BRIEFING

〈 **1083.4** 〉 **Supply Chain Integrity and Security.** A new series of general informational chapters describing various aspects of the pharmaceutical supply chain replaces *Good Distribution Practices—Supply Chain Integrity* 〈 1083 〉, which appeared as an *In-Process Revision* in *PF* 38(2) but since then has been canceled. USP is proposing a new series of Good Distribution Practices (GDP) General Chapters, which were developed based on a review of three existing general chapters, *Good Storage and Distribution Practices for Drug Products* 〈 1079 〉, *Good Distribution Practices* 〈 1083 〉, and *Good Distribution Practices for Bulk Pharmaceutical Excipients* 〈 1197 〉. These three existing general chapters provide information related to the storage, shipment, distribution, and transportation of pharmaceutical components and products. The review showed overlapping and complementary items among these general chapters and highlighted the need to revisit USP chapters on GDP from an overarching perspective. These new general chapters will cover material flow beginning with initial procurement and continuing throughout the supply chain to delivery to the end user for pharmaceutical components and products, medical devices, and dietary supplements. The chapters will address four main GDP topics—*Quality Management System* 〈 1083.1 〉, *Environmental Conditions Management* 〈 1083.2 〉, *Good Importation and Exportation Practices* 〈 1083.3 〉, and *Supply Chain Integrity and Security* 〈 1083.4 〉—highlighting best practices and principles.

(GCPS: D.G. Hunt.) Correspondence Number—C139775

Add the following:

〈 1083.4 〉 SUPPLY CHAIN INTEGRITY AND SECURITY

INTRODUCTION

Supply Chain Integrity and Security (SCIS) is defined as a set of policies, procedures, and technologies used to provide visibility and traceability of products within the supply chain. This is done to minimize the end-user's exposure to adulterated, economically motivated adulteration, counterfeit, falsified, or misbranded products or materials, or those which have been stolen or diverted. This is minimized by implementing procedures to control both the forward and the reverse supply chains.

SCIS involves reducing risks that arise anywhere along the supply chain, from sourcing materials and products to their manufacture and distribution. Importation and exportation are discussed under *Operations* in *Quality Management System* 〈 1083.1 〉

and in *Good Importation and Exportation Practices* 〈1083.3〉. The ultimate goal is to detect adulterated, falsified, or counterfeit products and prevent them from entering the supply chain.

The chapter is structured in three sections as shown in *Figure 1*.

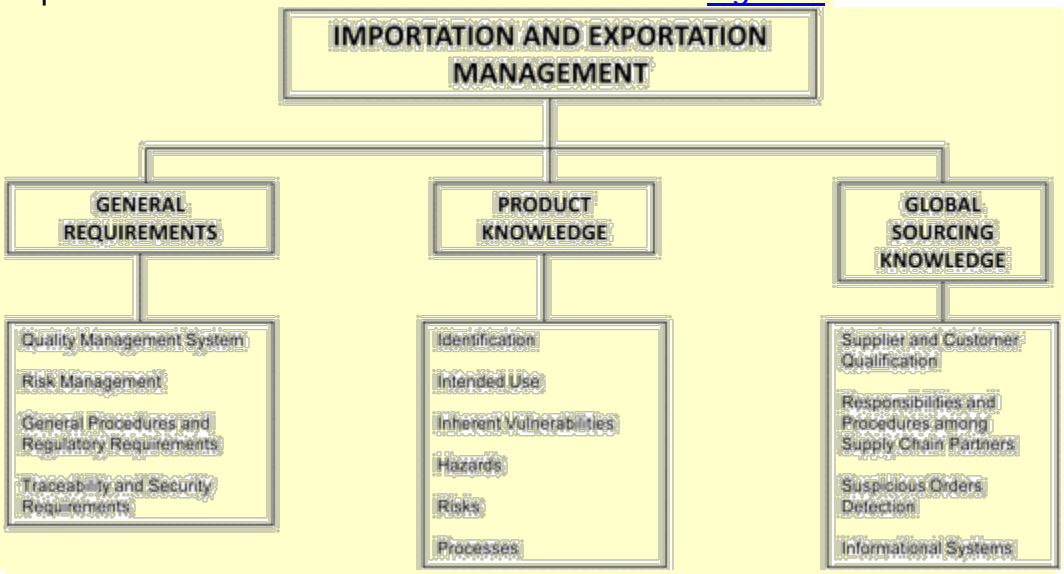

Figure 1. 〈1083.4〉 Supply chain integrity and security chapter structure.

