tenant responsible for maintaining premises leased from an airport operator in a safe condition, and the landlord would have little or no common-law duty to persons lawfully within such leased premises.

However, if the SMS adopted by an airport operator does not distinguish between portions of the airport controlled by the airport operator and portions under the control of a third party with respect to the SMS responsibilities of the airport operator, airport operators could be subject to new potential liability for accidents within such leased space. In such a case, an airport operator would have an obligation to undertake an SRM process both for areas under the airport operator's control and for areas leased to others. This requirement may conflict with the terms of existing leases, as the landlord airport operator may have a limited ability to enter onto such property and an even more limited ability to mitigate, or cause the tenant to mitigate, unacceptable risks that are identified through the SRM process. As discussed in Section VIII, it may be possible to mitigate this risk contractually, but until existing agreements expire or are amended, airport operators may be subject to heightened risk of liability that they have little legal or practical ability to control.

3. Liability of the Accountable Executive

Under SMS principles, an accountable executive must be responsible for the implementation and maintenance of an airport's SMS. Thus, the accountable executive may arguably owe a duty to persons who may be lawfully within the portions of the airport subject to SMS to ensure that the airport's SMS effectively identifies and mitigates all unacceptable risks. To the extent

[236] *Id.*

[237] *See id.* at 259; *see also id.* at 263 (also recognizing "burden shifting" in slip and fall cases).

[238] *Id.*, quoting *Owens*, 802 So. 2d at 332.

[239] *Id.* at 260.

[240] Marion v. City of Boca Raton, 47 So. 3d 334, 338 (Fla. Dist. Ct. App. 2010).

[241] *Id.*

[242] WIS. STAT. § 101.11(1).

[243] WIS. STAT. § 101.11(13).

[244] Barry v. Employers Mutual Casualty Co., 245 Wis. 2d 560, 571–572, 630 N.W.2d 517, 523 (2001).

[245] *Id.*

[246] Rizzuto v. Cincinnati Ins. Co., 261 Wis. 2d 581, 595–596, 659 N.W.2d 476, 483 (Ct. App. 2003 (Dist. 1)).

that a person is injured or their property is damaged at an airport, that person may claim that the accountable executive was negligent (for example, by failing to identify a risk, but improperly identifying the severity of the risk, or by failing to effectively mitigate) and is personally liable for the plaintiff's injuries.

In many jurisdictions, a government official is provided with "qualified immunity" and will not be held personally liable for torts when acting in good faith and within the scope of his or her official authority. However, the adoption by many states of tort claims acts, which abrogate to a limited extent the government's historic sovereign immunity, has also thrown common law qualified immunity into doubt in some jurisdictions, as the scope of the qualified immunity now may be determined by the scope of the applicable tort claims act.

For example, in Massachusetts, the state tort claims act has been interpreted to provide immunity to officers and employees of state agencies subject to its coverage, except as specifically set forth in the act.[247] Before the enactment of the Massachusetts Tort Claims Act, public officers were liable for their official actions "…only for their acts of misfeasance in connection with ministerial matters."[248] Where a public official's negligence amounted to no more than an omission or nonfeasance, the official was not liable.[249] Furthermore, public officials were never liable for their decisions made in the exercise of their judgment and discretion and acts performed as a result of such decisions where such decisions were within the scope of his or her duty, authority, and jurisdiction.[250] As stated by the Massachusetts Supreme Judicial Court,

> …if a public officer…is either authorized or required, in the exercise of his judgment and discretion, to make a decision and to perform acts in the making of that decision, and the decision and acts are within the scope of his duty, authority and jurisdiction, he is not liable for negligence or other error in the making of that decision at the suit of a private individual claiming to have been damaged thereby.[251]

Many jurisdictions also expressly permit a public entity to indemnify its officers and employees for their official acts when acting in good faith and within the scope of their authority.

B. Qualified Immunities for Governmental Entities

The vast majority of Part 139 airports are owned and operated by governmental entities, rather than private parties. In many U.S. jurisdictions, governmental entities are afforded immunity from suit for tort under certain circumstances. However, the law can vary significantly from one jurisdiction to another. Originally, most states recognized the law of sovereign immunity under which a governmental entity enjoyed blanket immunity from suit for tort. However, the trend has been for states to adopt tort claims acts that permit limited recovery against governmental entities under specified circumstances. Set forth below is an examination of certain immunities and limitations on liability that are available to governmental entities. As above, we have examined the law of three representative jurisdictions, Massachusetts, California, and Florida, as well as the line of cases in New York arising from the first World Trade Center (WTC) bombing, in 1993.

1. Sovereign Immunity

At common law, states were immune from suit. This was known as sovereign immunity, and was generally extended to the municipalities and agencies of a state. As the form of governmental entities grew more numerous and complex, the law struggled to keep pace. As a result, most states abrogated the common law rule of sovereign immunity, either by statute or by judicial decision. As is discussed below, as a result, a number of states have adopted statutes defining the scope of immunity for state entities and for governmental officials.

For example, in the 1970s, the Massachusetts Supreme Judicial Court announced in a line of cases that, absent legislative action, it would abrogate sovereign immunity.[252] As a result, the Massachusetts Legislature adopted the Massachusetts Tort Claims Act, which limits recovery for persons injured through the negligence of the state, or a municipality or state agency, to a maximum sum and sets forth a series of requirements in order to state such a claim.[253] However, the Act also exempts certain state entities, including the authority that owns and operates several airports in the Commonwealth, from its provisions.[254] Massachusetts courts have interpreted this exemption as making such an excluded entity not eligible for governmental or sovereign immunity, and therefore potentially subject for tort liability.[255]

---

[247] *Cf.* Karlin v. Mass. Turnpike Auth., 399 Mass. 765, 766, 506 N.E.2d 1149, 1150 (1987), interpreting MASS. GEN. LAWS ch. 258. However, note that the Massachusetts Tort Claims Act expressly excludes certain state authorities, including the Massachusetts Port Authority, from the ambit of the Act's provision (MASS. GEN. LAWS, ch. 258, § 1).

[248] Whitney v. Worcester, 373 Mass. 208, 220, 366 N.E.2d 1210, 1217 (1977) (quoting Fulgoni v. Johnston, 302 Mass. 421, 423 (1939)).

[249] *Id.*

[250] *Id.*

[251] Gildea v. Ellershaw, 363 Mass. 800, 820, 298 N.E.2d 847, 859 (1973).

[252] *See* Morash & Sons v. Commonwealth, 363 Mass. 612, 296 N.E.2d 461 (1973), *Whitney*, 373 Mass. 208.

[253] MASS. GEN. LAWS, ch. 258.

[254] *Id.*, § 1.

[255] *Karlin*, 399 Mass. at 766.

2. Tort Claims Acts, Governmental Immunity, and the WTC Cases

As described above, most states have waived their sovereign immunity for tort liability, limiting this waiver by allowing only a limited amount of potential monetary recovery to claimants, and then only after claimants comply with certain procedural requirements. For public entities facing tort liability—either in limited amounts under tort claims laws or in full because they are statutorily excluded from those laws' protections—governmental immunity is a potential alternative defense. Set forth below is an examination of limitations on liability available to governmental entities in three states—Florida, California, and Massachusetts—as well as the complex set of decisions in New York arising from the 1993 WTC bombing that resulted in recognition of limited governmental immunity for the Port Authority of New York and New Jersey (PANYNJ), then the WTC owner. Airport operators may be able to defend alleged negligence in balancing safety risks and implementing safety and security measures as discretionary decision-making, and an exercise of their police power. However, neither Florida nor California have any case law where police power was explicitly used to protect a public agency's safety-related decision-making (as it was in New York, as discussed below).

a. Massachusetts.—As described above, in the face of pressure from the Supreme Judicial Court, the Massachusetts legislature adopted the Massachusetts Tort Claims Act, which provides for limited recovery against state and municipal entities for victims of a tort.[256] However, the Act specifically exempts certain state authorities, including one that owns and operates several Part 139 airports, from its provisions,[257] and the Massachusetts courts have held that such exemption makes such authorities liable without limitation in tort. The former defenses of governmental or sovereign immunity are not available to such authorities.[258]

b. Florida.—Florida's legislature has waived sovereign immunity in tort for the state government and its agencies.[259] In so doing, it placed a monetary cap on tort recovery and allowed state agencies to continue to secure insurance policies.[260] Before filing legal action, a tort claimant must submit a written claim to the appropriate administrative agency within 3 years after such claim accrues.[261]

Public airports and port authorities have been included in this waiver of sovereign immunity.[262] Despite the waiver, governments and government agencies can still avoid tort liability in two relevant ways: first, if the act is a governmental function, making it nontortious, and second, if there was no duty of care owed to an individual claimant (rather than to the public) and no special relationship with that claimant. Florida district courts of appeal disagree over the proper way to determine whether a government agency's act was a governmental function. However, they agree that the police power is a fundamental governmental function, and have protected this power in the form of emergency police discretionary decision-making[263] and regulatory enforcement.[264]

c. California.—In 1963, California made sovereign immunity the rule and government liability the exception with its Tort Claims Act,[265] now referred to as the Government Claims Act (CTCA).[266] Liability must have a statutory basis, either in the CTCA or elsewhere, [267] and the CTCA enumerates an extensive list of immunities for public entities and employees. The CTCA specifically immunizes discretionary decisions.[268]

Notably, the CTCA allows liability, except as provided by statute, for injury caused by the "dangerous condition" of a public entity's property, as long as the claimant can prove the typical elements of a tort claim, and unless the public entity can show the act or omission that created the condition was "reasonable."[269] To pursue a tort or contract lawsuit against a public entity for money or damages, the CTCA requires that a plaintiff first submit a written claim within 6 months (personal injury and property damage) or 1 year (all other claims) after the claim accrues.[270]

Similar to Florida, tort liability in California can be avoided if the public agency has no duty of care to, and no special relationship with, the claimant. California also views police power as an inherent governmental function.

d. WTC Cases.—The chain of decisions in the negligence cases brought against PANYNJ as a result of the

[256] MASS. GEN. LAWS, ch. 258.

[257] *Id*. § 1.

[258] *Karlin*, 399 Mass. at 766.

[259] FLA. STAT. § 768.28 (2011).

[260] *Id*. § 768.28(5), (13).

[261] *Id.* § 768.28(6) (but only 2 years for wrongful death).

[262] *See, e.g.,* Labrada v. Metro. Dade Cnty., 715 So. 2d 1126 (1998) (discussing suit against Metropolitan Dade County as owner/operator of Miami International Airport); Florida Att'y Gen'l, Advisory Legal Op., Sovereign immunity, port authorities, AGO 78-127 (Oct. 30, 1978), *available at* http://myfloridalegal.com/ago.nsf/printview/833E72A570758EF885256593005B59E3.

[263] Laskey v. Martin Cty. Sheriff's Dep't, 708 So. 2d 1013 (Fla. Dist. Ct. App. 1998).

[264] *See, e.g.,* Trianon Park Condo. Assoc. v. City of Hialeah, 468 So. 2d 912 (Fla. 1985); Neumann v. Davis Water & Waste, Inc., 433 So. 2d 559 (Fla. Dist. Ct. App. 1983).

[265] CAL. GOV'T CODE §§ 810–996.6 (2012) ("Claims and Actions Against Public Entities and Public Employers").

[266] *See* City of Stockton v. Superior Court, 42 Cal. 4th 730, 741–42, 171 P.3d 20, 28 (2007).

[267] CAL. GOV'T CODE § 815.

[268] *Id.* § 820.2.

[269] *See id.* at §§ 835–835.4

> The reasonableness of the act or omission that created the condition shall be determined by weighing the probability and gravity of potential injury to persons and property foreseeably exposed to the risk of injury against the practicability and cost of taking alternative action that would not create the risk of injury or of protecting against the risk of injury.

[270] *See id.* § 911.2.

