Supply Chain Security: A Comprehensive and Practical Approach

An ISPE White Paper by the International Leadership Forum
ISPE White Paper:
Supply Chain Security:
A Comprehensive and Practical Approach

This White Paper was developed by members of the International Leadership Forum (ILF), a high level advisory group working through ISPE comprised of thought leaders from the Pharmaceutical Industry whose mission is to identify and influence direction and align the industry globally, establish dialogue with regulators to discuss critical technological issues, identify opportunities for innovation, promote consistency, and seek worldwide harmonization where appropriate.

Limitation of Liability
In no event shall ISPE or any of its affiliates, or the officers, directors, employees, members, or agents of each of them, be liable for any damages of any kind, including without limitation any special, incidental, indirect, or consequential damages, whether or not advised of the possibility of such damages, and on any theory of liability whatsoever, arising out of or in connection with the use of this information.

© Copyright ISPE 2010. All rights reserved.

No part of this document may be reproduced or copied in any form or by any means – graphic, electronic, or mechanical, including photocopying, taping, or information storage and retrieval systems – without written permission of ISPE.

All trademarks used are acknowledged.
# Table of Contents

1 **Introduction** ............................................................................................................. 5  
   1.1 Overview .................................................................................................................. 5  
   1.2 Key Terms .................................................................................................................. 5  
   1.3 Quality Risk Management Applied to Supply Chain Security ............................... 6  
   1.4 Augmenting the Pharmaceutical Quality System .................................................. 7  
      1.4.1 Packaging and Labeling Controls ................................................................. 7  
      1.4.2 Returned and Salvaged Product Controls .................................................... 8  

2 **Risk and Supply Chain Security** ............................................................................. 9  
   2.1 The Risk of Adulteration (including Economically Motivated Adulteration) .......... 9  
   2.2 The Risk of Counterfeit Medicines ....................................................................... 9  
   2.3 The Risk of Diverted Medicines ........................................................................... 9  
   2.4 The Risk of Cargo Theft ....................................................................................... 10  
   2.5 Risk Identification of Geographical Factors ........................................................ 10  
   2.6 Risk Ranking and Filtering to Differentiate Practices ............................................ 10  
   2.7 Risk Mitigation – Analytical/Characterization ...................................................... 10  

3 **Common Processes to Enhance Supply Chain Security** ..................................... 11  
   3.1 Signal Detection and Response ......................................................................... 11  
      3.1.1 Example: Dairy Product Shortage .............................................................. 11  
      3.1.2 Example: Acetonitrile Shortage ................................................................. 11  
      3.1.3 Example: Glycerin Contamination with Diethylene Glycol .................... 12  
      3.1.4 Other Signals .............................................................................................. 12  
   3.2 Linking Outcomes and Signals ............................................................................ 12  
   3.3 Signal Detection Process .................................................................................... 12  
      3.3.1 Defining Targets Using Quality Risk Management ..................................... 13  
   3.4 Environmental Scanning ..................................................................................... 13  
      3.4.1 Determining the Relevance ....................................................................... 14  
      3.4.2 Post Marketing Surveillance ..................................................................... 14  
      3.4.3 Signal Response ....................................................................................... 14  

4 **Supplier Quality Management** ............................................................................ 15  
   4.1 Supplier Assessment and Selection ..................................................................... 15  
   4.2 Written Agreements for Quality Activities ......................................................... 16  
   4.3 Supplier Monitoring and Review .......................................................................... 17  

5 **Logistics and Transportation Service Providers** ................................................. 20  
   5.1 Management of Logistics and Transportation Service Providers ..................... 20  
   5.2 Selection and Assessment of Logistics and/or Transportation Service Providers .... 20  
   5.3 Review of Physical Premises .............................................................................. 20  
      5.3.1 Physical Barriers ....................................................................................... 20  
      5.3.2 Gates ....................................................................................................... 20  
      5.3.3 Access Controls ...................................................................................... 21  
      5.3.4 Alarm Systems ......................................................................................... 21  
      5.3.5 Loading Docks ......................................................................................... 21  
   5.4 Assessment and Controls of Personnel ............................................................... 21  
      5.4.1 Employees ............................................................................................... 21  
      5.4.2 Visitors ..................................................................................................... 21  

© Copyright ISPE 2010
6 Transport and Control of Materials ................................................................. 22
  6.1 Materials Controls .................................................................................. 22
  6.2 Warehousing and Distribution Controls within the Organization .......... 22
  6.3 Containers .............................................................................................. 22
  6.4 Seals ........................................................................................................ 23
  6.5 Shipping and Receiving Processes ......................................................... 23

7 Specific Programs .......................................................................................... 24
  7.1 Specific Programs for Anti-Counterfeiting ................................................ 24
    7.1.1 Processes ......................................................................................... 24
    7.1.2 Enable Authentication of Products .................................................. 24
    7.1.3 Maintain a Counterfeiting Incident Management Plan .................. 24
  7.2 Specific Programs for Illegal Diversion .................................................... 24
    7.2.1 Interactions with Customers .............................................................. 24
    7.2.2 Interactions with Distributors ........................................................... 24
  7.3 Specific Programs to Prevent Cargo Theft ............................................... 25
    7.3.1 Cargo Theft Awareness .................................................................. 25
    7.3.2 Cargo Theft Prevention ................................................................. 26
1 Introduction

Pharmaceutical Quality Systems alone cannot ensure supply chain security or security. However, augmenting specific quality systems, being alert to signals in the environment, applying risk management principles, and developing specific programs to deal with counterfeiting and illegal diversion will help strengthen an organization’s overall supply chain security.

1.1 Overview

The pharmaceutical supply chain is a complex process which spans many geographical regions and involves numerous parties. To ensure supply chain security, several functional groups should be involved over the life cycle of the supply chain. For an organization, it is best organized as an integrated approach.

This White Paper presents how an integrated approach can facilitate supply chain security by suggesting ways of augmenting the pharmaceutical quality system to prevent and detect adulteration, counterfeiting, illegal diversion, and theft. While adulterated, counterfeit, or diverted materials and finished products entering the supply chain cannot be wholly prevented by pharmaceutical quality systems, organizations may be able to mitigate certain of these risks by applying the strategies and principles outlined in this White Paper.

