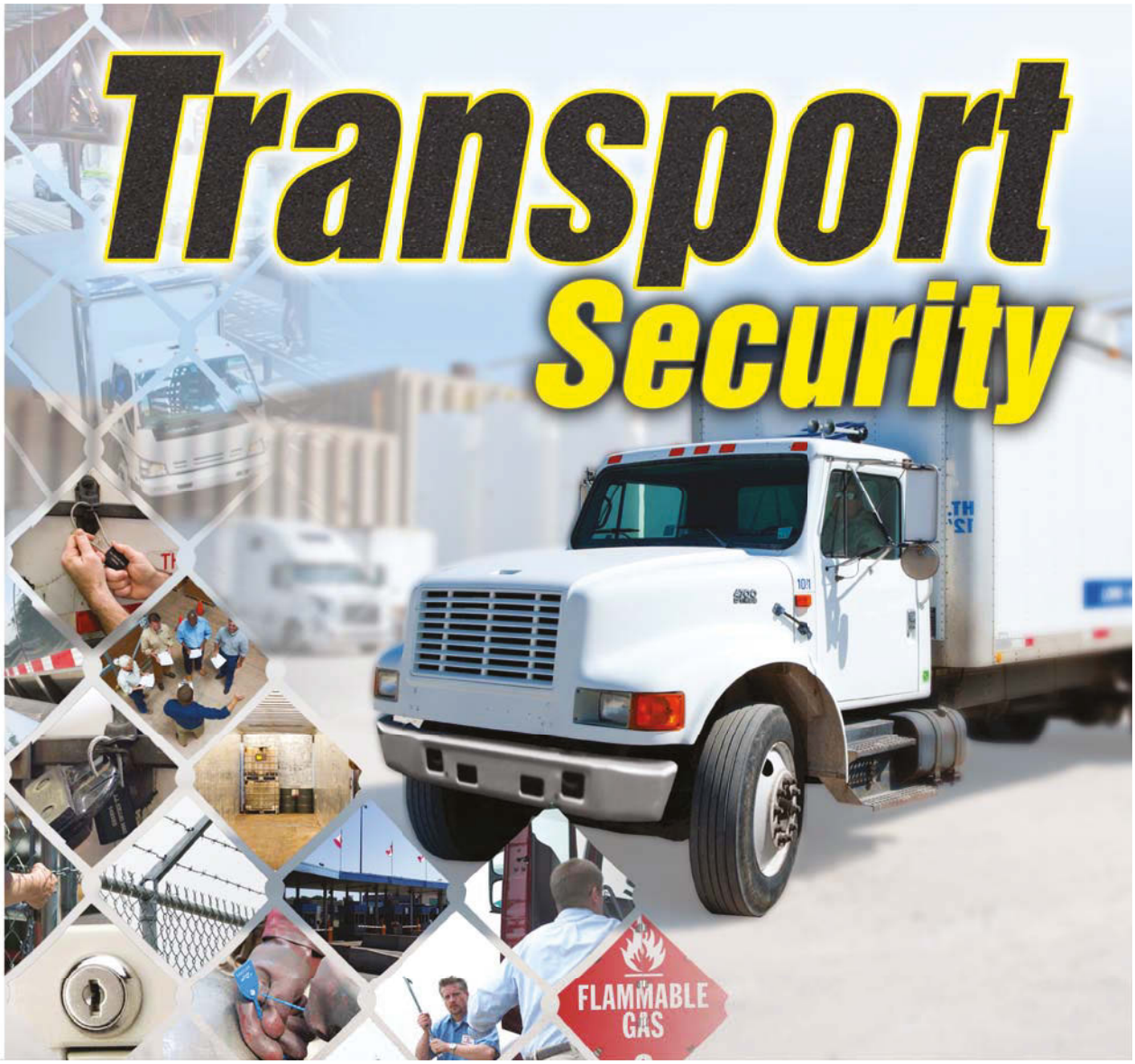



J. J. Keller
& Associates, Inc.®
*Since 1953*

**This publication updates in February/August**

**15-M (7359)**

ISBN 978-1-60287-970-6
90000
9 781602 879706

**J. J. Keller & Associates, Inc.**
3003 Breezewood Lane
P.O. Box 368
Neenah, Wisconsin 54957-0368
Phone: (800) 327-6868
Fax: (800) 727-7516
*JJKeller.com*

Library of Congress Catalog Card Number: 200197899

ISBN 9781602879706

Canadian Goods and Services Tax (GST) Number: R123-317687



Printed in the U.S.A.

