



White Paper

---

## Information Sharing Planning (ISP)

for Rail Transit Security

---

*“The important lesson learned is that it is highly effective to concentrate on the pre-execution phases of attempted terrorist attacks. Last-line fail-safe measures are critical to thwart undetected plots, as well as induce uncertainty into the terrorist planning process. However, the best way to influence the success or failure of an attack—at the tactical, operational, or strategic level—is to interdict the plot before the terrorists deploy to execute their plan.”*

— Homeland Security Institute Report

David Kamien  
CEO, Mind-Alliance Systems, LLC  
November 2010

## Executive Summary

Securing the passenger rail transit system from terrorist attacks requires coordination and information sharing between regional agencies. By sharing information, regional partners can enhance situational awareness about pre-operational threats and coordinate their protection and prevention missions.

This white paper first articulates the need for developing and exercising regional information sharing plans and procedures between rail transit operators and regional security stakeholders. It then describes the current state of planning commonly found in the United States. Finally, it briefly describes Information Sharing Planning (ISP), a software-enabled business process that all government agencies engaged in rail security need in order to share information effectively, comply with policy, and focus training and system integration efforts on the most critical capability gaps.

## The Need for Regional Transit Security Information Sharing Plans

The mass transit rail system is highly vulnerable to high-casualty terrorist attacks because of several characteristics:

- Limited capability to screen huge volumes of riders and bags
- Open architecture, with access through multiple entry points
- Operational predictability, with defined, publicly available schedules and patterns of movement
- Enclosed and underground stations
- Close geographic proximity to symbolic targets and critical infrastructure

According to a Homeland Security Institute study of past attacks on rail systems, terrorists are rarely caught in the act during the execution phase of an operation, other than instances in which their equipment or weapons fail.

*“The important lesson learned is that it is highly effective to concentrate on the pre-execution phases of attempted terrorist attacks. Last-line fail-safe measures are critical to thwart undetected plots, as well as induce uncertainty into the terrorist planning process. However, the best way to influence the success or failure of an attack—at the tactical, operational, or strategic level—is to interdict the plot before the terrorists deploy to execute their plan.”*  
Homeland Security Institute Report<sup>1</sup>

Because plots are most often foiled during the pre-execution phases, it is essential to create an environment in which indicators of terrorist activities can be quickly detected and reported to regional agencies. Effective information sharing between regional partners is essential to recognize the context into which a certain piece of information fits and to ultimately prevent an attack.

How does information need to flow between federal and state and local agencies, and between regional agencies in order to maximize the chances of detecting a nascent terrorist attack? The flow of information between organizations needs to be:

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

---

<sup>1</sup> “Underlying Reasons for Success or Failure of Terrorist Attacks: Selected Case Studies, Final Report” Homeland Security Institute, June 2007

Simply instructing security agencies to share information is not enough. Even funneling information to regional or state fusion centers may not be enough. While these fusion centers may have the analytic capability to synthesize disparate pieces of information and to produce threat reports, their efforts can take days or weeks which may not be fast enough to prevent a fast-moving terrorist plot.

Security services need to have documented peer-to-peer information sharing procedures with regional counterparts and regional situational awareness.<sup>2</sup> According to Lessons Learned Information Sharing (LLIS), a U.S. Department of Homeland Security resource, regional transportation and transit agencies can improve communication procedures between regional agencies by including formal communication and notification procedures in plans. These procedures should determine:

- What information needs to be disseminated
- When and why it should be sent out
- The path of notification

Formalizing these processes will help ensure access to accurate and timely information.

Today, most government agencies lack well-documented information sharing procedures with sufficient detail to guide the action of people in Intelligence Fusion Centers, Emergency Operations Centers, or out in the field. Vague guidelines and high-level PowerPoint flow charts that simply show arrows indicating information flow between organizations clearly don't achieve the required level of detail and responsibility. Plans that are too simple and vague ultimately undermine accountability for effective information sharing.

---

<sup>2</sup> TSA/FTA Security and Emergency Management Action Items for Transit Agencies (2006)

Having the tools and networks needed to transmit and receive information is vital, but even with these systems in place information doesn't spontaneously flow as needed between people and/or technology. To achieve the required information sharing, the flow of information needs to be planned prior to a critical incident, and analyzed in order to reduce the risk a communication breakdown.

Organizations must document their information sharing commitments and build actionable information sharing plans in order to avoid experiencing a communication breakdown. To do this, organizations need a framework for:

- Analyzing information needs associated with mission-critical tasks
- Evaluating internal communication protocols
- Determining the information needs of external parties and agencies
- Assessing the planned flow of information for compliance with procedures, directives and policies
- Evaluate the likely consequences of failing to receive or share information

Without a coherent framework or initiative, these planning tasks are rarely undertaken systematically. A key reason for this and a fundamental impediment to regional security is the absence of any single agency responsible for planning the flow of information between international, federal, state, local government agencies, non-governmental organizations, and private sector entities.

