I. Overview

At one time the World Heath Organization (WHO) defined food security as, "The implication that all people at all times have both physical and economic access to enough food for an active, healthy life." In 2004, the ideas behind food security reflect less of the ideals of the WHO and more along the lines of bioterrorism.

Bioterrorism is the unlawful use of biologic agents or toxins targeted at civilian populations to coerce political or social objectives. These attacks could easily be directed at numerous links in the farm-to-table chain, which include: crops, livestock, distribution, processing, retail, research facilities, transportation, and storage. This farm-to-table chain, or the US farms, foods, and agriculture systems, accounts for about 13 percent of the nation's gross domestic product and 18 percent of domestic employment. If a major act of bioterrorism occurred in any one is these segments of the chain, it could harm or even kill thousands of people. This in turn would cost the country billions of dollars in healthcare costs and lost wages and could cripple our vast agriculture system.

The terrorist events of the past few years heightened the nation's awareness of terrorism and placed a renewed focus on ensuring the protection of the nation's critical infrastructures. Protection of the nation's food supply is paramount and improving our capacity to prevent, detect, and respond to terrorist acts is a vital part of the BT Act.

This course is geared towards individuals who work on every level of our farm, food, and agricultural system throughout government and the private sector. After completing this course, students will have an increased awareness of the threat of intentional contamination of the US food supply. Specific portions of the food industry will learn about their unique responsibilities in reducing the risk of intentional contamination of the food supply. This course will focus on prevention of, rather than reaction to, intentional contamination.

II. Threat awareness

A. Attacks and incidents

In the US, the CDC reports that over 76 million illnesses, 325,000 hospitalization, and 5000 deaths each year are attributable to the inadvertent contamination to the food supply. Even though recent acts of terrorism have sparked a vigilance unseen in the US; acts of deliberate food contamination have been reportedly been occurring in the US since 1984.

These intentional and unintentional breeches to food security cost the country millions to billions of dollars in health care expenses, lost wages, decrease in consumer confidence, trade embargoes, etc. The CDC reports there are thee types of economic effects that may be generated by an act of food terrorism:

- Direct economic losses attributable to the costs of responding to the act;
- Indirect multiplier effects from compensation paid to affected producers and the losses suffered by affiliated industries, such as suppliers, transporters, distributors, and restaurant chains;
- And international costs in the form of trade embargoes imposed by trading partners.

1. Unintentional incidents

A review of unintentional foodborne outbreaks provides insight into the potential magnitude of the public health impact of a carefully planned intentional attack on the food supply, where the terrorist is in the position to harness the efficiency of the American food distribution system to accomplish their ends. In most cases, mortality associated with an unintentional attack is relatively low, but morbidity can be quite high. Selection of a more lethal agent could change high morbidity numbers to high mortality numbers. A review of noteworthy unintentional foodborne outbreaks also provides insight into the kinds of foods and the points in their production where intentional contamination could have catastrophic consequences. For example:

In March and April, 1985 more than 16,000 people became ill (culture-confirmed) and as many as 17 died in a six-state area from consumption of pasteurized milk contaminated with *Salmonella typhimurium*. Hospitalization was required for 22% of those affected. The actual number stricken was likely in excess of 200,000. The milk was produced by one dairy plant in the mid-west. Unintentional recontamination of the pasteurized milk, resulting from improper piping, is the most likely cause of the outbreak.

In September, 1994 150 people became ill (culture confirmed) from consumption of ice cream contaminated with *Salmonella enteritidis*. The ice cream was produced in a single facility. Hospitalization was required for 30% of those affected. The actual number stricken has been estimated at 224,000. Unintentional contamination of the pasteurized ice cream mix in a tanker truck previously used to haul unpasteurized liquid eggs is the most likely cause of the outbreak.

2. Intentional attacks

In some areas around the world terrorism is commonplace; but as stated before, intentional contamination of the food supply has only been documented in sporadic cases and as far back as 1984. This does not mean that that US does not have major concerns and problems about food security. Recent US General Accounting Office (GAO) reports have indicated that there are major gaps in the federal control of the food supply. This leaves the Unites States vulnerable in protecting the agriculture industry and makes the deliberate tampering of large amounts of food easier. A review of noteworthy intentional foodborne outbreaks can provide insight into the kinds of holes that we have in security which can lead to intentional contamination. For example:

In 1984, members of an Oregon cult headed by Bhagwan Shree Rajneesh used cultivated Salmonella bacteria to contaminate restaurant salad bars in the hopes of affecting the outcome of a local election. Fortunately there were no fatalities in the incident but there were approximately 751 cases of individuals becoming ill and 45 individuals needed to be hospitalized. This incident was detected by local public health officials but they in turn could not pinpoint the source of the outbreak. It took FBI officials one year to link the outbreak to the cult. Prior to the anthrax cases in September of 2001, this was the only recorded case of a bioweapon being used against citizens of the US.

