POTENTIAL INDICATORS OF TERRORIST ACTIVITY INFRASTRUCTURE CATEGORY: AGRICULTURAL PROCESSING FACILITIES – MILK PROCESSING

Protective Security Division
Department of Homeland Security

Draft Version 1, January 30, 2004

Preventing terrorism and reducing the nation's vulnerability to terrorist acts require identifying specific vulnerabilities at critical sites, understanding the types of terrorist activities—and the potential indicators of those activities—that likely would be successful in exploiting those vulnerabilities, and taking preemptive and protective actions to mitigate vulnerabilities so that terrorists are no longer able to exploit them. This report discusses potential indicators of terrorist activity with a focus on the milk processing industry.

INTRODUCTION

Terrorist activity indicators are observable anomalies or incidents that may precede a terrorist attack or that may be associated with terrorist surveillance, training, planning, preparation, or mobilization activities. The observation of any one indicator may not, by itself, suggest terrorist activity. Each observed anomaly or incident, however, should be carefully considered, along with all other relevant observations, to determine whether further investigation is warranted. The objective is to look for items of information that fit together to form a relevant and credible picture of how a threat might become real at the milk processing facility of interest and what it might look like. The key factor in early recognition of terrorist activity is the ability to recognize anomalies in location, timing, and character of vehicles, equipment, people, and packages.

The geographic location and temporal proximity (or dispersion) of observed anomalies are important factors to consider. Terrorists have demonstrated the ability to finance, plan, and train for complex and sophisticated attacks over extended periods of time and at multiple locations distant from the proximity of their targets. Often, attacks are carried out nearly simultaneously against multiple targets.

Indicators are useful in discerning terrorist activity to the extent that they help identify

- A specific asset that a terrorist group is targeting,
- The general or specific timing of a planned attack, and
- The weapons and deployment method planned by the terrorist.

In some cases, the choice of weaponry and deployment method may help to eliminate certain classes of assets from the potential target spectrum. Except for geographic factors, however, such information alone may contribute little to identifying the specific target or targets. The best indicator that a specific site or asset may be targeted is direct observation or evidence that the site or asset is or has been under surveillance. Careful attention to the surveillance indicators, especially by local law enforcement personnel and asset owners, is an important key to identifying potential terrorist threats to a specific site or asset. To increase the probability of detecting terrorist surveillance activities, employees, contractors, and local citizens need to be solicited to "observe and report" unusual activities, incidents, and behaviors highlighted in this report.

MILK PROCESSING BACKGROUND

Terrorists Targeting Objectives

To consider terrorist threat indicators in relationship to the milk processing industry, it is useful to understand the basic structure of the industry and what general types of facilities might be attractive targets for terrorist attack. Milk processing facilities are attractive terrorist targets because of the ability to distribute contaminated product to a wide population in a short period of time.

A generalized threat spectrum is depicted in Figure 1. Damage or destruction of the facility can be intended to inflict casualties, both on and off site, shut down or degrade the operation of the facility, or cause the release of hazardous materials to the surrounding area. Such damage or destruction is generally not a primary objective with milk processing facilities. Disruption of the facility without inflicting actual damage can be intended to interfere with facility operations and cause a decrease of output or to tamper with facility products to render them dangerous or unusable. This would be the primary focus of attacks on milk processing facilities; the intent would be to have contaminated milk and milk products widely distributed. Theft of equipment, materials, and products can be intended to divert them to other uses or to reap financial gain from their resale. Theft of information can be intended to acquire insight that is not made public or to gain data that can be used in carrying out attacks. Facility attacks can be intended to (1) cause economic, national security, or logistical harm; (2) contaminate product going into the food, medical, or health care system; or (3) "weaponize" the facility against the surrounding human population by causing the release of hazardous materials from the plant site.

