REPORT OF THE COMMITTEE ON FOOD SAFETY

Chair: Daniel E. LaFontaine, Columbia, SC
Vice Chair: Bonnie J. Buntain, Washington, DC

Marilyn F. Balmer, MD; John R. Behrmann, PA; Joseph L. Blair, VA; Dale D. Boyle, DC; Richard E. Breitmeyer, CA; Terry L. Burkhardt, WI; David M. Castellan, CA; Jan Charminski, WV; Max E. Coats, Jr., TX; Carl W. Cushing, VT; Kevin M. Elfering, Mn; Wyatt Frampton, UT; Bob Gerlach, AK; L. Wayne Godwin, FL; Eric C. Gonder, NC; Larry M. Granger, MD; Donald E. Hoenig, ME; Tom Holder, MD; Rex D. Holt, Ga; Danny R. Hughes, AR; John P. Huntley, NY; Lee C. Jan, TX; Robert F. Kahrs, FL; Susan J. Keller, ND; Spangler Klopp, DE; Elizabeth A. Krushinskie, GA; Daniel E. LaFontaine, SC; Elizabeth A. Lautner, IA; Kelli S. Ludlum, DC; Michael M. Mamminga, IA; Bret D. Marsh, IN; David T. Marshall, NC; James D. McKean, IA;; Lee M. Myers, GA; Jill A. Nezworski, MN; Carol A. Olmstead, MT; Kenneth E. Olson, IL; Gary D. Osweiler, IA; Gerardo Quaassdorff, VT; John R. Ragan, MD; Nancy J. Robinson, Mo; Kerry Rood, VT; Leon H. Russell, Jr., TX; John P. Sanders, Jr., WV; Glenn N. Slack, KY; Harry Snelson, NC; Philip Stayer, MS; Bruce N. Stewart-Brown, MD; Stanley A. Stromberg, OK; Manuel A. Thomas, Jr., TX; Lyle P. Vogel, IL; Larry L. Williams, NE; Nora E. Wineland, CO; John F. Wortman, Jr., NM; Ria de Grassi, CA.

The Committee met on October 15, 2006 at 12:30 p.m. Chair Daniel Lafontaine presided. Approximately 51 Committee members and guests were welcomed to the annual meeting by Dr. Lafontaine. He introduced this year's topic of food defense and related it to the emphasis at the local, state, and federal levels on developing food defense programs. After Dr. Lafontaine's welcoming and introductory remarks, the Committee received a series of three presentations. Following the presentations, a workshop was conducted. The workshop applied the Criticality, Accessibility, Recuperability, Vulnerability, Effect, and Recognizability (CARVER) + Shock Vulnerability Assessment Model to a food system.

The first Committee presentation, Intersection of Food Safety and Food Defense: Actions to Protect our Meat, Poultry and Egg Products Food Supply, was delivered by Dr. Kenneth Petersen, Assistant Administrator, Office of Field Operations (OFO), Food Safety and Inspection Service (FSIS), United States Department of Agriculture (USDA). FSIS traces its roots to food safety and the role of food safety in protecting public health. Since 2001, emphasis within FSIS has shifted to include food defense. Consequently, there have been significant accomplishments in developing food defense programs in the past five years. By definition, food safety focuses on unintentional contamination of food products whereas the focus of food defense is on intentional contamination of food products. There are both similarities and differences in developing programs directed at food safety and food defense. Regarding food system analysis, the food safety approach is more a traditional risk based analysis, founded on established science and historical data. When analyzing a food system from a food defense perspective, risk based analysis is still important, but vulnerability assessments must also be conducted. Scientific knowledge cannot be used to predict instances of intentional contamination. The analyst must learn to try to think like a terrorist. Later in the program, a vulnerability assessment model will be discussed in detail. Control strategies for food safety include good agricultural practices on the farm and good manufacturing practices in processing facilities. With food defense, the emphasis shifts to physical security, personnel security, and production security. When considering expected outcomes of breaks in food safety programs, one thinks of high rates of illness but relatively low mortality rates. But with intentional contamination, higher death rates are often the outcome, although not necessarily by design. Food products that are unintentionally contaminated can sometimes be reprocessed, such as recooking. If unintentionally contaminated food products cannot be reprocessed, disposal is usually by established procedures. With intentionally contaminated food products, reprocessing is not an option. Disposal is often very difficult and plant or farm clean-up can be very complex and expensive. Communicating food safety concerns is routine and includes such things as safe handling procedures. Any incident of intentional food contamination is an instant public relations nightmare, which can often lead to wide-spread public panic.

How is FSIS dealing with the concerns brought about by the specter of deliberate or intentional food contamination? Similar mechanisms are in place for dealing with food safety and food defense and the same workforce is used for both. However, additional training has been conducted to help the workforce recognize the signs of intentional contamination. Likewise, training in conduct of food vulnerability assessments is ongoing. Efforts to enhance industry awareness about the need for food defense programs continue. All surveillance programs are working to bring together a wide range of data to facilitate analysis. The laboratory infrastructure is changing to meet the challenges of intentional contamination. This will be covered in depth in the next presentation. This overview reviews similarities and differences between food defense and food safety and provides points for consideration during the subsequent presentations.

