

# Guidance for Industry

## **COSMETICS PROCESSORS AND TRANSPORTERS: COSMETICS SECURITY PREVENTIVE MEASURES GUIDANCE**

### ***DRAFT GUIDANCE***

**This guidance document is being distributed for comment purposes only.**

Draft released for comment on XXXX, 2003

Comments and suggestions regarding this draft guidance should be submitted by XXXX, 2003 to Dockets Management Branch (HFA-305), Food and Drug Administration, 5630 Fishers Lane, room 1061, Rockville, MD 20852. All comments should be identified with the Docket Number XXXX. For questions regarding this draft guidance contact John Kvenberg, (301) 436-2359 or Donald W. Kraemer, (301) 436-2300.

U.S. Department of Health and Human Services  
Food and Drug Administration  
Center for Food Safety and Applied Nutrition (CFSAN)  
XXXX, 2003

030-0092

GDL-2

## GUIDANCE FOR INDUSTRY

### COSMETICS PROCESSORS AND TRANSPORTERS: COSMETICS SECURITY PREVENTIVE MEASURES GUIDANCE

**This draft guidance represents the Agency's current thinking on appropriate measures that cosmetics establishments may take to minimize the risk that cosmetics under their control will be subject to tampering or other malicious, criminal, or terrorist actions. It does not create or confer any rights for or on any person and does not operate to bind FDA or the public.**

#### Purpose and Scope:

This draft guidance is designed as an aid to operators of cosmetics establishments (for example, firms that process, store, repack, re-label, distribute, or transport cosmetics or cosmetics ingredients). This is a very diverse set of establishments, which includes both very large and very small entities.

This draft guidance identifies the kinds of preventive measures operators of cosmetics establishments may take to minimize the risk that cosmetics under their control will be subject to tampering or other malicious, criminal, or terrorist actions.

Operators of cosmetics establishments are encouraged to review their current procedures and controls in light of the potential for tampering or other malicious, criminal, or terrorist actions and make appropriate improvements. FDA recommends that the review include consideration of the role that unit and distribution packaging might have in a cosmetics security program. This guidance is designed to focus operator's attention sequentially on each segment of the cosmetic production system that is within their control, to minimize the risk of tampering or other malicious, criminal, or terrorist action at each segment. To be successful, implementing enhanced preventive measures requires the commitment of management and staff. Accordingly, FDA recommends that both management and staff participate in the development and review of such measures.

#### Limitations:

Not all of the guidance contained in this document may be appropriate or practical for every cosmetics establishment, particularly smaller facilities and distributors. FDA recommends that operators review the guidance in each section that relates to a component of their operation, and assess which

preventive measures are suitable. Example approaches are provided for many of the preventive measures listed in this document. These examples should not be regarded as minimum standards. Nor should the examples provided be considered an inclusive list of all potential approaches to achieving the goal of the preventive measure. FDA recommends that operators consider the goal of the preventive measure, assess whether the goal is relevant to their operation, and, if it is, design an approach that is both efficient and effective to accomplish the goal under their conditions of operation.

#### Structure:

This draft guidance is divided into five sections that relate to individual components of a cosmetics establishment operation: management; human element – staff; human element – the public; facility; and operations.

#### Related Guidance:

FDA has published two guidance documents on food security entitled, “Food producers, processors, and transporters: Food security preventive measures guidance”, and “Importers and filers: Food security preventive measures guidance” to cover the farm-to-table spectrum of food production. The two documents are available at

[http://www.access.gpo.gov/su\\_docs/aces/aces140.html](http://www.access.gpo.gov/su_docs/aces/aces140.html).

#### Additional Resources:\*

A process called Operational Risk Management (ORM) may help prioritize the preventive measures that are most likely to have the greatest impact on reducing the risk of tampering or other malicious criminal, or terrorist actions against cosmetics. Information on ORM is available in the Federal Aviation Administration (FAA) System Safety Handbook, U.S. Department of Transportation, FAA, December 30, 2000, Chapter 15, Operational Risk Management. The handbook is available at:

[http://www.asy.faa.gov/Risk/SSHandbook/Chap15\\_1200.PDF](http://www.asy.faa.gov/Risk/SSHandbook/Chap15_1200.PDF).

---

\* Reference to these documents is provided for informational purposes only. These documents are not incorporated by reference into this guidance and should not be considered to be FDA guidance.

The U.S. Department of Transportation, Research and Special Programs Administration published an advisory notice of voluntary measures to enhance the security of hazardous materials shipments. It is available at: [http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=2002\\_register&docid=02-3636-filed.pdf](http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=2002_register&docid=02-3636-filed.pdf). The notice provides guidance to shippers and carriers on personnel, facility and en route security issues.