SUPPLY CHAIN INTEGRITY

Supply chain integrity should be ensured to provide quality and safe products to the end-user. Risks to the integrity of products entering the supply chain can include:

- Adulteration of the material or product
- Counterfeit or falsified material or product
- Misbranded products containing unlabeled ingredients
- Expired products that are relabeled and sold to end-users
- Materials or products meant for destruction that are diverted for sale
- Materials and products that are not effectively recalled
- Materials and products that are not transported and stored according to the environmental conditions stated on the label

The risks and strategies to combat a threat will vary depending on the area of the supply chain being addressed. In-depth guidance is presented in subsequent chapters. The organization should have in place a Supply Chain Management System integrated with the Quality Management System (chapter 〈1083.1〉). This system should be designed and implemented to identify and control risks within the supply chain and provide a response when adulterated or counterfeit products are detected or a deviation is observed from label environmental conditions during transportation and/or storage.

Organization should conduct a risk-based assessment of their supply chains to identify risks, estimate the likelihood of them occurring (probability), and their consequences

(severity). For this assessment, at least the following factors should be taken into account, but not limited to:

- Attractiveness of certain materials and products for adulteration or counterfeiting (e.g., products with high value, widely sold products, or those in short supply)
- Complexity and degree of control of the supply chain in obtaining materials and products from overseas suppliers
- The ability to maintain the product within specified labeled environmental conditions, especially during transportation

Based on the risk assessment, a plan should be designed and implemented to maintain supply chain integrity and formulate a response when an integrity breach is discovered containing, but not limited to, the following steps:

- Identification of the product description, product lot(s), and quantity
- Promptly reporting the adulteration or counterfeiting occurrence to the regulatory authorities
- Preparation of a public notification in the form of a press release and/or posting on the company's website
- Reviewing the company's security procedures in response to the breach
- Investigating the deviation from the labeled environmental conditions as to the extent of the deviation, the time period of its occurrence, and the reason(s) for the breach
- Determining the effect of the breach of the environmental conditions on the product's safety and effectiveness
- Reviewing the company's transportation or storage procedures in response to the breach

SUPPLY CHAIN SECURITY

Procedures should be in place to mitigate security risks to the supply chain, such as theft during storage and transportation and product diversion.

Product Theft

Thefts of cargo during transportation or from warehouses can occur at any point in the supply chain. Legitimate packaging and labeling materials can also be stolen or diverted in order to form counterfeited products. Thefts can be targeted to specific products, for example those of high value, or opportunistic where the cargo contents are unknown to the perpetrators at the time of the theft but do contain medical supplies. Procedures should be in place to evaluate the risk of theft and to establish procedures to respond to a theft when it occurs.

The organization should have in place a Security Management System integrated with the Quality Management System (chapter 〈 1083.1 〉). This system should be designed and implemented to identify and control risks within the supply chain, and how to respond to a theft when it occurs. A security policy should be established.

Organizations should conduct a risk-based assessment of their supply chains to identify risks, estimate the likelihood of them occurring (probability), and their consequences (severity). For this assessment, at least the following factors should be taken into account, but not limited to:

- Attractiveness of certain products for theft (e.g., products with high value or widely sold, products with potential for abuse, or those in short supply)
- Transportation routes and location, and design of storage facilities
- Security threats (known criminal index) associated with transportation mode, shipping routes, and/or storage locations
- The duration of shipments or time that the shipment is to be held at a particular location
- The country of origin and destination

Based on the risk assessment, a security plan should be designed and implemented. Legal, statutory, and other regulatory requirements should be observed.

- All security incidents should be recorded and periodically reviewed. If the security incident was a consequence of a failure in a system or procedure already in place, the incident should also be handled as a nonconformance.
- Organizations should perform security audits periodically to verify the level of compliance with the security plan and its efficiency.
- Historical data should be evaluated to address new security measures or maintain existing ones.
- Organizations should have layered defenses against cargo theft, which include but are not limited to procedures, technology for security and monitoring, high security locks and seals, intelligence and information analysis, well trained personnel, and others.