# TRANSPORT SECURITY

## Introduction

The Transport Security Manual provides a general background and solid foundation from which any commercial motor carrier can develop, implement, and monitor a comprehensive corporate security program.

There is little doubt that the motor carrier industry is critically important to the overall economic health and stability of North America, and in particular the United States. Every day the motor carrier industry transports billions of dollars worth of raw and finished goods and commodities, and serves virtually every segment of this country's economy and all of our critical infrastructures.

Because of this, there has always been a need for a high level of safety and security in the motor carrier industry. In the past, this need for security has focused on the prevention of cargo theft and personal (driver) safety. However, in the current transportation environment, the need for safety must be broadened to consider a wide range of potential risks and threats.

This manual is divided into six areas of concern, including: 1) Personnel Safety & Security, 2) Physical Facilities Security, 3) Driver/Employee Security Awareness Training, 4) Hazardous Material Control, 5) Management Initiatives, and 6) Emergency Response/Planning. By incorporating these six major areas of safety and security concern, the manual serves as a comprehensive and in-depth source for the entire motor carrier industry.

Revision bars, like the one at the left of this paragraph, are used in this publication to show where significant changes were made on update pages. The revision bar next to text on a page indicates that the text was revised. The date at the bottom of the page tells you when the revised page was issued.

Due to the constantly changing nature of government regulations, it is impossible to guarantee absolute accuracy of the material contained herein. The Publisher and Editors, therefore, cannot assume any responsibility for omissions, errors, misprinting, or ambiguity contained within this publication and shall not be held liable in any degree for any loss or injury caused by such omission, error, misprinting or ambiguity presented in this publication.

This publication is designed to provide reasonably accurate and authoritative information in regard to the subject matter covered. It is sold with the understanding that the Publisher is not engaged in rendering legal, accounting, or other professional service. If legal advice or other expert assistance is required, the services of a competent professional person should be sought.

**The Editors & Publisher**
**J. J. Keller & Associates, Inc.**

Published & Printed by

**J. J. Keller & Associates, Inc.**
3003 Breezewood Lane, P.O. Box 368
Neenah, Wisconsin 54957-0368
Phone: (800) 327-6868
Fax: (800) 727-7516
*JJKeller.com*

## Table of Contents

## BORDER CROSSING

C-TPAT/PIP
FAST
E-Manifests
Credentials

## REFERENCE

State Criminal Background Check Information
Laws
Part 383
Part 391
Hazmat Regs
Agency Contacts
Sample Forms

## SUBJECT INDEX

procedures of the security plans. Most importantly, supervisors are responsible for giving timely and accurate feedback regarding the overall effectiveness of the security plans. The plan must contain, based on revisions to the HMR effective October 1, 2010, security duties for each position or department that is responsible for implementing the plan or a portion of the plan and the process of notifying employees when specific elements of the security plan must be implemented.

- **Employees —** Are responsible for having the written security plans and procedures become a part of their daily work activities. Anything other than performing duties and activities according to established security procedure will be considered unacceptable. The security plan must, effective October 1, 2010, include a plan for training hazmat employees in accordance with §172.704 (a)(4) and (a)(5).

## Risk Assessment Tools

The security plan **must** include an assessment of possible transportation security risks for shipments of hazardous materials (as listed in §172.800). Assessing risk requires the management of an organization, representing all departments and functions, to take a critical look at the entire operation such as:

- How daily tasks and activities are performed;
- How and where important/sensitive records and documents are stored;
- How drivers and other employees are hired, screened, and managed; and
- What is the security risk to shipments of hazardous materials?

The following are a few of the more common ways to document a security risk assessment as you create your security plan or review and revise an existing plan.

## HAZARDOUS MATERIAL CONTROL

### Security Plan

**Flowcharts**

The use of flowcharts is a great way to examine security needs. If individuals, departments, or organizations do not want to create them freehand, they could invest in flowchart software, available from a variety of vendors in a range of prices based on tasks.

## HAZARDOUS MATERIAL CONTROL

### Security Plan

There are four kinds of flowcharts, depending upon the function. They are:

- **Basic.** Readers quickly identify all of the major steps in a process. They are general in nature.
- **Detailed.** This is a detailed examination of the smaller steps involved in a specific process.
- **Deployment.** This style is a detailed flowchart that adds another element – who is involved in the steps.
- **Opportunity.** It is a detailed flowchart that takes the reader to the left or right side based on whether or not the action is done correctly/incorrectly or effectively/ineffectively, or is costly/beneficial. It offers the opportunity to see where a process can be improved upon.