1993 bombing of the WTC provide insight into both the defense of governmental immunity and, as discussed further below, the public interest privilege preventing disclosure in discovery of certain documents. Because the PANYNJ's authorizing statutes waive its sovereign immunity to tort claims, the agency could not assert a sovereign immunity defense to the negligence claims made against it stemming from the 1993 WTC bombing.[271] However, it was held in the WTC cases that statutory waiver of sovereign immunity did not serve to more broadly waive PANYNJ's entitlement to a governmental immunity defense.[272]

In general, New York courts have held that "the mere waiver of sovereign immunity does not preclude a governmental agency from asserting an immunity-based defense where appropriate."[273] Specifically,

> [e]ven when a State is subject to tort liability, it and its governmental agencies are immune to the liability for acts and omissions constituting
>
> (a) the exercise of a judicial or legislative function, or
>
> (b) the exercise of an administrative function involving the determination of fundamental governmental policy.
>
> Consent to suit and repudiation of general tort immunity do not establish liability for an act or omission that is otherwise privileged or is not tortious.[274]

The New York courts relied upon this long-standing principle of common law to protect PANYNJ from tort liability for the 1993 WTC bombing.[275] However, this principle is not the law in all U.S. jurisdictions.[276]

When PANYNJ asserted the governmental immunity defense in the WTC cases, the question became whether the agency exercised a governmental function—the police power—in its actions related to the security of the WTC, or whether the agency acted in its proprietary capacity—as an ordinary landlord—to provide for the safety of its tenants and invitees.[277]

The New York trial court and the intermediate appeals court both analyzed PANYNJ's actions and duties as similar to those of a commercial landlord operating an office building that included a public parking garage. At the 2005 bifurcated trial solely on the issue of liability, the jury found PANYNJ liable for negligently failing to maintain the WTC parking garage in a reasonably safe condition, and apportioned 68 percent of fault to PANYNJ.[278] The New York Supreme Court denied PANYNJ's motion to set aside the verdict, and the Appellate Division unanimously affirmed, stating that the PANYNJ "failed in its capacity as a commercial landlord to meet its basic proprietary obligation to its commercial tenants and invitees reasonably to secure its premises, specifically its public parking garage, against foreseeable criminal intrusion."[279]

In contrast, New York State's highest appellate court employed PANYNJ's use of police powers to analyze its duties and actions relating to ensuring the security, rather than the safety, of those persons using PANYNJ's facilities. On appeal from the Appellate Division's order, the New York Court of Appeals reversed the Appellate Division and held that PANYNJ was entitled to the governmental immunity defense, first, because its security-related acts were within PANYNJ's police power and were thus a governmental function, and second, because PANYNJ utilized discretionary decision-making in the exercise of that police power.[280] The Court of Appeals determined that the acts for which the agency was found liable by the Supreme Court[281] were "not separable from the Port Authority's provision of security at the WTC."[282] Facts in the record

---

[271] *In re World Trade Center Bombing Litig*. (*WTC III*), 3 Misc. 3d 440, 459, 776 N.Y.S.2d 713, 728 (N.Y. Sup. Ct. 2004); *see also* MCKINNEY'S UNCONS. LAWS §§ 7101, 7106 (1979) ("Although the port authority is engaged in the performance of governmental functions," it is liable "in such suits, actions or proceedings for tortious acts committed by it and its agents to the same extent as though it were a private corporation.").

[272] *In re World Trade Center Bombing Litig*. (*WTC IV*), 17 N.Y.3d 428, 443, 957 N.E.2d 733, 742–43, 933 N.Y.S.2d 164, 173 (2011) (holding that neither the plain language nor the legislative history gave any "indication that the statute was meant to effectuate a concomitant, wholesale waiver of governmental immunity").

[273] *WTC IV*, 957 N.E.2d 733, 742–43 (2011).

[274] Restatement (Second) of Torts § 895B (3)(a), (b), (4) (1979). A similar principle holds true for local government entities. *Id.* § 895C (2)(a), (b), (3).

[275] *WTC IV*, 957 N.E.2d at 742–43.

[276] *See, e.g., Karlin*, 399 Mass. at 766.

[277] *See WTC IV*, 957 N.E.2d at 744–49; *WTC III*, 776 N.Y.S.2d at 729–34; *WTC I*, 709 N.E.2d at 458 (referring to "the nuance and subtlety of the continuum of governmental and proprietary functions that may overlap").

[278] *WTC IV*, 957 N.E.2d at 740.

[279] *Id.* (quoting *In re World Trade Center Bombing Litig*. (*WTC V*), 51 A.D. 3d 337, 344 (N.Y. App. Div. 2008)). Under New York law, the "relevant requirement in premises liability actions is ultimately notice, not history"—meaning that the mere fact that an event has not yet occurred on a public entity's premises cannot render that event unforeseeable in a negligence analysis. *See WTC IV*, 957 N.E.2d at 740–41 (quoting *WTC V*, 51 A.D. 3d at 345). Rather, if that event has occurred on a similar premises, or the entity has been informed of a threat of that event, or security analysis is conducted and the event is identified as a risk through that analysis, then the event can be considered "foreseeable." *See, e.g, WTC III*, 776 N.Y.S.2d at 735–36.

[280] *WTC IV*, 957 N.E.2d at 735, 740–41.

[281] *See WTC III*, 776 N.Y.S.2d at 732 (listing alleged acts and omissions).

[282] *WTC IV*, 957 N.E.2d at 746.

> While some of plaintiffs' claims may touch upon the proprietary obligations of a landlord, when scrutinizing the purported injury-causing acts or omissions, they allude to lapses in adequately examining the risk and nature of terrorist attack and adopting specifically recommended security protocols to deter terrorist intrusion. These actions are not separable from the Port Authority's provision of security at the WTC, as the dissent concludes; rather, they were a consequence of the Port Authority's mobilization of police resources for the exhaustive study of the risk of terrorist attack, the policy-based planning of effective counterterrorist strategy, and the consequent allocation of such resources. Thus, the ostensible acts or omissions for which plain-

that evidenced PANYNJ's exercise of police power included its constant communication with federal and state police agencies, involvement of law enforcement personnel in internal investigations, commission of security reports to identify vulnerabilities, and procurement of expert security recommendations.[283] In response to those reports, the PANYNJ's top security officials met with law enforcement personnel to assess safety at the WTC, including safety within the parking garage.[284]

Second, the Court of Appeals found PANYNJ's security decision-making to be discretionary because the determinations its officials made regarding the allocation of police resources "involve[d] reasoned consideration of varying alternatives."[285] For example, the officials rated different locations at the WTC as low- or high-risk for the possibility of terrorist attacks or destruction to property and human life.[286] They also "weighed the costs, benefits, and feasibility of various recommendations" before concluding what security measures to implement.[287] As a matter of policy, the Court continued, "to expose the Port Authority to liability because in the clarity of hindsight its discretionary determinations resulted in harm would engender a chilling effect on government and dissuade public entities from investigating security threats and exercising their discretion."[288]

The courts in both *WTC III* and *WTC IV* relied on *Miller v. State of New York* to provide the legal standard for the dichotomy between a governmental entity's proprietary and governmental responsibilities:

> A governmental entity's conduct may fall along a continuum of responsibility to individuals and society deriving from its governmental and proprietary functions. This begins with the simplest matters directly concerning a piece of property for which the entity acting as landlord has a certain duty of care, for example, the repair of steps or the maintenance of doors in an apartment building. *The spectrum extends gradually out to more complex measures of safety and security for a greater area and populace, whereupon the actions increasingly, and at a certain point only, involve governmental functions, for example, the maintenance of general police and fire protection*. Consequently, any issue relating to the safety or security of an individual claimant must be carefully scrutinized to determine the point along the continuum that the State's alleged negligent action falls into, either a proprietary or governmental category.[289]

To determine in which role PANYNJ acted, the New York courts in the WTC cases focused on "the specific act or omission out of which the plaintiffs' injuries are claimed to have arisen, and the capacity in which that act, or failure to act, occurred."[290]

In jurisdictions where governmental immunity is recognized, the Court of Appeals' reasoning may be transferrable to the SMS context. To craft a successful defense of governmental immunity, an airport operator would need to assert that the specific acts that allegedly caused tortious injury were part and parcel of the operator's exercise of a governmental function. Second, the airport operator would need to prove that those acts were discretionary in nature. Similar to PANYNJ's security operations at the WTC, airport operators' implementation of SMS will "feature[] policy-based decision-making involving due consideration of pertinent factors such as the risk of harm, and the costs and benefits of pursuing a particular allocation of resources."[291] However, each time a public entity is accused of tort liability and asserts the defense of governmental immunity, the courts will be required to inquire into the governmental nature of each of the entity's alleged "precise failures."[292] This individualized inquiry will make predictability for airport operators in ascertaining which of their failures can be defended with governmental immunity (and which cannot) difficult to achieve, as the determination of what risks are "acceptable" to an airport operator will inherently be a policy-based decision involving consideration of factors such as the risk of harm and the costs and benefits of pursuing a particular allocation of resources that may be the subject of second-guessing by plaintiffs and their attorneys.

VII. DATA PROTECTION AND SMS

Because most Part 139 airport operators are state or local governmental entities, the vast majority of commercial service airports in the United States must disclose most information (including safety information) held by those airport operators upon request. As discussed below, state sunshine laws and FOIA generally mandate that all information, data, documents, and other materials (collectively, "information") held by a governmental entity be disclosed upon request, unless such information falls within one of a very few statutorily enumerated exceptions.[293] State sunshine laws are

tiffs seek to hold the Port Authority liable stem directly from its failure to allocate police resources as these failures lie, not within the safety measures that a reasonable landowner would implement, but within security operations featuring extensive counterterrorism planning and investigation that required discretionary decision-making with respect to the strategic allocation of police resources.

[283] *Id.* at 747.

[284] *Id*.

[285] *Id.* at 749.

[286] *Id*.

[287] *Id.* at 750.

[288] *Id*.

[289] Miller v. State of New York, 62 N.Y.2d 506, 467 N.E.2d 493 (1984); *see, e.g., WTC IV*, 957 N.E.2d at 744–45 (quoting *Miller*, 467 N.E.2d at 496).

[290] *WTC III*, 776 N.Y.S.2d at 732 (citing *Miller*, 467 N.E.2d at 497).

[291] *See WTC IV*, 957 N.E.2d at 747.

[292] *See id.* at 745.

[293] *See, e.g.*, 5 U.S.C. § 552(a)(3)(A)

> …except as provided in subparagraph (E), [relating to intelligence agencies] *each agency*, upon request for records which (i)

modeled on the Federal FOIA, although each state's act differs in certain particulars. In general, aviation safety information is not an exception to disclosure under state sunshine laws, other than certain limited statutorily created exceptions. Thus, it is likely that the safety data gathered by Part 139 airports will be disclosable upon request. One strategy, discussed in more detail below and in Section VIII below, is to "de-identify" certain aspects of the data collected before it is recorded, so that the records maintained by the airport operator do not contain certain information, such as the name of the person reporting an incident or the identities of the entities involved in an incident. Thus, although the de-identified data must be disclosed upon request, it would not contain certain deleted identifying information.

It should be noted that as part of the recently adopted FAA Modernization and Reform Act of 2012, Congress expanded the scope of aviation safety data exempt from disclosure under Federal FOIA to include "reports, data, or other information produced or collected for purposes of developing and implementing a safety management system acceptable to the Administrator [of the FAA]."[294] This broad exception evidences a congressional intent and understanding that the protection of aviation safety data from disclosure will promote a more vigorous gathering and submission of such data. The exception has limitations, however, as the new protections only apply to data or other information that is submitted to the FAA voluntarily and that is not required to be submitted to the FAA under any other provision of law. Moreover, these provisions only apply to the Federal FOIA, not to the various cognate state sunshine laws.[295]

As discussed, where data provided is held in confidence, reporting is improved.[296] The success of the ASAP and ASRS programs, through which safety data are not subject to public disclosure and are de-identified before being used, amply demonstrate that reporting increases significantly where data are held in confidence. Furthermore, the requirement that public airport operators provide information on request pursuant to state sunshine laws significantly inhibits most private entities from participation in a voluntary program of self reporting safety-related information to such airport operators. Thus, safety data gathered by airport tenants, such as air carriers and ground handlers, are not likely to be made available to an airport operator absent protection from mandatory disclosure of such data under state sunshine laws. As described above, in Canada, where most large airports are owned and operated by private entities, safety data are more readily shared by tenants. Thus, Canadian safety analysis has the opportunity to review a much greater scope of data for trends.

By stripping out, or de-identifying, certain data that identify the person reporting a hazard or incident or the entities that may have been involved in an incident before such data are recorded in an airport operator's records, an airport operator may be able to encourage more reporting. As discussed in more detail below, information held by a governmental entity, including airport operators, is presumed to be a public record and disclosable. However, where data-gathering processes are established in a manner so that certain identifying data are not recorded, that information will not be disclosable. The disadvantage of this approach, though, is that because such data are not recorded, follow-up with the person reporting and trend analysis showing recurring incidents by the same entity can be difficult.