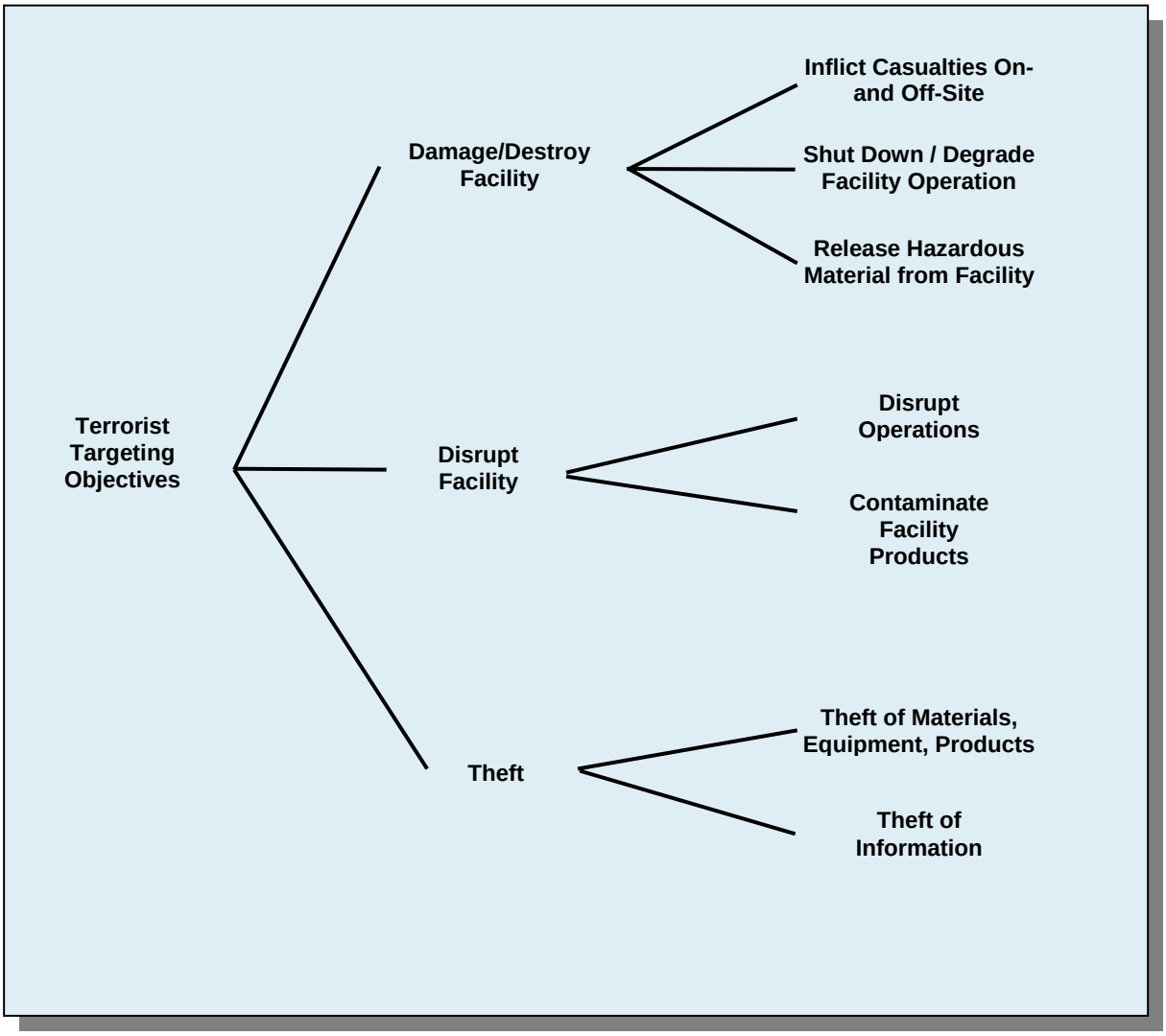

Figure 1 Terrorist Targeting Objectives

Sector Description

This section provides basic information about the structure of the industry. Figure 2 shows milk production in the United States (U.S.) from 1993 to 2002 by state. The top 5 states are California, Wisconsin, New York, Pennsylvania, and Minnesota; these states account for 52% of the total U.S. milk production. The top 10 states, which include the 5 states listed above plus Idaho, Michigan, New Mexico, Washington, and Texas, account for more than 70% of total milk production. Of all dairy products, fluid milk enters and leaves the distribution channel most rapidly. Cream and butterfat can be extracted from whole fluid milk to produce a variety of other dairy products: reduced-fat milk and higher-butterfat products, such as butter, cheese, cottage cheese, cream cheese, and ice cream. Value-added products, such as flavored yogurts, yogurt drinks, and nutritional and sports beverages, have shorter product life cycles. Dairy products and their derivatives are also often used as ingredients for re-manufacturing (e.g., whey, nonfat-dry-milk solids, cheeses). Most dairies that produce whole and reduced-fat milk for retail sale also produce many of these value-added products. The consumption of milk products (as both fluid milk and processed products) per capita varies widely, with highs occurring in Europe and North America and lows occurring in Asia. In 2001, per-capita consumption in the U.S. diet was significant: 587.2 pounds of dairy products, 207.5 pounds of fluid whole milk and cream, 4.5 pounds of butter, 30 pounds of cheese, and 16.1 pounds of ice cream (U.S. Department of Agriculture [USDA] Marketing Service).