More recently in January of 2003, a Michigan supermarket employee was indicted for intentionally contaminating 200 pounds of ground beef with nicotine. The Centers for Disease Control and Prevention released the information that 92 individuals became ill after purchasing and consuming the ground beef. This case helps document the idea that it is quite simple for one person to intentionally contaminate the food supply and have a major impact.

In October 1996, a former laboratory employee, plead guilty to contaminating a tray of doughnuts and muffins with the foodborne pathogen Shigella dysenteriae Type 2. The former St. Paul Medical Center (located in Dallas, Texas) employee used an unoccupied supervisor's office computer to send out an email inviting 45 other laboratory workers that pastries were available in the employee break room. 12 of the 45 employees ate some amount of a pastry and eventually contracted severe gastrointestinal disease. 4 of those employees required hospitalization but there were no fatalities. The origin of the pathogen was the laboratory itself, which was found to have great conditions to house the pathogen and lax security which made it possible for this intentional contamination to occur.

3. Reasons to attack

Intentional and unintentional harm can have a sizable impact upon the agricultural industry of the United States. In order to put this impact into perspective, here are statistics on the national economic value of agriculture.

- Agriculture equals about $1.24 trillion (13 %) of the Gross National Product.
- Jobs in agriculture equal to about 2% of all U.S. jobs (24 million Americans).
- One in every six jobs are related to agriculture.

- In 2003, U.S. exports equaled an estimated $60 billion.
- 2.2 million farms are located through the country.
- There are 6,500 meat, poultry, and egg processing facilities nationwide.

4. Threats made

Product tampering and the threat of product tampering are very serious problems in the US economy and also overseas. Overseas market terrorism are said to fall into two main categories: malicious tampering and politically-motivated tampering, where the end result is either money to fund a cause or straight political reasons.

One documented case of a major threat that had an economic impact on US soil and abroad, was the 1989 threat made to Chilean grown grapes imported to the US. The treat started when a terrorist group phoned the US Embassy in Santiago, Chile claiming to have laced Chilean grapes with cyanide. The grapes were used for the purpose of wine production and table use, and the threat was directed towards US consumers, US wine companies, and the Chilean economy. The Food and Drug Administration worked in concert with the press and other major stakeholders in the marketing chain to access the severity of the threat and to pull Chilean imported fruit off the shelves.

B. Why the food supply is a potential target (elements of risk)

1. Vulnerability of high-risk foods

a. Attributes of the food target

Four factors are consistently associated with higher risk foods. Foods that are prepared or held in large batches at some point in their production or distribution tend to represent a higher risk. This is because a large batch size generally equates to a large number of servings from that batch, and a large number of servings is necessary in order to result in high morbidity/mortality.

Short shelf life and/or rapid turnaround at retail and rapid consumption also tend to increase risk. Rapid turnaround and consumption of the product provides little time for public health officials to identify the problem and effectively intervene before the outbreak runs its course (i.e., all product from the contaminated batch has been consumed).

Uniform mixing of a food at or following the point at which a contaminant may be introduced is an important contributor to risk because it is in this way that all servings in the batch may contain the lethal dose. Such a condition significantly improves the efficiency of the attack.

Ease of access to product at some point in its production or distribution where the above conditions apply is also an important risk contributor. All intentional contamination

events require access to the product; the more accessible a site is, the more probable it may be targeted.

Besides the preceding four characteristics of higher risk foods, a number of additional factors also increase the risk that a food may be the subject of intentional contamination. They include the following:

Consumption of a food by children or the elderly increases risk, because these groups may succumb to a lower dose. Some foods are consumed in very small quantities (i.e. very small serving size), and with these foods it may be difficult to incorporate the lethal/infective dose in a single serving. A lower lethal/infective dose may reduce this barrier.

Conversely, a large serving size facilitates incorporation of the lethal/infective dose into a single serving.

Preparation of many foods includes processing steps, such as heat treatment, filtration, chlorination, decolorization, washing, removal of outer layers, or other steps by the establishment or consumer, which may dilute (i.e., below the lethal/infective dose), remove or destroy a contaminant that has been previously added. Potential contaminants vary in their response to these and other food handling steps.

Some potential contaminants have flavors or odors than could cause an individual to not consume product to which it has been added; others may imperfectly dissolve in a food. Foods vary in their ability to disguise a contaminant. For example, some foods exhibit a strong flavor, odor, or texture, intense color, or high optical density. These attributes may conceal the presence of a contaminant.

The absence of tamper evident packaging or other packaging that reduces the potential for the product to be tampered with or counterfeited may elevate its risk of be subject to intentionally contaminated.

Certain foods present a highly desirable target. This may be because they are typically consumed by children, for which public reaction to harm is likely to be more intense. Or, it may be because the product has a marked association with the American culture (e.g., brand name icons).

Risk may be increased if a food is produced in a country of concern for terrorism. Risk may also be increased if there has been a pattern of past incidents of terrorist activity, tampering, or counterfeiting with a type of food.