Businesses would use these flowcharts to determine where bottlenecks, costs, weak links, and ill-defined steps occur.

Flowcharts typically have shapes that symbolize specific elements. Here are some examples of shapes and what they represent:

 = Beginning and end of the chart

 = Action or task

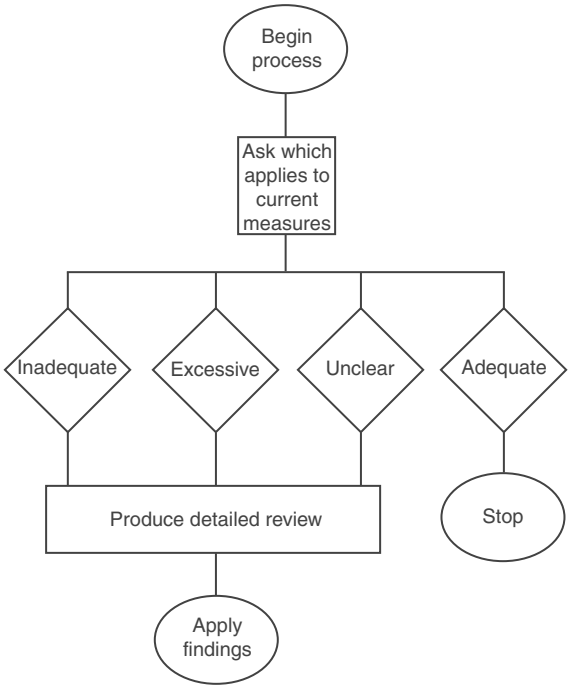
 = Yes or No decision must be made

There are more standardized symbols, but the examples presented below will only use these three basic elements.

In the **basic flowchart**, you create levels and paths so a specific security concern can be evaluated and a logical conclusion drawn.

## HAZARDOUS MATERIAL CONTROL

### Security Plan




First, individuals must decide what need for security should be addressed. A basic flowchart will be very general about the organization. The employee drafting the flowchart must ask him/herself why this assessment is needed. He or she will have four possible rationales:

1. The company's current security measures are inadequate;
2. The company's current security measures may be excessive;
3. He or she is uncertain what the current need and/or regulatory requirements are; or
4. The company's current security measures seem adequate.

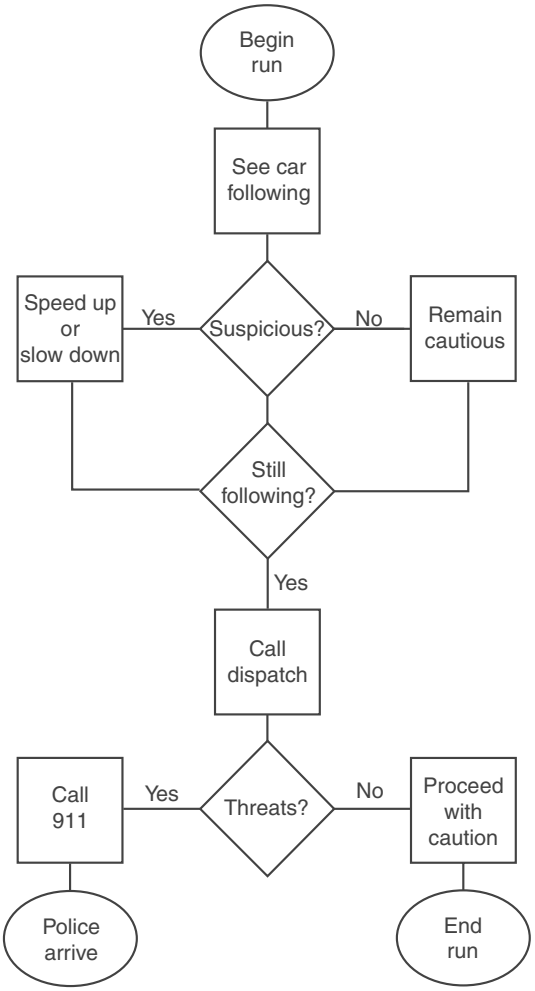
Based on which option he or she selects about the security program, he or she moves on to the next level of the flowchart. A response to:

## HAZARDOUS MATERIAL CONTROL

### Security Plan

- Numbers 1-3 above would lead the creator of the flowchart to produce other flowcharts, more detailed and that yield possible outcomes.
- Number 4 above ends the process right there.

A **detailed flowchart** will have numerous detailed steps and potential alternatives. The following is a flowchart that could be used for commercial drivers in identifying suspicious activity.