Set forth below is an examination of both Federal FOIA and the public records or sunshine laws in three states: Massachusetts, California, and Florida. In general, the laws are similar and provide a presumption that data held by a governmental entity will be made available to the public upon request, unless such data are subject to a specific exception. Certain exceptions that may apply to aviation safety data are examined. In addition, certain privileges such as the public interest privilege, a qualified privilege for safety data under federal common law, and the attorney-client privilege are examined to determine if certain aviation safety data may be exempted from disclosure under state or federal public records laws.

Other states, however, may provide for broader exceptions to disclosure that may permit airport operators to protect safety-related data under certain circumstances. For example, the Wisconsin Open Records Act excludes drafts, notes, preliminary computations, and like materials from the definition of "records" subject to

---

reasonably describes such records and (ii) is made in accordance with published rules stating the time, place, fees (if any), and procedures to be followed, *shall make the records available to any person*."

(emphasis added). Section 552(b) goes on to state that § 552 does not apply to matters that are listed under nine separate listed exceptions, most of which are narrowly drawn, including matters that are "specifically exempted from disclosure by statute…provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld." (§ 552(b)(3)). Safety information in general is not a specific exception to the federal FOIA, but § 40123 provides for exceptions to FOIA.

[294] FAA Modernization and Reform Act of 2012, § 310(a), Pub. L. No. 112-95, 126 Stat. 11 (Feb. 14, 2012) (adding new 49 U.S.C. § 44735; see § 44735(b)(4)).

[295] 49 U.S.C. § 44735(a). Note that the Proposed Rule does not require airport operators to submit safety data directly to the FAA.

[296] *See, e.g.,* Werfelman, *supra* note 52 ("the majority of the information on which such [safety] enhancements now depend would not surface at all if not voluntarily disclosed." *Quoting* Independent Review Team, *Managing Risks in Civil Aviation: A Review of the FAA's Approach to Safety*, Sept. 2, 2008); *Id*. at 43 ("The [Flight Safety] Foundation and others have estimated that about 98 percent of the safety information obtained from voluntary disclosure programs would no longer be available if participants were subject to prosecution and penalties.").

the disclosure requirements of the Act.[297] Further, Wisconsin's law has been interpreted to permit custodians of public records to withhold such records under a balancing test where the custodian determines that the disclosure would potentially be more harmful than the presumed benefit of public openness.[298] One factor in such a balancing test is an exception to disclosure under Federal FOIA.[299] Thus, the recent congressional action protecting SMS data from disclosure under FOIA may provide an argument under Wisconsin law for preventing disclosure of such safety data under the Wisconsin Open Records Act. Note, however, that most state sunshine laws provide a presumption that public records should be disclosed, and exceptions to disclosure are generally narrowly interpreted. Airport operators will need to be familiar with the provisions of and exceptions to the sunshine law applicable to their jurisdiction.

A. FOIA and State Sunshine Laws

1. Federal FOIA

The Federal FOIA requires that, with certain specified exceptions, each federal agency, "upon request for records which (i) reasonably describes such records and (ii) is made in accordance with published rules stating the time, place, fees (if any), and procedures to be followed, shall make the records available to any person."[300] FOIA presumes that public records held by a federal agency will be made public, absent a specified exception. Thus, safety data provided to the FAA will be made public upon request, absent a specified exception.

Congress enacted legislation (Section 40123) that protects certain voluntarily-submitted aviation safety- or security-related information from disclosure.[301] The FAA has implemented Section 40123 through regulations.[302] Under those regulations, FAA has adopted several safety programs, notably including ASAP,[303] for air carriers and their employees. As described above, in the most recent FAA reauthorization act, Congress expanded the scope of Section 40123 to exclude a wide variety of voluntarily-provided aviation safety information from disclosure under FOIA, including "reports, data, or other information produced or collected for purposes of developing and implementing a safety management system acceptable to the Administrator [of the FAA]."[304]

Given both the fact that the Proposed Rule does not require data to be provided to the FAA and that the scope of the exception to FOIA for aviation safety data was recently expanded by Congress, the implementation of SMS by Part 139 airports is unlikely to be affected by FOIA.

2. Massachusetts Public Records Law

The Massachusetts law regarding public inspection and copies of records is codified at Massachusetts General Laws ch. 66, Section 10 (2012) (Public Records Law), with associated regulations located at 950 Massachusetts Code of Regulations 32.00–32.09 (2012). The Public Records Law only applies to governmental entities, and the burden lies on each entity to show that the Public Records Law does not apply.[305] Under the Public Records Law, any person with custody of public records must permit any segregable portion of an independent public record to be inspected and examined by any one person, under the custodian's supervision, and must furnish a copy of the record for a reasonable fee.[306] Anyone who requests records under the Public Records Law must pay the actual expenses of any search the custodian performs of the public records.[307] The custodian must comply with or deny a request within 10 days following receipt of the request.[308]

Custodians may not require proof of the requester's identity or require the requester to disclose the reasons for which it seeks access to the records.[309] Therefore, if a record is public, unless an exemption applies, the re-

---

[297] *See* WIS. STAT. 19.32(2) (definition of "Record").

[298] *See* Public Records Law, WIS. STAT. §§ 19.31–19.39, Compliance Outline Aug. 2007, Department of Justice, Attorney General Report 28, http://www.doj.state.wi.us/AWP/2007OMCG-PRO/2007_PR_Outline.pdf.

[299] *Id*.

[300] 5 U.S.C. § 552(a)(3)(A).

[301] *See* 49 U.S.C. § 40123(a),

> Notwithstanding any other provision of law, neither the Administrator of the Federal Aviation Administration, nor any agency receiving information from the Administrator, shall disclose voluntarily-provided safety or security related information if the Administrator finds that—(1) the disclosure of the information would inhibit the voluntary provision of that type of information and that the receipt of that type of information aids in fulfilling the Administrator's safety and security responsibilities; and (2) withholding such information from disclosure would be consistent with the Administrator's safety and security responsibilities.

[302] *See* 14 C.F.R. pt. 193 (Protection of Voluntarily Submitted Information).

[303] *See* FAA Order 8000.82 Designation of Aviation Safety Action Program (ASAP) Information as Protected from Public Disclosure Under 14 CFR Part 193 (Sept. 3, 2003) ("Order 8000.82").

[304] FAA Modernization and Reform Act of 2012, § 310(a), Pub. L. No. 112-95, 126 Stat. 11 (Feb. 14, 2012) (adding new 49 U.S.C. § 44735; see § 44735(b)(4)).

[305] A GUIDE TO THE MASSACHUSETTS PUBLIC RECORDS LAW 5, www.sec.state.ma.us/pre/prepdf/guide.pdf (hereinafter, "GUIDE"); *see* 950 MASS. CODE REGS. 32.03 (defining governmental entity as "any authority established by the General Court to serve a public purpose, any department, office, commission, committee, council, board, division, bureau, or other agency within the Executive Branch of the Commonwealth, or within a political subdivision of the Commonwealth").

[306] MASS. GEN. LAWS ch. 66, § 10(a).

[307] *Id.* at 32.08(1).

[308] *Id*. at 10(b).

[309] 950 MASS. CODE REGS. 32.05(5).

quest for the record must be honored—even if made for a commercial purpose or to assist the requester in a lawsuit against the record holder.[310]

If the custodian denies a request for any portion of records that are not public, he or she must make such denial in writing, setting forth the reasons for the denial, and specifically identifying the exemption in the definition of public records upon which the denial is based. The custodian's failure to make written response within 10 days is deemed a denial.[311] Requests for records may be made orally or in writing, but if denied, only requests submitted in writing can be appealed to the Supervisor of Records.[312]

Public records are broadly defined in Massachusetts as:

> …all books, papers, maps, photographs, recorded tapes, financial statements, statistical tabulations, or other documentary materials or data, regardless of physical form or characteristics, made or received by any office or employee of any agency, executive office, department, board, commission, bureau, division or authority of the commonwealth, or of any political subdivision thereof, or of any authority established by the general court to serve a public purpose….[313]

Certain materials and data are exempt from this definition, including:

> (a) [those] specifically or by necessary implication exempted from disclosure by statute;….
>
> (d) inter-agency or intra-agency memoranda or letters relating to policy positions being developed by the agency; but this subclause shall not apply to reasonably completed factual studies or reports on which the development of such policy positions has been or may be based;…[and]
>
> (n) records including, but not limited to, blue prints, plans, policies, procedures and schematic drawings, which relate to internal layout and structural elements, security measures, emergency preparedness, threat or vulnerability assessments, or any other records relating to the security or safety of persons, buildings, structures, facilities, utilities, transportation or other infrastructure located within the commonwealth, the disclosure of which, in the reasonable judgment of the custodian, subject to review by the supervisor of public records under subsection (b) of section 10 of chapter 66, is likely to jeopardize public safety.[314]

These three exemptions are those most likely to have bearing on the public records airport operators create pursuant to SMS requirements, as discussed below.

a. Statutory Exemption—(26)(a).—Currently no Massachusetts statute specifically exempts records created pursuant to SMS from disclosure under the Public Records Law, so this narrow exemption would not currently apply. However, the recent federal exemption of SMS data from FOIA may allow an argument that Massachusetts state law should follow the federal lead.

b. Policy-Making Exemption—(26)(d).—Also known as the Deliberative Process Privilege, this exemption was included in the Public Records Law instead of and as a rejection of the broader attorney work product privilege.[315] The purpose of exemption (26)(d) is "to foster independent discussions between those responsible for a governmental decision in order to secure the quality of the decision."[316]

If used to protect SMS data, this exemption would only apply to memoranda or correspondence reflecting policy deliberations occurring *before* an airport operator takes a specific policy position regarding SMS risks. Therefore, the exemption could potentially be used to protect memoranda and letters used by the airport operator in developing its SMS program. However, the final program, including decisions and actions taken regarding mitigation, would likely not be exempted from disclosure. In addition, the underlying factual studies and reports—those that collected information and identified risks—would likely not be exempted and would therefore be subject to disclosure.

c. Public Safety Exemption—(26)(n).—Exemption (26)(n) was added in response to the events of September 11, 2001.[317] It is intended to secure the safety of persons and public places by restricting access to records that may have been previously open to public inspection.[318] This exemption affects only public buildings, public transportation, and public areas.[319] The public safety exemption does not allow records custodians to reject outright all requests for the exempt documents; rather, it gives a custodian the right to ask a requester to voluntarily provide information about himself or herself and the reason for the request.[320] The custodian is still prohibited from *requiring* that the requester provide this additional information.[321]

A custodian may deny a public records request under the public safety exception because in his or her "reasonable judgment" the disclosure of the requested records "is likely to jeopardize public safety."[322] Such a denial, which must be in writing and must articulate with specificity the reasons for denial, must also clearly address the factors surrounding the custodian's "reasonable judgment" and why the custodian believes that access to the requested records is "likely to be used" to

---

[310] GUIDE at 7.

[311] *Id*.

[312] *Id.* at 32.05(3), 32.08(2).

[313] MASS. GEN. LAWS ch. 4, § 7(26) (2012).

[314] *Id*.

[315] Suffolk Constr. Co. v. Div. of Capital Asset Mgmt., 449 Mass. 444, 457, 870 N.E.2d 33, 43–44 (2007).

[316] Gen'l Elec. Co. v. Dep't of Envtl. Protec., 429 Mass. 798, 807, 711 N.E.2d 589, 595 (1999).

[317] Supervisor of Public Records, SPR Bulletin No. 04-03 (Apr. 1, 2003), http://www.sec.state.ma.us/arc/arcrmu/rmubul/bul403.htm.

[318] *Id*.

[319] *Id*.

[320] *Id*. at Action 5.

[321] *Id*.