Quality control programs differ for different foods. Some such programs include sensory, microbiological, or chemical analyses which might detect a contaminant. Other programs do not.

In the preparation of some foods, there are steps that may serve to aerosolize or otherwise liberate an agent from the food. These steps may expose processing employees to the effects of the agent before the general public is exposed. In such a case, employee illnesses could serve as a sentinel of the contamination event. Other foods lack such steps in their production.

b. Attributes of the agent used

Potential contaminants may include biological, chemical, or radiological agents. Some may be agents normally associated with unintentionally contamination events and may be familiar to those involved in food safety work. Others may be so-called "exotic" agents or agents more commonly associated with chemical or biological warfare. The following factors increase the risk that a potential agent may be selected for use in intentional contamination:

Contaminants that have the potential to cause death or severe illness are more likely selections.

The time between ingestion of a contaminant and the beginning of symptoms (e.g., incubation period), especially severe symptoms, varies widely for the range of potential contaminants. A long incubation period could minimize opportunity for public health intervention, by allowing for more of the contaminated lot to be consumed before the first symptoms are reported to public health officials.

Agents vary widely in their ability to maintain their toxicity or infectivity when subjected to the conditions that may be present in food, such as pH and water activity. Higher stability may increase the likelihood that an agent will be selected for use.

Some agents have legitimate commercial applications and are, therefore, readily available to a would-be aggressor. Others are the subject of strict government controls or require complex synthesis, providing a possible barrier to their use.

Some agents have a history of use in poisonings, tampering, or terrorist activity. These may be more likely to be selected for future contamination events.

2. Attitudes of employees

The attitude of employees in a food service establishment can also be a vulnerability. It's a natural tendency to think that nothing bad will happen in our own work place – the "It won't happen to me" syndrome. However, this attitude can lead to complacent workers. Apathy about their work place can also result in employees who are not concerned about food security. The employee who thinks it's not her job to worry about food security and the arrogant know-it-all who thinks he's provided enough food security both make the food supply vulnerable. Too few resources and a lack of commitment to food security may also hamper employees. In these situations, it is important to educate employees of the establishment about the importance of food security and let them know that the typical aggressor thrives on their lack of vigilance.

C. Aggressors

1. Overview

For anyone to successfully tamper with a food product, the aggressor must have access to it for a sufficient time, be technically capable of introducing a suitable contaminant, and be able to commit the crime without discovery. In addition, the aggressor must have the behavioral resolve (desire) to contaminate food and the technical feasibility (appropriate materials) to succeed. The product's manufacturing and distribution process must make the operation practical; in other words, the ability to contaminate the product must be readily present somewhere along the life cycle. The aggressor must be knowledgeable about the food product's life cycle and be competent enough to avoid detection of the adulterated product later in the manufacturing and distribution process.

2. Types of Motivation

Aggressors can be divided into one of five categories: disgruntled insiders; criminals; protestors; subversives; and terrorists. Each has distinct characteristics and motivations.

- *Disgruntled insiders* are generally motivated by their own emotions and self-interests. They may be mentally unstable, operating impulsively with minimal planning. This may be the most difficult group to stop, because they may have legitimate access to the product.
- *Criminals* may be either sophisticated or unsophisticated. The former may possess relatively refined skills and tools and are generally interested in high-value targets. The latter may possess only relatively crude skills and tools, and typically have no formal organization. They are generally interested in targets that pose a low risk of detection.
- *Protestors* are usually politically or issue-oriented. They generally act out of frustration, discontent, or anger. They are primarily interested in publicity for their cause, and, as a result generally do not intend to injure people, but may be superficially destructive. They are usually unsophisticated in their tactics and planning. However, some protest groups have adapted tactics similar to terrorists. In this way, they may be moderately sophisticated and moderately destructive. In fact, they may target individuals for harm.
- *Subversives* are also known as saboteurs, assassins, guerrillas, or commandos. They are sophisticated, highly skilled, and capable of meticulous planning. Subversives typically operate in small groups. Their objectives include death and destruction, targeting personnel, equipment and operations.
- *Terrorists* are usually politically or ideologically oriented. They typically work in small, well organized groups. They are typically well funded, sophisticated, and capable of efficient planning. Terrorists may use other types of aggressors to accomplish their goals. Their objectives include death, destruction, theft, and publicity.

Organizationally, terrorists organizations can be divided into three groups. They may be nonstate-supported groups (e.g. Italy's Red Brigades), in which case they operate autonomously, with no significant support from any government. They may be state-supported (e.g. Popular Front for the Liberation of Palestine), in which case they operate

independently but receive support from one or more governments. Or, they may be state directed (e.g. Libyan "hit teams"), in which case they operate as agents of their government.

3. Tactics

An aggressor intending to contaminate the food supply may use one or more of the following types of tactics: insider compromise, exterior attack, forced entry, and covert entry.

With insider compromise the attacker takes advantage of his/her legitimate access to the food (e.g., as an employee of a food handling facility) to contaminate the food.

