Vulnerability Assessments of Food Systems

Final Summary Report

June 2009 – February 2012

Table of Contents

I. Executive Summary

Following the attacks of September 11, 2001, the U.S. government set out to better understand and protect critical infrastructures. The food and agriculture sector was identified as one of 17 such infrastructures. A military offensive targeting tool known as CARVER was adapted, based on the principles of risk assessment, for use in assessing the food and agriculture sector. By conducting a CARVER+Shock assessment of a food production facility or process, the user can determine the most vulnerable points in the infrastructure, and focus resources on protecting the most susceptible points in the system.

From 2005 to 2008, under the Strategic Partnership Program Agroterrorism (SPPA) initiative, the U.S. Food and Drug Administration (FDA), along with the United States Department of Agriculture (USDA), Federal Bureau of Investigation (FBI), and Department of Homeland Security (DHS), conducted CARVER+Shock threat assessments on 36 products, processes, or commodities in the food and agriculture sector. In keeping with the requirements of Homeland Security Presidential Directive 9 (HSPD 9), *Defense of U.S. Agriculture and Food*, the FDA revisited assessments conducted during 2005 to 2008. In addition, the FDA continued this assessment process with FDA regulated food products or processes not previously assessed. During this task, 18 products were assessed that had not been previously assessed and 16 previously assessed products underwent an update assessment.

Assessments were conducted on a voluntary basis between one or more industry representatives for a particular product or commodity, trade association(s), the FDA, and Battelle assessment facilitators. Together, they conducted a vulnerability assessment of that industry's production process using the CARVER+Shock vulnerability assessment method.

As a result of each assessment, participants identified individual nodes, or process points that were of highest concern, and protective measures and mitigation steps that may reduce the vulnerability of these nodes. Discussions of mitigation steps and good security practices were general in nature, typically focusing on physical security improvements, employment practices, or process changes for food processing facilities.

Participants also identified research gaps and needs during each assessment. The research needs most often identified during each assessment were related to the need for enhanced scientific capabilities to detect various potential agents to provide an early awareness of an event. Early detection capabilities would also permit a rapid response thereby reducing the impact of an event. Other commonly identified gaps and needs included developing a better understanding of threat-agent characteristics and improved testing methodologies.

User testing for the CARVER+Shock Vulnerability Assessment Software tool was performed. The software was operated side-by-side with the manual process at assessments of new products to validate the functionality, usability, and results generated by the software. Based on user testing, a comprehensive report detailing suggested improvements, functionality upgrades, and interface modifications to enhance the software's ease of use and operation for widespread use by the food industry was developed.

At all assessments wherein the manual and software based CARVER + Shock tool was utilized, both methods produced useful distinctions between nodes of higher and lower concern for each food process assessed. The manual version of CARVER + Shock relies on a subjective scoring method and requires the use of a moderator. These tabletop assessments typically take a full day or more to complete depending on the assessment group and moderator. The software version of CARVER + Shock relies on automated scoring calculated based on user responses to a software-generated questionnaire. A single user can complete the software version in three to five hours with access to information about the process or product being assessed. The consistent results between both manual and software versions of CARVER + Shock demonstrate that the software can be a viable alternative to conducting manual, tabletop, CARVER + Shock assessments.

II. Background

Following the attacks of September 11, 2001, the U.S. government set out to better understand and protect critical infrastructures. The food and agriculture sector was identified as one of 17 such infrastructures. A military offensive targeting tool known as CARVER was adapted, based on the principles of risk assessment, for use in assessing the food and agriculture sector. CARVER is an acronym for the following six attributes used to evaluate the attractiveness of a target for attack:

- Criticality - measure of public health and economic impacts of an attack
- Accessibility - ability to physically access and egress from target
- Recuperability - ability of system to recover from an attack
- Vulnerability - ease of accomplishing attack
- Effect - amount of direct loss from an attack as measured by loss in production
- Recognizability - ease of identifying target.

A seventh attribute, "Shock", was added to the original six attributes to assess the combined health, economic and psychological impacts of an attack within the food industry. CARVER+Shock is a tool that can be used to assess the vulnerabilities within a system or infrastructure prior to an attack. It allows the user to think like an attacker to identify the most attractive targets for an attack. By conducting a CARVER+Shock assessment of a food production facility or process, the user can determine the most

vulnerable points in the infrastructure, and focus resources on protecting the most susceptible points in the system.