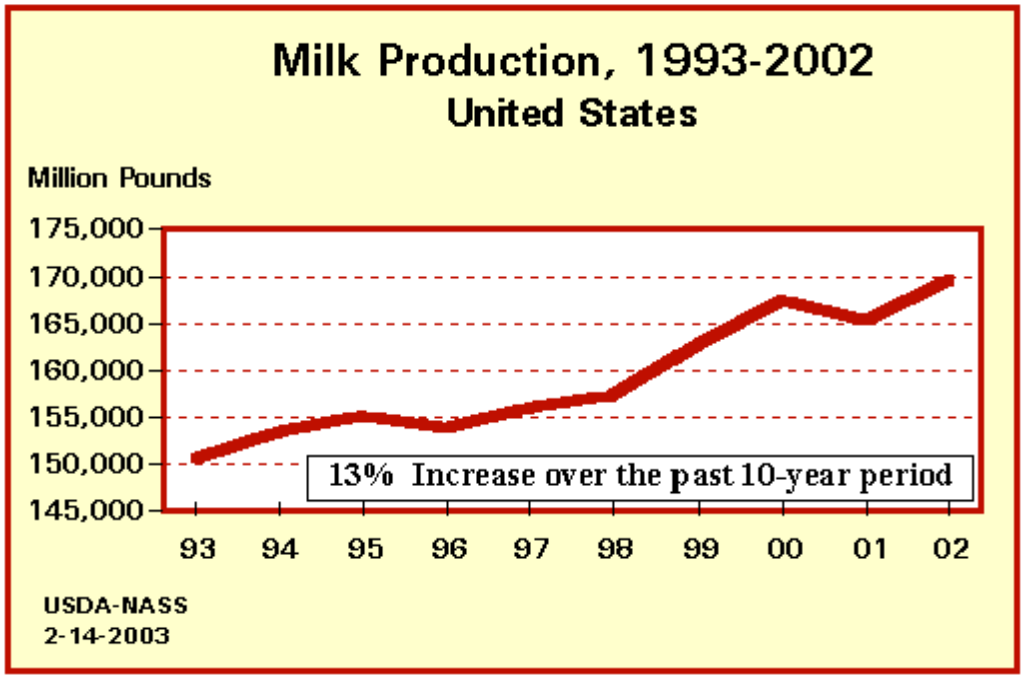

Figure 2 U.S. Milk Production

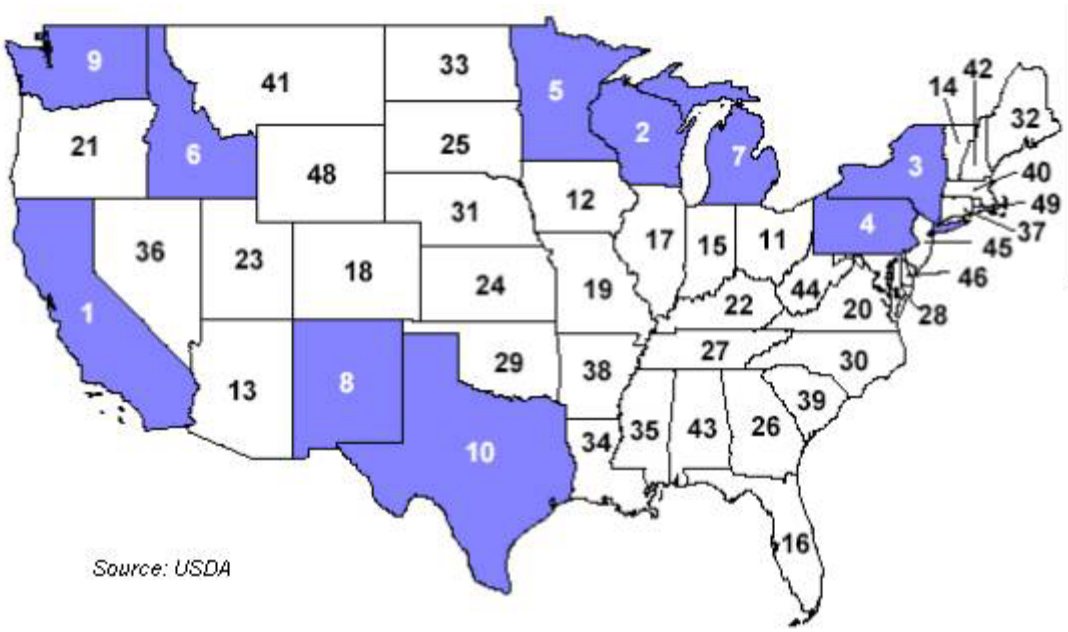

Figure 3 Rank Order of Milk-producing States — Top Ten States Highlighted

The USDA uses the following terminology to characterize participants in the industry:

- *Marketing Area.* A marketing area is an area designated in the provisions of a federal milk order, within which the handling of milk is regulated by the order. In general, the size of the marketing area is determined by the sales territory of competing handlers.

- *Producer.* A producer is usually defined as any dairy farmer who sells milk to a pool handler. Producers must produce milk in compliance with Grade A inspection requirements, and their milk must either be received at a pool plant or diverted to a non-pool plant for the account of a pool handler. Producer handlers are not producers.

- *Handler.* A handler is an individual, partnership, corporation, association, or other business unit that is subject to the provisions of an order. A handler can be an operator of a plant that is approved by a duly constituted regulatory agency for the handling of Grade A milk. A handler also can be a milk distributor or a broker. Furthermore, a cooperative association that does not operate a plant can be a handler.

- *Pool Handler.* A pool handler is a handler that is subject in full to the provisions of the order. A pool handler can be an operator of a plant that meets the minimum performance standards included in each order (i.e., a pool plant). Such plants include distributing plants, plants primarily engaged in processing packaged fluid milk products, and supply plants (i.e., plants primarily engaged in producing manufactured

dairy products). A cooperative association that does not operate a plant can be a pool handler. A milk distributor or broker cannot be a pool handler.

- *Receipts of Milk.* Receipts of milk primarily come from producers. The volume of milk from producers reported as received by handlers includes all milk, regardless of where it may be sold. Milk identified as received from producers for a given market may come directly from nearby producers or from producers associated with a supply plant, which, although it may be located several hundred miles from the marketing area, is pooled on the market. Producer milk also may include milk that is diverted by a pool plant operator to another pool plant or to a non-pool plant.

Handlers regulated under federal milk orders process about 75% of all the milk marketed in the U.S. Table 1 shows the number of plants operating under federal milk orders. The USDA identifies four basic classes of milk use:

- *Class I* – Fluid milk products (products intended to be used as a beverage);
- *Class II* – Cream products, cottage cheese, ice cream, and other food uses;
- *Class III* – Hard and spreadable cheeses; and
- *Class IV* – Butter and dried milk products.

Figure 4 shows the flow through a typical milk processing plant. The configuration varies from plant to plant, depending on the output product stream, production capacity, production line requirements, and design and layout of the facilities and equipment. Because of the variety of both continuous and batch-style, product-handling steps, many dairy product manufacturing practices and procedures cannot be described in this document. Examples are included to provide information on some techniques used to produce several different products, including whole and reduced-fat retail fluid milk, butter, cream, cheeses, ice cream, and yogurt products. For fluid milk, there are process access points that could be targeted by an adversary. For process applications other than packaged fluid milk, including products such as butter, cottage cheese, yogurt, and ice cream, there are a greater number of product access points at which a contaminant could intentionally be added into the manufacturing stream. Furthermore, in a milk processing facility, the assembled (clean-in-place) and disassembled (clean-out-of-place) equipment parts are routinely cleaned and sanitized. Insider opportunities exist to not adequately clean some equipment, substitute wrong parts or reinstall parts incorrectly into the process line, or introduce an odorless and tasteless contaminant that is not analytically tested for in finished products.

Raw fluid milk is collected from individual dairy farms where dairy cattle are fed and milked: milk is temporarily stored there until transport. Trucks deliver the raw milk to the processing plant. Human access to stored ingredients and packaging material and the process of adding ingredients and vitamins to milk products and product derivatives create the greatest opportunities for intentional contamination with biological or chemical agents.

Table 1 Federal Milk Order Plants, 2003

State	Distributing Plants	Supply Plants	State	Distributing Plants	Supply Plants
Alabama	5	0	Nebraska	3	0
Arizona	3	1	New Hampshire	1	0
Arkansas	5	1	New Jersey	6	0
Colorado	9	2	New Mexico	1	2
Connecticut	3	0	New York	20	3
Delaware	2	0	North Carolina	6	0
Florida	12	0	North Dakota	1	1
Georgia	4	0	Ohio	14	1
Idaho	5	0	Oklahoma	3	0
Illinois	16	5	Oregon	10	5
Indiana	10	1	Pennsylvania	22	5
Iowa	6	15	Rhode Island	1	0
Kansas	2	0	South Carolina	5	0
Kentucky	8	1	South Dakota	1	3
Louisiana	7	1	Tennessee	9	1
Maine	3	0	Texas	20	4
Maryland	3	1	Utah	7	0
Massachusetts	4	1	Vermont	2	3
Michigan	15	0	Virginia	6	1
Minnesota	14	10	Washington	8	3
Mississippi	2	4	West Virginia	1	0
Missouri	4	2	Wisconsin	11	61
Montana	1	0			
Total for All States	**301** (distributing plants)	**138** (supply plants)			

Source: USDA.