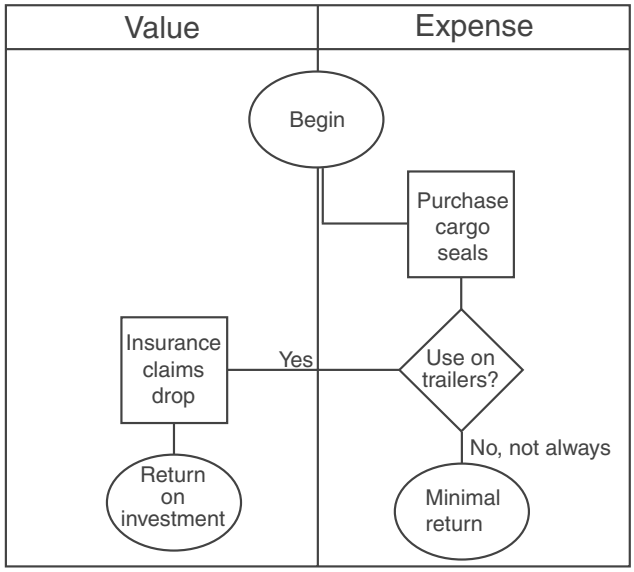


## HAZARDOUS MATERIAL CONTROL

### Security Plan

If one took this detailed flowchart a step further, he or she could include each department's role — dispatch, management, and drivers — to make a deployment version.

To create an **opportunity flowchart**, individuals divide their paper into two sides — one that has a positive value and one that has a negative value. They list all of the steps, placing them in the appropriate column and connect them with lines. The following is an example of an opportunity flowchart for the use of cargo seals.




**Risk-Assessment Graph**

Everyone knows that the average business does not have a security budget that can accommodate every aspect and every scenario at risk for the organization. By using a risk-based security program, businesses can use a variety of tools to determine the best allocation of their security dollars and assets. How does it work? Organizations would select a range of topics. The level of impact (effectiveness) versus cost or time would justify, delay, or rule out the investment in the policy, procedure, staff, equipment, facility, etc.

To visualize the information being reviewed, the company could use a graph as a measurement tool. One axis (vertical,

## HAZARDOUS MATERIAL CONTROL

### Security Plan

Y-axis) represents the impact that specific security measures would have (low to high), while the other axis (horizontal, X-axis) would show how difficult it would be to implement security processes in this area. The easiest implementation would be on the left-hand side, graduating in degrees of difficulty as it goes to the right. Individuals can measure ease using time and/or money.

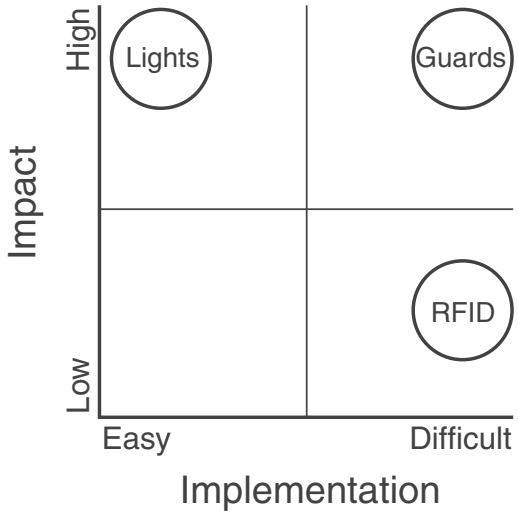
The graph is then broken up into quadrants. The upper left-hand corner would represent immediacy. The upper right-hand corner would represent items that hold value, but would be placed on the back burner until more feasible. The lower left-hand side includes those low-impact, easily implemented measures that might as well be done. The lower right-hand side encompasses those security measures that have not proven themselves valuable enough to take on the necessary resources to implement. They are those items that are safe to ignore until prices come down and/or technology is improved.

**Example 1.** A mid-sized organization wants to look at its facility security, and they have selected lights, security guard personnel, and an inventory Radio Frequency Identification (RFID) system for its warehouse as areas to pursue. The diagram might look something like this.