Today’s supply chains are complex and include raw material suppliers, contract manufacturers, logistics, and transportation providers. This White Paper looks at supply chain security holistically across the supply chain, including the application of environmental scanning methods and risk management principles at each step in the supply chain.

This White Paper is not intended to be an exhaustive or definitive review of best practices, standards and regulations, but rather a description of a type of thinking consistent with an integrated and risk-based approach toward supply chain security.

1.2 Key Terms

The following key terms used within this White Paper are defined as follows:

**Adulteration**

Adulteration can be defined as a drug which is not what it is purported to be. Adulteration can take many forms, including product that is contaminated, unsafe, manufactured in conditions not meeting good manufacturing practices, product that does not meet its requirements for purity and strength, or is unapproved to be marketed in a particular country. Adulteration can be accidental or intentional. Additional controls are required to reduce the risk of adulteration when there are complex supply chains which involve significant outsourcing of manufacturing and distribution.

**Counterfeit**

A counterfeit medicine is one which is deliberately and fraudulently mislabeled with respect to identity and/or source. Counterfeiting can apply to both branded and generic products and counterfeit products may include products with the correct ingredients or with the wrong ingredients, without active ingredients, with insufficient active ingredients, or with fake packaging. (From World Health Organization.)

**Customer**

Where the first change in ownership of a product takes place.
Environment Scanning

A process for reviewing external information which may have an impact on selected targets. It involves the collection and analysis of information relevant to pre-defined targets.

First, Second, and Third Tier Suppliers

A first tier supplier is a supplier who directly invoices the organization for goods and/or services rendered directly by the first tier supplier to the organization as a customer. A second tier supplier is a supplier who invoices a first tier supplier for goods and/or services which will ultimately be part of the first tier supply to the organization. A third tier supplier is a supplier who invoices a second tier supplier.

Illegal Diversion

Illegal diversion occurs when a genuine pharmaceutical product is approved and intended for sale in one country, but is then illegally intercepted and sold in another country. (From the Pharmaceutical Security Institute.)

Signal

New information indicating the potential for economically motivated adulteration of a material or a product, the use of counterfeit material, or the illegal diversion of legitimate product into unlawful channels.

Signal Detection Process

The signal detection process involves:

1. defining targets for enhanced, ongoing scrutiny
2. applying environmental scanning to those targets (reviewing external information that may have an impact on the targets)
3. determining the relevance of the results of environmental scans

Target

A particularly vulnerable material or physical point in the supply chain where adulteration, counterfeiting, or illegal diversion could occur. Risk management approaches should be used to help identify targets.

1.3 Quality Risk Management Applied to Supply Chain Security

The process described in ICH Q9, Quality Risk Management¹, can be used to develop a risk-based approach to supply chain security. This includes assessing risks, developing controls, conducting risk reviews, and communicating appropriately (reference ICH Q9 and diagram below). To perform a qualitative risk assessment, begin by posing three simple questions:

1. What might go wrong?
2. What is the likelihood (probability) it will go wrong?
3. What are the consequences (severity)?

Quality Risk Management is an ongoing process and should be updated as new information is received.

Figure 1.1: Quality Risk Management Process (from ICH Q9)

As part of the risk management process, processes should be established to assure risks are communicated throughout the organization. This is particularly important for supply chain security as there are numerous disciplines and functional groups involved. Information regarding identified risks from the signal detection process, discussed later in this White Paper, should be communicated throughout the organization.

1.4 Augmenting the Pharmaceutical Quality System

Within this White Paper, there are specific sections which discuss how the Pharmaceutical Quality System (PQS) can be augmented with respect to controls for material, warehousing, and distribution systems. Further consideration should be given to assessing established controls for packaging and labeling systems and controls on returned and salvaged products.

1.4.1 Packaging and Labeling Controls

As part of the PQS, procedures should be established which describe the destruction of packaging and labeling materials.

Careful attention should be paid to the destruction of labeling and packaging materials. These can be used to illegally package counterfeit or diverted product.
Destruction of rejected materials should be accounted for and proof of the destruction should be obtained and documented. Accountability for the destruction of labels, and packaging materials, and destruction of returned products, should extend to the management of third party suppliers, contract manufacturers, and logistics service providers.

### 1.4.2 Returned and Salvaged Product Controls

Customers should be directed to return all unsold product to the manufacturer for evaluation. Returned materials should be dispositioned in accordance with an organization’s processes. If the customer is in another country where the return is not feasible, special care should be taken to arrange for destruction by a trusted third party. Returned product should be analyzed to determine authenticity. If the product is not authentic, the organization should investigate where the potentially diverted or counterfeit product entered the supply chain.
2 Risk and Supply Chain Security

2.1 The Risk of Adulteration (including Economically Motivated Adulteration)

In the context of a drug product, adulteration can be defined as a drug which is not what it is purported to be. Adulteration can take many forms including product that:

- is contaminated
- is unsafe
- is manufactured in conditions that do not meet good manufacturing practices
- does not meet its requirements for purity and strength
- is not approved to be marketed in a particular country

Adulteration can be accidental or intentional. Additional controls are required to reduce the risk of adulteration when there are complex supply chains which involve significant outsourcing of manufacturing and distribution.

Recently the term “Economically Motivated Adulteration” has come to mean the fraudulent, intentional substitution or addition of a substance in a product for the purpose of increasing the apparent value of the product or reducing the cost of its production, i.e., for economic gain.

2.2 The Risk of Counterfeit Medicines

Within this White Paper, the definition of counterfeit medicines is in accordance with the definition from the World Health Organization:

“A counterfeit medicine is one which is deliberately and fraudulently mislabeled with respect to identity and/or source. Counterfeiting can apply to both branded and generic products and counterfeit products may include products with the correct ingredients or with the wrong ingredients, without active ingredients, with insufficient active ingredients or with fake packaging.”