[322] MASS. GEN. LAWS ch. 4, § 7(26)(n).

jeopardize public safety.[323] If the requester provides additional information in response to a denial showing why the public safety would not be in jeopardy, the custodian may reverse the initial denial and grant access to the records.[324]

d. Protective Orders Can Protect Documents from Public Records Law.—The Massachusetts Supreme Judicial Court has ruled that the Public Records Law does not abrogate judicial protective orders.[325] Because the Public Records Law is silent as to protective orders, the Court upheld this "long-standing and fundamental power of the judiciary."[326] Judges may permit intervention if a records requester—who is otherwise uninvolved in the litigation in which the protective order was issued—wishes to challenge the order.[327] Permissive intervention need not be granted in every case where a third party intervenes for this purpose. Rather, a judge may consider factors such as "a party's delay in seeking intervention (and the circumstances of such delay), the number of intervention requests or likely intervention requests, the adequacy of representation of the intervening party's interests, and other similar factors."[328]

If the judge grants permissive intervention, the requester may challenge whether the materials he seeks are validly covered by the standing protective order.[329] The judge undertakes the same inquiry as he or she would into whether to issue a protective order, but assessed at the time of intervention.[330] The judge may therefore consider changed circumstances that may render certain materials no longer validly protected (e.g., material is no longer a trade secret) and consideration of a party's reasonable reliance on the order in producing information it would not otherwise have disclosed.[331]

3. California Public Records Act

The California Public Records Act (CPRA)[332] is similar to the Massachusetts Public Records Law and generally presumes that public records will be made available upon request. Each agency covered by the CPRA must respond to a request for a copy of records within 10 days of receipt of the request, and must make any reasonably segregable portion of a record available for inspection after deleting the portions exempted by law or make a copy of the records available upon payment of fees.[333] Access to records may not be limited based on the purpose of the request alone.[334] If an agency denies a written request for inspection or copies, in whole or in part, the denial must be in writing.[335]

The CPRA defines public records to include "any writing containing information relating to the conduct of the public's business prepared, owned, used, or retained by any state or local agency regardless of physical form or characteristics."[336] Under the CPRA, "writing" is defined as:

> any handwriting, typewriting, printing, photostating, photographing, photocopying, transmitting by electronic mail or facsimile, and every other means of recording upon any tangible thing any form of communication or representation, including letters, words, pictures, sounds, or symbols, or combinations thereof, and any record thereby created, regardless of the manner in which the record has been stored.[337]

The CPRA is meant to be broadly applied, though it specifically exempts from disclosure more categories of documents than do the public records laws of either Massachusetts or Florida. An agency must either justify withholding a record by one of these express exemptions *or* by demonstrating that "on the facts of the particular case the public interest served by not disclosing the record clearly outweighs the public interest served by disclosure of the record."[338] The exemptions are meant to be narrowly construed, and an agency opposing disclosure bears the burden of proving that they apply.[339]

Disclosure of a public record that would otherwise be exempt from disclosure under the CPRA constitutes a waiver of the exemption, unless the record is disclosed in legal proceedings or disclosure is made to a governmental agency that agrees to treat the disclosed material as confidential.[340] Therefore, airport operators in California should exercise care when determining whether to disclose a particular record in response to the first request for such a record, as even if it had satisfied an exemption, that record must thereafter be disclosed to all requesters.

a. Deliberative Process Exemption.—The CPRA exempts from disclosure "[p]reliminary drafts, notes, or interagency or intra-agency memoranda that are not retained by the public agency in the ordinary course of business, if the public interest in withholding those records clearly outweighs the public interest in disclosure."[341] Its purpose is to provide a measure of agency

---

[323] SPR Bulletin No. 04-03, at Action 6-7.

[324] *Id.* at Action 5.

[325] Commonwealth v. Fremont Investment & Loan, 459 Mass. 209, 220, 944 N.E.2d 1019, 1027 (2011)

[326] *Id.* at 1024.

[327] *Id.* at 1026.

[328] *Id*.

[329] *Id*. at 1027.

[330] *Id*.

[331] *Id*.

[332] Codified at CAL. GOV'T CODE §§ 6250–6276.48 (West 2012).

[333] CAL. GOV'T CODE § 6253(a), (b), (c).

[334] CAL. GOV'T CODE § 6257.5.

[335] CAL. GOV'T CODE § 6255(b).

[336] CAL. GOV'T CODE § 6250(e).

[337] CAL. GOV'T CODE § 6250(g).

[338] CAL. GOV'T CODE § 6255(a).

[339] County of Los Angeles v. Super. Ct., 82 Cal. App. 4th 819, 825, 98 Cal. Rptr. 2d 564, 568 (2000).

[340] CAL. GOV'T CODE § 6254.5.

[341] CAL. GOV'T CODE § 6254(a).

privacy for written discourse concerning matters pending administrative action.[342]

If the preliminary materials are retained in the ordinary course of business—if they are not customarily discarded or have not in fact been discarded—they must be disclosed.[343] California airport operators thus may want to consider creating a standard policy for the destruction of preliminary SMS recommendations used to prepare final reports on SMS hazards and mitigation strategies, and ensure that preliminary materials are destroyed in compliance with that policy. To the extent that facts contained in preliminary materials can be severed from the recommendations they juxtapose, those facts must be disclosed.[344]

b. Pending Claims and Litigation Exemption.—Also exempted from disclosure under the CPRA are records pertaining to pending litigation to which the public agency is a party, or to claims brought against public entities and employees, until the pending litigation or claim has been finally adjudicated or otherwise settled.[345] Note that this exemption only runs until the conclusion of the claim or litigation, after which the records become once again subject to disclosure. Only documents specifically prepared for use in litigation are protected from disclosure by this exemption.[346] However, this exemption is more broad than the attorney work product exception (discussed below), in that public agencies may use Section 6254(b) to protect "work product" that nonattorneys generate in anticipation of litigation.[347]

With regard to both the pending claims and attorney client-privilege exemptions (see below), California courts have cautioned that "[n]either the attorney's presence nor the happenstance of some kind of lawsuit may serve as the pretext for secret consultations whose revelation will not injure the public interest."[348] Simply involving an attorney in SMS investigation and decision-making, without otherwise fulfilling the requirements for attorney-client privilege, will not protect SMS records from disclosure.

c. Official Information Privilege.—The CPRA also exempts records whose disclosure is exempted or prohibited by federal or state law, explicitly identifying as exempt the privileges outlined in California's Evidence Code.[349] Agencies can also seek exemptions to disclosure for official information, if disclosure is forbidden by law or if disclosure is against the public interest.[350] Official information is defined as "information acquired in confidence by a public employee in the course of his or her duty and not open, or officially disclosed, to the public prior to the time the claim of privilege is made."[351] An agency could assert this privilege to protect records that, if disclosed, could jeopardize safety, welfare, and security.[352] In light of the congressional exemption of voluntarily provided safety data from the Federal FOIA, California airports may be able to argue that the official information privilege of the CPRA exempts at least certain safety data from disclosure.

d. Miscellaneous Exemptions.—Finally, two miscellaneous exemptions in the CPRA might offer protection from disclosure for SMS records. First, "information security records" may not be disclosed if, on a case-by-case determination, "disclosure of the record would reveal vulnerabilities to, or otherwise increase the potential for an attack on, an information technology system of a public agency."[353] Second, withholding from disclosure of "a risk assessment or railroad infrastructure protection program filed with the Public Utilities Commission, the Director of Homeland Security, and the California Emergency Management Agency…" is permitted.[354] Though this provision does not expressly protect SMS records, the exemption illustrates California's interest in protecting risk analyses and transportation infrastructures for homeland security and emergency management purposes.

4. Florida Public Records Act

Florida has the most strict public records law of the three states surveyed—with civil fines and criminal penalties for violation of its provisions and very few permitted exemptions.[355] Access to public records in Florida is a constitutional right.[356]

Under the Florida Public Records Act, records of public agencies must be made available for inspection or copying at any reasonable time and under reasonable conditions.[357] The agency must acknowledge requests to inspect or copy records promptly and respond to them

[342] Citizens for a Better Env't v. Dep't of Food & Agric., 171 Cal. App. 3d 704, 712, 217 Cal. Rptr. 504, 509 (1985).

[343] *Id.* at 714.

[344] *Id.* at 716–17; cf. Times Mirror Co. v. Super. Ct., 53 Cal. 3d 1325, 1343–44, 813 P.2d 240, 251 (1991) (holding that if facts reflect the deliberative process or are its "functional equivalent," they are exempt).

[345] CAL. GOV'T CODE § 6254(b); *see* CAL. GOV'T CODE §§ 810-998.3 (West 2012) (Claims and Actions Against Public Entities and Public Employees).

[346] *County of Los Angeles*, 82 Cal. App. 4th at 830.

[347] *Id.* at 831.

[348] Register Div. of Freedom Newspapers, Inc. v. Cnty. of Orange, 158 Cal. App. 3d 893, 907, 205 Cal. Rptr. 92, 101 (1984).

[349] CAL. GOV'T CODE § 6254(k).

[350] *See* CAL. EVID. CODE § 1040 (West 2012).

[351] *Id.* § 040(a).

[352] *See County of Los Angeles*, 82 Cal. App. 4th at 835 (citing the overriding public interest in ensuring these qualities for inmates and the deputies working with them).

[353] CAL. GOV'T CODE § 6254.19.

[354] CAL. GOV'T CODE § 6254.23.

[355] *See* FLA. STAT. §§ 119.01–119.15 (2012) ("Florida Public Records Act"). Florida also has an open meetings requirement for public agencies, referred to as the Sunshine Law, and also mandated by its Constitution. *See* FLA. CONST. art. I, § 24(b); FLA. STAT. §§ 286.001–286.29 (2012).

[356] *See* FLA. CONST. art. I, § 24(a).

[357] FLA. STAT. § 119.07(1)(a).

in good faith.[358] When an action is filed to enforce the provisions of the Florida Public Records Act, the court must set an immediate hearing, giving the case priority over other pending cases.[359]

If a Florida governmental agency asserts that all or part of a record is exempt from inspection and copying, it must state the basis of the exemption, including the statutory citation.[360] Upon request, this assertion must be made in writing, stating with particularity the reasons why the record is exempt or confidential.[361] If an exemption applies to only a portion of a record, the exempt portion must be redacted and the remainder of the record must be disclosed.[362]

Any public officer who violates any provision of the Florida Public Records Act commits a noncriminal infraction, punishable by a fine not exceeding $500.[363] Any public officer who willfully and knowingly violates any provision of the Public Records Act commits a misdemeanor in the first degree.[364] If a public officer knowingly violates the disclosure provisions in Section 119.07(1), he or she is subject to suspension and removal or impeachment and, in addition, commits a misdemeanor in the first degree.[365]

a. Security System Plans Exemption.—Security system plans (or portions thereof) for property owned by or leased to the state or any of its political subdivisions, or any privately owned or leased property that are held by an agency, are confidential and exempt from disclosure under the Florida Public Records Act.[366] A "security system plan" includes all:

> a. Records, information, photographs, audio and visual presentations, schematic diagrams, surveys, recommendations, or consultations or portions thereof relating directly to the physical security of the facility or revealing security systems;
>
> b. Threat assessments conducted by any agency or any private entity;
>
> c. Threat response plans;
>
> d. Emergency evacuation plans;
>
> e. Sheltering arrangements; or
>
> f. Manuals for security personnel, emergency equipment, or security training.[367]

Information made confidential or exempt may be disclosed to property owners or leaseholders and to another state or federal agency "to prevent, detect, guard against, respond to, investigate, or manage the consequences of any attempted or actual act of terrorism, or to prosecute those persons who are responsible for such attempts or acts."[368]

b. Building Plans Exemption.—Also exempt from disclosure under the Florida Public Records Act are building plans, blueprints, schematic drawings, and diagrams, including draft, preliminary, and final formats, which depict the internal layout and structural elements of a building, arena, stadium, water treatment facility, or other structure owned or operated by an agency.[369] These records may be disclosed to another governmental entity if necessary for that entity to perform its duties and responsibilities.[370] Any entity or person receiving information exempted as a building plan must maintain its exempt status.[371]

c. The Florida Courts Will Not Create Exemptions to the Florida Public Records Act.—As a final note, Florida courts will not imply an exemption that is not outlined in the Florida Public Records Act.[372] Exemptions to the Act can only be added by "a two-thirds vote of each house [of the Legislature]…provided that such law shall state with specificity the public necessity justifying the exemption and shall be no broader than necessary to accomplish the stated purpose of the law."[373]

B. Qualified Privileges

Courts have recognized certain privileges that prevent disclosure of otherwise disclosable documents in certain instances. These privileges often also prevent the disclosure of such materials in litigation through the discovery process. Described below are three qualified privileges that may be applicable, directly or indirectly, to certain safety data gathered by an airport operator pursuant to its SMS. The first is a qualified immunity for ASAP data that was recognized by a U.S. District Court in Florida. However, it is important to note that more recent cases in other federal district courts have failed to recognize this privilege. The second is the public interest privilege that was recognized by the New York Court of Appeals in the WTC cases. Last, the attorney-client privilege, both under federal law and as interpreted in the states of Massachusetts, California, and Florida, is examined.