The incoming tanker milk delivered to the processing/production facility is routinely tested. If its temperature is below 40°F, the delivery is rejected. In addition, raw milk received at the plant is routinely checked for additional quality and safety factors, including biological, chemical, and physical contaminants (i.e., odors, temperature, appearance, acidity, bacterial counts, drug residues, antibiotics, herbicides, pesticides). Measures of product quality, such as the amount of solids, lactose, protein, and butterfat in the milk, are also taken. A lab technician may perform a taste test on every shipment of milk. If any abnormalities are detected, the entire shipment of milk is rejected. These off-loading and analytical sampling procedures, in addition to providing important quality and safety checkpoints, can also create human access points and opportunities to intentionally introduce contamination. If the milk is accepted, it is pumped into raw milk storage tanks, which can hold several hundred thousand gallons of milk. Because milk from many different sources is combined in these large tanks, any contamination that might escape

initial detection by the lab technicians' qualitative and quantitative analytical testing could affect a large volume of raw milk.

When the raw milk is ready for processing, the first step may be to use a clarifier to separate out foreign substances (i.e., non-milk solids, such as dirt, epithelial cells, bacteria sediment, and sludge). In general, if the quality of the raw milk is good, a separate clarifier stage is not included; only a separator is used.

A milk *separation* process is designed to separate the cream from the skim milk. A separator centrifuge consists of disks stacked together and separated by a small gap or separation channel. Milk is introduced at the outer edge of the disk stack. Under the influence of centrifugal force, the fat globules (cream), which are less dense than the skim milk, move inward through the separation channels toward the axis of rotation. The skim milk moves outward and leaves the unit through a separate outlet. Standardized streams of milk with various fat contents can be produced by adjusting the mixture of cream and skim milk at the separator.

Milk is an oil-in-water emulsion, with the fat globules dispersed in a continuous skim milk phase. If raw milk were left to stand, the fat would rise and form a cream layer. *Homogenization* is a mechanical treatment of the fat globules in milk that is brought about by passing milk under high pressure (2,000 pounds per square inch or higher) through a tiny orifice, which results in a decrease in the average diameter and an increase in the number and surface area of the fat globules and thus more dispersion. The net result, from a practical view, is that the tendency for creaming of fat globules is greatly reduced.

Pasteurization is designed to heat the raw milk to a temperature that is high enough so that when it is held for a required minimum time, it kills or inactivates certain (but not all) microorganisms (i.e., common pathogenic and non-pathogenic bacteria, yeast, molds, viruses) and disables certain enzymes, while minimizing the effects on taste. Pasteurization involves heating the milk to a minimum of 145°F (62.8°C) for 30 minutes or to 163°F (72.8°C) for 15 seconds. For any method of heat treatment employed, federal and state regulations require that milk must be pasteurized within 72 hours of milking.

Ultrahigh-temperature (UHT) pasteurization completely sterilizes the dairy product and is designed to render it free of microorganisms capable of reproducing in the food under normal non-refrigerated conditions of storage and distribution. In this case, a thermal process referred to as "aseptic" is applied to separately sterilize the product, package, filling, and packaging system by heat, hot water, and/or chemical agents, with all components being brought together in a pre-sterilized "sterile zone" for filling and package sealing. The UHT method creates shelf-stable "boxes of milk" that can be stored without refrigeration, allowing extended dairy-product shelf life. In UHT pasteurization, the temperature of the milk is raised to about 285°F (141°C) for 1 or 2 seconds, thereby sterilizing the milk. The milk is cooled in a closed system and aseptically filled and sealed in plastic containers (e.g., fluid milk, coffee creamer). Equipment access and improper opening of pre-sterilized sections of this system during operation can potentially cause process failure and product spoilage.