In an exterior attack, the aggressor may contaminate a raw material used in the production of the desired target food, at a point where it is grown, transported or processed. In this way the contamination can be performed under conditions that may be more favorable to the terrorist than at the target facility. The contaminated raw material can then enter the target facility through a normal distribution route. Subverting shipments of legitimate product for black-market money making schemes is another form of exterior attack. It may be that the money making scheme is the extent of the attack, or it may be that access to the subverted product is used to contaminate it and then re-enter it into normal commerce.

Forced entry, e.g., picking a lock in order to enter a facility at night, may be used in order to contaminate the food contained within a facility. For such a scheme to be successful, the aggressor must be able to egress without raising suspicion that the product was contaminated. However, suspicion may be averted by employing some sort of diversionary activity, such as vandalism or theft.

Covert entry consists of using deception or stealth in order to gain access to food within a facility. For example, an aggressor may pose as a member of a tour group in order to gain access.

III. Preventive measures

A. General

Some preventive measures may be useful in minimizing the risk of all forms of aggressor tactics.

The first step is to perform an initial vulnerability assessment. A number of methodologies are available for performing such an assessment, such as Operational Risk Management (ORM) and CARVER. Based on the results of the assessment, a food security strategy (e.g., plan) can be developed. This plan should include a recall strategy. Staff should be trained on the contents of the strategy and it should be tested regularly, in the form of an exercise. Because the nature of the potential threat and the physical facility and the operations within may change over time, the food security strategy should be reassessed at least annually.

Efforts should be made to inform and involve staff in food security. At its core, this means to promote food security awareness by staff. An informed and alert staff is more likely to detect weaknesses in a food security system and to detect and properly respond to signs of intentional contamination. Employees should be encouraged to report suspicious activities, possible product tampering or suspected security system weaknesses to management of the facility.

Routine security checks should be performed of the premises for signs of criminal activity or areas that may be vulnerable to such activity. These security checks should concentrate on sensitive areas (e.g., places where the product is exposed, especially in large batches, in-plant laboratory facilities, water, gas and electric utilities, computer data and ventilation systems). Additionally, management of the facility should aggressively investigate threats or information about signs of tampering should and report to law enforcement.

Management should be alert to staff health conditions that may serve as an early alert of a tampering event. In the event of an intentional contamination event, staff may be the first to be exposed to the contaminant. In some cases production or Q.C. staff involved in sensory analysis (e.g. taste testing) may become ill because of their exposure. Additionally, some agents may become airborne during food preparation and may cause illness when inhaled, or may be absorbed through the skin when the food is handled.

Local permitting offices should be requested to notify facility management when a copy of the facility blueprints or other detailed facility information is requested. Such information may be useful to an aggressor conducting reconnaissance.

B. Preventing insider compromise

One of the most effective means of reducing the risk of insider compromise is an appropriate level of supervision of staff. Supervision should extend to cleaning and

maintenance staff, and should concentrate on new staff. There are a number of behaviors for which the manager should be particularly watchful, for example: (1) unexplained early arrival or late departure; (2) staff accessing information or areas not related to their job function; (3) staff removing documents from the facility; (4) staff asking sensitive questions; or (5) staff bringing a camera to work. A disgruntled employee that is collecting intelligence or taking other actions in support of an intentional contamination scheme may engage in these types of behavior.

Management should screen the background of staff, especially those with access to sensitive areas (e.g., places where the product is exposed, especially in large batches, in-plant laboratory facilities, water, gas and electric utilities, computer data and ventilation systems). Screening employee backgrounds can reduce the likelihood that someone will be hired or placed in a sensitive position that is predisposed to illegal activity.

Management should also keep track of who is and should be on duty, and where they are scheduled to work. This can take the form of a shift roster. A disgruntled employee who has intentionally contaminated product may not return to work. On the other hand, a disgruntled employee who plans to intentionally contaminate product may access areas not normally associated with their job function in order to collect intelligence or take other actions in support of the scheme.

Staff access to sensitive areas should be restricted to those who need access based on their job function. A disgruntled employee who plans to intentionally contaminate product may access areas not normally associated with their job function in order to collect intelligence or take other actions in support of the scheme.

Personal items should be restricted in the facility, especially in sensitive areas. A disgruntled employee who plans to intentionally contaminate product may need to bring the contaminant into the facility, using personal items, such as a purse, thermos, or lunch bag as a means of disguising it. Similarly, provision should be made to inspection staff lockers. A disgruntled employee may use their locker as a temporary storage location for a contaminant that they have managed to bring into the facility.

Cleaning and pest control chemicals and laboratory reagents and controls should be controlled. Those stored on the premises should be limited to those needed. They should be stored away from food and kept properly labeled. Access to storage areas for these items should be limited to those who need access based on their job function. An effort should be made to keep track of the inventory of these items and to investigate any missing articles. Additionally, any unneeded items should be disposed of properly to prevent their unwanted use. Readily available toxic substances are often the contaminant of choice for a disgruntled employee.