1. Qualified Privileges for ASAP Data

The courts are divided on whether ASAP creates a qualified immunity from discovery of ASAP data. In a federal case in Florida, heard before the adoption of Section 40123 or Part 193, the court found that ASAP

[358] FLA. STAT. § 119.07(1)(c).

[359] FLA. STAT. § 119.11(a).

[360] FLA. STAT. § 119.07(1)(d).

[361] FLA. STAT. § 119.07(1)(f).

[362] FLA. STAT. § 119.07(1)(e).

[363] FLA. STAT. § 119.10(1)(a).

[364] FLA. STAT. § 119.10(2)(a).

[365] FLA. STAT. § 119.10(1)(b).

[366] FLA. STAT. § 119.071(3)(a)(2).

[367] FLA. STAT. § 119.071(3)(a)(1).

[368] FLA. STAT. § 119.071(3)(a)(3)(a), (b).

[369] FLA. STAT. § 119.071(3)(b)(1).

[370] FLA. STAT. § 119.071(3)(b)(3)(a).

[371] FLA. STAT. § 119.071(3)(b)(4).

[372] *See* Memorial Hospital-West Volusia, Inc. v. News-Journal Corp., 729 So. 2d 373, 380 (1999) ("[W]e believe that an exemption from public records access is available only after the legislature has followed the express procedure provided in…the Florida Constitution.").

[373] FLA. CONST. art. I, § 24(c).

data was protected from disclosure pursuant to a qualified common-law privilege.[374] In a later case heard in federal court in Kentucky, however, the court interpreted Part 193 as not creating a common-law privilege and permitted discovery of the requested ASAP information.[375] This has led some commentators to call on Congress to enact legislation that expressly creates a qualified privilege against discovery for ASAP data.[376]

In the *Cali* case, litigation arose from the crash of an American Airlines flight on December 20, 1995, near Cali, Columbia.[377] The plaintiffs sought production from American of a series of documents, including a total of 23 documents prepared in connection with the ASAP program.[378] American claimed that such documents were not subject to disclosure, either through the "self-critical analysis privilege" or through a new, common-law privilege protecting such documents.[379] The *Cali* court was not persuaded that the self-critical analysis privilege applied in this context,[380] but it found that, although it was not aware of a state or federal court that had previously recognized a privilege for data developed as part of ASAP, the ASAP documents should be protected from discovery.[381] The *Cali* court stated that

> the ASAP materials in dispute (unlike the vast majority of documents prepared by American in the wake of the crash) were prepared voluntarily, in confidence and for use in a discrete, limited context in cooperation with the FAA and the pilots' union. There is a genuine risk of a meaningful and irreparable chill from the compelled disclosure of ASAP materials in connection with the pending litigation.[382]

However, the *Cali* court stated that this privilege is qualified, rather than absolute.[383] The court found that in this case, the plaintiffs must make a "highly particularized showing of the need for the documents, and establish that the information sought is not known or available to the Plaintiffs," which they had not yet done.[384]

In the more recent *Blue Grass* case, however, the court rejected the defendant's motion to protect ASAP reports from discovery.[385] Like the *Cali* case, *Blue Grass* arose from the crash of an aircraft, in this case operated by Comair while taking off from the Blue Grass Airport in Lexington, Kentucky. The court noted that the defendants had admitted that "Congress did not create a statutory privilege specifically for ASAP or other voluntary safety reports"[386] and concluded that Comair's policy arguments were being made in the wrong forum.[387] The *Blue Grass* court relied upon the language of Section 40123 and Part 193 that permits disclosure of ASAP information pursuant to a court order to find that there is no common-law privilege protecting ASAP data from discovery.[388] The *Blue Grass* court concluded that Comair should implore the FAA or Congress to change the regulations or statute to preclude disclosure to litigants, rather than authorizing disclosure pursuant to a court order, as the regulations do now.[389] Since adoption of Section 40123 and Part 193, the court noted that two other courts have come to the same conclusion regarding the nonexistence of a privilege under Section 40123 as the *Blue Grass* court.[390]

2. WTC Public Interest Privilege

In *In re World Trade Center Bombing Litigation* (*WTC I*), the New York Court of Appeals held as a matter of law that PANYNJ was not required to disclose security-related materials in litigation related to the 1993 WTC bombing.[391] Instead, the court remanded for further judicial in camera review to "weigh whether the particular, requested data are shielded by a public interest privilege against disclosure of confidential governmental communications."[392] The documents at issue were reports and related data in the possession of PANYNJ and a third-party security consultant, including "security audit[s]" that identified "possible vulnerabilities of security systems" at the WTC.[393] Separate inquiries were undertaken by the court when determining whether the public interest privilege attached and whether PANYNJ should be immunized from liability.[394]

Under New York law, the party asserting the public interest privilege must show that "the public interest might be harmed if the sought-after materials were to lose their confidentiality shield, such that, on balance,

---

[374] *See In re Air Crash Near Cali, Columbia on December 20, 1995*, 959 F. Supp. 1529, 1530 (S.D. Fla. 1997) (*Cali*).

[375] *See In re Air Crash at Lexington, KY, Aug. 27, 2006*, 545 F. Supp. 2d 618, 619 (E.D. Ky. 2008) (*Blue Grass*).

[376] *See* Christa Meyer Hinckley, Hays Hettingert & Jeremy E. Juenger, *The Argument for Federal Legislation Protecting the Confidentiality of Aviation Safety Action Program Information,* 75 J. AIR L. & COM. 161 (2010).

[377] *Cali*, 959 F. Supp. at 1530.

[378] *Id.*

[379] *Id*. at 1531.

[380] *Id*. at 1532.

[381] *Id*. at 1535.

[382] *Id*.

[383] *Id*.

[384] *Id*. at 1536–1537.

[385] *Blue Grass*, 545 F. Supp. 2d at 624.

[386] *Id*. at 620.

[387] *Id*. at 621.

[388] *Id*.

[389] *Id*.

[390] *Id*., citing Vinton v. Adam Aircraft Indus., Inc., 232 F.R.D. 650, 665 (D. Colo. 2005) and *In re: Air Crash at Belle Harbor, New York*, 02 MDL 1448, Order dated Aug. 14, 2007, at 13 (S.D.N.Y. 2007).

[391] *In re World Trade Center Bombing Litig*. (*WTC I*), 93 N.Y.2d 1, 4, 709 N.E.2d 452, 453 (1999).

[392] *Id.* at 453–54, 456–57.

[393] *Id.* at 455.

[394] *Id.* at 458 ("Notably, nothing requires a defendant to establish immunity from liability as a prerequisite to qualifying for an otherwise available privilege at the pretrial discovery stage.").

disclosure might produce results more harmful to the public good than beneficial to the private litigating parties."[395] Though it left the final disclosure determination to the lower court, the Court of Appeals stated that PANYNJ's arguments were "vital and, arguably, unassailable in view of the stark specter of worldwide terrorism and domestic efforts to deal with these growing threats to highly visible public targets of terrorist opportunism."[396]

On remand, however, the Appellate Division ordered disclosure of the documents for which PANYNJ sought the protection of the public interest privilege.[397] The court articulated its specific mission as balancing "the [PANYNJ]'s interest in maintaining public safety at the World Trade Center and the plaintiffs' interest in advancing their claims that [PANYNJ] either negligently or recklessly ignored a stated potential risk…."[398] The *WTC II* court denied PANYNJ's first rationale for the privilege—that the materials contained sensitive security information that would be useful to "persons bent on destruction"—because the disclosure would only reveal security vulnerabilities that had already been exploited by terrorists and publicized in the media and at public proceedings.[399] PANYNJ's second rationale for asserting the privilege was that the potential future disclosure of security information could "subconsciously motivate those who prepare such reports to avoid making them 'detailed, unrestrained, and full.'"[400] The *WTC II* court also rejected this argument, stating that the "candor" of government officials would be improved, not impaired, by the knowledge of potential future disclosure.[401] The PANYNJ further argued that even if only portions of a document contained sensitive information, the entire document should be protected because:

> [a]n author of a security analysis in an environment in which the dissection of the document could be anticipated would always have doubts as to whether an *ex post facto* examination of the document to determine which passages will be protected from disclosure would result in an analysis consistent with that of the author.[402]

The court found this logic unpersuasive, instead crediting the plaintiffs' assertion that disclosure benefited the public interest, balancing that interest against the public interest advanced by PANYNJ, and finding proper the disclosure of documents in their entirety.[403]

The public interest, as described by plaintiffs and given credence by the court, was that disclosure would enable holding PANYNJ to task for its breach of its duty of care in ignoring repeated warnings of the substantial risk of the exact type of terrorist act that occurred.[404] Thus, in addition to accepting the plaintiffs' argument that disclosure would motivate improved "performance in [officials'] preparation," the court agreed that the documents were "crucial to the prosecution of [plaintiffs'] claim, which is directly related to the Port Authority's alleged prior awareness of deficiencies in its security system and its alleged failure to address them."[405] The court concluded that if it were to protect the documents and promote candor, potentially limiting PANYNJ's liability in this matter, it would also limit "the incentive provided by the specter of such liability to maintain appropriate security."[406]

In distinguishing this case from one where the public interest privilege was held to shield documents concerning the death of a child, the Court pointed out that "[t]he security analyses at issue here were performed before any potential liability had arisen. Their goal was not to analyze prior mistakes but to recommend future action."[407]

C. Attorney-Client Privilege

Although the majority of data gathered in the development and implementation of an SMS will not have been prepared by an attorney, it is likely that in the initial development of the program, at least some materials will be prepared by an attorney for an airport operator. Set forth below is a brief examination of the federal law relating to the attorney-client privilege, as well as the relevant law of Massachusetts, California, and Florida.

1. Federal Law

The federal standard for attorney-client privilege is articulated in *Upjohn Co. v. United States*, in which the Supreme Court allowed the corporation to invoke the privilege after its counsel developed and circulated a questionnaire to employees in an internal investigation.[408] The Internal Revenue Service later sought ac-

---

[395] *Id.* at 457. The PANYNJ set forth three reasons why the public interest might be harmed:

- The documents, in full or in part, contained confidential information concerning safety or security systems, methods, devices, and practices of vulnerabilities, whose disclosure would endanger lives and property and adversely affect security;
- Their disclosure would inhibit candor among persons engaged in efforts undertaken by government agencies to promote public safety; and
- Disclosure would reveal confidential information regarding criminal activity obtained from law enforcement under a pledge of confidentiality.

[396] *Id*.

[397] *In re World Trade Center Bombing Litig.* (*WTC II*), 263 A.D. 2d 417, 693 N.Y.S.2d 586 (1999).

[398] *Id.* at 420.

[399] *Id.* at 421.

[400] *Id.* at 422–23.

[401] *Id.* at 425.

[402] *Id.* at 423.

[403] *Id*. at 424.

[404] *Id.* at 420.

[405] *Id.* at 425.

[406] *Id.*

[407] *Id.* at 424.

[408] Upjohn Co. v. United States, 449 U.S. 383, 101 S. Ct. 677, 66 L. Ed. 2d 584 (1981).

cess to the questionnaire. The Court ruled that the questionnaire feedback was privileged because it was "made by Upjohn employees to counsel for Upjohn acting as such, at the direction of corporate superiors in order to secure legal advice from counsel."[409]

One classic formulation of the elements necessary to establish the attorney-client privilege is:

> (1) Where legal advice of any kind is sought (2) from a professional legal adviser in his capacity as such, (3) the communications relating to that purpose, (4) made in confidence (5) by the client, (6) are at his instance permanently protected (7) from disclosure by himself or by the legal adviser, (8) except the protection be waived.[410]

Federal attorney-client privilege law will apply to federal question cases handled in the federal courts. However, in federal civil cases based on state law claims, the federal courts apply the law of the forum state. Federal Rule of Evidence 501 (FRE 501) states:

> [The] privilege of a witness, person, government, State, or political subdivision thereof shall be governed by the principles of the common law as they may be interpreted by the courts in the light of reason and experience. However, in civil actions and proceedings, with respect to an element of a claim or defense as to which State law supplied the rule of decision, the privilege of a witness, person, government, State, or political subdivision thereof shall be determined in accordance with State law.