## HAZARDOUS MATERIAL CONTROL

### Security Plan

Diagram 1




One can see from the diagram:

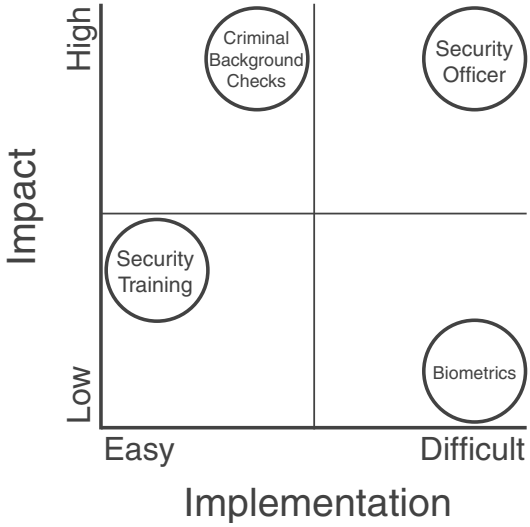
- A guard service makes for high security impact, but the cost puts it in a futuristic spot for a smaller, tight-budgeted operation.
- Security lights are effective and within the budget, and can be installed in a relatively short time frame. It is in an area to pursue.
- The RFID system being looked at is too expensive, takes time away from the maintenance and IT staffs, and has been known to be unreliable at times. The graph suggests that it is safe to put this in a category to ignore for the time being, until it moves to another quadrant in the graph (i.e., becomes more cost effective or the RFID become more standardized).

**Example 2.** In this next example, a small company wants to investigate its options for personnel security. They opt to look at security training, criminal background checks on applicants, hiring a security officer, and using biometrics as a form of keyless entry. The diagram might look something like this.

## HAZARDOUS MATERIAL CONTROL

### Security Plan

Diagram 2




One can see from the graph:

- Security training has a middle ground of effectiveness. It depends on the individuals — whether or not they take the training into real life. On the other hand, it takes little time and at a minimal cost for training materials and is a requirement for compliance with 49 CFR 172. It lands in an area of "might as well be done."
- Conducting thorough criminal background investigations on applicants ranks high on impact, and it falls within the time and cost of the operation. It ranks in the "do-it-now" category on the graph.
- Hiring a security officer has a high impact, but is not within the current staffing budget. It would be better suited for a future goal.
- Installing biometric readers on all points of entry for employees would add a middle area of effectiveness, especially since the operation is small and people still hold doors open for visitors and off-duty employees. One cannot justify the cost of investing in the technology. It would

## HAZARDOUS MATERIAL CONTROL

### Security Plan

be something to keep in mind if the organization grows and the technology comes down in price.

Periodically, a designated person within the firm should pull out these analyses of the operation. What has changed? What is more realistic with the passage of time? Revisiting these graphs will also help to jog one's memory of what the organization was thinking, planning, and strategizing earlier.

Always remember to file, under lock and key, these tools along with other sensitive, confidential security information. They can reveal a lot to a terrorist or criminal as to what the corporation deems as important in its security efforts.

**Risk-Assessment Tables**

Security analysis tools vary in shape and form. How one lays out the information about the organization for a risk analysis is driven by its use. Some organizations use a simple checklist, or yes/no format, while others have boxes to enter comments. Many formats just identify strengths and weaknesses, but offer no specific solutions to the problems. The following assessment tool is an example that is used when someone wants to pinpoint security deficiencies and actually set target dates to have corrective measures in place. It contains some sample topics and how information could be entered:

| **Date: 2/13/09<br>Completed By: (Name/Title)<br>John Doe, Manager** | | | | **Expected Review Date: 9/01/09** |
|---|---|---|---|---|
| **Issue** | **Current Status*** | **Future Status*** | **Target Date** | **Comments** |
| **Yard**<br>Lights are in good working order, illuminating the entire yard. | A (I) | (A) I | 6/01/10 | Lights are outdated and need to be replaced. In budget for 2010. |
| Fences are free of objects/debris that could allow an intruder to scale the fence. | A (I) | (A) I | 3/15/09 | Tree trimmer scheduled on site. |

J. J. Keller & Associates, Inc.®
Since 1953

# Want to Keep Reading?

**Visit JJKeller.com now** to order or get more details on this manual written by our safety & compliance experts.

Convenient Update Service subscriptions are also available to help you make sure your information is always up to date.

## NOW AVAILABLE - Access Your Manual Online

With our NEW Online Edition options, you can access this manual's content from any browser or mobile device. You'll get:

- Search capabilities for easy navigation and fast research
- Bookmarks to help you to quickly flip to sections you frequently use
- Continuous updates to ensure you always have the most current info
- Notifications via homepage and email to help you stay on top of changes
- Easy access to ask questions of our subject matter experts

**Order Now to Keep Reading!**

Connect With Us

@jjkeller | jjkeller.com/LinkedIn | google.com/+jjkeller | contact us