A pharmaceutical manufacturer may not be able to fully prevent counterfeiting across the global marketplace. The goal is to define appropriate controls to minimize the risk of counterfeit product.

Organizations can perform risk assessments to help identify which products and regions present the greatest risk of counterfeiting. This can be used to help prioritize the allocation of anti-counterfeiting resources.

2.3 The Risk of Diverted Medicines

It is useful to understand the definition for illegal diversion (from the Pharmaceutical Security Institute):

“Illegal diversion occurs when a genuine pharmaceutical product is approved and intended for sale in one country, but is then illegally intercepted and sold in another country. These schemes are often accomplished through the use of false statements or declarations. At times, drug regulators in the second country have not approved the use of the diverted drug. Illegal diversion may also occur within the same geographic area, within the same country or city. This type involves diverting discounted medicines from one intended group of consumers to another group buying medicines in an unregulated open market.”
Illegal diversion means ‘diverting’ finished products from the intended supply chain, where the intended supply chain refers to the lawful channels by which a pharmaceutical manufacturer transfers drug product to the first legal owner. Most occurrences of illegal diversion cannot be easily prevented; however, there are prudent steps which organizations can take to prevent and detect illegal diversion.

Preventing and detecting illegal diversion cannot be accomplished by a single organization. Each member in the supply chain can use the recommendations below to help to prevent and detect illegal diversion to develop a comprehensive approach.

Quality Risk Management should be used to know and understand the drug product and to assess the probability of it being diverted. Risk factors can include high-value drug products, drug products in short supply, drug products with a high potential for abuse, or drug products widely used. Understanding the nature of the illegal diversion risk is an important element in designing a proactive anti-diversion program.

2.4 The Risk of Cargo Theft

Cargo theft of finished pharmaceuticals during transportation or warehousing is increasing on a global basis. Understanding the risks associated with a product being stolen is key to prevention. Many of the same risk factors defined above for illegal diversion also apply to theft. In addition to the risk factors identified above, high value drug products, drug products with a high potential for abuse, and widely used drug products are also risk factors for cargo theft. How and where the product is being transported are key risk factors which should be understood. Some regions of the world and areas within specific regions represent higher levels of risk with regard to cargo theft.

2.5 Risk Identification of Geographical Factors

Organizations should determine ‘security risk geographies’ with respect to local crime rate, educational system, political and legal conditions hindering or even supporting counterfeiting activities. Comprehension of these risks can be used to augment audit content, investigational activities, and controls.

2.6 Risk Ranking and Filtering to Differentiate Practices

As part of a quality risk management approach, risk mitigation activities may include implementation of more stringent measures for drug products with high risk of counterfeiting, theft, and/or illegal diversion. The range of stringent practices will be dependent upon the risks identified at the different points within the supply chain, e.g., regional differences, modes of transportation, legal/regulatory framework.

The risk assessment should be reviewed to determine if an organization should maintain specific operations themselves, to help prevent counterfeiting, theft, and/or illegal diversion. An operational example could be labeling. When an organization performs its own labeling, there is greater control of the physical labels. When the labeling operation is outsourced, the risks are increased and should be controlled through a Quality Agreement and monitored/audited appropriately.

2.7 Risk Mitigation – Analytical/Characterization

Good analytics are essential to ensuring the security of supplied materials and detecting adulteration, whether intentional or unintentional. Recent experience has shown criminals responsible for adulteration for profit have an increasingly sophisticated understanding of the limitations of long-standing analytical methods to detect surreptitious adulteration. Manufacturers should carry out a quality risk assessment of manufacturing processes and identify any potentially vulnerable materials. The limitations of current methods should be understood, and where appropriate, orthogonal physical, chemical, or biological test methods should be developed to uniquely identify the material. The manufacturer is responsible for the security of all materials used in manufacturing and the utilization of the most appropriate analytics.
3 Common Processes to Enhance Supply Chain Security

There are several processes common to helping control the risk of adulteration, counterfeiting, theft, and illegal diversion. They include:

- signal detection and response
- supplier quality management
- management of logistics and transportation services providers

3.1 Signal Detection and Response

A signal is new information indicating the potential for economically motivated adulteration of a material or a product, the use of counterfeit material, or the diversion of legitimate product into unlawful channels. Often, a signal consists of information related to a change in the availability or price of a material or product, or it can be a precursor event likely to lead to such a change. The change may create an incentive to substitute alternative material for legitimate material or to divert legitimate material into unlawful channels. Some geopolitical or weather events also can be considered signals of a potential for economically motivated adulteration of a material.

Within this White Paper, three examples are presented. These were chosen to exemplify how adulteration of an excipient, low in cost and widespread in use, can have broad effects on the quality of finished products across several countries and impacting several organizations. Unfortunately, there are several other recent high profile examples, for which space prevented inclusion, further underscore the importance of this topic.

3.1.1 Example: Dairy Product Shortage

Culminating in 2006 there were a number of global events which created a shortage of dairy products. This shortage caused an increase in the price of dairy products, signaling a potential for suppliers to substitute a less expensive material for the expected product. Inexpensive materials such as melamine were used to inflate the protein content of foods when tested with traditional analytical methodology. The adulteration was first detected in cat and dog food resulting in pet food recalls in the US in 2007 in response to reports of kidney failure in pets. Similarly, reports of melamine adulteration of baby food surfaced in late 2008 with reports of kidney stones in children in China.

3.1.2 Example: Acetonitrile Shortage

Another example of a market-shortage related signal involved the shortage of Acetonitrile. Acetonitrile is an organic solvent, produced mainly as a byproduct of acrylonitrile manufacture. It is widely used in the analytical laboratory as a mobile phase solvent and as a solvent in Active Pharmaceutical Ingredient manufacturing. Shortages of acetonitrile began in late 2008 as a result of:

- a US plant being damaged by Hurricane Ike
- the reduction of factory operations in China prior to the Beijing Summer Olympics
- a downturn in the demand for acrylonitrile in the car industry

The shortage created the potential for counterfeit materials to be introduced in the acetonitrile marketplace.
3.1.3 Example: Glycerin Contamination with Diethylene Glycol

The US Federal Food Drug and Cosmetic Act was passed following the 1937 “Elixir Sulfanilamide” incident wherein diethylene glycol was used in a preparation of sulfanilamide elixir resulting in a number of deaths. Over the years, there have been many deaths associated with contamination of glycerin used in the preparation of medicines. More recently, in Panama, cough syrup was tainted with diethylene glycol, resulting in more than 100 deaths. In this example, the presumed signal was lower cost and availability of the diethylene glycol.