Dr. Patrick McCaskey, Director of Laboratories, Office of Public Health and Science (OPHS), FSIS, USDA then gave a Committee presentation entitled, Overview of Food Defense Surveillance- Laboratory Perspectives*.* When considering food defense surveillance, the scope of the problem is partially defined by the commodity itself. First, we all need food and we all eat food. It is an ideal vehicle for dissemination of harmful agents and the agents can be easily masked. Often times agents are not homogeneous in food. They can be rapidly disseminated through the food distribution chain. This makes it difficult to identify the food source that caused the event and equally difficult to trace it back to the origin. Finally, intentional contamination may be confused with a natural event. All of this gives the perpetrator time to act and escape. Adding to the complexity of the problem is the fact that there are over 50,000 food types. In the laboratory this means potentially 50,000 food matrices for which analytical methods must be developed. Also, those 50,000 food types are from many different sources and contain many different ingredients. The food distribution chain is large and diffuse. It is a complex web usually starting on a farm and subsequently involving various vehicles, processing plants, warehouses, retail stores, restaurants and homes. Everywhere in the chain, vulnerabilities exist.

Potential agents contribute to the surveillance problem. There are over 80,000 different chemicals. Almost every one of them can cause illness, given the right concentration. In addition, there are hundreds of naturally occurring biological pathogens, toxins, heavy metals, parasites, radioisotopes, genetically engineered organisms, and others. On the other side of the coin are the people. There are 300,000,000 Americans to protect and it only takes one properly motivated and equipped terrorist to cause havoc. An intentional food contamination event may take on many different appearances. It may be widespread, or it may be at one time and in one location. It may be ongoing, and/or multicentric. It may cause death and/or illness. It may involve one agent or multiple agents and there may be attacks on multiple sectors. It may cause panic or unrest and it may have severe economic ramifications.

Where were we five years ago in dealing with this problem? September 11th and the anthrax attacks identified multiple national deficiencies in our surveillance programs in numerous areas including expertise, workload capability, facilities, analytical methodologies, established points of contact, communication and coordination. At first, the problem seemed so complex that the solution seemed to be, "Stick our heads in the sand and hope someone sends help!" Obviously that solution would not work. Soon Option 2 became development of a plan to deal with surveillance of intentional attacks on the food supply. This was a multi-step process including assess the situation, determine capabilities, identify barriers and roadblocks, assess safety issues, determine facilities needs, identify gaps in needed methodologies, and develop a plan of action.

From the laboratory perspective, the real question was whether or not we can have an effective laboratory-based food defense surveillance program for food. The solution was to develop the Food Emergency Response Network (FERN). It is a cooperative agreement between FSIS and the Food and Drug Administration (FDA). FERN's mission is to integrate the nation's food-testing laboratories for the detection of threat agents in food at the local, state, and federal levels; test for chemical, biological, and radiological agents; and have capability to test a full range of food commodities. The objectives are:

- prevention through use of federal/state surveillance sampling programs
- preparedness by strengthening lab capabilities/capacities
- response by providing surge capacity
- recovery by provide assurance to the consumer

FERN's organizational structure consists of Co-Chairs from FSIS and FDA, an executive board, support programs, a national program office, and five regional coordinating centers across the U.S. FERN members consist of 133 laboratories representing all 50 states and Puerto Rico. There are 27 federal labs, 96 state or territorial labs, and 10 local labs. The network is composed of public health, agricultural, environmental, and veterinary diagnostic labs. There are 94 chemical, 105 microbiological, and 29 radiological disciplines represented in the participating laboratories.

FERN has developed a training plan which includes both web-based and face-to-face training on methods, biosafety laboratory BSL-3 lab protocols and others. To date, FERN training includes 10 separate programs involving over 100 individual training encounters. FERN also developed standard operating procedures for proficiency testing and has conducted approximately 148 proficiency training events. Integrated surveillance is a primary goal of FERN. To make the surveillance value added, FERN is working to incorporate food defense training and testing into existing food safety programs. For example, the Interstate Travel Program was first. Twelve labs were asked to test aircraft water for chemical and biological contaminants in May 2005. In another testing round, twelve labs were issued an assignment in the Import Produce Program, testing for chemical and biological contaminants in November 2005. Currently, FERN is conducting a pilot surveillance program for special agents on National School Lunch Program products. This is being conducted in coordination with USDA's Agricultural Marketing Service (AMS) and Food and Nutrition Service (FNS). The sampling is done in plants and warehouses and the testing done at FERN-member labs. So far, there has been very limited testing in this pilot project.

Electronic communication is another important component in developing any network. FERN is no exception. The data capture and exchange mechanism for the FERN is the Electronic Laboratory Exchange Network (eLEXNET). FERN uses eLEXNET for Collaboration and Data Sharing in several ways:

- The FERN National Program Office shares current information, meeting minutes, documentation, and guidance information;
- There is a FERN Methods Repository on eLEXNET; and
- Participants can review information on samples that have been submitted by eLEXNET's participating laboratories.

FERN Surveillance Assignments and FERN related data can be captured and reported independently. In addition to FERN, several other laboratory networks are currently in use. These include:

- Laboratory Response Network;
- National Animal Health Laboratory Network;
- National Plant Diagnostic Network; and
- e-Laboratory Response Network.