C. Preventing the exterior attack

Food items should only be purchased from known and trusted sources. Counterfeit or contaminated product may be offered for sale, likely at a reduced price, by an unknown

entity, posing as a legitimate businessperson. Additionally, suppliers should be encouraged to practice food security. Contamination of raw materials or finished products can occur at a supplier's facility, circumventing the security measures that may be present at the customer's facility. Consideration should be given to making specific security measures part of a supplier's contract.

Delivery vehicles should be properly secured, especially those carrying bulk fluids. Locked and/or sealed vehicles can discourage in-transit contamination, especially where the seal number at receipt is compared to the number at loading. Pick-up and delivery schedules should be established in advance and unscheduled pick-ups or deliveries should be questioned. Delivering counterfeit or contaminated product may require a delay to switch or tamper with the load and may require a replacement of the original driver (e.g., in the case of a hijacked load). Knowing when a delivery is due and the name of the driver enables the customer to question the cause for a delayed or unscheduled pick-up, delivery or driver. When a delivery arrives, its off-loading should be supervised. Contamination can occur as the load is being off-loaded, especially if it occurs during off hours. The product type and quantity received should be reconciled at delivery with the product and quantity ordered and listed on the paperwork. Delivering counterfeit or contaminated product may require substitution of part or all of a load, possibly resulting in an error in the type or quantity of product in the load.

Finally, product, packaging and paperwork should be inspected at receipt. Attempts to contaminate product can leave detectable signs, such as abnormal powders, liquids, stains or odors, evidence of resealing, or compromised tamper-evident packaging. Counterfeit product may show inappropriate or mismatched product identify, labeling or product coding. Counterfeit or contaminated loads may be accompanied by shipping documents with suspicious alterations, created to disguise changes necessary to accomplish the substitution or contamination.

D. Preventing forced entry

Perimeter fencing should be provided for non-public areas of the facility. This is the first line of defense against attack by an intruder.

Doors, windows, roof and vent openings, and other access points, including access to food storage tanks and bins outside the primary buildings should be protected. Locks, alarms, video surveillance, and guards can increase the difficulty of an intruder gaining access to the interior of a facility. Bulk unloading equipment and trailer bodies should also be secured, and should be inspected before use. Contaminants introduced into unloading equipment when it is not in use or empty trailer bodies can later become incorporated into the food.

Access to gas, electric and water utilities should be secured. Water is of particular concern because contaminants introduced into water can become incorporated into the food.

Provision should be made for the facility to be monitored, including during off-duty hours. Adequate interior and exterior lighting should be provided because a well lit facility can increase the risk that an intruder will be detected.

E. Preventing covert entry

Management should establish a system of staff identification, such as uniforms or name tags. Staff identification measures allow an intruder to be more easily spotted.

Entry to non-public areas of the facility should be restricted. This can be accomplished by establishing security check points or by accompanying all visitors to the facility. Ensuring that visitors are who they claim to be and that their visit has a legitimate purpose reduces the risk that someone with criminal intent will enter the facility. Accompanying visitors that are permitted entry reduces their ability to cause harm.

Vehicles and packages that enter non-public areas should be examined because a visitor may conceal a contaminant in his/her vehicle, or in a package or briefcase that he/she brings into the facility.

Vehicle access and parking in non-public areas should be controlled. Keeping vehicles away from sensitive areas of the facility (e.g., places where the product is exposed, especially in large batches, in-plant laboratory facilities, water, gas and electric utilities, computer data and ventilation systems) can increase the difficulty that a contaminant can be transferred from a vehicle to the interior of the facility or that critical systems can be compromised.

Public areas should be monitored for suspicious activity. A customer who is intent on contaminating product may return product to a shelf that he/she has already contaminated or may spend an inordinate amount of time in one part of the store while contaminating product on site. In particular, self-service areas (e.g. salad bar, product display area) should be monitored. As previously mentioned, intentional contamination at a self-service location has already occurred in the U.S.

IV. Federal action

The United States government has taken several important steps toward securing the nation's food supply.

A. Homeland Security Presidential Directive 7

On December 17, 2003, President Bush issued Homeland Security Presidential Directive (HSPD) 7. This directive establishes a national policy for Federal departments and agencies to identify and prioritize US critical infrastructure *(definition: Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.)* and key resources and to protect them from terrorist attacks.

Food was designated as a critical infrastructure. The Departments of Agriculture (USDA) and Health and Human Services (HHS) share responsibility for the food infrastructure sector. Their responsibilities include…

- collaborating with key persons and entities;
- conducting or facilitating vulnerability assessments;
- encouraging risk management strategies; and
- identifying, prioritizing, assessing, remediating, and protecting their respective internal critical infrastructure and key resources.