3.1.4 Other Signals

New information about the abuse of a material or product also can be viewed as a signal of an incentive for theft or illegal diversion of legitimate material/product into unlawful supply channels.

3.2 Linking Outcomes and Signals

The table below contains information to help link the outcomes in the examples described above with potential signals. A good signal detection process can aid the anticipation of likely outcomes and enable preventative measures to be taken to limit the consequences.

Table 3.1

<table>
<thead>
<tr>
<th>Example</th>
<th>Signal(s)</th>
<th>Outcomes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dairy Product Shortage</td>
<td>• Global shortage of dairy products</td>
<td>• Intentional adulteration of dairy products to artificially inflate the</td>
</tr>
<tr>
<td></td>
<td>• Significant rise in the price of dairy products</td>
<td>tested protein content – injury to patients and consumers</td>
</tr>
<tr>
<td></td>
<td>• Adulteration of pet food with melamine</td>
<td></td>
</tr>
<tr>
<td>Acetonitrile (ACN) Shortage</td>
<td>• Global economic downturn led to significantly decreased demand for plastics which led to shortage of ACN precursor</td>
<td>• Misrepresentation of other solvents as ACN or dilution of ACN – inability of labs to carry out registered methods, inability to manufacture API, or undetected impurities in API</td>
</tr>
<tr>
<td></td>
<td>• Loss of plant capacity for ACN production due to hurricane damage</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Sharp rise in the price of commodity ACN due to shortage</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Ready availability of solvent represented as ACN at a below market price</td>
<td></td>
</tr>
<tr>
<td>Diethylene Glycol Contamination of Glycerin</td>
<td>• Commodity glycerin available at below-market price</td>
<td>• Intentionally adulterated glycerin used to manufacture medicines – illness and death among patients consuming contaminated product</td>
</tr>
<tr>
<td></td>
<td>• Commodity material passing through multiple brokers across the globe</td>
<td></td>
</tr>
<tr>
<td></td>
<td>without testing</td>
<td></td>
</tr>
</tbody>
</table>

3.3 Signal Detection Process

The signal detection process involves:

1. defining targets for enhanced, ongoing scrutiny
2. applying environmental scanning for signals to identified targets (reviewing external information that may have an impact on the targets)
3. determining the relevance of the results of the environmental scans

### 3.3.1 Defining Targets Using Quality Risk Management

As part of a global supply chain, numerous goods and materials from various supply chains are shipped, received, and used to manufacture products. Any of these materials can be considered targets of economically-motivated adulteration, counterfeiting, or illegal diversion and should be subject to increased on-going scrutiny. Moreover, various points in the transport of material throughout the supply/distribution chain also could be considered potential targets and should be subject to scrutiny. Thus, the number of potential targets could be overwhelming. In order to make the signal detection process practical, it is important to use quality risk management principles in selecting targets. Risk Management tools, as described in ICH Q9, including basic risk management facilitation methods, such as flow charts and check sheets or more formal tools, such as Hazard Analysis and Critical Control Points (HACCP), may be helpful in deciding the relative importance of potential targets. The table below has expanded to include the target and the impact of the event in conjunction with the signal.

<table>
<thead>
<tr>
<th>Example</th>
<th>Target</th>
<th>Signal</th>
<th>Outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dairy Product Shortage</td>
<td>• Lactose</td>
<td>• Shortage of dairy products</td>
<td>• Babies with kidney problems</td>
</tr>
<tr>
<td></td>
<td>• High value dairy products</td>
<td>• Rise in the price of dairy</td>
<td>• Pets dying</td>
</tr>
<tr>
<td>Acetonitrile Shortage</td>
<td>• Acetonitrile</td>
<td>• Shortage of acetonitrile</td>
<td>• No impact to large companies due to risk</td>
</tr>
<tr>
<td></td>
<td>• Acrylonitrile</td>
<td>• Rise is the price of the commodity</td>
<td>mitigation. Some smaller companies and</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>laboratories were impacted due to cost</td>
</tr>
<tr>
<td>Diethylene Glycol</td>
<td>• Complex supply chain with distributors,</td>
<td>• Dramatic cost reduction of the adulterated</td>
<td>• Numerous deaths</td>
</tr>
<tr>
<td>Contamination of Glycerin</td>
<td>brokers, and repackagers</td>
<td>material as opposed to general market costs</td>
<td></td>
</tr>
</tbody>
</table>

A target can be both the actual material and the transport of the material through the supply chain. The quality risk assessment should identify the greatest risks for adulteration, substitution, counterfeiting, theft, or illegal diversion associated with a material and its transport.

### 3.4 Environmental Scanning

Environmental scanning is a process for reviewing external information with the potential to have an impact on selected targets. It involves the collection and analysis of information relevant to pre-defined targets. With defined targets and signals, it can be used in a proactive manner, looking for threats to the security of the supply chain and for updating risk assessments and controls.

Environmental scanning can be used to better understand supplier and supply chain data, either on an ongoing basis or in response to an event, typically a high profile event or crisis. Relevant signals from environmental scans include market shortages, rapidly increasing costs, geopolitical, meteorological, or other environmental events. Continuous environmental scanning helps identify problems before they result in widespread economically motivated adulteration, counterfeiting, or illegal diversion.
3.4.1 Determining the Relevance

A variety of information from environmental scans may be linked to form a signal. In the case of the dairy product shortage, there were several pieces of information which could have been linked to form a signal of potential economically motivated adulteration.