Homeland Security Presidential Directive 9 (HSPD-9), *Defense of US Agriculture and Food*, requires the US Food & Drug Administration (FDA) to conduct vulnerability assessments of the food sector and to update these assessments every two years. The FDA's Center for Food Safety and Applied Nutrition (CFSAN) Office of Food Defense, Communication and Emergency Response (OFDCER) is responsible for coordinating the Agency's food defense efforts. The OFDCER identified the need to conduct vulnerability assessments of key areas within the food system and to identify the means for prevention and protection of food systems, including detection, decontamination, disposal and recovery in the event that such a contamination should occur. From 2005 to 2008, under the SPPA Initiative, the FDA, along with the United States Department of Agriculture (USDA), the Federal Bureau of Investigation (FBI), and the Department of Homeland Security (DHS), conducted CARVER+Shock threat assessments on 36 products, processes, or commodities in the food and agriculture sector. In keeping with the requirements of HSPD 9, the FDA revisited assessments conducted during 2005 to 2008. In addition, the FDA continued this assessment process with FDA regulated food products or processes not previously assessed. Tables 1 and 2 list the new and update assessments, respectively, conducted during this program.

Table 1. New Assessments

Product/Process	Assessment Date	Location	Trade Association
Restaurants	10/6/2009	Woodrow Wilson Service Area, NJ Turnpike	New Jersey Restaurant Association
Coffee Shops	10/7/2009	Woodrow Wilson Service Area, NJ Turnpike	New Jersey Restaurant Association
Pet Food	10/16/2009	Washington, DC	Pet Food Institute
Animal By-Products	12/1/2009	Arlington, VA	National Renderers Association
Baked Goods	1/15/2010	Arlington, VA	American Bakers Association
Ice Cream	3/31/2010	Arlington, VA	International Dairy Foods Association
Breaded Fish Products	4/22-23/2010	Arlington, VA	National Fisheries Institute
Ready to Eat Seafood (Surimi)	7/29/2010	Arlington, VA	National Fisheries Institute
Deli-Salads	5/6/2010	Atlanta, GA	NA
Imported Product: Spices	5/18/2010	Arlington, VA	American Spice Trade Association
Chocolate: Candy Bar	10/7/2010	Washington, DC	National Confectioners Association
Milk Transportation	1/18/2011	Arlington, VA	International Dairy Foods Association
Orange Juice Storage and Transportation	1/12/2011	Arlington, VA	Juice Products Association
Canned Tuna	4/28-29/2011	Hat Yai, Thailand	NA
Retail/Distribution	5/3-4/2011	Bangkok, Thailand	NA
Rice	5/6-7/2011	Chiang Mai, Thailand	NA
Canned Fruit	4/25-26/2011	Katsetsart, Thailand	NA
Catering	10/5/2011	Arlington, VA	International Association of Venue Managers

NA = Not Applicable

Table 2. Update Assessments

General Industry	Update Assessment Date	Location	Original Assessment Date(s)	Original Assessment Location(s)
Feed Mill	9/8/2009	Arlington, VA	June 2007	Indiana
Grocery Store	10/14/2009	Arlington, VA	August 2007	Pennsylvania
Retail Milk	10/15/2009	Arlington, VA	January 2007	Texas
Frozen Food	10/22/2009	Arlington, VA	March 2006	Wisconsin/Florida
High Fructose Corn Syrup	10/29/2009	Arlington, VA	September 2007	Alabama
Infant Formula	12/2/2009	Arlington, VA	June 2006	Arizona
Fresh Produce	11/17/2009	Arlington, VA	May 2006	California
Distribution Centers	11/17/2009	Arlington, VA	November 2007	Virginia
Dry Breakfast Cereal	12/1/2009	Arlington, VA	July 2007	Minnesota
Baby Food	12/1/2009	Arlington, VA	February 2006	Michigan
Bottle Water	12/9/2009	Arlington, VA	January 2006	New Jersey
Dairy (Fluid Milk)	3/30/2010	Arlington, VA	July 2006	New York
Apple Juice	5/19/2010	Arlington, VA	April 2006	New Hampshire
Yogurt	6/4/2010	Bloomington, MN	November 2005	Tennessee/Minnesota
Grain	6/11/2010	Arlington, VA	November 2006	Illinois
Concession-Stadium	10/4/2011	Arlington, VA	March 2007	Kansas

III. Method Overview

Thirty-four (34) assessments were conducted under this program. Prior to each assessment, a generic process flow diagram was developed in coordination with the industry to capture the major process nodes. Additionally the assessment group agreed upon a terrorist scenario. This scenario included selection of a terrorist profile and threat agent or threat agent characteristics.

Eighteen (18) new assessments were conducted under this program. Fourteen (14) assessments were held in the United States and four (4) assessments were held in Thailand. At each new U.S. assessment, the full CARVER + Shock manual method was performed by the assessment group using all seven CARVER + Shock factors. Also performed, was a side-by side assessment using the appropriate module of the new CARVER+Shock software tool. The main purpose of the assessments held in Thailand was to train participants in the use of the CARVER + Shock software; therefore, a manual assessment was not performed.

Sixteen (16) update assessments were conducted under this program. To conduct an update assessment, participants were presented with the previous process flow diagram and unclassified notes collected on each node of the previous CARVER+Shock analysis. Participants were not provided with the CARVER+Shock scores generated in the previous assessment because these data are now part of a government classified report. In addition, viewing the original scores could have biased the results of the update assessments.