The food infrastructure sector plan calls for improved information sharing with states and the private sector, and the implementation of communications and geographical information systems. USDA and HHS were also tasked to develop indications and early warning mechanisms, integrate their cyber and physical protection plans, and submit regular status reports on private sector coordination. Efforts are underway to establish a food and agriculture information sharing council based on the current Food Sector Information Sharing and Analysis Center hosted by the Food Marketing Institute (FMI). FMI is coordinating with the Department of Homeland Security (DHS), the Food Safety and Inspection Service (FSIS), the Food and Drug Administration (FDA), states, and industry in this effort.

B. Homeland Security Presidential Directive 9

HSPD 9 was issued on January 30, 2004 to establish a national policy to defend the US agriculture and food system against terrorist attacks, major disasters, and other emergencies. This is to be accomplished by USDA, HHS, and the Environmental Protection Agency (EPA) through...

- identifying and prioritizing sector-critical infrastructure and key resources for establishing protection requirements;
- developing awareness and early warning capabilities to recognize threats;

- mitigating vulnerabilities at critical production and processing nodes;
- enhancing screening procedures for domestic and imported products; and
- enhancing response and recovery procedures.

Under this directive, agencies were tasked with developing surveillance and monitoring systems for animal disease, plant disease, wildlife disease, food, public health, and water quality. As appropriate, specific animals and plants are tracked, as well as specific commodities and food.

The Food Emergency Response Network (FERN) is a nationwide laboratory network for food, veterinary, plant health, and water quality that resulted from this directive. FERN integrates existing Federal and state laboratory resources and utilizes standardized diagnostic protocols and procedures. FERN is co-chaired by USDA's FSIS and HHS' FDA and plays a number of critical roles related to foodborne terrorism. It provides a national surveillance program that will offer early means of detecting threat agents in the US food supply, and prepares the nation's labs to be able to respond to food-related emergencies. The FERN network also offers significant surge capacity that will allow the nation to respond to widespread, complex emergencies related to agents in food. This, in turn, will enhance the ability to restore public confidence after an emergency or in response to threats.

Working in conjunction with FERN is the Electronic Laboratory Exchange Network (eLEXNET), a web-based system that provides a rapid laboratory results reporting system among FERN members. eLEXNET also lists test methods approved by the FERN Methods Committee to be used by FERN Labs for analysis of certain agents.

C. Vulnerability/Threat Assessments

FDA, FSIS, and the Food and Nutrition Service (FNS) have conducted threat assessments on the food supply to focus limited government and industry resources on those foods and agents that may be of greatest concern.

As part of the White House's Interagency Food Working Group, FSIS conducted vulnerability assessments for domestic and imported meat, poultry, and egg products, applying several different methodologies. Targeting four high-risk products, FSIS has worked closely with FDA in conducting these vulnerability assessments. Specific information on vulnerabilities is classified, but these assessments have allowed the agencies to identify high risk commodities; identify chemical, biological, and radiological threat agents that could potentially contaminate food; identify physical places in the farm-to-table continuum <*definition: A continuous process that includes each and every link involved with food reaching the consumer - from the way it is grown or raised, to how it is collected, processed, packaged, sold, and consumed.*> that are critical nodes, and use the CARVER + Shock method < *definition: A collaborative effort of FSIS and FDA, commissioned by DHS, this is an offensive target prioritization tool to identify critical nodes most likely to be targets for terrorist attack and design shields to reduce risk.*> to identify critical nodes.

The results from these assessments will provide agencies with critical information to develop strategies and policies, as well as food shields, or countermeasures, to reduce or eliminate potential risks at vulnerable points along the farm-to-table continuum.

D. Emergency preparedness

Emergency response preparedness activities have also benefited from the threat assessments. For example, Agencies target preparedness exercises to scenarios that may present greater risk, and they are ensuring that there are sufficient laboratory capacity and technical capability to respond to events present in an elevated risk scenario. Similarly, Agencies are evaluating available medical countermeasures, both with respect to effectiveness and quantity of materials, for elevated risk scenarios. The abilities to effectively dispose of food products that may become contaminated and decontaminate food facilities are also being considered.

E. Research

These assessments allow agencies to target research to areas where it can have the greatest impact, such as:

- development of analytical methods for agents not normally associated with food contamination (rapid and confirmatory);
- understanding the nature of disease caused by agents not normally associated with food contamination (e.g., oral toxic/infective dose);
- evaluating the compatibility of agents in food matrices; and
- exploring the utility of food processing (e.g., increases in processing temperatures) and physical security (e.g., improved bulk container sealing procedures) steps in the reduction of risk.

F. Guidance

These threat assessments have enabled the government to target food security outreach efforts to stakeholders. In an effort to reduce risk where it may be highest, government agencies are tailoring guidance, industry and regulator training, technical assistance, and communications efforts to address the areas of greatest concern.

1. FSIS guidance

FSIS developed guidelines to assist small food processors, shippers, and distributors. These voluntary guidelines provide a list of safety and security measures these entities should consider to strengthen their food safety and food security plans. These publication are available at http://www.fsis.usda.gov/Food_Security_&_Emergency_Preparedness/Security_Guidelines/index.asp.