The earliest glimmer of a potential issue was the drought in Australia which caused a dairy product shortage. Another event was the shortage of feed for the cattle prompted by smaller rainfall in other locations, further contributing to the dairy product shortage. Another event was the detection of melamine as an adulterant in pet food to raise the protein assay. Separately, these events may not have been viewed as a signal for intentional adulteration of dairy products. However, when linked together, these three events could have been viewed as a signal for potential economically motivated adulteration of dairy products with melamine.

3.4.2 Post Marketing Surveillance

An unusual complaint and/or adverse event and/or an unusual increase in adverse events, also may be used as a signal. Monitoring criminal activity levels related to cargo theft or counterfeiting in certain geographical locations is also a signal. Combining post market surveillance information with other information from environmental scans may signal potential economically motivated adulteration, theft, or counterfeiting within the supply chain.

3.4.3 Signal Response

A signal detected by an environmental scan should be evaluated using multidisciplinary approaches to determine its potential impact on a material, product, or point in the supply chain. If it is determined there is a potential impact, plans should be developed consistent with the risk. A plan should include steps to assure a safe and continued supply of the potentially affected material. For example, where there is an identified higher risk for cargo theft, changing routes, adding additional drivers/escorts, and/or adding covert tracking devices should be considered, to mitigate the risk of theft. Alternatively, where there is an identified higher risk for the potential use of a known adulterant, there should be consideration of additional testing of material for the adulterant. With respect to the signals showing an increased potential for illicit use of melamine in dairy products, additional testing for melamine could have been used as an enhanced supplier control.
Supplier Quality Management

Supplier Quality Management has three key elements:

- supplier assessment and selection
- written agreements for quality activities
- supplier monitoring and review

These elements of an organization’s Supplier Quality Management Program should be integrated to allow appropriate modes of control to be implemented. When these controls are integrated, there is a higher level of assurance over suppliers and outsourced activities.

4.1 Supplier Assessment and Selection

It is recommended that organizations apply quality risk management principles to the process of assessing and selecting a potential supplier. The risk-based approach should be appropriate to the material being supplied. For example, the approach to assess and select a potential supplier of drug product will be different both in depth and content to that of the approach of assessing and selecting a potential supplier of a packaging material. The risks and approach toward the assessment also may differ based on geographic location of the supplier and the regulatory environment under which the supplier operates.

It is recommended that the organization’s requirements and standards are clearly documented and communicated at the start of the assessment/selection process. It is good business practice to communicate these requirements in advance of the bidding process so potential suppliers can assess their capability and willingness to meet these expectations. This allows for effective pre-screening of new suppliers. It is important to ensure clarity of expectations. For example, documenting specific requirements such as material specifications is as important as documenting performance expectations. The assessment of capability against these requirements greatly improves when clearly communicated at the initiation of the process.

A multidisciplinary approach is recommended for the supplier selection process. Including functional groups such as Regulatory, Quality, Environmental Health & Safety (EHS), Technical, Security, and Procurement will frequently lead to a more balanced assessment of potential suppliers.

For all new suppliers, a risk assessment should be conducted to determine if an on-site audit is warranted as part of the selection process. The scope, duration, number of auditors, depth, and content of the audit should be risk-based. For example, where there is a risk of economically motivated adulteration or when assessing suppliers in regions where the regulatory framework is still developing, a special approach to the audit may be required to assess additional risks such as fraud, illegal diversion, and counterfeiting. The decision to have cross functional representatives participate in the audit is also risk-based. For example, there is a greater likelihood of including EHS, Finance, and Technology experts in an audit of a contract manufacturer of a drug product than in an audit of a commodity excipient supplier. Financial soundness through analysis of indicators such as credit information also should be assessed.

The full extent of the supply chain should be known and documented in a manner providing the necessary visibility. The organization should have current information from 2nd and 3rd tier suppliers on the logistics of the supply chain from the origin of procured materials through to receipt at the manufacturing location. Organizations also should have current information from the site of manufacture to the next legal owner or buyer of the product.
Organizations may not receive material directly from the original manufacturer. For example, the organization may receive the material through a company that sells, distributes, transports, and/or forwards material, but does not actually make the material (distributor/broker). In some cases, the distributor/broker also may perform a repackaging and/or relabeling operation. This should be assessed as a potential target for adulteration.

When conducting an assessment of a distributor/broker, it is important to understand expectations with regard to supervision of the original manufacturer. If the organization is not directly managing the manufacturer (supplier) and will rely on the distributor/broker to manage the supply chain, then the assessment should focus on this capability. Whether working directly with the manufacturer or through a broker, the ultimate responsibility for the safety and quality of the material remains with the organization releasing the drug product to the market.

Any deficiencies found as part of the supplier assessment should be ranked as to seriousness and timing for remediation. For example, a critical deficiency could disallow the selection of the supplier until corrections and/or preventive actions have been put in place.

At the completion of the selection process, a formal risk assessment should be conducted, capturing the risks identified during the evaluation and any risk controls required. The assessment should include quality, regulatory, technical, and performance strategies to reduce and/or mitigate identified risks. Costs associated with risk mitigation should be captured. It is recommended that the final costs of the product or material are calculated near the end of the overall selection process so that all costs, including risk controls, can be built into the true total cost. This assessment is an important aid in supporting the decision to select or reject a vendor/supplier.

At this point in the risk management process, there should be defined processes for communicating the risk assessments and the risk controls.

The assessment and selection process should be complete and documented before proceeding to approval of a new supplier.

4.2 Written Agreements for Quality Activities

Once the selection process is completed, written agreements for quality activities should be developed with the supplier of choice. Quality/Technical Agreements, Supply Agreements, contracts, or comparable written agreements should clearly communicate and document the organization’s requirements and standards, and should specify the need for the supplier to conform to the organization’s requirements. The content (detail, specificity, etc.) of the agreements should be risk based, and as an example, may be more prescriptive for a supplier of drug product than for a supplier of a packaging material. These agreements should be developed as part of the formal supplier control process. An understanding of the supply chain and assurance that appropriate quality and technical agreements exist throughout the supply chain is critically important.