Another of FERN's goals is to facilitate integration of FERN with other networks.

The result is a Memorandum of Agreement (MOA) establishing the Integrated Consortium of Laboratory Networks (ICLN). The Consortium's vision is, "A U.S. homeland security infrastructure with a coordinated and operational system of laboratory networks that provide timely, high quality, and interpretable results for early detection and effective consequence management of acts of terrorism and other events requiring an integrated laboratory response." The purpose of the MOA is to define Federal relationships by establishing a leadership structure while concurrently respecting existing network policies and procedures. The Department of Homeland Security, at the Assistant Secretary Level, chairs the Consortium and there are 10 Federal Agency signatories:

Department of Agriculture
Department of Commerce
Department of Defense
Department of Energy
Department of Homeland Security
Department of the Interior
Department of Justice
Department of State
Environmental Protection Agency
Department of Health & Human Services

The central working body of the Consortium is the Network Coordinating Group. There are six subgroups:

- Scenarios/agent prioritization;
- Methods;
- Proficiency testing;
- Training;
- Accreditation/quality control; and
- IT/data exchange/communications.

These subgroups make recommendations to the Network Coordinating Group, which in turn, presents coordinated positions to the Joint Leadership Council. It has proven challenging to get the six subgroups to move in the same direction, but significant progress has been accomplished across the spectrum. Another positive effect is getting the right people together to work out the issues. The current status of the national food defense surveillance laboratory perspective consists of several observations and conclusions. It is impractical, but not impossible, to do comprehensive surveillance. It is possible to do a limited, focused program. Comprehensive surveillance is beneficial for the laboratories and it allows labs to maintain competence and capability. It helps maintain expertise and assists in providing cross training. Finally, it keeps supply and reagent chains operational. The Consortium is working actively to establish the proper integrated surveillance program. It is not there yet, but significant progress is being made.

Following Dr. McCaskey's remarks, Dr. Isabel Walls, Senior Scientist, Office of Food Defense and Emergency Response (OFDER), FSIS, USDA presented a Committee paper entitled, Food Defense Vulnerability Assessment Overview. The OFDER was established in 2002. Its mission is to prevent, prepare for and coordinate a response to an intentional attack on the food supply and large scale emergencies. OFDER's goals for food defense are:

- Raise awareness of the threat that terrorists pose to our food supply;
- Provide outreach and training;
- Conduct vulnerability assessments;
- Develop countermeasures;
- Conduct surveillance;
- Manage food defense and food safety emergencies; and
- Facilitate FSIS' continuity of operations during a crisis.

It is important to note that in its efforts to achieve these food defense goals, FSIS is working closely with its industry members, including small and very small facilities.

There are three main objectives to the presentation. First is to raise awareness about food defense issues. At the end of this presentation, you should understand how vulnerable the food supply is, the types of situations where and how food can be deliberately contaminated, and the impact that will have on the U.S. The second objective is to discuss countermeasures. Countermeasures may be defined as strategies to prevent, delay or detect the effects of an incident that threatens meat, poultry and egg products. Third is to discuss research needs. Some hypothetical scenarios will be presented along with suggested keywords that can help in collecting information useful for threat analysis.

Before proceeding, a distinction between food defense and food safety is necessary. Food defense is the protection of food products from intentional adulteration by biological, chemical, physical or radiological agents. Food safety is the protection of food products from unintentional contamination by agents. Why are we concerned about food defense? There has been no specific targeting information indicating an attack on the food supply is imminent. However, intelligence reports indicate that terrorists have discussed food sector attacks. Manuals for intentional contamination of food are widely available. Also significant is the fact that food supply is soft target. Some people might ask why the food supply would be considered a potential terrorist target. There are several reasons. The food supply has a great deal of economic, health, societal, psychological, and political significance. Deliberate contamination of the food supply could have significant public health consequences. It could result in widespread public fear. It could have devastating economic impacts that extend beyond the food industry. In addition, such an attack could also result in the loss of public confidence in the safety of food and effectiveness of government in protecting the Nation's food supply.

Some older Center for Disease Control and Prevention (CDC) data gives some insight into the public health effect of unintentional food contamination. Greater than 76 million illnesses, 325,000 hospitalizations, and 5,000 deaths occur each year from inadvertent contamination of the U.S. food supply. Unintentional foodborne outbreaks provide insight into the points in food production where intentional adulteration could have catastrophic consequences and the magnitude of public health impact of a carefully planned, intentional attack on the food supply. CDC's data is in the process of being updated, but similar conclusions will likely be drawn from the new data. An example of an unintentional contamination event occurred in March/April 1985: an estimated 200,000 illnesses (16,000 culture confirmed) and up to 17 deaths in a six state area resulted from pasteurized milk contaminated with *Salmonella typhimurium.* The milk was produced at a single dairy plant in Midwest and the most likely cause was post-pasteurization contamination from improper piping. To date, the largest intentional food contamination event occurred in 1984 in Oregon when cult members added *Salmonella* bacteria to restaurant salad bars. Their intent was to affect the outcome of a local election. The result was 751 illnesses reported and 45 individuals required hospitalization. There were no fatalities. Intentional contamination events do not have to be perpetrated by terrorists. In January 2003 a disgruntled Michigan supermarket employee intentionally contaminated 200 pounds of ground beef with a nicotine-based pesticide. The result was that 92 individuals reported becoming ill after consuming the ground beef. Another consideration is that even the threat of tampering with a food product could pose serious problems for public health and the international economy. For example in 1989, the threat of introducing cyanide into Chilean grapes imported into the U.S. cost over $200 million in lost revenue.