- **FSIS Safety and Security Guidelines for the Transportation and Distribution of Meat, Poultry, and Egg Products**
  This brochure for the food industry provides recommendations to ensure the security of food products through all phases of the distribution process. The publication is available in different formats and languages.
- **FSIS Security Guidelines for Food Processors**
  These guidelines assist federal and state inspected plants that produce meat, poultry, and egg products in identifying ways to strengthen their biosecurity protection.
- **Keep America's Food Safe**
  This guidance is designed to assist transporters, warehouses, distributors, retailers and restaurants with enhancing their security programs to further protect the food supply from contamination due to criminal or terrorist acts.

2. FDA guidance
Under the Bioterrorism Act of 2002, FDA requires the registration of food facilities as well as prior notice for importing foods. Information about these requirements can be found at http://www.fda.gov/oc/bioterrorism/bioact.html.

In addition, FDA has issued the following guidance documents, which can all be found at http://www.cfsan.fda.gov/~dms/guidance.html#sec.

- **Cosmetics Processors and Transporters: Cosmetics Security Preventive Measures Guidance**
  This 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.
- **Retail Food Stores and Food Service Establishments: Food Security Preventive Measures Guidance**
  This guidance is designed to focus operators' attention sequentially on each segment of the food delivery system that is within their control, to minimize the risk of tampering or other malicious, criminal, or terrorist action at each segment.
- **Dairy Farms, Bulk Milk Transporters, Bulk Milk Transfer Stations and Fluid Milk Processors: Food Security Preventive Measures Guidance**
  This guidance is designed as an aid to operators of dairy farms, bulk milk transportation operations, bulk milk transfer stations and fluid milk processing facilities. It identifies the kinds of preventive measures operators of these establishments may take to minimize the risk that fluid milk under their control will be subject to tampering or other malicious, criminal, or terrorist actions.
- **Food Producers, Processors, and Transporters: Food Security Preventive Measures Guidance**
  This guidance identifies the kinds of preventive measures operators of food establishments may take to minimize the risk that food under their control will be subject to tampering or other malicious, criminal, or terrorist actions. It is relevant to all sectors of the food system, including farms, aquaculture facilities, fishing vessels, producers, transportation operations, processing facilities, packing

facilities, and warehouses. It is not intended as guidance for retail food stores or food service establishments.

- **Importers and Filers: Food Security Preventive Measures Guidance**
  This guidance is designed as an aid to operators of food importing establishments, storage warehouses, and filers. It identifies the kinds of preventive measures that they may take to minimize the risk that food under their control will be subject to tampering or other malicious, criminal, or terrorist actions.

V. Awareness responsibilities and actions

A. Communication with industry

1. Regulators

FSIS

FSIS Inspectors in Charge (IICs) should refer establishment management to FSIS's *Food Security Guidelines for Food Processors* for additional security measures they may want to incorporate in their Food Security Action Plans. IICs should meet regularly with establishment management to discuss the content of the Food Security Plan. However, keep in mind that establishments are not required to develop Food Security Action Plans. IICs are to notify the establishment management immediately of any observation of concern.

FDA

FDA's goal is to facilitate an exchange of information to heighten awareness of food security. Management of the establishment should be encouraged to voluntarily implement those preventive measures that are appropriate for their operations. However, FDA investigators should not perform a comprehensive food security audit of an establishment, nor should they conduct an extensive interview in an attempt to determine the level of adoption of preventive measures.

Food regulatory officials should cover the preventive measures during regular inspections or audits of food establishments, food importers, warehouses, and evaluation of filers. Based on conditions observed during the normal course of the inspection/audit, the appropriate material in the guidance documents should be discussed with management of the establishment and a copy of the guidance should be provided during the close-out meeting. Additionally, any opportunities for improvement or enhancement of the establishment's preventive measures that were identified during the inspection/audit should be discussed with management, but should not be listed as violations unless they likewise constitute deviations from regulations.

The fact that the discussion took place and that a copy of the guidance document was provided should be recorded in the inspection report (e.g. FDA's Establishment Inspection Report [EIR]) or evaluation report, but the details of the inspectional findings in this regard should not be recorded. Additionally, investigators should minimize the quantity and detail of notes taken relative to the establishment's food security program, taking only those needed to serve as a "memory jog" during the discussion with management.

In addition to the guidance documents listed previously, the following Internet resources should be provided to food establishments:

- USDA's "Keeping America's Food and Agriculture Safe" page http://www.usda.gov/homelandsecurity/homeland.html

- USDA FSIS' "Food Security and Emergency Preparedness" page http://www.fsis.usda.gov/Food_Security_&_Emergency_Preparedness/index.asp
- FDA's "Ensuring the Safety and Security of the Nation's Food Supply" page http://www.fda.gov/oc/initiatives/foodsecurity/
- FDA CFSAN's "Food Safety and Terrorism" page http://www.cfsan.fda.gov/~dms/fsterr.html

2. Administrators

a. Food security and contracts

Food establishment administrators should ensure that adequate food security procedures are built in to all contracts the establishment holds with outside vendors.

b. State procedures

Administrators should also be aware of any state-specific food security procedures that are applicable.