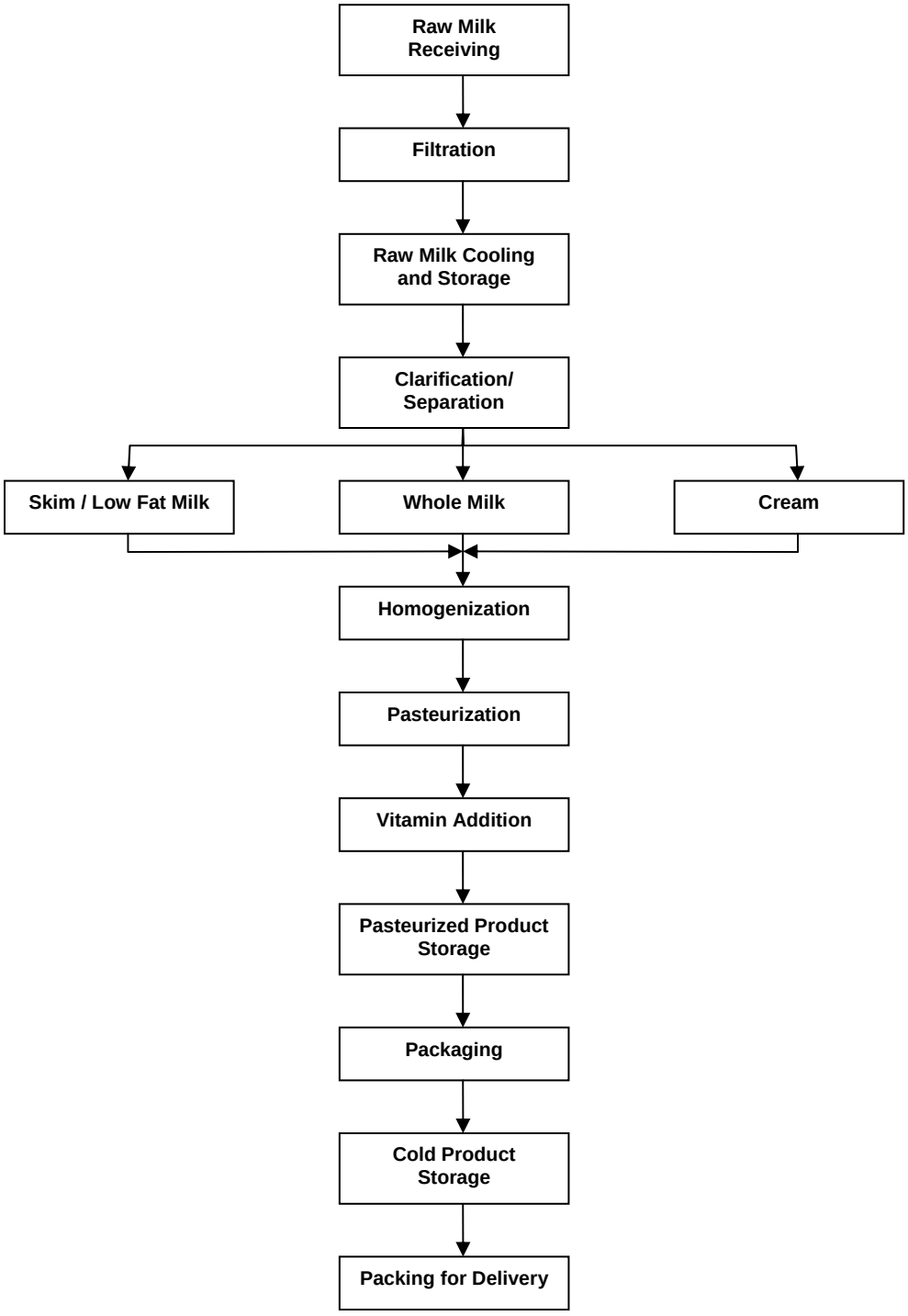

Figure 4 Process Flow for a Typical Milk Processing Plant

Because vitamins are degraded by thermal treatment, they may be added to selected products after pasteurization; fortification vitamins A and D are the most common additions. The product is then moved to holding tanks used only for pasteurized products. It is after pasteurization and before packaging of the fluid milk that opportunities arise for addition of biological or chemical contaminants that would later move into the food supply.

Products are then packaged. The packaged products are held in cold storage until they are packed for delivery. In most facilities, there are no routine analytical checks for determining whether biological or chemical contaminants have been introduced prior to distribution.

TERRORIST ACTIVITY INDICATORS

There are several indicators of possible terrorist activity that should be monitored on a regular basis. Constant attention to these indicators can help alert officials to the possibility of an incident.

Surveillance Indicators

Terrorist surveillance may be fixed or mobile. Fixed surveillance is done from a static, often concealed position, possibly an adjacent building, business, or other facility. In fixed surveillance scenarios, terrorists may establish themselves in a public location over an extended period of time or choose disguises or occupations, such as street vendors, tourists, repair- or deliverymen, photographers, or even demonstrators, to provide a plausible reason for being in the area.

Mobile surveillance usually entails observing and following persons or individual human targets, although it can be conducted against non-mobile facilities (i.e., driving by a site to observe the facility or site operations). To enhance mobile surveillance, many terrorists have become more adept at progressive surveillance.

Progressive surveillance is a technique whereby the terrorist observes a target for a short time from one position, withdraws for a time (possibly days or even weeks), and then resumes surveillance from another position. This activity continues until the terrorist develops target suitability and/or noticeable patterns in the operations or target's movements. This type of transient presence makes surveillance much more difficult to detect or predict.

More sophisticated surveillance is likely to be accomplished over a long period of time. This type of surveillance tends to evade detection and improve the quality of gathered information. Some terrorists perform surveillance of a target or target area over a period of months or even years. The use of public parks and other public gathering areas provides convenient venues for surveillance because it is not unusual for individuals or small groups in these areas to loiter or engage in leisure activities that could serve to cover surveillance activities.

Terrorists are also known to use advanced technology, such as modern optoelectronics, communications equipment, video cameras, and other electronic equipment. Such technologies include commercial and military night-vision devices and global positioning systems. It should be assumed that many terrorists have access to expensive technological equipment.

Electronic surveillance, in this instance, refers to information gathering, legal and illegal, by terrorists using off-site computers. This type of data gathering might include obtaining site maps, key facility locations, site security procedures, or passwords to company computer systems. In addition to obtaining information useful for a planned physical attack, terrorists may launch an electronic attack that could affect data (e.g., damage or modify), software (e.g., damage or modify), or equipment/process controls (e.g., damage a piece of equipment or cause a dangerous chemical release by opening or closing a valve using off-site access to the supervisory control

and data acquisition [SCADA] system). Terrorists may also use technical means to intercept radio or telephone (including cell phone) traffic.

An electronic attack could be an end in itself or could be launched simultaneously with a physical attack. Thus, it is worthwhile to be aware of what information is being collected from company and relevant government websites by off-site computer users and, if feasible, who is collecting this information. It is also important to know whether attempts are being made to gain access to protected company computer systems and whether any attempts have been successful.

The surveillance indicators in Exhibit 1 are examples of unusual activities that should be noted and considered as part of an assimilation process that takes into account the quality and reliability of the source, the apparent validity of the information, and how the information meshes with other information at hand. For the most part, surveillance indicators refer to activities in the immediate vicinity of the milk processing facility; most of the other indicator categories address activities in a much larger region around the facility.

Other Local and Regional Indicators

The sets of indicators described in Exhibits 2–5 refer to activities not only in the immediate vicinity of the facility, but also within a relatively large region around the plant (e.g., 100 to 200 miles). Local authorities should be aware of such activities and may not be able to associate them with a specific critical asset because several may be within the region being monitored. The objective is to look for items of information that fit together to form a relevant and credible picture of how a threat might become real at the facility of interest and what it might look like.