Prevention strategies to lessen the likelihood of intentional contamination have been developed. These are:

- Perform a screening assessment to identify and prioritize product-agent-process combinations that warrant more detailed analysis.
- Perform a farm-to-table CARVER + Shock vulnerability assessment on prioritized foods.

- Industry then develops a food defense plan based on results of assessment.
- Implement and test the plan. Review and revise it regularly. Management should inform and involve staff in food defense, and promote food defense awareness on a regular basis.

Why are vulnerability assessments valuable? Vulnerability assessments help to prepare for, prevent, and mitigate the effects of an attack on the food supply in several ways. First, they can be used to identify products most at risk for adulteration. Second, they can be used to identify likely threat agents for attacking the food supply. Third, they can identify potential sites of contamination within a food processing system that are the most attractive targets. And finally, they can facilitate the development of countermeasures to minimize or reduce risks. In doing so, vulnerability assessment is a way to focus limited resources toward the foods and agents of greatest concern. The CARVER + Shock model, developed by the Department of Defense for vulnerability assessments in military operations, is the tool currently being used by Federal agencies for food defense vulnerability assessments. This model prompts the user to systematically consider seven factors that affect the attractiveness of a target. Those factors are:

- Criticality - public health and economic impacts to achieve the attacker's intent;
- Accessibility - physical access to the target;
- Recuperability **-** ability of the system to recover from the attack;
- Vulnerability - ease of accomplishing the attack;
- Effect **-** amount of direct loss from the attack;
- Recognizability - ease of identifying the target; and
- Shock - the combined physical, public health, psychological, and economic impact of an attack.

The model has been adapted for use in the food industry as an offensive targeting prioritization tool. Modifications of the model are being considered so that it can be more effectively applied to food system vulnerability assessments.

FSIS has assessed and is assessing vulnerabilities both independently and in conjunction with FDA, USDA-Agricultural Marketing Service (AMS), Food and Nutrition Service (FNS) and the Department of Defense (DOD) depending on the product or food chain. Some of these assessments are:

- National School Lunch Program;
- Meals, Ready-to-Eat;
- Ground beef, deli meats, hot dogs, liquid eggs;
- Legally imported food;
- Illegal imports; and
- Ricin in FSIS-regulated food.

A lesson learned from these vulnerability assessments is that there are four common characteristics of foods that are at higher risk for contamination. These are:

- Production in large batches – because a large number of individuals may consume contaminated product. Larger numbers of consumers equal potentially higher illnesses and deaths. There are more casualties expected from contamination of a 5,000 gal. commercial kettle than from a 5 gal. food service pot of spaghetti sauce.

- Uniform mixing – Adding agents before or during mixing steps results in contamination of all of the servings in a batch, improving the efficiency of the attack. Uniform mixing is relatively easy in non-viscous liquids, such as fluid milk and liquid eggs. The equipment used to process these products is designed to ensure thorough mixing.
- Short shelf life – Short shelf life or rapid turnaround at retail and rapid consumption also tend to increase risk. Individuals may consume perishable products before public health officials are able to identify the cause and take action to prevent further illness. For shelf-stable products, reaction to sentinel cases can prevent casualties through recalls.
- Ease of access –Intentional adulteration requires access to the product or raw materials. The more accessible a site, the more likely it will be a target. The food and agriculture sectors encompass a wide range of access conditions, from unfenced farmlands to relatively secure infant formula manufacturers.

Some additional factors that may also affect the risk of intentional contamination are:

- Some foods are consumed in large quantities**,** so it may be easy to ingest a lethal dose in a single serving.
- Foods vary in their ability to disguise a contaminant; some foods exhibit a strong flavor (e.g., spaghetti sauce), odor (e.g., fish sauce), texture (e.g., ground meat), intense color (e.g., soy sauce), or opaqueness (e.g., chocolate syrup). These characteristics may conceal the presence of a contaminant (versus, for example, bottled water).
- The absence of tamper evident packaging may elevate the risk that a food is targeted.
- Emotional Aspects - Certain foods present a highly desirable target because children (e.g., infant formula) typically consume them, and thus public reaction to harm would likely be intense. Similarly, products that have a marked association with the American culture may be highly desirable because of their iconic association. An example could be hot dogs.
- Certain foods may also be at risk based upon their country of origin. Products produced in a country with a pattern of past incidents of terrorist activity, tampering, or counterfeiting may be at greater risk for intentional contamination.
- Ready-to-eat foods may be at greater risk because of the decreased opportunity for contaminant dilution via consumer preparation such as cooking or washing.