B. Who to contact

Report suspicious activity to local law enforcement officials first.

1. FDA

If the situation is an emergency that requires immediate action, such as a case of food-borne illness or a drug product that has been tampered with, call the Agency's main emergency number, staffed 24 hours a day, 301-443-1240.

2. FSIS

FSIS Contact information:
USDA Technical Service Center - 1-800-233-3935

In addition to the above contacts, these additional resources are available. If a suspect food is a meat or poultry product, call the USDA Meat and Poultry Hotline at 1-888-MPHotline (1-888-674-6854) or E-mail MPHotline.fsis@usda.gov. For all other food products, notify FDA at 1-888-SAFEFOOD (1-888-723-3366).

C. Additional activities under heightened awareness conditions

Additional actions to ensure food security should be taken by industry when the US is under an elevated terrorism threat level – High (orange) or Severe (red). (See http://www.dhs.gov/dhspublic/interapp/press_release/press_release_0046.xml for more information on DHS' Homeland Security Advisory System.)

FSIS issued its emergency Food Security Monitoring Procedures in Directive 5420.1 in March 2003. (See http://www.fsis.usda.gov/Frame/FrameRedirect.asp?main=http://www.fsis.usda.gov/OPPDE/rdad/FSISDirectives/5420.1.htm.) The FSIS Office of Food Security and Emergency Preparedness (OFSEP) will communicate heightened threat conditions to field personnel through their District offices (DO).

If a High or Severe threat is not specific to the agricultural sector or food supply, USDA field personnel must notify the establishment of the threat condition, but take no further action unless instructed by the DO.

If a High threat condition is related to the agricultural sector or the food supply, USDA field personnel are to inform establishment management and implement emergency food security monitoring procedures. IICs will determine whether, and if so what, additional monitoring procedures are appropriate at their assigned establishments. At a minimum, additional food security procedures must include:

- Observing the outer perimeter of the establishment to ensure that fences and gates (if any) are intact.
- Ensuring that entrances to the establishment are secured against unauthorized entry.
- Observing incoming raw materials to ensure that all deliveries are verified against shipping documents.
- Observing live animals arriving at the establishment for symptoms of specific diseases that may indicate the introduction of a biological agent (e.g., foot and mouth disease) into the livestock population. (Also, promptly notify the Animal and Plant Health Inspection Service (APHIS) when signs and lesions of foreign animal diseases are noted on livestock or poultry during ante-mortem and post-mortem inspection.)
- Observing the use and storage of any hazardous materials in the establishment; and ensuring that entry into storage areas is controlled and that usage logs are maintained and current.
- Observing products in storage areas for evidence of tampering.
- Observing the security of the plant's water systems, especially water storage facilities and reuse systems. (Check the plant's potable water supply and report any change in the appearance, taste or odor to the establishment.)
- Observing maintenance, construction, and repair activity at the establishment to ensure personnel performing such activities are properly identified and authorized to perform such activities.
- Observing production processes (slaughter, processing, fabrication, packaging, etc.) where exposed products are being handled for indications of any possible attempts to introduce contaminants.
- Observing the behavior and in-plant movement of establishment employees, especially those who suddenly appear in areas where they are not assigned to work.

- Observing loading dock areas and vehicular traffic in and out of the establishment. (Report all unattended deliveries on loading docks and unmarked vehicles parked on the premises to establishment management immediately.)

If a Severe threat is specific to the food supply or a particular product or process, the IIC at the affected establishment will receive specific instructions from the DO, in addition to the implementation of the above food security verification procedures. Such measures may include sampling specific products and taking regulatory actions, if warranted. The DO will deploy inspection program personnel to establishments where the products named in the threat condition are produced. This will ensure that FSIS has an onsite presence during any type of operational activity. Import inspectors will re-inspect 100% of imported product.

IICs are to perform the designated emergency food security monitoring procedures daily for as long as the declared threat condition remains at the High or Severe level.

[I couldn't find any equivalent information from FDA . If they review it and feel left out, they'll have to provide the info.]

VI. Conclusion

The nation's awareness of terrorism has been heightened and there is a renewed focus on ensuring the protection of the nation's critical infrastructures. Efforts to improve the security of the food supply, must focus on prevention, early detection, containment of the contaminated product, and mitigation and remediation of any problems that do occur.

Individuals who work at every level of our food and agricultural system should have an increased awareness of the threat of intentional as well as unintentional contamination of the food supply. They should know their unique responsibilities in reducing that risk. Being aware of these responsibilities helps ensure better security in all links of the farm-to-table chain.

As you deal with issues involving a possible attack on the food supply, carefully consider physical security, surveillance and monitoring, personnel security, and emergency response. In addition, become familiar with the FDA, FNS, and FSIS references listed previously in this course and be ready to share them with the employees and management of the food industry establishments with which you come into contact.