EXHIBITS

Every attempt has been made to be as comprehensive as possible in listing the following terrorist activity indicators. Some of the indicators listed may not be specific to the critical infrastructure or critical asset category that is the topic of this report. However, these general indicators are included as an aid and reminder to anyone who might observe any of these activities that they are indicators of potential terrorist activity.

Exhibit 1 Surveillance Indicators Observed Inside or Outside an Installation

What are surveillance indicators? Persons or unusual activities in the immediate vicinity of a critical infrastructure or key asset intending to gather information about the facility or its operations, shipments, or protective measures.

	Persons Observed or Reported:
1	Persons using or carrying video/camera/observation equipment.
2	Persons with installation maps or facility photos or diagrams with facilities highlighted or notes regarding infrastructure or listing of installation personnel.
3	Persons possessing or observed using night-vision devices near the facility perimeter or in the local area.
4	Persons parking, standing, or loitering in the same area over a multiple-day period with no apparent reasonable explanation.
5	Non-military persons seen with military-style weapons and clothing/equipment.
6	Facility personnel being questioned off site about practices pertaining to the facility, or an increase in personal e-mail, telephone, faxes, or mail concerning the facility, or key asset.
7	Non-facility persons showing an increased general interest in the area surrounding the facility.
8	Facility personnel willfully associating with suspicious individuals.
9	Computer hackers attempting to access sites looking for personal information, maps, or other targeting examples.
10	An employee who changes working behavior or works more irregular hours.
11	Persons observed or reported to be observing facility receipts or deliveries, especially of hazardous, toxic, or radioactive materials.
12	Aircraft flyover in restricted airspace; boat encroachment into restricted areas, especially if near critical infrastructure.
	(Continued on next page.)

Activities Observed or Reported:	
13	A noted pattern or series of false alarms requiring a response by law enforcement or emergency services.
14	Theft of facility or contractor identification cards or uniforms, or unauthorized persons in possession of facility ID cards or uniforms.
15	Recent damage (e.g., significant holes or cuts) to a perimeter fence or gate, or damage to perimeter lighting, security cameras, motion sensors, guard dogs, or other security devices.
16	Downloading of materials (e.g., maps, photographs, schematics, or similar materials) that could be used in conjunction with surveillance or attack planning activities.
17	Repeated attempts from the same location or country to access protected computer information systems.
18	Successful penetration and access of protected computer information systems, especially those containing information on site logistics, procedures, shipment schedules, security measures, passwords, and other sensitive information.
19	Attempts to obtain information about the facility (e.g., blueprints of buildings or information from public sources).
20	Unfamiliar cleaning crews or other contract workers with passable credentials; crews or contract workers attempting to access unauthorized areas.
21	A seemingly abandoned or illegally parked vehicle in the area of the facility or asset.
22	Increased interest in facility outside components (i.e., an electrical substation not located on site and not as heavily protected or not protected at all).
23	Sudden increases in power outages. This could be done from an off-site location to test the backup systems or recovery times of primary systems.
24	Increase in buildings being left unsecured or doors being left unlocked that are normally locked all the time.
25	Arrest by local police of unknown persons. This would be more important if facility or asset is located in a rural area rather than located in or around a large city.
26	Traces of explosive or radioactive residue on facility vehicles during security checks by personnel using detection swipes or devices.
27	Increase in violation of security guard standard operating procedures for staffing key posts.
28	Increase in threats from unidentified sources by telephone, postal mail, or through the e-mail system.
29	Increase in reports of threats from outside known, reliable sources.
30	Sudden losses or theft of guard force communications equipment.
31	Displaced or misaligned manhole covers or other service access doors on or surrounding the facility or asset site.
32	Unusual maintenance activities (e.g., road repairs) near the facility or asset.
33	Observations of unauthorized facility or non-facility personnel collecting or searching through facility trash.

Exhibit 2 Transactional and Behavioral Indicators

What are transactional and behavioral indicators? Suspicious purchases of materials for improvised explosives or for the production of biological agents, toxins, chemical precursors, or chemicals that could be used in an act of terrorism or for purely criminal activity in the immediate vicinity or in the region surrounding a facility, critical infrastructure, or key asset.

Transactional Indicators:

What are transactional indicators? Unusual, atypical, or incomplete methods, procedures, or events associated with inquiry about or attempted purchase of equipment or materials that could be used to manufacture or assemble explosive, biological, chemical, or radioactive agents or devices that could be used to deliver or disperse such agents. Also included are inquiries and orders to purchase such equipment or materials and the subsequent theft or loss of the items from the same or a different supplier.

1	Approach from a previously unknown customer (including those who require technical assistance) whose identity is not clear.
2	Transaction involving an intermediary agent and/or third party or consignee that is atypical in light of his/her usual business.
3	A customer associated with or employed by a military-related business, such as a foreign defense ministry or foreign armed forces.
4	Unusual customer request concerning the shipment or labeling of goods. (e.g., offer to pick up shipment personally rather than arrange shipment and delivery).
5	Packaging and/or packaging components that are inconsistent with the shipping mode or stated destination.
6	Unusually favorable payment terms, such as a higher price or better interest rate than the prevailing market or a higher lump-sum cash payment.
7	Unusual customer request for excessive confidentiality regarding the final destination or details of the product to be delivered.
8	Orders for excessive quantities of personal protective gear or safety/security devices, especially by persons not identified as affiliated with an industrial plant.
9	Requests for normally unnecessary devices (e.g., an excessive quantity of spare parts) or a lack of orders for parts typically associated with the product being ordered, coupled with an unconvincing explanation for the omission of such an order or request.
10	Sale canceled by customer but then customer attempts to purchase the exact same product with the same specifications and use but using a different name.
11	Sale canceled by customer but then the identical product is stolen or “lost” shortly after the customer’s inquiry.
12	Theft/loss/recovery of large amounts of cash by groups advocating violence against government/civilian sector targets (also applies to weapons of mass destruction).
13	Customer does not request a performance guarantee, warranty, or service contract where such is typically provided in similar transactions.
	(Continued on next page.)