The U.S. Postal Service has prepared guidance for identifying and handling suspicious mail. It is available at: <http://www.usps.com/news/2001/press/mailsecurity/postcard.htm>.

The Federal Anti-Tampering Act (18 USC 1365) makes it a federal crime to tamper with or taint a consumer product, or to attempt, threaten or conspire to tamper with or taint a consumer product, or make a false statement about having tampered with or tainted a consumer product. Conviction can lead to penalties of up to \$100,000 in fines and up to life imprisonment. The Act is available at: <http://www.fda.gov/opacom/laws/fedatact.htm>.

The National Infrastructure Protection Center (NIPC) serves as the federal government's focal point for threat assessment, warning, investigation, and response for threats or attacks against U.S. critical infrastructure. The NIPC has identified the food system as one of the eight critical infrastructures, and has established a public-private partnership with the food industry, called the Food Industry Information and Analysis Center (Food Industry ISAC). The NIPC provides the Food Industry ISAC with access, information and analysis, enabling the food industry to report, identify, and reduce its vulnerabilities to malicious attacks, and to recover from such attacks as quickly as possible. In particular, the NIPC identifies credible threats and crafts specific warning messages to the food industry. Further information is available at <http://www.nipc.gov/> and <http://www.foodisac.org/>.

FDA encourages cosmetics trade associations to evaluate the preventive measures contained in this guidance document and adapt them to their specific products and operations and to supplement this guidance with additional preventive measures when appropriate. FDA welcomes dialogue on the content of sector specific guidance with appropriate trade associations.

## Cosmetics Establishment Operations:

### **Management**

FDA recommends that cosmetics establishment operators consider:

#### Preparing for the possibility of tampering or other malicious, criminal, or terrorist actions

- assigning responsibility for security to knowledgeable individual(s)
- conducting an initial assessment of cosmetics security procedures and operations, which we recommend be kept confidential
- having a security management strategy to prepare for and respond to tampering or other malicious, criminal, or terrorist actions, both threats and actual events, including identifying, segregating, and securing affected product
- planning for emergency evacuation, including preventing security breaches during evacuation
- maintaining any floor or flow plan in a secure, off-site location
- becoming familiar with the emergency response system in the community
- making management aware of 24-hour contact information for local, state, and federal police/fire/rescue/health/homeland security agencies
- making staff aware of who in management they should alert about potential security problems (24-hour contacts)
- promoting cosmetics security awareness to encourage all staff to be alert to any signs of tampering or other malicious, criminal, or terrorist actions, or areas that may be vulnerable to such actions, and reporting any findings to identified management (for example, providing training, instituting a system of rewards, building security into job performance standards)
- having an internal communication system to inform and update staff about relevant security issues
- having a strategy for communicating with the public (for example, identifying a media spokesperson, preparing generic press statements and background information, and coordinating press statements with appropriate authorities)

#### Supervision

- providing an appropriate level of supervision to all staff, including cleaning and maintenance staff, contract workers, data entry and computer support staff, and especially, new staff
- conducting routine security checks of the premises, including utilities and critical computer systems (at a frequency appropriate to the operation), for signs of tampering or other malicious, criminal, or terrorist actions, or areas that may be vulnerable to such actions

### Recall strategy

- identifying the person responsible, and a backup person
- providing for proper handling and disposition of recalled product
- identifying customer contacts, addresses and phone numbers

### Investigation of suspicious activity

- investigating threats or information about signs of tampering or other malicious, criminal, or terrorist actions
- alerting appropriate law enforcement and public health authorities about any threats of or suspected tampering or other malicious, criminal, or terrorist actions

### Evaluation program

- evaluating the lessons learned from past tampering or other malicious, criminal, or terrorist actions and threats
- reviewing and verifying, at least annually, the effectiveness of the security management program (for example, using knowledgeable in-house or third party staff to conduct tampering or other malicious, criminal, or terrorist action exercises and mock recalls and to challenge computer security systems), revising the program accordingly, and keeping this information confidential
- performing random cosmetics security inspections of all appropriate areas of the facility (including receiving and warehousing areas) using knowledgeable in-house or third party staff and keeping this information confidential
- verifying that security contractors are doing an appropriate job, when applicable

## **Human element – staff**

Under Federal law, cosmetics establishment operators are required to verify the employment eligibility of all new hires in accordance with the requirements of the Immigration and Nationality Act, by completing the INS Employment Eligibility Verification Form (INS Form I-9). Completion of Form I-9 for new hires is required by 8 USC 1324a and nondiscrimination provisions governing the verification process are set forth at 1324b.