Organizations should have incident management procedures in place to respond to a theft which should contain, but is not limited to, the following steps:

- Identification of the product(s) involved and source, including quantity, lot number(s), and/or any other unique identifier(s) used to control the product or shipment
- Date and location of incident occurrence
- Promptly reporting the theft to both law enforcement and regulatory authorities in the country of origin and where the theft occurred
- Communicating with the intended customer(s) of the shipment(s)
- Preparation of a public notification in the form of a press release and posting on the company's website in the case of drug products, dietary supplements, and medical devices
- Reviewing the company's security procedures in response to the theft
- Incidents should be investigated, tracked, and trended and the results used to formulate continuous improvement to security systems

Product Diversion

Products can be diverted from the legitimate supply chains and re-introduced back into legal or illegal markets. The examples of security breaches of a supply chain include, but are not limited to, the following:

- Products sent for destruction are diverted
- Products are obtained from black-market prescriptions and resold
- Products purchased from patients or unlicensed sources are resold
- Product samples are diverted and/or repackaged
- The diversion and resale of drugs intended for use by non-profit organizations
- Donated product that is diverted
- Expired product diverted, relabeled with a new expiration date, and resold
- Products are illegally imported from another country through internet purchases either by medical professionals or by patients

Organizations should have procedures in place to address the risk of product diversion and to respond when it occurs. The procedures should contain, but not be limited to, the following steps:

- Investigation of unusually high levels of dispensing activities by medical professionals for products with the potential for abuse and/or high street value
- Investigation of product offered below normal market value

APPENDIX

In the context of this chapter, the following definitions are used.

Adulteration: A drug or device shall be deemed to be adulterated, if "(2)(A) it has been prepared, packed, or held under insanitary conditions whereby it may have been contaminated with filth, or whereby it may have been rendered injurious to health; or (B) ...the methods used in, or the facilities or controls used for, its manufacture, processing, packing, or holding do not conform to or are not operated or administered in conformity with current good manufacturing practice to assure that such drug meets the requirements of this [Act] as to safety and has the identify and strength, and meets the quality and purity characteristics, which it purports or is represented to possess" (FDA, Food, Drug, and Cosmetic Act, Sec. 501, §351).

Counterfeit drug: "A drug which, or the container or labeling of which, without authorization, bears the trademark, trade name, or other identifying mark, imprint, or device, or any likeness thereof, of a drug manufacturer, processor, packer, or distributor other than the person or persons who in fact manufactured, processed, packed, or distributed such drug and which thereby falsely purports or is represented to be the product of, or to have been packed or distributed by, such other drug manufacturer, processor, packer, or distributor" [21 U.S.C. §321(g)(2) (2004)]. This is comparable to Falsified Medicinal Product in the EU.[a]

Criminal indices: Comprehensive databases maintained at the local, state, and federal level (National Crime Information Center) that provide detailed statistics of

criminal offenses and offenders.

Diversion: The unlawful redirection of pharmaceutical products, components, or devices from the authorized distribution system and subsequent distribution to legal and illegal markets. The diversion can occur anywhere in the chain of distribution from the pharmaceutical manufacturer, drug packager, transporter, or wholesaler, to the institutions where the product is dispensed, i.e., retail pharmacies, clinics and hospitals, or the patient.

Economically motivated adulteration: 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.

Falsified medical product: Any medicinal product with a false representation of its identity, including its packaging and labeling, its name, or its composition as regards any of the ingredients including excipients and the strength of those ingredients; its source, including its manufacturer, its country of manufacturing, its country of origin, or its marketing authorization holder; or its history, including the records and documents relating to the distribution channels used.

Forward supply chain: Refers to the movement and holding of materials or products from the manufacturer to the customers.

Integrity: Ensuring the identity and authenticity of a material or product by a set of procedures.

Reverse supply chain: Refers to the movement and holding of materials or products from the customers to the previous supply chain partner, e.g., the pharmacy, the distributor, the manufacturer. Examples of a reverse supply chain are: returns, recalls, remanufacturing, and refurbishment.

Supply chain integrity: An unbroken chain of custody beginning with sourcing of materials, through manufacture and distribution, ending in the receipt of the product by the intended end-user.

Supply chain security: Mitigation of security risks to the supply chain such as theft during storage and transportation, and diversion.

Supply chain security management: Establishment, implementation, and maintenance of processes and procedures to mitigate security risks in the supply chain.

[a] U.S. definition for counterfeit drugs at the time of publication.