



Mind-Alliance

**Enhancing Airport Security
and Emergency Preparedness
with Information Sharing Planning (ISP)**

David Kamien
CEO, Mind-Alliance Systems, LLC
November 2011

Executive Summary

Many different organizations are involved in airport security and emergency response operations. Airports represent a microcosm of society, and include government agencies, security personnel, and business enterprises—all of which must be able to communicate effectively and share information to meet the challenges inherent in the secure operation of the airport and the protection of the public. The diverse organizations at the airport are not part of a hierarchical and unified command with shared doctrine. In order to succeed in airport security, these organizations, agencies, and businesses need to share information, and communicate reliably. This cannot be achieved without the collaborative sharing of information and creation of information sharing plans and procedures in advance of a critical incident. This involves knowledge of each other's tasks, languages, and protocols.

Information Sharing Planning (ISP) is a software-enabled management process focused on specifying information needs and the flow of information essential to achieving the security mission—including which participants should and should not be involved in particular situations. Understanding which information flows are missing or need improvement enables airports to dramatically enhance security and emergency preparedness.

Mind-Alliance works with airports and their consulting and system integration firms to improve security and emergency preparedness via a systematic ISP process to reveal how to enhance information flow between airport stakeholders and their partners.

The Need for Information Sharing Plans

In commercial airports, many different organizations are involved in security and emergency response operations. These typically include:

- Transportation Security Administration (TSA) (e.g., screening passengers and baggage)
- Airfield operations (e.g., preventing unauthorized access to aircraft)
- Airlines (e.g., securing cargo and catering)
- Airport police (e.g., protection and emergency response)
- Firefighters (e.g., fire and HAZMAT response)
- FBI (e.g., counterterrorist incident response)
- U.S. Coast Guard (patrolling the waters around the airport)
- Local police departments in towns around the airport
- Airport vendors (e.g., shops, restaurants, cleaning)

No single agency or role carries responsibility for the command of all aspects of security (including deterrence), emergency preparedness, and rapid incident response. Who responds if perimeter intrusion detection systems detect attackers or if a passenger attempts to detonate explosives? How quickly? A different organization might be responsible depending on the particular type of event or incident. Without proactive information sharing plans, the diffusion of responsibility in the airport environment may undermine security. The only alternative to the establishment of a

hierarchically unified command for all event/incident types is developing unity of effort through joint-planning, clear definitions of roles and task assignments, and effective information sharing. Among other attributes, the flow of information between organizations needs to be:

- Fast/ Timely
- Policy Compliant
- Secure
- Reliable
- Classified Appropriately
- Relevant to Recipient and Situation

Even with traditional and new systems in place (phone, email, websites, Twitter, Wikis, etc.) information doesn't spontaneously flow as needed between people and/or technologies. In order to prevent communication breakdown and promote the information sharing that results in the right information flowing to the right people at the right time via the appropriate means of transmission, organizations need a systematic planning and needs analysis framework. Such a framework must support:

- Analyzing stakeholder information needs associated with events, tasks and decisions relating to threat deterrence, detection, prevention, response, and recovery
- Expressing existing communication protocols in a modeling, visualization, and analysis environment
- Assessing the planned flow of information for compliance with procedures, directives, and policies
- Evaluating the consequences of failing to receive or share information

Information Sharing Planning

Mind-Alliance offers airport security directors an effective way to analyze information requirements and preemptively identify communication issues that need to be fixed via improved procedures, system integration, and new systems. ISP serves as a platform for creating a common language for information sharing.

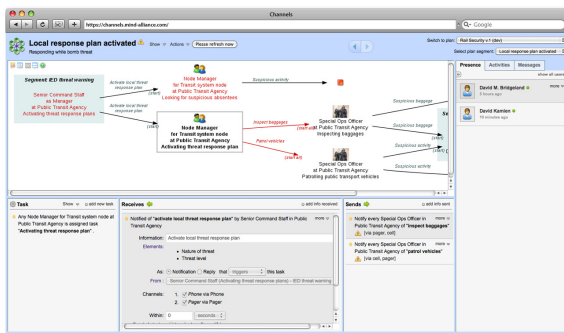
Information Sharing Planning (ISP) is a structured management process developed by Mind-Alliance Systems for planning and modeling the flow of information and presenting visual maps and other artifacts to end-users without a technical background. The ISP planning process is complementary to configuring policies for Physical Security Information Management (PSIM) and Situational Awareness software (i.e., tools that correlate events detected in Access Control, CCTV, and Perimeter intrusion Detection Systems).

ISP provides a practical framework for analyzing and improving the flow of information (internally and with partners) and reducing the likelihood of communication failure that could magnify the impact of adverse events.

ISP enables organizations to associate information flows with assigned tasks, and analyze information sharing requirements in the context of policies that either require or prohibit information sharing. ISP builds awareness between organizations and people that have interrelated tasks. When critical or suspicious events occur, people trained in ISP procedures will know how to share information more effectively.

ISP is implemented with the help of a collaborative software application called CHANNELS. The CHANNELS web application:

- Generates visualizations and analytics to make even complex plans comprehensible
- Supports mission integration
- Presents reports on current information sharing requirements to decision makers
- Automatically detects a wide variety of potential information sharing problems
- Identifies the cascading consequences of failing to share information according to plan
- Illustrates where shared elements of information originate and move through the organization



CHANNELS outputs procedures that can be appended to plans and training material and integrated into other applications. Each time there is a new requirement it can be embodied in procedures, trained, and exercised.

Benefits to Airport Security Directors

Information Sharing Planning with CHANNELS enables airport security directors to evaluate the flow of information between airport security stakeholders, allowing them to identify information flow issues and fix them in order to enhance safety, operational performance, and regulatory compliance. The information flow maps available in CHANNELS reports enable customers to see how to make the flow of vital information faster, policy-compliant, and more resilient.

Security directors can leverage Channels to:

- Plan and assess information flow associated with different security scenarios
- Support the design of new solutions and procedures, prioritized based on mission-driven needs and capability gaps
- Build stronger relationships with partners

Information Sharing Planning with CHANNELS software is an important part of an airport security director's tool chest.

To learn more about **Mind Alliance** visit www.mind-alliance.com or call **1-888-731-6018**.