FDA recommends that cosmetics establishment operators consider:

### Screening (pre-hiring, at hiring, post-hiring)

- examine the background of all staff (including seasonal, temporary, contract, and volunteer staff, whether hired directly or through a recruitment firm) as appropriate to their position, considering candidates' access to sensitive areas of the facility and the degree to which they will be supervised and other relevant factors (for example, obtaining and verifying work references, addresses, and phone numbers, participating in one of the pilot programs managed by the Immigration and Naturalization Service and the Social Security Administration [These programs provide electronic confirmation of

employment eligibility for newly hired employees. For more information call the INS SAVE Program toll free at 1-888-464-4218, fax a request for information to (202) 514-9981, or write to US/INS, SAVE Program, 425 I Street, NW, ULLICO-4th Floor, Washington, DC 20536. These pilot programs may not be available in all states], having a criminal background check performed by local law enforcement or by a contract service provider [Remember to first consult any state or local laws that may apply to the performance of such checks])

Note: screening procedures should be applied equally to all staff, regardless of race, national origin, religion, and citizenship or immigration status.

#### Daily work assignments

- knowing who is and who should be on premises, and where they should be located, for each shift
- keeping information updated

#### Identification

- establishing a system of positive identification and recognition (for example, issuing uniforms, name tags, or photo identification badges with individual control numbers, color coded by area of authorized access), when appropriate
- collecting the uniforms, name tag or identification badge when a staff member is no longer associated with the establishment

#### Restricted access

- identifying staff that require unlimited access to all areas of the facility
- reassessing levels of access for all staff periodically
- limiting access so staff enter only those areas necessary for their job functions and only during appropriate work hours (for example, using key cards or keyed or cipher locks for entry to sensitive areas, color coded uniforms [remember to consult any relevant federal, state or local fire or occupational safety codes before making any changes])
- changing combinations, rekeying locks and/or collecting the retired key card when a staff member is no longer associated with the establishment, and additionally as needed to maintain security

#### Personal items

- restricting the type of personal items allowed in establishment
- allowing in the establishment only those personal use medicines that are necessary for the health of the staff and ensuring that these personal use medicines are properly labeled and stored away from cosmetics handling or storage
- preventing staff from bringing personal items (for example, lunch containers, purses) into cosmetics manufacturing and storage areas
- providing for regular inspection of contents of staff lockers (for example, providing metal mesh lockers, company issued locks), bags, packages, and vehicles when on company property (Remember to first

consult any federal, state, or local laws that may relate to such inspections)

#### Training in cosmetics security procedures

- incorporating cosmetics security awareness, including information on how to prevent, detect, and respond to tampering or other malicious, criminal, or terrorist actions or threats, into training programs for staff, including seasonal, temporary, contract, and volunteer staff
- providing periodic reminders of the importance of security procedures (for example, scheduling meetings, providing brochures or payroll stuffers)
- encouraging staff support (for example, involving staff in cosmetics security planning and the cosmetics security awareness program, demonstrating the importance of security procedures to the staff)

#### Unusual behavior

- watching for unusual or suspicious behavior by staff (for example, staff who, without an identifiable purpose, stay unusually late after the end of their shift, arrive unusually early, access files/information/areas of the facility outside of the areas of their responsibility; remove documents from the facility; ask questions on sensitive subjects; bring cameras to work)

#### Staff health

- being alert for atypical staff health conditions that staff may voluntarily report and absences that could be an early indicator of tampering or other malicious, criminal, or terrorist actions (for example, an unusual number of staff who work in the same part of the facility reporting similar symptoms within a short time frame), and reporting such conditions to local health authorities

### **Human element – the public**

FDA recommends that cosmetics establishment operators consider:

Visitors (e.g., contractors, supplier representatives, delivery drivers, customers, couriers, pest control representatives, third-party auditors, regulators, reporters, tours)

- inspecting incoming and outgoing vehicles, packages and briefcases for suspicious, inappropriate or unusual items or activity, to the extent practical
- restricting entry to the establishment (for example, checking visitors in and out at security or reception, requiring proof of identity, issuing visitors badges that are collected upon departure, accompanying visitors)
- ensuring that there is a valid reason for the visit before providing access to the facility - beware of unsolicited visitors
- verifying the identity of unknown visitors

- restricting access to cosmetics manufacturing and storage areas (for example, accompanying visitors, unless they are otherwise specifically authorized)
- restricting access to locker rooms

## **Facility**

FDA recommends that cosmetics establishment operators consider:

### Physical security

- protecting perimeter access with fencing or other deterrent, when appropriate
- securing doors (including freight loading doors, when not in use and not being monitored, and emergency exits), windows, roof openings/hatches, vent openings, ventilation systems, utility rooms, loft areas, trailer bodies, tanker trucks, railcars, and bulk storage tanks for liquids, solids, and compressed gases, to the extent possible (for example, using locks, "jimmy plates," seals, alarms, intrusion detection sensors, guards, monitored video surveillance [remember to consult any relevant federal, state or local fire or occupational safety codes before making any changes])
- using metal or metal-clad exterior doors to the extent possible, when the facility is not in operation, except where visibility from public thoroughfares is an intended deterrent (remember to consult any relevant federal, state or local fire or occupational safety codes before making any changes)
- minimizing the number of entrances to restricted areas (remember to consult any relevant federal, state or local fire or occupational safety codes before making any changes)
- securing bulk unloading equipment (for example, augers, pipes, conveyor belts, and hoses) when not in use and inspecting the equipment before use
- accounting for all keys to establishment (for example, assigning responsibility for issuing, tracking, and retrieving keys)
- monitoring the security of the premises using appropriate methods (for example, using security patrols [uniformed and/or plain-clothed], video surveillance)
- minimizing, to the extent practical, places that can be used to temporarily hide intentional contaminants (for example, minimizing nooks and crannies, false ceilings)
- providing adequate interior and exterior lighting, including emergency lighting, where appropriate, to facilitate detection of suspicious or unusual activities
- implementing a system of controlling vehicles authorized to park on the premises (for example, using placards, decals, key cards, keyed or cipher locks, issuing passes for specific areas and times to visitors' vehicles)

- keeping parking areas separated from cosmetics manufacturing and storage areas and utilities, where practical

#### Laboratory safety

- restricting access to the laboratory (for example, using key cards or keyed or cipher locks [remember to consult any relevant federal, state or local fire or occupational safety codes before making any changes])
- restricting laboratory materials to the laboratory, except as needed for sampling or other appropriate activities
- restricting access (e.g., using locks, seals, alarms, key cards, keyed or cipher locks) to sensitive materials (e.g., reagents and bacterial and toxin positive controls) to sensitive materials (for example, reagents and bacterial, drug and toxin positive controls)
- assigning responsibility for integrity of positive controls to a qualified individual
- knowing what reagents and positive controls should be on the premises and keeping track of them
- investigating missing reagents or positive controls or other irregularities outside a normal range of variability immediately, and alerting appropriate law enforcement and public health authorities about unresolved problems, when appropriate
- disposing of unneeded reagents and positive controls in a manner that minimizes the risk that they can be used as a contaminant

#### Storage and use of poisonous and toxic chemicals (for example, cleaning and sanitizing agents, pesticides)

- limiting poisonous and toxic chemicals in the establishment to those that are required for the operation and maintenance of the facility
- storing poisonous and toxic chemicals as far away from cosmetics manufacturing and storage areas as practical
- limiting access to and securing storage areas for poisonous and toxic chemicals (for example, using keyed or cipher locks, key cards, seals, alarms, intrusion detection sensors, guards, monitored video surveillance [remember to consult any relevant federal, state or local fire or occupational safety codes before making any changes])
- ensuring that poisonous and toxic chemicals are properly labeled
- using pesticides in accordance with the Federal Insecticide, Fungicide, and Rodenticide Act (for example, maintaining rodent bait that is in use in covered, tamper-resistant bait stations)
- knowing what poisonous and toxic chemicals should be on the premises and keeping track of them
- investigating missing stock or other irregularities outside a normal range of variation and alerting appropriate law enforcement and public health agencies about unresolved problems, when appropriate

## Operations

FDA recommends that cosmetics establishment operators consider:

### Incoming materials and contract operations:

- using only known, appropriately licensed or permitted (where applicable) contract manufacturing and packaging operators and sources for all incoming materials, including ingredients, compressed gas, packaging, labels and materials for research and development
- taking steps to ensure that suppliers, contract operators and transporters practice appropriate cosmetics security measures (for example, auditing, where practical, for compliance with cosmetics security measures that are contained in purchase and shipping contracts or letters of credit, or using a vendor approval program)
- authenticating labeling and packaging configuration and product coding/expiration dating systems (where applicable) for incoming materials in advance of receipt of shipment, especially for new products
- requesting locked and/or sealed vehicles/containers/railcars, and, if sealed, obtaining the seal number from the supplier and verifying upon receipt, making arrangements to maintain the chain of custody when a seal is broken for inspection by a governmental agency or as a result of multiple deliveries
- requesting that the transporter have the capability to verify the location of the load at any time, when practical
- establishing delivery schedules, not accepting unexplained, unscheduled deliveries or drivers, and investigating delayed or missed shipments
- supervising off-loading of incoming materials, including off hour deliveries
- reconciling the product and amount received with the product and amount ordered and the product and amount listed on the invoice and shipping documents, taking into account any sampling performed prior to receipt
- investigating shipping documents with suspicious alterations
- inspecting incoming materials, including ingredients, compressed gas, packaging, labels, product returns and materials for research and development for signs of tampering, contamination or damage (for example, abnormal powders, liquids, stains, or odors, evidence of resealing, compromised tamper-evident packaging) or “counterfeiting” (for example, inappropriate or mismatched product identity, labeling, product lot coding or specifications, absence of tamper-evident packaging when the label contains a tamper-evident notice), when appropriate
- evaluating the utility of testing incoming ingredients, compressed gas, packaging, labels, product returns and materials for research and development for detecting tampering or other malicious, criminal, or terrorist action

- rejecting suspect cosmetics or cosmetics ingredients
- alerting appropriate law enforcement and public health authorities about evidence of tampering, “counterfeiting” or other malicious, criminal, or terrorist action

#### Storage

- having a system for receiving, storing and handling distressed, damaged, returned, and rework products that minimizes their potential for being compromised or to compromise the security of other products (for example, destroying products that are unfit for use, products with illegible codes, products of questionable origin, and products returned by consumers to retail stores)
- keeping track of incoming materials and materials in use, including ingredients, compressed gas, packaging, labels, salvage products, rework products, and product returns
- investigating missing or extra stock or other irregularities outside a normal range of variability and reporting unresolved problems to local appropriate enforcement and public health authorities, when appropriate
- storing product labels in a secure location and destroying outdated or discarded product labels
- minimizing reuse of containers, shipping packages, cartons, etc., where practical

#### Security of water and utilities

- securing, to the extent practical, access to controls for airflow, water, electricity, and refrigeration
- securing non-municipal water wells, hydrants, storage and handling facilities
- ensuring that water systems and trucks are equipped with backflow prevention
- chlorinating water systems and monitoring chlorination equipment, where practical, and especially for non-municipal water systems
- testing non-municipal sources for potability regularly, as well as randomly, and being alert to changes in the profile of the results
- staying attentive to the potential for media alerts about public water provider problems, when applicable
- identifying alternate sources of potable water for use during emergency situations where normal water systems have been compromised (for example, trucking from an approved source, treating on-site or maintaining on-site storage)

#### Finished products

- ensuring that contract warehousing and shipping operations (vehicles and vessels) practice appropriate security measures (for example, auditing, where practical, for compliance with cosmetics security measures that are contained in contracts or letters of guarantee)
- performing random inspection of storage facilities, vehicles, and vessels

- evaluating the utility of finished product testing for detecting tampering or other malicious, criminal, or terrorist action
- requesting locked and/or sealed vehicles/containers/railcars and providing the seal number to the requesting that the transporter have the capability to verify the location of the load at any time
- establishing scheduled pickups, and not accepting unexplained, unscheduled pickups
- keeping track of finished products
- investigating missing or extra stock or other irregularities outside a normal range of variation and alerting appropriate law enforcement and public health authorities about unresolved problems, when appropriate
- advising sales staff to be on the lookout for counterfeit products and to alert management if any problems are detected

#### Mail/packages

- implementing procedures to ensure the security of incoming mail and packages (for example, locating the mailroom away from cosmetics manufacturing and storage areas, securing mailroom, visual or x-ray mail/package screening, following U.S. Postal Service guidance)

#### Access to computer systems

- restricting access to computer process control systems and critical data systems to those with appropriate clearance (for example, using passwords, firewalls)
- eliminating computer access when a staff member is no longer associated with the establishment
- establishing a system of traceability of computer transactions
- reviewing the adequacy of virus protection and procedures for backing up critical computer based data systems
- validating the computer security system

### **Emergency Point of Contact:**

U.S. Food and Drug Administration  
5600 Fishers Lane  
Rockville, MD 20857

If a cosmetics establishment operator suspects that any of his/her products that are regulated by the FDA have been subject to tampering, "counterfeiting," or other malicious, criminal, or terrorist action, FDA recommends that he/she notify the FDA 24-hour emergency number at 301-443-1240 or call their local FDA District Office. FDA District Office telephone numbers are listed at [http://www.fda.gov/ora/inspect\\_ref/iom/iomoradir.html](http://www.fda.gov/ora/inspect_ref/iom/iomoradir.html). FDA recommends that the operator also notify local law enforcement and public health agencies.