Several countermeasures, identified during vulnerability assessments, have been and are being developed. Four prevention strategies are categorized as surveillance, outreach/training, securing the food chain, and changing processing technologies. Surveillance can be used to help develop threat information. Over 6,000 inspectors assess food defense measures in facilities, discuss potential vulnerabilities with facility management, and report results in a database. Food defense tasks are dependent upon Department of Homeland Security Threat Conditions. The data are used to identify potential countermeasures and outreach needs. Also, the inspection force is determining the prevalence of facilities with written food defense plans. FSIS is developing a consumer complaints monitoring system to provide an early warning system for illnesses that might be associated with a threat agent. It integrates state and local consumer complaint data into a national database permitting early detection and response to potential hazards in our nation's food supply. In addition, FSIS has expanded its laboratory analysis and testing programs to include surveillance for threat agents in foods. FSIS laboratories analyzed about 56,000 samples for 13 biological and chemical threat agents since March 3, 2003. Currently, all FSIS food safety samples are screened for presence of radioisotopes. The FSIS Import Surveillance System is a cooperative program between FSIS and Customs and Border Protection (CBP) through CBP's National Targeting Center (NTC). It targets incoming shipments of product that might be at risk of having been intentionally contaminated using criteria developed by FSIS.

Concurrent with surveillance programs, FSIS is actively pursuing outreach and training initiatives. FSIS is providing training for federal, state and local officials, as well as industry, in assessing vulnerabilities and developing countermeasures to protect the food supply. In addition, FSIS has developed guidance documents and model food defense plans that pertain to food processing environments, transportation systems, and storage or warehousing companies. These are being used to raise awareness and educate government and industry officials. Four large Food Defense Exercises have been conducted so far in 2006. Eleven more are scheduled over the next several months. Securing the food chain is the third prevention strategy. The key issues along the food chain are physical security, e.g., monitoring the premises for suspicious activity, or locking chemical storage facilities; personnel security, e.g., screening employees and use of name badges; and operational security, e.g., monitoring production to prevent sabotage or use of tamper-evident packaging. Fourth, changes to processing technologies are needed to protect the food supply. Changes could include raising pasteurization temperatures to destroy threat agents, or re-designing equipment for improved security, e.g., increase use of closed systems.

Two detection countermeasure strategies are laboratory detection methods and government inspection activities. FSIS has developed new detection methods and confirmatory tests for threat agents. The Food Emergency Response Network has already been discussed. As indicated above, government inspectors and investigators are looking for vulnerabilities within meat, poultry, and egg processing plants; at distributors, warehouses, and retail establishments; and at border crossings and ports of entry.

Lastly, research needs have been developed as a result of completed vulnerability assessments. Additional research is need in all of the following:

- Prioritized threat agents in food matrices identified by FSIS vulnerability assessments;
- Impact of food processes (e.g., cooking, freezing, and acidification) on stability/ survivability;
- Improved lab detection methods;
- Equipment re-design (e.g., development of closed systems);
- Decontamination technologies (e.g., effect of sanitizers);
- Oral Infectious Dose/Toxic Dose Studies;
- Anti-tampering technologies; and
- Organoleptic changes in foods in response to addition of threat agents.

In conclusion, we need to prevent, detect, and respond to terrorist acts against the nation's food supply. We need to be aware of threats. We need to act to reduce vulnerability of food supply. Potential contaminants must be recognized. We must understand characteristics and tactics of aggressors and use preventive measures to thwart their intent. We must strengthen communication lines and follow applicable federal directives.

Dr. Walls' overview of vulnerability assessments set the stage for the workshop she then conducted, applying the CARVER + Shock Model to a specific food system, ground beef production. The CARVER + Shock assessment methodology systematically takes you through a five step process in which each of the seven attributes; criticality, accessibility, recuperability, vulnerability, effect, recognizability, and shock; are considered, using a measurable scale with objective criteria for each attribute. The method breaks a food system into its smallest pieces (nodes) in the farm to table continuum. As you work through the "Criticality Worksheet" and "CARVER + Shock summary worksheet," each node is given a score. The score helps to identify "critical nodes" in food systems that are the most likely targets for terrorist attack after the systematic analysis is applied to each node. This, in turn, leads to the identification of countermeasures to reduce the risk at those nodes.

The method has been used previously to train groups from the Federal Bureau of Investigation (FBI), Department of Homeland Security (DHS), USDA, industry, and international activities. When applied properly, the method leads you to think about the type of aggressors who might want to attack a food system, the various methods by which those attacks might be carried out, and the potential agents to be used. Successful adulteration of products requires an aggressor to have:

- access to sufficient contaminant;
- access to product for sufficient time to allow contamination;
- knowledge of product, process, and pathway to consumer; and
- desire to do harm.

Similarly, a successful aggressor must be able to commit crime without discovery and prevent detection of the adulterated product. Aggressors can be from a wide variety of backgrounds. They can be:

- Disgruntled insiders - motivated by own emotions or self interests and they may have legitimate access to product;
- Criminals - looking for high value targets, low risk of detection;
- Protesters- politically or issue-oriented, looking for publicity;
- Subversives- highly skilled, capable of detailed planning with objectives of destruction and death; and
- Terrorists- politically or ideologically oriented with goals of death, destruction or publicity.

Various tactics can be used to carry out attacks. Those are:

- Insider compromise – take advantage of legitimate access;
- Exterior attack – contaminate raw material;
- Forced entry – need to enter and exit without detection; could use distraction (vandalism, theft); and
- Covert entry – use deception or stealth to enter.