Organizations can use written agreements to drive transparency of the supply chain, and oblige down-stream supply chain partners to meet standards of good practice and cooperation in the prevention and management of any suspected cases of counterfeiting. These requirements can be reviewed during partner audits to help ensure compliance.

The written agreement should define the:

- roles, responsibilities, and communication processes for quality related activities
- required quality systems, and the organization’s expectations of those systems
- agreed upon supply chain
- expected controls
• need to conform to the defined supply chain at all times

• the documentation expectations to ensure chain of custody when materials move through the supply chain

Minimum requirements should be established around notification of changes, notification of significant deviations, notification of any regulatory inspections, a provision for documentation review, and a provision for on-site audits.

There should be written agreements with distributor/brokers which include the requirements listed above.

The written agreement is a dynamic document and should be reviewed and revised (if necessary) periodically to ensure ongoing effectiveness. Supplier performance should be compared to expectations defined in the written agreement on a periodic basis. This allows for continuous monitoring and alignment around written agreement requirements. Performance metrics when established to monitor written agreement compliance can be an effective ongoing supervisory tool. Audits of compliance with written agreement requirements should be conducted on a periodic basis.

Written agreements for quality activities can be expanded to include control for prevention and detection of counterfeits. These agreements should include clear language identifying responsibilities related to the prevention and detection of counterfeits. This could include, but is not limited to:

• identify responsibilities of each party in responding to a suspected counterfeit event

• detail the processes for the handling, shipment, and storage of suspected counterfeit products

• detail the procedures for supplying retention samples and other support for suspected counterfeit analyses

• agreed upon methods of determining manufacturing production yield and disclosures when target values are not met

• processes for mutual notification of any suspected counterfeit event or intelligence indicating the potential for the counterfeit event.

Once satisfactory agreements are in place and any deficiencies/improvements identified in the selection processes are resolved, the organization should proceed to approve the supplier for use.

4.3 Supplier Monitoring and Review

Supplier performance should be monitored and reviewed on a regular basis. There should be a process to monitor performance across the supply chain. This starts with a complete understanding of the supply chain. Ongoing verification of the effectiveness of an organization’s supplier’s quality systems to manage suppliers and supply chain is important. This can be accomplished through targeted auditing of these quality systems. There should be periodic verification of the chain of custody.

The goal of supplier monitoring and review is to promote continuous improvement and check the effectiveness of the supplier controls. Monitoring and review of supplier quality performance, the effectiveness of the supplier quality system, and the identification and implementation of required improvements are essential elements of the PQS.

The level of risk controls or quality supervisory activities associated with a supplier and the associated supply chain depends on the risk determined in the Risk Assessment. In general, as the quality risk increases, so will the level of activity associated with quality supervision of the supplier.

The program should include a process to review mandated changes from the quality agreement such as changes to the process and associated controls, changes to the quality system, changes to logistics and distribution.
The program should include a process for significant quality deviation management to include notification to the organization, as well as a process by which needed improvements are managed. A process should be in place to notify the organization of any major deficiencies per the written agreement.

A defined audit program should be established with risk-based criteria for frequency and duration of audits. For suppliers identified as high risk (nature of material, regulatory environment, culture, and economics), the audit program should be designed to identify risk outside of traditional quality system weaknesses (fraud, intentional adulteration). Utilizing an audit team with special skills (language, training, culture, etc.) and an understanding of local risks is beneficial. These audits should include a risk-based approach to determine periodic requirements for ‘on site’ audits to ensure continued compliance to regulatory requirements.

Audits of an organization’s own manufacturing facilities and their distributors and suppliers should include product security elements, quality systems, and cGMPs. In some cases, specific audits for product security may be completed by security specialists. In other cases, cGMP auditors can be trained to evaluate product security during routine GMP audits.

To augment supplier audits in order to include product security, including the following items should be considered:

- physical security of facility (how easy is it to gain entry into the facility, are there security cameras in place, are there barriers in place to prevent removal of product from the facility, etc.)
- procedures for the handling and destruction of waste, particularly rejected product and packaging components
- procedures for the secure handling and storage of product security features such as tamper evident labels, holograms, and other components including packaging materials
- procedures for the secure storage and control of master artwork files, product security specifications, and manufacturing formulas
- adherence to company and/or site specific procedures for the handling of suspected counterfeit events
- review of production yields, capacity, and/or product amounts compared with raw material purchases
- systems to prevent and/or detect conflicts of interests by management and personnel (including commercial, political, or financial pressures)
- training and qualification of personnel directly involved in product security and counterfeit detection
- logistics and transportation systems and controls

Deficiencies found during auditing or monitoring should be managed via Corrective and Preventive Action (CAPA) for the supplier, with documented CAPA, as well as timing and proof of completion. A process to assess the effectiveness of implemented actions should be established.

Where supplier monitoring and review indicates a supplier may need enhanced supervision activities as part of risk reduction/risk mitigation strategies an organization should consider enhanced supervisory activities which could include the following in order to reduce/mitigate risk:

- review of Batch Records for every lot
- review of Deviations for every lot
- review and approval of all changes by the supplier
• additional testing upon receipt of every lot
• increased audit frequency
• targeted audits (e.g., for fraud)
• unannounced visits
• assignment of organization’s employee inside a supplier’s plant (‘person in the plant’)
• routine quality review meetings at supplier
• chain of custody verification for supply chain controls
• review of documentation from 2nd and 3rd tier suppliers
• business continuity strategies

An organization should have a defined and agreed upon improvement plan with the supplier to obviate the need for the additional controls.
5 Logistics and Transportation Service Providers

5.1 Management of Logistics and Transportation Service Providers

The management of Logistics and Transportation Service Providers is analogous to Supplier Quality Management in that the processes for the assessment, selection, monitoring, and review are similar; however, the focus includes more elements of security features.

Assuring supply chain security is largely about securing physical distribution channels. Controls are needed to assure logistics service providers do not become an avenue for either illegal diversion of product outside of the legitimate supply chain or introduction of counterfeit or diverted product into the legitimate supply chain.