Customer Behavioral Indicators: *What are customer behavioral indicators? Actions or inactions on the part of a customer for equipment or materials that appear to be inconsistent with normal behavioral patterns expected from legitimate commercial customers.*	
14	Reluctance to give sufficient explanation of the chemicals or other suspicious materials to be produced with the equipment and/or the purpose or use of those chemicals or materials.
15	Evasive responses.
16	Reluctance to provide information on the plant locations or place where the equipment is to be installed.
17	Reluctance to explain sufficiently what raw materials are to be used with the equipment.
18	Reluctance to provide clear answers to routine commercial or technical questions.
19	Reason for purchasing the equipment does not match the customer's usual business or technological level.
20	No request made or declines or refuses the assistance of a technical expert/training assistance when the assistance is generally standard for the installation or operation of the equipment.
21	Unable to complete an undertaking (due to inadequate equipment or technological know-how) and requests completion of a partly finished project.
22	Plant, equipment, or item is said to be for a use inconsistent with its design or normal intended use, and the customer continues these misstatements even after being corrected by the company/distributor.
23	Contract provided for the construction or revamping of a plant, but the complete scope of the work and/or final site of the plant under construction is not indicated.
24	Theft of material or equipment with no practical use outside of a legitimate business facility or industrial process.
25	Apparent lack of familiarity with nomenclature, chemical processes, packaging configurations, or other indicators to suggest this person may not be routinely involved in purchasing chemicals.
26	Discontinuity of information provided, such as a phone number for a business, but the number is listed under a different name.
27	Unfamiliarity with the "business," such as predictable business cycles, etc.
28	Unreasonable market expectations or fantastic explanations as to where the end product is going to be sold.

Exhibit 3 Weapons Indicators

What are weapons indicators? Purchase, theft, or testing of conventional weapons and equipment that terrorists could use to help carry out the intended action. Items of interest include not only guns, automatic weapons, rifles, etc., but also ammunition and equipment, such as night-vision goggles and body armor and relevant training exercises and classes.

Activities Observed or Reported:	
1	Theft or sales of large numbers of automatic or semi-automatic weapons.
2	Theft or sales of ammunition capable of being used in military weapons.
3	Reports of automatic weapons firing or unusual weapons firing.
4	Seizures of modified weapons or equipment used to modify weapons (silencers, etc.).
5	Theft, loss, or sales of large-caliber sniper weapons .50 cal or larger.
6	Theft, sales, or reported seizure of night-vision equipment in combination with other indicators.
7	Theft, sales, or reported seizure of body armor in combination with other indicators.
8	Paramilitary groups carrying out training scenarios and groups advocating violence.
9	People wearing clothing that is not consistent with the local weather (also applicable under all other indicator categories).

Exhibit 4 Explosive and Incendiary Indicators

What are explosive and incendiary indicators? Production, purchase, theft, testing, or storage of explosive or incendiary materials and devices that could be used by terrorists to help carry out the intended action. Also of interest are containers and locations where production could occur.

Persons Observed or Reported:	
1	Persons stopped or arrested with unexplained lethal amounts of explosives.
2	Inappropriate inquiries regarding explosives or explosive construction by unidentified persons.
3	Treated or untreated chemical burns or missing hands and/or fingers.
Activities Observed or Reported:	
4	Thefts or sales of large amounts of smokeless powder, blasting caps, or high-velocity explosives.
5	Large amounts of high-nitrate fertilizer sales to nonagricultural purchasers or abnormally large amounts to agricultural purchasers.[1]
6	Large thefts or sales of combinations of ingredients for explosives (e.g., fuel oil, nitrates) beyond normal.
7	Thefts or sales of containers (e.g., propane bottles) or vehicles (e.g., trucks, cargo vans) in combination with other indicators.
8	Reports of explosions, particularly in rural or wooded areas.
9	Traces of explosive residue on facility vehicles during security checks by personnel using explosive detection swipes or devices.
10	Seizures of improvised explosive devices or materials.
11	Purchase or theft of explosives or restricted or sensitive chemicals.
12	Theft of truck or van with minimum one-ton carrying capacity.
13	Modification of light-duty vehicle to accept a minimum one-ton load.
14	Rental of self-storage units and/or delivery of chemicals to such units.
15	Chemical fires, noxious or toxic odors, brightly colored stains, or rusted metal fixtures in apartments, hotel rooms, or self-storage units.
16	Suspicious packages, especially unexpected deliveries with no or an unknown return address and/or with excessive postage.
17	Unattended packages, briefcases, or other containers.
18	Unexpected or unfamiliar delivery trucks or deliveries.
19	Vehicles containing unusual or suspicious parcels or materials.
20	Unattended vehicles on or off site in suspicious locations or at unusual times.

[1] The Fertilizer Institute developed a "Know Your Customer" program following the terrorist attack in Oklahoma City. The information is available from TFI at http://www.tfi.org/.

Exhibit 5 Chemical, Biological, and Radiological Indicators

What are chemical, biological, and radiological indicators? Activities related to production, purchase, theft, testing, or storage of dangerous chemicals and chemical agents, biological species, and hazardous radioactive materials.

Equipment Configuration Indicators:	
1	Equipment to be installed in an area under strict security control, such as an area close to the facility or an area to which access is severely restricted.
2	Equipment to be installed in an area that is unusual and out of character with the proper use of the equipment.
3	Modification of a plant, equipment, or item in an existing or planned facility that changes production capability significantly and could make the facility more suitable for the manufacture of chemical weapons or chemical weapon precursors. (This also applies to biological agents and weapons.)
4	Suspicious packages, especially unexpected deliveries with no or an unknown return address and/or with excessive postage.
5	Unattended packages, briefcases, or other containers.
6	Unexpected or unfamiliar delivery trucks or deliveries.
7	Vehicles containing unusual or suspicious parcels or materials.
8	Theft, sale, or reported seizure of sophisticated personal protective equipment, such as “A’” level Tyvek, self-contained breathing apparatus (SCBA), etc.
9	Theft or sale of sophisticated filtering, air-scrubbing, or containment equipment
Chemical Agent Indicators:	
10	Inappropriate inquiries regarding local chemical sales/storage/transportation points.
11	Purchase or theft of explosives or restricted or sensitive chemicals.
12	Rental of self-storage units and/or delivery of chemicals to such units.
13	Chemical fires, noxious or toxic odors, brightly colored stains, or rusted metal fixtures in apartments, hotel rooms, or self-storage units.
14	Treated or untreated chemical burns or missing hands and/or fingers.
15	Unusual packages or containers, especially near heating, ventilating, and air-conditioning (HVAC) equipment or air intake systems.
16	Unusual powders, droplets, or mist clouds near HVAC equipment or air-intake systems.
	(Continued on next page.)