For the remainder of the presentation, Dr. Walls led the group through the USDA-FSIS document entitled, "*CARVER + SHOCK PRIMER,* An Overview of the CARVER plus Shock Method for Food Sector Vulnerability Assessments*.*" It explains the CARVER + Shock process in detail and presents the metrics used for each attribute analysis. This paper is included in its entirety in these proceedings.

After completion of the workshop, Dr. Lafontaine added summary comments of the presentations and the workshop. A short business meeting was then conducted.

During the business session a comment was made from the floor that the American Association of Veterinary Laboratory Diagnosticians (AAVLD) also has a Food Safety Committee. The feasibility of combining the AAVLD and the United States Animal Health Association (USAHA) Committees on Food Safety was discussed. The Chair stated that the issue would be researched and he would report back to the Committee.

The Chair briefly explained the Resolution process. He asked that any resolutions desired by the Committee members be developed prior to next year's meeting. A discussion ensued regarding the need to develop a resolution to support increased funding for food defense research for specifically identified research needs. It was generally agreed that this would be an appropriate resolution for the Committee to develop for consideration at the next Annual Meeting.

CARVER PLUS SHOCK METHOD FOR FOOD SECTOR VULNERABILITY ASSESSMENTS

Dr. Isabel Walls
Food Safety and Inspection Services
United States Department of Agriculture

Overview

The CARVER plus Shock method is an offensive targeting prioritization tool that has been adapted for use in the food sector. This tool can be used to assess the vulnerabilities within a system or infrastructure to an attack. It allows you to think like an attacker by identifying the most attractive targets for attack. By conducting such a vulnerability assessment and determining the most vulnerable points in your infrastructure, you can then focus your resources on protecting your most vulnerable points.

CARVER is an acronym for the following six attributes (discussed in further detail later) used to evaluate the attractiveness of a target for attack:

- **C**riticality - measure of public health and economic impacts of an attack
- **A**ccessibility – ability to physically access and egress from target
- **R**ecuperability – ability of system to recover from an attack
- **V**ulnerability – ease of accomplishing attack
- **E**ffect – amount of direct loss from an attack as measured by loss in production
- **R**ecognizability – ease of identifying target

In addition, the modified CARVER tool evaluates a seventh attribute, the combined health, economic, and psychological impacts of an attack, or the **SHOCK** attributes of a target.

The attractiveness of a target can then be ranked on a scale from one to 10 on the basis of scales that have been developed for each of the seven attributes. Conditions that are associated with lower attractiveness (or lower vulnerability) are assigned lower values (e.g., 1 or 2), whereas, conditions associated with higher attractiveness as a target (or higher vulnerability) are assigned higher values (e.g., 9 or 10). Evaluating or scoring the various elements of the food sector infrastructure of interest for each of the CARVER-Shock attributes can help identify where within that infrastructure an attack is most likely to occur. Federal agencies, such as the Food Safety and Inspection Service (FSIS) and the Food and Drug Administration (FDA), have used this method to evaluate the potential vulnerabilities of farm-to-table supply chains of various food commodities. The method can also be used to assess the potential vulnerabilities of individual facilities or processes.

Steps for Conducting a CARVER + Shock Analysis

Step 1 – Establishing Parameters

Before any scoring can begin, the scenarios and assumptions you wish to use in the analysis must be established in order to guide all further steps. That is, you need to answer the question of what you are trying to protect and what you are trying to protect it from. Those parameters include:

- what food supply chain you are going to assess (e.g., hot dog production versus deli meat production versus chicken nugget production, overall assessment based on generic process from farm to table versus post-slaughter processing in a specific facility, etc.);
- what is the endpoint of concern (e.g., foodborne illness and death versus economic impacts, etc.);
- what type of attacker and attack you are trying to protect against. Attackers could range from disgruntled employees to international terrorist organizations. Those different attackers have different capabilities and different goals. For example, a major assumption used by FSIS and FDA in their vulnerability assessments is that one of the goals of terrorist organizations is to cause mass mortality by adding acutely toxic agents to food products. That assumption has a major impact on the scoring of the various parts of the supply chain and the scales for the attributes (see below) have been developed with that in mind;
- what agent(s) might be used. The agent used in your scenario will impact the outcome of the assessment. Potential agents include biological, chemical or radiological agents. Different agents have different properties—potency, heat stability, pH stability, half-life, etc.—that will determine the impact of an intentional contamination incident.

Step 2 – Assembling Experts

A team of subject matter experts should be compiled to conduct the assessment. The team should consist, at a minimum, of experts in food production (specifically for the food process being evaluated), food science, toxicology, epidemiology, microbiology, medicine (human and veterinarian), radiology, and risk assessment. The team will apply the CARVER-Shock method to each element of food system infrastructure and come to a consensus on the value from one to 10 for each attribute, using the scenario and assumptions established in Step 1.

Step 3 – Detailing Food Supply Chain

The analysis begins by developing a description of the system under evaluation.

A graphical representation (flow chart) of the system and its subsystem, complexes, components and nodes (its smaller structural parts) should be developed to facilitate this process. For example, if you are evaluating hot dog production, the food system is hot-dog production, which can be broken down into subsystems (production of live animals subsystem, slaughter/processing subsystem, distribution subsystem). Those subsystems can be further broken down into complexes (e.g., slaughterhouse facility and processing facility) Those can be broken down into components and would include the raw materials receiving area, processing area, storage area, shipping area, etc.), and to the smallest possible nodes (e.g., individual pieces of equipment).