The presence of third parties will generally disrupt the application of attorney-client privilege. However, under certain circumstances, attorneys need the assistance of third parties in order to render advice or assistance to their clients. In these limited circumstances, the presence of individuals such as technical experts, accountants, and investigators will not necessarily destroy the attorney-client privilege.[411]

Federal law recognizes the work product doctrine, which protects from discovery "documents prepared by a party's representative 'in anticipation of litigation.'"[412] Some federal courts have adopted a much narrower definition of the phrase "in anticipation of litigation," holding:

> [i]t is not enough to trigger work product protection that the *subject matter* of a document relates to a subject that might conceivably be litigated. Rather, as the Supreme Court explained, "the literal language of [Rule 26(b)(3)] protects materials *prepared for* any litigation or trial" …It is only work done in anticipation of or for trial that is protected…"[M]aterials assembled in the ordinary course of business, or pursuant to public requirements unrelated to litigation, or for other nonlitigation purposes are not under the qualified immunity…."[413]

[409] *Id*. at 394.

[410] Cavallaro v. United States, 284 F.3d 236, 245 (1st Cir. 2002), quoting 8 J.H. Wigmore, *Evidence* 554, § 2292 (McNaughton rev. 1961).

[411] United States v. Kovel, 296 F.2d 918, 922 (1961).

[412] *See Upjohn*, 449 U.S. at 402.

[413] United States v. Textron Inc., 577 F.3d 21, 30 (1st Cir. 2009).

2. The American Bar Association Model Rules

The American Bar Association's (ABA) Model Rule 1.6 deals with privilege, work product, and confidentiality, and imposes no more obligation on attorneys than that imposed by each state's rules of professional conduct.[414] The Model Rules state that "[a] lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted" because the lawyer reasonably believes disclosure is necessary to "comply with other law or a court order" (among other reasons).[415] Though an attorney's obligation to maintain confidentiality encompasses more information than attorney-client privilege and work product, the Model Rules allow disclosure of all three categories of information "as authorized or required" by the Rules or by other laws that supersede Rule 1.6.[416] Whether a law supersedes Rule 1.6 is a question of law.[417] In general, it is unlikely that the Model Rules of Professional Conduct (or those of individual states) could be used to protect SMS data if a particular state does not exempt that data from disclosure by statute.

3. Massachusetts Attorney-Client Privilege Analysis

In Massachusetts the attorney-client privilege applies to confidential communications between public officers, employees, and governmental entities and their legal counsel undertaken for the purpose of obtaining legal advice or assistance.[418] The Public Records Law does not abrogate the privilege.[419] Though Proposed Massachusetts Rule of Evidence 502(d)(6) allows the attorney-client privilege for public clients only when a court determines that disclosure would "seriously impair the ability of the public officer or agency to process the claim or conduct a pending investigation, litigation, or proceeding in the public interest," that Rule has not yet been adopted.[420] Many states that have adopted versions of Uniform Rule of Evidence 502(d)(6)—to which the proposed Massachusetts rule is identical—have rejected this proposed limitation.[421]

However, the Public Records Law has no express or implied exemption for information protected by the at-

[414] *See* ABA Model Rules of Prof'l Conduct, R. 1.6 (2012).

[415] Model Rules of Prof'l Conduct, R. 1.6(a), 1.6(b)(6) (2012).

[416] *See id*. at cmts. [3], [12].

[417] *See id*. at cmt. [12].

[418] Suffolk Constr. Co. v. Div. of Capital Asset Mgmt., 449 Mass. 444, 449, 870 N.E.2d 33, 38–39 (2007).

[419] *Id.* at 36, 46 ("Nothing in the language or history of the public records law, or in our prior decisions, leads us to conclude that the Legislature intended the public records law to abrogate the privilege for those subject to the statute.").

[420] *Id.* at 40 n.12.

[421] *Id*.

torney work-product doctrine.[422] To the contrary, the Public Records Law reflects the Massachusetts Legislature's "intent to abrogate attorney work-product protections for public records that do not otherwise fall under one of the specified statutory exemptions."[423] Only records contained in the narrower Deliberative Process Privilege exemption of clause (26)(d) will be protected.

Under Massachusetts law, the attorney-client privilege generally arises "when (1) a person seeks advice or assistance from an attorney, (2) the advice or assistance sought pertains to matters within the attorney's professional competence, and (3) the attorney expressly or impliedly agrees to give or actually gives the desired advice or assistance."[424] In Massachusetts state courts, the privilege "extends to all communications made to an attorney or counselor…with a view to obtain his advice and opinion in matters of law, in relation to his legal rights, duties and obligations."[425] The Supreme Judicial Court has ruled that attorney-client privilege applies to public officers, employees, and governmental entities. [426]

Massachusetts courts have distinguished between "legal" advice, which is privileged, and "business" advice, which is not. The test applied in Massachusetts is whether the attorney is performing a lawyer-related function. This may include applying law to a set of facts, reviewing client documents in light of effective laws or regulations, or advising the client about the status of or trend in the law.[427] Documents that typically do *not* receive privileged treatment include "business correspondence; interoffice reports; file memoranda; and minutes of business meetings."[428] Massachusetts does not recognize a general self-critical analysis privilege.[429] In the event that a company conducts an internal investigation without the assistance of an attorney, the results thereof are not protected by attorney-client privilege.[430]

In general, the presence of third parties disrupts the application of attorney-client privilege. In Massachusetts, however, "at times, attorneys need the assistance of third parties in order to render advice or assistance to their clients. In these limited circumstances, the presence of individuals such as technical experts, accountants and investigators does not necessarily destroy the attorney-client privilege."[431]

4. California Attorney-Client Privilege Analysis

The CPRA exempts records whose disclosure is exempted or prohibited by federal or state law, explicitly identifying as exempt the privileges outlined in California's Evidence Code, including the attorney-client privilege.[432] Because attorney work product is also protected under California law, it is exempted from disclosure by Section 6254(k).[433] Protection for work product applies both to writings prepared by a lawyer in anticipation of litigation and to writings prepared by a lawyer while acting in a nonlitigation capacity.[434] However, a plaintiff who has filed suit against a public agency may request public records for use in his or her civil action—even if he or she does so to circumvent the discovery process—and if no independent exemption applies, those documents must be produced.[435]

The California Evidence Code states that the client "has a privilege to refuse to disclose, and to prevent another from disclosing, a confidential communication between client and lawyer."[436] This rule applies to both information communicated *to and from* the attorney. A communication is confidential if it is sent

> in confidence by a means which, so far as the client is aware, discloses the information to no third persons other than those who are present…or those to whom disclosure is reasonably necessary for the transmission of the information or the accomplishment of the purpose for which the lawyer is consulted.[437]

In the event that confidential information is intermixed with unprivileged material, the attorney-client privilege "attaches to a confidential communication between the attorney and the client and bars discovery of

---

[422] *Suffolk*, 870 N.E.2d at 35 (characterizing its decision in Gen'l Elec. Co. v. Dep't of Envtl. Protec., 711 N.E.2d 589 (Mass. 1999)); *see* MASS. R. CIV. P. 26(b)(3) (2012).

[423] *Id.* at 40 n.12.

[424] Devaux v. Am. Home Assurance Co., 387 Mass. 814, 818, 444 N.E.2d 355, 357 (1983).

[425] Hatton v. Robinson, 31 Mass. 416, 421 (1833), quoted by Hanover Ins. Co. v. Rapo & Jepsen Ins. Servs., 449 Mass. 609, 615, 870 N.E.2d 1105, 1111 (2007).

[426] *See Suffolk*. *Suffolk* should be read in contrast to the SJC's previous holding that "where a government agency is the client, the Legislature may prescribe different laws and regulations concerning client confidentiality," including the fact that "public records law reflects Legislature's intent to abrogate attorney work-product protections for public records that…do not otherwise fall under one of the specified statutory exemptions." Gen. Elec. Co. v. Dep't of Envtl. Protection, 429 Mass. 798, 802–803 (1999).

[427] Nat'l Employment Serv. Corp. v. Liberty Mut. Ins. Co., 3 Mass. L. Rep. 221 (1994).

[428] *Id*.

[429] Harris-Lewis v. Mudge, 9 Mass. L. Rep. 572 (1999).

[430] Rhodes v. AIG Domestic Claims, Inc., 20 Mass. L. Rep. 491 (Mass. Super. Ct. 2006)

> If the corporation wished to protect the documents generated by the internal investigation from disclosure in discovery, it would need to direct its attorney to conduct an internal investigation for the purpose of providing legal advice to the company regarding the accident, and have the internal investigation conducted under the direction of that attorney.

[431] Marc C. Laredo, *The Attorney-Client Privilege in the Business Context in Massachusetts*, 87 MASS. L. REV. 143 (2003).

[432] *See* CAL. EVID. CODE § 954 (West 2012) (protecting confidential communications between clients and lawyers); CAL. EVID. CODE § 952 (West 2012) (defining confidential communications).

[433] *See* CAL. CIV. PROC. CODE §§ 2018.020, 2018.030 (West 2012).

[434] *County of Los Angeles*, 82 Cal. App. 4th at 833.

[435] *Id.* at 826.

[436] CAL. EVID. CODE § 954.

[437] CAL. EVID. CODE § 952.

the communication irrespective of whether it includes unprivileged material."[438] The *Costco* court also found that, in the event that the lawyer is acting as a fact-finder instead of a legal adviser, the facts as communicated are protected in the confidential communication.[439]

The California Court of Appeal has expanded the traditional scope of the attorney-client privilege, holding that communications among nonlawyer corporate employees about the company's legal strategy may be privileged if they refer to legal matters, strategy, or pending litigation, even if the communications were not received from, authored by, or sent to lawyers.[440] The case refers clearly to discussion of actual pending litigation, but the scope of the phrase "legal matters" remains an open question. The theory behind the ruling is that not every corporate employee responsible for implementing legal advice given by counsel will meet with attorneys or read explicit directions for that implementation. The court emphasized that the first step is to ask whether the communication discusses legal advice or strategy. If yes, the second step is to discuss whether the communication was "reasonably necessary to the transmission of the information or the accomplishment of the purpose for which the lawyer is consulted," as stated in Section 952 of the California Evidence Code. This case also speaks to the involvement of third persons in attorney-client communications, which is allowed on a "need to know" basis in this context. This holding extends the traditional rule that the privilege is not destroyed if disclosure is reasonably necessary to further the purpose of the legal consultation.[441]

5. Florida Attorney-Client Privilege Analysis

In Florida, public agencies cannot assert attorney-client privilege to hold closed meetings with their attorneys to discuss pending legislation.[442] However, government executives may still meet privately (and confidentially) with their attorneys without violating the Sunshine Law.[443]

By extension, since the Florida legislature did not specifically exempt attorney-client privilege in the Florida Public Records Act, it is likely that public agencies—including airport operators—generally cannot use attorney-client privilege to protect records from disclosure. However, the Florida Public Records Act specifically exempts from disclosure a public record prepared by an agency attorney, or at his or her direction, that reflects a mental impression, conclusion, litigation strategy, or legal theory of the attorney or the agency, and that was prepared exclusively for civil or criminal litigation or for adversarial administrative proceedings, or that was prepared in anticipation of imminent civil or criminal litigation or imminent adversarial administrative proceedings—until the conclusion of the litigation or adversarial administrative proceeding.[444] "Agency attorney" includes an attorney employed or retained by the agency or employed or retained by another public officer or agency to protect or represent the interests of the agency having custody of the record.[445] However, these documents are subject to *in camera* review in any civil action in which an exemption is asserted.[446] If a document or record is improperly withheld by an agency claiming this exemption, the party requesting access will be awarded reasonable attorney's fees and costs.[447]

VIII. STRATEGIES FOR MANAGING LEGAL RISKS DUE TO SMS

As has been discussed in this digest, there are a number of legal issues that are likely to arise when airport operators implement an SMS. These issues include the potential for increased risk of liability in negligence for both the airport operator and the accountable executive tasked with implementing and maintaining SMS, the likelihood that SMS data will not be protected from disclosure under state sunshine laws or from discovery in litigation, and the potential conflicts between the implementation of just culture and state and local law. Although, absent congressional or FAA action limiting such liability and protecting SMS data from disclosure, U.S. airport operators are not likely to completely avoid the legal consequences of implementing SMS, by taking certain steps airport operators may reduce their legal risks.