Biological Agent Indicators:	
17	Sales or theft of large quantities of baby formula (medium for growth), or an unexplained shortage of it.
18	Break-ins/tampering at water treatment or food processing/warehouse facilities.
19	Solicitation for sales or theft of live agents/toxins/diseases from medical supply companies or testing/experiment facilities.
20	Persons stopped or arrested with unexplained lethal amounts of agents/toxins/ diseases/explosives.
21	Multiple cases of unexplained human or animal illnesses, especially illnesses not native to the area.
22	Large number of unexplained human or animal deaths.
23	Sales (to non-agricultural users) or thefts of agricultural sprayers or crop-dusting aircraft, foggers, river craft (if applicable), or other dispensing systems.
24	Inappropriate inquiries regarding local or regional chemical/biological sales/storage/transportation points.
25	Inappropriate inquiries regarding heating and ventilation systems for buildings/facilities by persons not associated with service agencies.
26	Unusual packages or containers, especially near heating, ventilating, and air-conditioning (HVAC) equipment or air-intake systems.
27	Unusual powders, droplets, or mist clouds near HVAC equipment or air-intake systems.
Radioactive Material Indicators:	
28	Break-ins/tampering at facilities storing radioactive materials or radioactive wastes.
29	Solicitation for sales or theft of radioactive materials from medical or research supply companies or from testing/experiment facilities.
30	Persons stopped or arrested with unexplained radioactive materials.
31	Any one or more cases of unexplained human or animal radiation burns or radiation sickness.
32	Large number of unexplained human or animal deaths.
33	Inappropriate inquiries regarding local or regional radioactive material sales/storage/transportation points.

USEFUL REFERENCE MATERIAL

1. The White House, *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, Feb. 2003 [http://www.whitehouse.gov/pcipb/physical.html].

2. *Terrorist Attack Indicators*. Html version [http://afsf.lackland.af.mil/Organization/AFSFC/SFP/AF%20Pubs/Terrorist%20Attack%20Indicators]. PDF version [http://216.239.53.100/search?q=cache:YMHxMOEIgOcJ:afsf.lackland.af.mil/Organization/AFSFC/SFP/AF%2520Pubs/Terrorist%2520Attack%2520Indicators.PDF+terrorist+attack+indicators&hl=en&ie=UTF-8].

3. U.S. Department of Homeland Security, "Potential Indicators of Threats Involving Vehicle-Borne Improvised Explosive Devices (VBIEDs)," *Homeland Security Bulletin,* May 15, 2003 [http://www.apta.com/services/security/potential_indicators.cfm]. This document includes a table of chemicals and other demolitions paraphernalia used in recent truck bomb attacks against U.S. facilities.

4. U.S. Federal Bureau of Investigation, *FBI Community Outreach Program for Manufacturers and Suppliers of Chemical and Biological Agents, Materials, and Equipment* [http://www.vohma.com/pdf/pdffiles/SafetySecurity/ChemInfofbi.pdf]. This document includes a list of chemical/biological materials likely to be used in furtherance of WMD terrorist activities.

5. Defense Intelligence College, Counterterrorism Analysis Course, *Introduction to Terrorism Intelligence Analysis, Part 2: Pre-Incident Indicators* [http://www.globalsecurity.org/intell/library/policy/dod/ct_analysis_course.htm].

6. Princeton University, Department of Public Safety, *What is a Heightened Security State of Alert?* [http://web.princeton.edu/sites/publicsafety/].

7. Kentucky State Police: Homeland Security/Counter-Terrorism, *Potential Indicators of WMD Threats or Incidents* [http://www.kentuckystatepolice.org/terror.htm]. This site lists several indicators, protective measures, and emergency procedures.

8. U.S. Air Force, Office of Special Investigations, *Eagle Eyes: Categories of Suspicious Activities* [http://www.dtic.mil/afosi/eagle/suspicious_behavior.html]. This site has brief descriptions of activities such as elicitation, tests of security, acquiring supplies, suspicious persons out of place, dry run, and deploying assets.

9. Baybutt, Paul, and Varick Ready, "Protecting Process Plants: Preventing Terrorism Attacks and Sabotage," *Homeland Defense Journal,* Vol. 2, Issue 3, pp. 1–5, Feb. 12, 2003 [http://www.homelanddefensejournal.com/archives/pdfs/Feb_12_vol2_iss3.pdf].

10. Tetra Pak, *Dairy Processing Handbook*, S-221 86, Tetra Pak Processing Systems, Lund, Sweden, 1995.

11. Kosikowski, F.V., and V.V. Mistry, *Cheese and Fermented Milk Foods. Volume 1: Origins and Principles,* 3rd edition, FV Koskkowski LLC, Westport, CT, 1997.

12. U.S. Department of Health and Human Services, Food and Drug Administration, "Cheeses and Related Cheese Products," *Code of Federal Regulations*, Title 21, Part 133, pp. 294–346, Washington, DC, April 1998.

13. Goff, D., *Dairy Science and Technology Education Series,* University of Guelph, Canada [www.foodsci.uoguelph.ca/dairyedu/home.html].

RELATED WEBSITES

1. U.S. Department of Homeland Security [http://www.dhs.gov/dhspublic/index.jsp].

2. Federal Bureau of Investigation [http://www.fbi.gov/].

3. Agency for Toxic Substances and Disease Registry [http://www.atsdr.cdc.gov/].

4. Centers for Disease Control and Prevention [http://www.cdc.gov/].

5. U.S. Department of Commerce, Bureau of Industry and Security [http://www.bis.doc.gov/].