Step 4 – Assigning Scores
Once the infrastructure has been broken down into its smallest parts (i.e., components and nodes), these can be ranked or scored for each of the seven CARVER-Shock attributes to calculate an overall score for that node. The nodes with the higher overall scores are those that are potentially the most vulnerable nodes (i.e., most attractive targets for an attacker). The rationale for a particular consensus score should be captured.

Step 5 – Applying What Has Been Learned
Once the critical nodes of the system have been identified, a plan should be developed to put countermeasures in place that minimize the attractiveness of the nodes as targets. Countermeasures might include enhancements to physical security, personnel security, and operational security that help to minimize aggressor access to the product or process.

Description of Attributes and Scales

The following section defines the attributes used by FDA and USDA to conduct their vulnerability assessments and provides the scales used by the agencies for scoring each attribute. These scales were developed with the mindset that mass mortality is a goal of terrorist organizations. It is important to remember, however, that any intentional food contamination could also have major psychological and economic impacts on the affected industry. Tables to assist in calculating the public health impacts and the overall CARVER+Shock scores can be found in Appendix A and B, respectively.

Criticality: A target is critical when introduction of threat agents into food at this location would have significant health or economic impact. Example metrics are:

Criticality Criteria	**Scale**
Loss of over 10,000 lives OR loss of more than $100 billion	9 – 10
Loss of life is between 1,000 – 10,000 OR loss between $10 billion and $100 billion	7 – 8
Loss of life between 100 and 1000 OR loss between $1 and $10 billion	5 – 6
Loss of life less than 100 OR loss less than $1 billion	3 – 4
No loss of life OR loss less than $100 million	1 – 2

Accessibility: A target is accessible when an attacker can reach the target to conduct the attack and egress the target undetected. Accessibility is the openness of the target to the threat. This measure is independent of the probability of successful introduction of threat agents. Example metrics are:

Accessibility Criteria	**Scale**
Easily Accessible (e.g., target is outside building and no perimeter fence).	9 – 10

Limited physical or human barriers or observation. Attacker has relatively unlimited access to the target. Attack can be carried out using medium or large volumes of contaminant without undue concern of detection. Multiple sources of information concerning the facility and the target are easily available.	
Accessible (e.g., target is inside building, but in unsecured part of facility). Human observation and physical barriers limited. Attacker has access to the target for an hour or less. Attack can be carried out with moderate to large volumes of contaminant, but requires the use of stealth. Only limited specific information is available on the facility and the target.	7 – 8
Partially Accessible (e.g. inside building, but in a relatively unsecured, but busy, part of facility). Under constant possible human observation. Some physical barriers may be present. Contaminant must be disguised, and time limitations are significant. Only general, non-specific information is available on the facility and the target.	5 – 6
Hardly Accessible (e.g., inside building in a secured part of facility). Human observation and physical barriers with an established means of detection. Access generally restricted to operators or authorized persons. Contaminant must be disguised and time limitations are extreme. Limited general information available on the facility and the target.	3 – 4
Not Accessible. Physical barriers, alarms, and human observation. Defined means of intervention in place. Attacker can access target for less than 5 minutes with all equipment carried in pockets. No useful publicly available information concerning the target.	1 – 2

Recuperability: A target's recuperability is measured in the time it will take for a food system to recover productivity. The effect of a possible decrease in demand is considered in this criterion. Example metrics are:

Recuperability Criteria	**Scale**
> 1 year	9 – 10
6 months to 1 year	7 – 8
3-6 months	5 – 6
1-3 months	3 – 4
< 1 month	1 – 2

Vulnerability: A measure of the ease with which threat agents can be introduced in quantities sufficient to achieve the attacker's purpose once the target has been reached. Vulnerability is determined both by the characteristics of the target (e.g., ease of introducing agents, ability to uniformly mix agents into target) and the characteristics of the surrounding environment (ability to work unobserved, time available for introduction of agents). It is also important to consider what interventions are already in place that might thwart an attack. Example metrics are:

Vulnerability Criteria	**Scale**
Target characteristics allow for easy introduction of sufficient agents to achieve aim.	9 – 10

Target characteristics almost always allow for introduction of sufficient agents to achieve aim.	7 – 8
Target characteristics allow 30 to 60% probability that sufficient agents can be added to achieve aim.	5 – 6
Target characteristics allow moderate probability (10 to 30 %) that sufficient agents can be added to achieve aim.	3 – 4
Target characteristics allow low probability (less than 10%) sufficient agents can be added to achieve aim.	1 – 2

<u>Effect:</u> Effect is a measure of the percentage of system productivity damaged by an attack at a single facility. Thus, effect is inversely related to the total number of facilities producing the same product. Example metrics are:

Effect Criteria	**Scale**
Greater than 50% of the system's production impacted	9 – 10
25-50% of the system's production impacted	7 – 8
10-25% of the system's production impacted	5 – 6
1-10% of the system's production impacted	3 – 4
Less than 1% of system's production impacted	1 – 2

<u>Recognizability:</u> A target's recognizability is the degree to which it can be identified by an attacker without confusion with other targets or components. Example metrics are:

Recognizability Criteria	**Scale**
The target is clearly recognizable and requires little or no training for recognition	9 – 10
The target is easily recognizable and requires only a small amount of training for recognition	7 – 8
The target is difficult to recognize or might be confused with other targets or target components and requires some training for recognition	5 – 6
The target is difficult to recognize. It is easily confused with other targets or components and requires extensive training for recognition	3 – 4
The target cannot be recognized under any conditions, except by experts.	1 – 2

<u>Shock:</u> Shock is the final attribute considered in the methodology. Shock is the combined measure of the health, psychological, and collateral national economic impacts of a successful attack on the target system. Shock is considered on a national level. The psychological impact will be increased if there are a large number of deaths or the target has historical, cultural, religious or other symbolic significance. Mass casualties are not required to achieve widespread economic loss or psychological damage. Collateral economic damage includes such items as decreased national economic activity, increased unemployment in collateral industries, etc. Psychological impact will be increased if victims are members of sensitive subpopulations such as children or the elderly.

The metrics for this criterion are:

Shock	**Scale**

Target has major historical, cultural, religious, or other symbolic importance. Loss of over 10,000 lives. Major impact on sensitive subpopulations, e.g., children or elderly. National economic impact more than $100 billion.	9-10
Target has high historical, cultural, religious, or other symbolic importance. Loss of between 1,000 and 10,000 lives. Significant impact on sensitive subpopulations, e.g., children or elderly. National economic impact between $10 and $100 billion.	7-8
Target has moderate historical, cultural, religious, or other symbolic importance. Loss of life between 100 and 1,000. Moderate impact on sensitive subpopulations, e.g., children or elderly. National economic impact between $1 and $10 billion.	5-6
Target has little historical, cultural, religious, or other symbolic importance. Loss of life less than 100. Small impact on sensitive subpopulations, e.g., children or elderly. National economic impact between $100 million and $1 billion.	3-4
Target has no historical, cultural, religious, or other symbolic importance. Loss of life less than 10. No impact on sensitive subpopulations, e.g., children or elderly. National economic impact less than $100 million.	1-2

By definition, terrorists attempt to achieve strong emotional responses from their target audience. Aspects of targets that terrorists view as increasing a target's shock value are symbolism (e.g., the Pentagon), large number of casualties, sensitive nature of facilities (e.g., nuclear facilities), and the ability to strike at core values and primal emotions (e.g., targeting children).

Calculation of Final Values and Interpretation

Once the ranking on each of the attribute scales has been calculated for a given node within the food supply system, the ranking on all of the scales can then be totaled to give an overall value for that node. This should be repeated for each node within a food supply system. The overall values for all the nodes can then be compared to rank the vulnerability of the different nodes relative to each other. The summary table provided in Appendix B can assist in summarizing the rankings. The nodes with the highest total rating have the highest potential vulnerability and should be the focus of countermeasure efforts

APPENDIX A

This appendix provides a table that can be used to calculate the potential number of deaths and illnesses resulting from addition of a particular adulterant at a particular point in a given food production process. Details of the batch size to which the adulterant is added, the number of servings that will be sold and eaten from that batch, and the characteristics of the adulterant (including its lethality) must be known to use this worksheet. The numbers generated in this worksheet will help determine where on the criticality scale a given attack will fall.

Table A-1: WORKSHEET FOR CALCULATING CRITICALITY

Product:

Entry Point	Agent	**A** Batch Size	**B** Serving Size	**C** Servings per Batch A/B	**D** Dose Required per Serving	**E** Total Amount Required per Batch C x D	**F** Distribution Unit	**G** Units Produced A/F

H % of Units Sold Before Warning	**I** Units for Potential Consumption H/100 x G	**J** Consumers per Distribution Unit	**K** Number of Potential Exposures I x J	**L** % of Units Consumed Before Warning	**M** Number of Exposures K x L/100	**N** Morbidity/ Mortality Rate	**O** Number of Illnesses/ Deaths M x N

APPENDIX B

This appendix provides a table that can be used to total the scores across the CARVER+Shock attributes for each node. The totals can then be compared across the various nodes to determine which nodes are critical. The nodes with the highest scored are the ‘critical nodes’ and should be the focus for beginning to implement countermeasures.

Table B-1: Summary sheet for totally scores for nodes across CARVER+Shock attributes.

FOOD: ___________________________________

TARGET (Nodes)	CRITICALITY	ACCESSIBILITY	RECUPERABILITY	VULNERABILITY	EFFECT	RECOGNIZABILITY	SHOCK	OVERALL SCORE

APPENDIX C

This appendix provides a table that can be used to summarize the CARVER+Shock score on each attributes for given node. The table includes a place for a brief narrative of the rational or justification for giving a node a particular score, allowing the thoughts that went into the scoring to be captured.

Table C-1: Summary sheet for analysis of individual nodes, including the justification for the score given.

Product:		
Target Complex:		
Target Node:		
FACTOR	**SCORE**	**JUSTIFICATION**
CRITICALITY		
ACCESSIBILITY		
RECUPERABILITY		
VULNERABILITY		
EFFECT		
RECOGNIZABILITY		
SHOCK		
OVERALL		
RANK		