For many, if not most, Part 139 airport operators, implementing an SMS will be a complex process giving rise to issues well beyond the preparation of an SMS manual and an initial risk assessment. In order to develop an SMS program that is most effective and provides the maximum degree of legal protection, advance planning will be necessary so that an airport operator can coordinate its SMS with applicable legal requirements and with its existing documents, processes, and procedures, as well as those of other governmental units and airport stakeholders. Set forth below are a series of steps that airport operators implementing or

[438] Costco Wholesale Corp. v. Superior Court, 47 Cal. 4th 725, 219 P.3d 736 (Cal. Sup. Ct. 2009).

[439] *Id*.

[440] Zurich Am. Ins. Co. v. Superior Court, 155 Cal. App. 4th 1485, 66 Cal. Rptr. 3d 833 (2007).

[441] *See* Ins. Co. of N. Am. v. Superior Court, 108 Cal. App. 3d 758, 166 Cal. Rptr. 880 (2d Dist. 1980).

[442] Neu v. Miami Herald Pub. Co., 462 So. 2d 821, 824–25 (Fla. 1985) ("[W]e have no constitutional or statutory authority to create an exception to the Sunshine Law for governmental bodies to meet privately with their attorneys to discuss pending litigation.").

[443] *Id.* at 826 (Overton, J., concurring).

[444] FLA. STAT. § 119.071(1)(d)(1).

[445] *Id.*

[446] FLA. STAT. § 119.071(1)(g).

[447] FLA. STAT. § 119.071(1)(d)(2).

considering implementation of SMS may wish to undertake to provide a measure of legal protection.[448]

A. Review of State and Local Law

As noted above, each state's laws with respect to issues critical to SMS differ, often in important respects. It would be beneficial for general counsel to analyze and prepare a summary describing the laws applicable to the airport that may affect implementation of SMS. The airport's SMS can then be designed, to the greatest extent possible, within such legal constraints. These laws would include the local standards for liability for negligence; whether there is a duty for an airport operator to seek out and mitigate hazards, independent of SMS, such as under a premises liability statute; the applicable state and local (if any) sunshine laws and any exceptions to such laws, including the ability to protect the identity of persons reporting incidents and limitations on the ability to de-identify aspects of safety data; record retention requirements; and laws and other restrictions that may affect the implementation of just culture (which may include applicable union contracts).

More specifically, as described in this digest, implementation of SMS may change the legal standards applicable to an airport operator's exposure for liability. Airport operators must understand whether implementation of SMS will alter the airport operator's standard of care under applicable state law. In addition, an understanding of the applicable public records laws would allow the airport operator to design its SMS data collection and retention process to best encourage the reporting and sharing of such data.

One of the fundamental issues that will confront a Part 139 airport operator implementing an SMS is its breadth. If the FAA implements regulations requiring that all participants in the commercial aviation system, including airlines, air traffic control, and airport operators, undertake separate, integrated SMS programs, and if the FAA also provides concrete guidance identifying the boundaries of each of the participants' responsibilities, it will likely be significantly simpler for airport operators to regulate their tenants and others engaged in operations at their airport. However, absent such a comprehensive approach to SMS or the failure to adequately separate SMS responsibilities, airport operators will have to determine the proper scope of their SMS program, including determining whether to require that tenants and others participate in some way. Thus, the breadth of an airport's SMS may include both its geographic reach (i.e., whether or not to include landside as well as airside operations, and with respect to airside, whether all operations or only selected areas), and the scope of those persons and entities that will be expected or encouraged to provide information for inclusion in the airport's SMS database or other safety records.

B. Audit of Applicable Regulatory Documents

Airport operators may have to amend or revise their standard documents in order to implement or include SMS. These documents may include the airport's minimum standards, rules and regulations, standard lease terms, insurance coverages, personnel policies, whistleblower protection rules and programs, and record retention policies. Ideally, this review will be undertaken prior to implementing SMS, so that the SMS can be developed to coordinate with necessary changes. The airport operator should undertake a review of these documents to determine what current provisions may be in conflict with implementation of SMS, as well as which documents would benefit from revision due to implementation of SMS.

For example, an airport operator may be able to limit certain of its potential liability for personal injury or property damage within leased areas or areas at the airport otherwise subject to the control of a third party by revising its minimum standards and standard lease provisions to require all tenants or others that control airport property to permit the airport operator to enter upon such premises for the purpose of conducting SRM processes, and to require such third parties either to undertake mitigation activities recommended as part of the SRM process or to allow the airport operator to perform such mitigation. Such an agreement should also contain a strong self-help provision, consistent with governing law, permitting the airport operator to take such steps as may be necessary in the judgment of the operator to mitigate any such hazard if the tenant does not do so in a reasonable period of time, and allowing the airport operator to charge the cost of such measures back to the tenant. An airport operator will also likely want to review its standard indemnity provisions to ensure that the indemnity provisions apply to actions arising from a failure by a third party to permit or undertake such mitigation.

In general, the airport operator owns and controls the airport and thus has the ability to order its relationship with its tenants and others permitted to operate on the airport through several different means, including agreements voluntarily entered into between the operator and its tenants and service providers, as well as through adoption of minimum standards or airport-wide rules, regulations, and directives. There are, of course, certain legal limits to the requirements that an airport operator may impose upon such entities. These include constitutional limits on the impairment of existing contracts, limitations on the ability of a third

[448] *See also* Peter Kirsch, *Ready, Set, Go: Legal Considerations in Implementing a Safety Management System*, AIRPORT MAGAZINE 26 (Apr./May 2011), for an excellent summary of the preliminary steps that an airport operator may want to undertake prior to implementing SMS. The following recommendations include many of the steps recommended by Mr. Kirsch. *See also* AIRPORT COOPERATIVE RESEARCH PROGRAM, REPORT 1: SAFETY MANAGEMENT SYSTEMS FOR AIRPORTS, Vol. 1: OVERVIEW OF SAFETY MANAGEMENT SYSTEMS FOR AIRPORTS (2007), and AIRPORT COOPERATIVE RESEARCH PROGRAM, REPORT 1: SAFETY MANAGEMENT SYSTEMS FOR AIRPORTS, Vol. 2: GUIDEBOOK (2009) for useful guidance on implementation of SMS.

party to regulate labor arrangements, and FAA contractual requirements that prohibit unjust discrimination.

C. Organizational Review

The requirement that an accountable executive be responsible for the implementation and maintenance of an airport's SMS requires that the airport's organizational chart and personnel structure be examined to determine whether there is a position that can serve in that role and, if not, to identify the position to be tasked with these responsibilities and modify the job description accordingly. With that said, the standard ICAO definition of accountable executive is so broad that it is unlikely that any airport operator will be able to identify a single individual who currently is provided with the full authority to perform the full range of the required duties. For example, airports generally have a governing board with final approval of financial matters and overlapping responsibilities for human resources matters. Nevertheless, identifying a single accountable executive is a critical requirement for the implementation of SMS. It generally will be the person who has control over the airport itself, such as the director of aviation or the chief executive officer of the airport operator.

In addition, the airport operator can take specific steps to help protect the person designated as the accountable executive from personal liability for his or her decisions and actions relating to implementation and maintenance of SMS. Clearly including the requirements of implementing and maintaining SMS in the job description of the accountable executive may provide some level of legal protection to the accountable executive where he or she is able to avail himself or herself of a qualified immunity for public officials for actions and decisions made in good faith and within the scope of his or her authority. In addition, if the airport operator is authorized to indemnify its officers and employees, it may wish to consider specifically amending (or implementing) its indemnity policy to protect the accountable executive for his or her decisions and actions taken in good faith and within the scope of his or her authority. It may also be worthwhile exploring obtaining directors and officers insurance or revising existing coverage to cover this potential liability.

The airport operator will want to review its organizational chart, as well as personnel policies, job descriptions, reporting mechanisms, recordkeeping processes, and other related matters to adapt its administrative structure to its SMS program. Depending on the size and complexity of airport operations, it may be necessary to add additional staff or to assign new duties to existing staff, both relating to the initial implementation of SMS as well as the ongoing SRM processes, such as training, data collection, and analysis and audit of safety data and practices. The airport operator will want to coordinate these functions with its current staff plan.

D. Audit of FAA Approvals

Implementation of SMS will also require advance planning, especially for new capital projects on the airside and for certain changes to rules and regulations, to coordinate the program with existing regulatory requirements. One example is the FAA's Order 5200.11, which is already applicable to large hub airports, and requires that, if the FAA determines a project or other change warrants an SRM assessment, an independent panel (on which the airport operator is likely to have a minority of the participants) must undertake an SRM assessment of such action before it may be commenced. Applicable actions consist of those that could affect the airside or air traffic, such as large capital projects, rule changes, and similar matters. It is possible that this process could require extensive review similar to a state or federal environmental review in cases of large or complex actions. Thus, airport operators may want to consider including the possibility of such a review in project schedules and anticipating the issues that may require review. Although the FAA's project manager will determine the scope of the SRM review of the proposed action, by factoring the SRM process into project development at an early stage, airport operators may be able to better maintain project schedules and anticipate regulatory requirements imposed as a result of the Order 5200.11 review process. By reviewing what governmental approvals may be required, an airport operator should be able to coordinate these approvals with the implementation of its SMS.

E. Assembly of SMS Review Team

Implementation of SMS will generally not be a simple undertaking. Like other major projects, airport operators will likely seek to develop a team-based approach to implementation. Although an airport operator may engage a consultant's assistance with development of SMS, the airport's own staff have the best knowledge of the airport, how it operates, potential hazards and means to mitigate them, and other SMS issues. Thus, an airport operator will likely be best served by beginning with an internal team that includes both senior-level and line-level operating staff, counsel, planners, information technology staff, potentially an internal auditor, and airport users and other stakeholders.

An airport's operational staff are often the drivers for adopting SMS programs. They are generally very knowledgeable about airport operations and existing hazards, and are often passionate about finding ways to prevent injuries from occurring. By ensuring that the airport's internal team includes such staff as well as those persons with a variety of expertise to address the broad range of issues that SMS will affect, the airport operator will likely experience a smoother and better coordinated implementation process.

F. Outline of Development of Initial SMS

An airport operator would be well advised to develop an outline of the program, integrating the results of

several of the above steps, before proceeding to implement SMS. To take one example, the SMS requirement that safety data be collected and analyzed can be implemented in numerous ways. Absent affirmative regulatory action by Congress or the FAA, data collected by airports as part of their SMS will likely be subject to disclosure under state and local sunshine laws. As discussed above, airport operators will need to consult with legal counsel to determine the requirements of the applicable sunshine laws to the data to be gathered and analyzed and to the reporting structure that may be developed. Airport operators can then take actions that are designed to mitigate the disincentives to reporting created by such disclosure.

An airport operator would want to review its existing recordkeeping capacity and consider applicable law regarding disclosure of public records, maintenance of such records, the airport operator's legal ability to de-identify safety data, and its goals for the SMS program before structuring the SMS data collection processes. The airport operator would also want to review its current information technology systems to determine how best to coordinate with the SMS data collection and analysis function and to consider how to structure reporting opportunities to best encourage the reporting of safety data. As discussed above, implementing just culture is likely to lead to more robust data reporting, but there may be legal and other impediments to establishing such a just culture environment at the airport.

G. Data Gathering and Data Protection

Absent federal action to exempt all safety data from both federal and state sunshine laws, airport operators may wish to consider taking some or all of the following steps with respect to SMS data. First, airport operators can de-identify data as it is collected to prevent the public disclosure of either the name of the person reporting the safety data or the identity of the persons or entities described in the report. Although this action may make follow-up more difficult, it is probable that it will increase the likelihood that persons will report incidents and near misses, and it may also encourage tenants and other third parties to share de-identified safety data. Second, airport operators can take steps to adopt just culture. They should seek legal counsel to determine whether applicable state or local law limits the ability of the airport operator to grant immunities from sanctions, at least those that can be imposed by the airport operator, for certain violations of law or negligence. It is also likely that the airport operator's existing internal policies will require revision to provide for just culture through practices and procedures consistent with applicable law that excuse or limit sanctions imposed by the operator for violations of airport rules and regulations or other policies if such violations are promptly reported, were inadvertent or not deliberate, and did not involve a criminal offense or an accident. Third, airport operators should seek legal counsel regarding applicable state and local sunshine laws and, especially, the exceptions to such laws for certain safety or security data that may permit at least some safety-related data gathered under an SMS to be maintained confidentially. Fourth, legal counsel should consider whether the attorney-client privilege is another potential avenue for protecting data from disclosure, recognizing that this is likely to be applicable, at best, to a limited scope of safety data prepared by or for the airport's counsel in connection with such counsel's legal duties. Lastly, airport operators can work with their state legislatures to obtain an exemption from the state's sunshine laws for data gathered pursuant to an SMS.