Each organization has its own rules, roles, responsibilities, and interests, and planning sessions that unite organizations from different disciplines and jurisdictions are held relatively infrequently. Developing multi-organizational information sharing plans still has not been

systematically institutionalized. However, proactively defining and institutionalizing information sharing procedures is increasingly being recognized as a lever for more effective management and for enhanced transparency and performance.

## **A Better Process for Developing Actionable Information Sharing Plans**

Information Sharing Planning (ISP) is a structured process developed by Mind-Alliance Systems, and for building information sharing plans and communication procedures. Piloted successfully for the U.S. Department of Homeland Security in 2006, ISP combines principles of strategic and scenario planning with capabilities-based planning, risk management and performance assessment.

ISP builds awareness between organizations and people that have inter-related missions. If anticipated events occur (or are suspected to have occurred), people know how to share information effectively. ISP provides a practical framework for 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 Planners check that their organizations have identified the tasks that need to be executed in order to mitigate risk (or capture opportunities), and assign them to qualified members of their organizations. The “agents” who execute these tasks commonly have assigned roles (e.g. in a NIMS framework) in a relevant jurisdiction.

In order to execute their tasks and assess situations, people very specific elements of information. Information sharing procedures specify what information people need to send

and receive as they execute their assigned tasks. ISP Planners identify the tasks that produce the needed information (“source tasks”) and the tasks that need to receive and consume the information (“target tasks”), and procedurally link them via appropriate information sharing flows.

The information flows need to take place via approved communication channels (means of transmission and endpoints, such as telephone numbers, email addresses, etc.) and in a manner compliant with policies that either require or prohibit information sharing. Parties agree to an information sharing agreement or Memorandum of Understanding, and commit to sharing information according to plan, with the understanding that the information they provide is strictly to be used for the execution of the target task.

ISP is complementary to Business Process Management (BPM) processes and tools that help an (extended) enterprise maximize value creation and minimize operating costs via business processes. Information Sharing Planning (ISP) focuses on helping (decentralized) ecosystem of organizations better manage systemic risks and seize opportunities via information sharing procedures, regardless of whether communication can be automated.

ISP is implemented with the help of a software application called CHANNELS. This web application enables organizations to apply the ISP process collaboratively. It helps planners organize the information collected in interviews and group planning sessions and construct an information sharing plan. The software automatically analyzes the plan to identify improperly defined elements, uncover gaps, and points out weaknesses. It extracts actionable and up-to-date information sharing

procedures for each organization, role or individual.

The CHANNELS web application:

- Generates visualizations and analytics to make even complex plans comprehensible and supports mission integration
- Presents current information sharing procedures 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

The procedures created in Channels can be appended to plans and training material and integrated into other applications.

### **Regional Transit Security Information Sharing Planning in the Philadelphia Area**

The Philadelphia Area Regional Transit Security Working Group (PARTSWG)<sup>3</sup> received a DHS Transit Security Grant and, with its regional partners, is collaboratively developing a Regional Information Sharing Plan with actionable procedures and protocols that can be followed to prevent an Improvised Explosive Device (IED) terror attack, in order to:

- Enhance the flow of information and improve the coordination between regional stakeholders
- Reduce the risk of breakdown or delay in the flow of communication
- Align PARTSWG plans with regional and national plans

<sup>3</sup> PARTSWG members include: AMTRAK, Delaware River Port Authority (DRPA), NJ Transit, Pennsylvania Emergency Management Agency (PEMA), Southeastern Pennsylvania Transportation Authority (SEPTA), Philadelphia Police Department, Federal Emergency Management Agency (FEMA), Transportation Security Agency (TSA), the Delaware Valley Intelligence Center (DVIC), and other agencies.

ISP provides homeland security organizations with a wide range of planning, operations and management benefits. Organizations get an opportunity to make the flow of vital information faster, policy-compliant, and more resilient. Information flow becomes less likely to break down due to technical issues, human factors, or unforeseen circumstances.

The enhanced understanding of a partner's information needs improves organizational intelligence and operational efficiency. This understanding is key to better directed, more timely and reliable operational information sharing, leading to effective coordination and policy compliance.

By developing information sharing plans and actionable procedures regional stakeholders will:

- Enhance prevention of a terrorist attack
- Reduce the risk of communication failures in a crisis that can undermine regional inter-agency coordination needed to save lives and reduce damages
- Discover where the mission is most at risk because of interdependencies, information flow issues, and missing procedures
- Retain institutional knowledge often lost with personnel turnover
- Be able to plan more effectively with a wide scope of organizations
- Deal pro-actively with issues that could impact the flow of information
- Allocate limited resources wisely, to fix the most critical information sharing and communication issues

To learn more about how **Mind Alliance** can help your region develop robust information sharing plans visit [www.mind-alliance.com](http://www.mind-alliance.com) or call **1-888-731-6018**.