5.2 Selection and Assessment of Logistics and/or Transportation Service Providers

In selecting logistics and/or transportation service providers, the same principles used in the selection of a supplier should be applied. Organizations should have processes for the selection of new logistics and transportation service providers. New providers should always be carefully screened. The use of physical visits to the facility and examination of equipment, conveyances, and building security measures can provide useful information.

Specific attention should be paid to ensure pertinent security measures are in place and adhered to at the logistics and/or transportation service provider.

As part of the selection and assessment, there should be evidence of financial soundness, capability of meeting contractual security requirements, and the ability to identify and correct security deficiencies. This should be reviewed by the organization prior to selecting carriers and/or storage providers.

Background information including a history of claims, the types of commodities handled, and the geographic areas served should be provided by the service provider and used as part of the assessment and selection process. Hiring practices of the provider should be reviewed.

As part of the assessment, the organization should confirm whether the sales volume of the provider makes sense relative to the size of the operation. A review of the relevant permits will also demonstrate if the provider is authorized to handle pharmaceutical products where such permits are required. If the provider will be handling controlled substances, those permits should also be reviewed along with necessary security measures such as caged areas.

5.3 Review of Physical Premises

5.3.1 Physical Barriers

Physical barriers are an important part of assuring the security at service providers. Fences provide necessary physical barriers and deterrents guarding against unauthorized access. Perimeter fencing should enclose the areas around cargo handling and storage facilities. Interior barriers within a cargo handling structure should be used to segregate domestic, international, high value, and hazardous cargo. All barriers should be regularly inspected for integrity and damage.

5.3.2 Gates

Gates providing access through a fenced-in area through which vehicles and/or personnel enter or exit should be manned and/or monitored. The number of gates should be kept to the minimum necessary for proper access and safety. Gates should be secured with locking devices. The issuance of these locks and keys to the locks should be controlled by management and/or security personnel.
5.3.3 Access Controls

Access controls should include the positive identification of all employees and visitors at all points of entry. Access controls prevent unauthorized entry to facilities, maintain control of employees and visitors, and protect company assets.

5.3.4 Alarm Systems

Alarm systems and video surveillance cameras should be utilized to monitor premises and prevent unauthorized access to cargo handling and storage areas. The receiving and loading areas of the provider should be evaluated for need for monitoring capabilities.

5.3.5 Loading Docks

Loading docks should not have a space between the tail of the truck and the building where product can be stolen or counterfeit materials can be introduced.

5.4 Assessment and Controls of Personnel

5.4.1 Employees

Background checks (such as employment history and references) and verifications should be conducted for prospective employees, and where applicable, current employees. Such screening processes should be consistent with government regulations and legal considerations. Once employed, checks should be performed based on cause, and/or the sensitivity of the employee’s position. Organizations should have processes established to remove identification, and access to facilities and systems for terminated employees.

An employee identification system should be in place for positive identification and access control purposes. Employees should only be given access to those secure areas needed for the performance of their duties. Company management or security personnel should adequately control the issuance and removal of employee identification badges. Procedures for the issuance, removal, and changing of access devices (e.g., keys, key cards) should be documented.

5.4.2 Visitors

Visitors should present photo identification for documentation purposes upon arrival. All visitors should be escorted and visibly display temporary identification. Control of visitor badges should be consistent with employee badge controls.
6 Transport and Control of Materials

6.1 Materials Controls

Both customers and intercompany receivers of drug product should be especially careful to monitor for the intrusion of diverted product. Seal numbers taken off arriving trucks should be checked against the seal numbers recorded on shipping papers. The number of boxes received should be the same as the number of boxes recorded on shipping papers and invoices as shipped. Boxes should be physically examined for evidence of original closures, such as tape, which may have been replaced. Boxes with visible differences, e.g., different shade or size of carton, should be examined carefully.

6.2 Warehousing and Distribution Controls within the Organization

Organizations should monitor their packaging, packing, and shipping departments, e.g., use surveillance equipment. Detection processes should be consistent with the risk of illegal diversion of given drug products. Workers in these areas should be aware of the area surveillance as a deterrent. Periodic job rotation, to include security personnel, should be considered. The identity of the person who packs from bulk and who packs for shipping should be recorded. Claims for shortages should be checked for correlation to these workers. Product pilfered by workers is considered diverted product and may find its way into illegal channels. Additional controls could include the removal of pockets from lab coats and uniforms and surveillance cameras could be mounted where they can be easily seen.

6.3 Containers

Processes should be in place to verify the physical integrity of the container structure prior to loading, including the reliability of the locking mechanisms of the doors.

A seven-point inspection process is recommended for all containers, including:

1. front wall
2. left side
3. right side
4. floor
5. ceiling/roof
6. inside/outside doors
7. outside/undercarriage

Containers should be stored in a secure (e.g., locked, controlled entry) area to prevent unauthorized access and/or manipulation. A process should be in place for reporting unauthorized entry into containers or container storage areas.
6.4 **Seals**

Numbered single use seals should be used and recorded on shipping papers when the entire conveyance is used for one shipment. Only designated employees should distribute container seals for integrity purposes. There should be procedures in place for the control and reconciliation of seals; describing how to properly affix seals onto loaded containers and how to recognize and report compromised seals or seal discrepancies to the organization.

6.5 **Shipping and Receiving Processes**

Arriving cargo should be reconciled against information on the cargo manifest. The cargo should be accurately described, and the weights, labels, marks, and piece count indicated and verified. Departing cargo should be verified against purchase or delivery orders. Drivers delivering or receiving cargo should be positively identified before cargo is received or released.

All shortages, overages, and other significant discrepancies or anomalies should be resolved and/or investigated appropriately.

There should be processes in place to cover shipping and receiving in warehouses, including procedures for pickup and delivery from trucking companies and examination of the physical facility for access controls.
7 Specific Programs

7.1 Specific Programs for Anti-Counterfeiting

7.1.1 Processes

There should be defined anti-counterfeiting processes, including the handling of suspected counterfeit events, the development and use of product security features, and other measures to protect product against the threat of counterfeits.