H. Gap Analysis

The initial step in implementing SMS at most airports will be undertaking a "gap analysis." This step allows the airport operator to review all safety programs and processes already in place and compare that to the full range of activities, programs, and processes required by SMS. As one commentator has noted, this review must be "candid, analytical, non-punitive and practical."[449] As the gaps between the airport's current safety structure and an ideal SMS program are likely to raise questions concerning potential liability, airports should consider assigning this task to the airport's general counsel, perhaps assisted by third-party experts, thereby seeking to protect the analysis under the attorney-client privilege. In all events, legal counsel should be involved during this analysis in order to provide legal advice regarding mitigating short-term liability issues until the gaps identified have been adequately mitigated through the SRM process. Advance planning can assist the airport operator in structuring this process in a manner best designed to seek out and correct gaps that could lead to liability.

I. Hazard Identification and Analysis

It may also be advantageous to perform the initial hazard identification and analysis through subject matter experts subcontracted by the airport operator's legal counsel, thus potentially protecting this data from disclosure, at least initially, as an attorney-client privileged communication. Even if this data is initially protected, it will ultimately be included as part of the airport's risk register, along with the mitigation elements deemed necessary to make identified hazards acceptable risks. Because it seems likely that airport operators will be at greatest risk for liability at the earlier stages of implementing SMS, similar to the exposure during the gap analysis noted above, when the airport operator will be aware of certain previously unidentified and unmitigated risks but may not have been able to undertake the necessary tasks to mitigate them, the most critical period for maintaining safety data in confidence may be this initial period.

J. Risk Mitigation and the Predictive Risk Matrix

It will be important for airport operators to develop a budget for their SMS program that includes funds to

[449] *Id*. at 28.

mitigate previously unidentified risks, as well as funding for the initial development and ongoing elements of the SMS program. Although it seems likely that significant risk mitigation activities may be required at some airports, until the initial hazard identification is undertaken there will likely be no way to accurately estimate the necessary costs. It is likely that the identified risks that remain unmitigated will be reduced over time as the airport operator undertakes mitigation measures. Accordingly, it is likely that the greatest costs associated with undertaking mitigation measures will be in the early years of implementation of an SMS (or application of an SMS to a new area of an airport, if the program is phased in). Thus, airports that adopt SMS will need to commit adequate resources not only to undertake the program itself, but also to mitigate the more significant risks that are identified. Nevertheless, it will be prudent for airport operators to undertake mitigation of newly identified risks as promptly as possible to prevent accidents and incidents from occurring.

The best evidence that an airport operator is acting reasonably, and is therefore not liable for negligence to persons injured or suffering property damage as a result of identified hazards, may be that the airport operator undertook mitigation of such hazards consistent with its SMS program. Returning to the standard definition of negligence, where a risk presenting an unreasonable possibility of causing damage or injury has been identified and not mitigated, the person or entity responsible for such risk may be held liable in negligence to those injured or damaged. If the airport operator can demonstrate that it reasonably determined the risk of a particular hazard occurring and its potential consequences, and then undertook mitigation activities reasonably expected to reduce the risk of such a hazard occurring to an acceptable level, the airport operator can minimize its potential liability. Although the reasonableness of the airport operator's actions will ultimately be determined at a trial by the fact-finder—generally a jury—an airport operator that can demonstrate that it has taken actions consistent with its SMS program will be in a much better position to demonstrate that it acted reasonably and, therefore, was not negligent.

The predictive risk matrix recommended by the FAA[450] and generally developed as a key element of the SRM process can be compared to the "signed admission of liability" that so concerned hospitals subject to the Joint Commission's sentinel event policy.[451] This matrix will clearly set forth those hazards located at an airport that are determined to pose an unacceptable risk, as well as the mitigation steps required to reduce the level of risk to an acceptable level. Should an airport operator fail to promptly undertake such mitigation measures (or to discontinue activities posing an unacceptable level of risk that cannot be adequately mitigated), and injury or damage results from the occurrence of the stated risk, the airport operator may have difficulty avoiding liability to persons lawfully at the airport who are injured or suffer property damage as a result of an identified but unmitigated risk.

However, the opposite is also true to a certain degree. To the extent that an airport operator works promptly and consistently to mitigate identified risks to an acceptable level, it should be able to avail itself of the defense of acting reasonably. The hallmark of SMS is the acknowledgment that it is impossible to completely avoid risk, and that instead, risk must be managed to an acceptable level. This is consistent with the law of negligence, which does not impose liability for all injuries, but requires for liability to be found that a duty to a person be breached and, due to that breach, an injury occur. The duty with respect to airport operations is to take reasonable steps to mitigate identified risks; an operator is not strictly liable to do away with all risk. The difficulty with this reasoning is that the determination of reasonableness is generally left to a jury, which may be influenced by many factors, some of which can be extraneous to the strict application of negligence principles. Nevertheless, by promptly and consistently mitigating identified risks in accordance with its SMS, an airport operator should be able to develop a strong case that, even where a foreseen risk results in injury or property damage, it has acted as a reasonable airport operator would and it is not liable.

Inherent in the SRM process is judgment regarding the likelihood that a given risk will result in an incident and regarding the potential seriousness of the consequences of such an incident. Many mitigation alternatives will require a cost-benefit analysis. If the risk is remote or the potential for injury low, and the cost to mitigate the risk is high, an airport may choose not to mitigate a given risk. In such a case, in the unfortunate event that the identified risk leads to an accident, there will inevitably be second guessing of the decision not to mitigate that risk, and evidence will exist that the airport was both aware of the risk and chose not to correct it.

Airports will need to be rigorous in their analysis of risks that are determined to be remote or that present low risk of harm. Airports should maintain careful records regarding their analysis and any changes in the determination that may be warranted in order to demonstrate the reasonableness of the decision not to undertake mitigation measures. The continuous loop of SRM and the reevaluation of the effectiveness of hazards, risks, and mitigation efforts also provides an ongoing opportunity to demonstrate an airport operator's diligence and reasonableness. These elements of SMS will, however, like all of the SMS process, require consistent application in order to avail the airport operator of the defense of acting reasonably. In addition, an airport operator may help demonstrate its reasonableness by including in its SMS a clear process for categorizing risks and by establishing a clear practice of mitigating risks determined to be above the established threshold. Conversely, where an airport operator demonstrably

[450] *See* Order AC 150/5200-37, ch. 2.

[451] *See* § V.A above, quoting Liang.

fails to mitigate identified risks in accordance with its SMS or otherwise fails to adhere to the policies and provisions adopted in its implemented SMS, it will more likely be found to have acted unreasonably and be held liable where an identified risk results in injury.

K. FAA Approval of SMS

The FAA's approval of an airport operator's SMS may provide strong, independent evidence of the airport operator's reasonableness in the event of an action arising from personal injury or property damage resulting from an identified risk at an airport. As noted above, the determination of what level of risk is reasonable is to some extent subjective. Although an airport operator is likely to demonstrate reasonableness by adhering to its SMS, FAA approval of the SMS program may provide the added benefit of independent review and approval by an outside party with expertise in the field of aviation safety. Thus, obtaining the FAA's approval of the airport's SMS manual and its SMS program may provide an additional, significant benefit beyond maintenance of Part 139 certification.

Evidence that an airport operator has complied with the FAA's guidance, as well as other relevant guidance, regarding SMS will also be important to defending any negligence claims arising from accidents resulting from identified risks. To the extent that the FAA provides guidance regarding which hazards must be mitigated and which risks may be addressed through other means, the FAA's standards will provide strong evidence of reasonableness. Furthermore, to the extent that the FAA develops consistent standards for rating risks and quantifying those risks that must be mitigated versus those risks that are acceptable, airports may be able to obtain some protection from liability where the airport acts consistently in accord with the FAA's guidance.

IX. CONCLUSION

Implementation of SMS could lead to increased possibility of liability for airport operators because the process identifies otherwise unknown risks and quantifies the potential impact of such incidents. By being on notice of these risks through an SRM analysis, an airport operator arguably has a duty to persons lawfully at the airport to take all reasonable steps to mitigate the identified risk. If the SRM analysis had not been performed, the lack of knowledge of a risk, and thus failure to mitigate it, could be a defense in some jurisdictions.

The scope of the area covered by the SMS adopted by Part 139 airport operators could also expand the scope of persons to whom the airport operator arguably owes a duty of care to those persons lawfully within areas of the airport subject to SMS but under the control of a third party, such as portions of the nonmovement area leased to an air carrier or another party. While an airport operator cannot avoid all liability under such circumstances, it can seek to shift this risk contractually back to the tenant through appropriate lease provisions, indemnity provisions, and self-help rights.

Accountable executives may also run the risk of personal liability for decisions made or actions taken in their oversight of the airport's SMS program. However, the law in most jurisdictions will protect a public officer from personal liability for his or her decisions or actions if they are within the scope of the person's authority and made in good faith. Airport operators can take concrete steps to provide some protection to the accountable executive by clearly spelling out his or her duties as accountable executive in the position's job description; by providing the accountable executive with indemnity, if legally permitted; and obtaining directors and officers insurance, if available, to cover such liability.

The most difficult problem confronting airport operators that undertake an SMS will likely be the gathering and protection of data. SMS is founded on the principle that by collecting and analyzing safety data, trends can be spotted and accidents avoided. For this process to work as envisioned, however, there must be a regular and robust flow of data into the system. Studies and experience in other jurisdictions and industries have amply demonstrated that the more difficult it is to protect safety data, the less likely it is that persons will report that data. And as noted by the Flight Safety Foundation with respect to safety data gathered under the ASAP and similar programs, the majority of information on which safety enhancements now depend would not have surfaced at all if not voluntarily disclosed. Airport operators will need to become familiar with the law regarding disclosure of public records, and they would be wise to develop their SMS programs, to the greatest extent possible, to prevent disclosure of such data. Because the vast majority of Part 139 airport operators are governmental entities, and therefore subject to state sunshine laws, SMS safety data will not be likely to be maintained confidentially. Nevertheless, airport operators can take steps, such as de-identifying safety data, implementing elements of just culture, and providing for anonymous reporting, that will encourage reporting of safety data.

Implementation of SMS, like any large new program, will often be a complicated and time-consuming endeavor, especially at large and complex airports. By understanding in advance the legal issues that arise with respect to SMS and developing the airport's SMS in a manner designed to minimize adverse legal consequences, and by adhering strictly to the airport's SMS program's provisions, airport operators have the opportunity to significantly enhance safety at their airport while minimizing the adverse legal consequences of doing so.

ACKNOWLEDGMENTS

This study was performed under the overall guidance of the ACRP Project Committee 11-01. The Committee was chaired by TIMOTHY KARASKIEWICZ, General Mitchell International Airport, Milwaukee, Wisconsin. Members are THOMAS W. ANDERSON, Metropolitan Airports Commission, Minneapolis, Minnesota; CARLENE MCINTYRE, Port Authority of New York & New Jersey, New York, New York; BARRY MOLAR, Unison Consulting, Inc., Wheaton, Maryland; MARJORIE PERRY, Tucson Airport Authority, Tucson, Arizona; E. LEE THOMSON, Clark County, Las Vegas, Nevada; and KATHLEEN YODICE, Yodice Associates, Aircraft Owners and Pilots Association, Washington, DC.

DAPHNE A. FULLER provides liaison with the Federal Aviation Administration, FRANK SANMARTIN provides liaison with the Federal Aviation Administration, MONICA HARGROVE KEMP provides liaison with the Airports Council International-North America, and MARCI A. GREENBERGER represents the ACRP staff.

Transportation Research Board
500 Fifth Street, NW
Washington, DC 20001

ISBN 978-0-309-25877-7

Subscriber Categories: Aviation • Law