Because counterfeits are generally inserted into the supply chain by those working externally to the license-holding manufacturer, it is useful for organizations to build systems deterring these actions in the first place, detecting insertion and abuse of distribution channels and preparing to disrupt identified incidents efficiently. A common phrase used by those working in this area is “Deter, Detect, and Disrupt.” Discuss below are some of the steps and processes an organization can use to augment their PQS to more effectively deter, detect, and disrupt counterfeit activity.

7.1.2 Enable Authentication of Products

Security features (overt, covert, forensic, tamper-evidence, and serialization/track and trace) offer opportunities for deterrence, detection, and even aspects of disruption. While manufacturers and regulators generally acknowledge there is no technological best solution, the very use of security features can discourage criminals from attempting to simulate or tamper with medicines. Likewise, the use of these features coupled with appropriate communications to user groups (e.g., patients, medical staff, channel partners, and law enforcement) can greatly enhance the ability to detect counterfeit products.

7.1.3 Maintain a Counterfeiting Incident Management Plan

A counterfeit incident management plan is a process describing an organization’s governance and management of incidents of counterfeits. By having and exercising a counterfeit incident management plan, organizations can be better prepared to effectively disrupt counterfeit incidents as they occur. A key part of this plan is to establish and maintain contacts with regulators and law enforcement and cooperation with industry anti-counterfeiting organizations.

7.2 Specific Programs for Illegal Diversion

7.2.1 Interactions with Customers

A customer is defined as the point where the first legal change in ownership of a product takes place. New customers should always be screened carefully. Determining if the customer is legitimately allowed to supply drug products and does so for the drug product’s intended purpose and not off-label usage is extremely important.

A risk-based approach should be used in developing a program for physical visits to the customer’s distribution center or pharmacy. Prescription medicines should be stored securely with limited access. The hiring practices of the customer should be reviewed to see if there are background checks of new employees and other security processes.

7.2.2 Interactions with Distributors

Distributors should be willing to share information on their customer base. If sales are directly to pharmacies, the distributor, where permitted by law, should be willing to share information about expected sales volume. The purchase volume should make sense relative to the size of the customer’s business and population served.
Particular attention should be paid to buyers who claim to be purchasing for export purposes only. The same kinds of capabilities should be evidenced in the case of buyers for export as for domestic purchasers. The market to which the drug products are to be exported should be identified. It is advisable to determine the following prior to agreeing to a specific transaction:

- Determine if the organization supplying the drug product is already represented in the foreign market and the implications of selling to a given buyer.
- Determine if there is alignment between the export market and the therapeutic indication of the product.
- Determine if the buyer has the required licenses and permits.
- Determine if the buyer is in a compatible or the same line of business.
- Determine and validate the credentials of the business through the exporting country’s trade ministry or through private means.
- Determine if the buyer is listed as a prohibited party for a given country.

Attention should be paid to specific signals such as a willingness to pay in cash, a domestic delivery address, or inconsistencies in facility/equipment and purported business.

Additional controls could include using an organization’s own freight forwarder to arrange the export, and unannounced visits to the customer to walk through the facility.

There should be processes in place to assure subsidiaries and distributors are applying similar controls.

Customers can assist in detection of illegal diversion. Clear communication channels should be in place to notify the organization of any suspect activity.

Organizations should monitor inexplicable variations in sales volume or sales volume not correlated to the size of the market population. Point of sales information indicating unusually large purchases by customers or end users can be used as an additional signal of illegal diversion activity.

### 7.3 Specific Programs to Prevent Cargo Theft

#### 7.3.1 Cargo Theft Awareness

Cargo theft in the pharmaceutical industry continues to grow and pose an increased threat. Many of the same preventative measures outlined for diversion and adulteration apply to this threat. Regionally, the threat varies greatly, both in degree and type. Most often the threat is non-violent and non-confrontational with the parked truck simply being stolen at a rest stop with the driver away from the vehicle. However, some regions are more direct and confrontational in approach; with theft happening on the road, forcing drivers to stop, and at traffic stops with guns threatening harm if resistance is met.
7.3.2 Cargo Theft Prevention

While the threats may be different and preventative measures will vary to meet those threats, the idea of how to stop a theft prior to the event happening is the most important aspect in protecting against cargo theft. The process is never a simple, one dimensional solution. A lock may only slow and not stop a determined thief. The most effective approach is one of layered defenses. The process starts with the selection of partnered carriers, vetting and selecting those with good equipment, security programs and providing identification lists of selected drivers for shipments. Briefing those drivers prior to departure to create awareness of the threat and the need to know what is happening around the vehicle is an important first step. Good locks or high security seals are an important indicator for someone tampering with your shipment, and may slow a thief down sufficiently to identify them and possibly allow them to be caught in the act. Route selection and the risk analysis for the route selection process is an often over looked aspect of how material can be safely shipped. Avoiding areas of known activity or questionable stops are key to avoiding problems.

Most of these solutions are passive, but active monitoring and tracking of shipments of higher value or higher risk also help in maintaining a safer shipment and to assure materials are moving as planned. This can be done through a number of methods, from having the drivers call in periodically to report their location and progress to using common dispatching/communication systems with satellite communication. These can be easily defeated in the event of hijacking. There also are covert embedded tracking devices that can be hidden within the shipment or on the truck able to give exact location of the trailer at anytime. With geo-fencing of the planned routings, alerts can be provided if the vehicle goes off the planned route. This type of device is extremely effective in product recovery, if needed.

It is important to remember these devices are simply tools to be applied, and they should be used in tandem with other programs or services. If the tracking device does not provide an alert, then it should be actively monitored to be of use. The monitoring service can be done in house, but is probably best accomplished with a service with trained analysts and connections with law enforcement in the event of an active theft. A final layer could be escort, or guard services to trail behind the vehicle. While this can be very manpower intensive, there are times this level of security can be justified.

The key to a good cargo security program is still a layered approach with multiple procedures being applied as the threat requires. The process should be integrated and actively monitored to assure it is being successfully employed. Any static security plan is subject to becoming routine and taken for granted. Involvement by the shipper and supported engagement by all partners in the supply chain are critical factors to the success of cargo theft prevention program.