During an update assessment, participants again used the CARVER+Shock method to evaluate each node in the process, but only the batch size (related to Criticality), Accessibility, and Vulnerability factors were discussed in depth. It was determined that focusing on Criticality, Accessibility, and Vulnerability scores at update assessments was the most effective method to update a previous vulnerability assessment.

Criticality is based primarily on batch size and distribution units produced and should not change dramatically overtime unless there is a change in the production process (thereby reducing or enlarging typical batch sizes). The Criticality score at each process node was based on the possible mortality calculated using the batch size and CARVER+Shock Criticality worksheet. Participants were not asked to assign a Criticality score; scores were instead derived from the CARVER+Shock Criticality table.

The two CARVER+Shock factors that are most likely to change over time, based on process changes or implementation of mitigation strategies, are Accessibility and Vulnerability. In essence, these two factors measure the possibility of an event occurring at each node in the process. Scores for Accessibility and Vulnerability factors were collected during discussions of each process node and combined with the Criticality scores to form the CAV score (Criticality + Accessibility + Vulnerability). The addition of Criticality to the CAV score for each node adjusts for the severity of a possible terrorist attack. Conducting update assessments using this abbreviated CARVER + Shock method allowed participants to complete the manual CARVER +

Shock assessment in one day or less. Additionally, no facility tour was conducted. During the SPPA program, facility tours normally constituted 4-6 hours. Previous assessments conducted under the SPPA program typically took two days or more to complete.

The Recuperability, Effect, Recognizability, and Shock components of the CARVER+Shock method were generally consistent between the original assessment and update assessment. These components are largely outside the control of any facility and are more indicative of the overall industry itself. For example, Effect is a measure of the ability of the overall industry to continue to produce a product after an attack and is unrelated to any process improvement or security upgrades conducted at a specific facility.

At each of the thirty-four (34) assessments, mitigation recommendations and good security practices were proposed and discussed. Mitigation recommendations were typically general in nature due primarily to the fact that multiple companies and facilities/sites were represented at each assessment. Participants also identified research gaps and needs during each assessment

IV. Assessment Results

The intent of assessments conducted on food products was to determine the presence and extent of vulnerabilities at each node in an industry's production and propose possible mitigation strategies or research needs to address these vulnerabilities. Vulnerability assessments focused on a generic company or facility in an effort to capture and assess industry-wide practices. The results of each vulnerability assessment can be categorized into the following key areas:

- Critical process nodes
- Mitigation recommendations
- Research gaps and needs
- Assessment tool observations

<u>Critical process nodes</u>

Assessment participants discussed each node within the generic process flow diagram in efforts to accurately assign CARVER + Shock scores to each node within the production process. Participants discussed each node's characteristics and potential vulnerability to a terrorist attack. By conducting this in-depth analysis, participants were able to determine which nodes were of higher (critical) or lower concern. With this information, participants were able to identify where mitigation measures might be most useful and to prioritize resources to obtain maximum benefit.

Mitigation recommendations

After identifying the nodes of higher concern, participants discussed potential mitigation strategies that may help reduce the likelihood of a successful terrorist attack. Some of the proposed strategies discussed addressed a very basic level of security (i. e. issuing ID badges to all personnel) while other strategies may be very costly and complex (i. e. conduct vulnerability assessments and audits of all ingredient suppliers). In addition, not all of the measures suggested were applicable or practical for all sizes and types of food production facilities represented at the assessment. It is the responsibility of the participant to choose which measures would be appropriate for their facility.

Research gaps and needs

Participants at each assessment also discussed existing research gaps and information needs. This provided all participants (i.e. industry and government) with situational awareness on where gaps lie within a particular industry. More importantly, participants recognized the need to build or foster industry and government relationships.

Assessment tool observations

Prior to the closing of each assessment, Battelle would provide a short demonstration on the Vulnerability Assessment software tool and other food defense resources available to industry. Upon demonstration, participants were asked to provide feedback regarding the CARVER + Shock tool. Overall, participants deemed the CARVER + Shock software a valuable tool that has shown consistency with the manual CARVER + Shock node rankings. The participants deemed the advantages to be: simple distribution by internet download, an easy to use interface, flexibility within the user's schedule to perform a software assessment, and private use by food companies.

Commonalities of Critical Process Nodes

During the course of conducting vulnerability assessments on various food products, it became evident that products could be grouped according to their operational environment. Food products assessed under this task fell into three subgroups based on the nature of the industry; farm, manufacturing, and retail/distribution. Table 3 details the products in each subgroup. Nodes highlighted as critical in each industry experienced common attributes, which caused an increase in the possibility that an adulteration could occur at nodes where specific activities take place.

Table 3. Subgroup Assignments

Farm	Manufacturing	Retail/Distribution
Dairy: Fluid Milk	Animal By-Products	Catering
Feed Mill	Apple Juice	Coffee Shops
Fresh Produce*	Baby Food	Concession - Stadium
Grain	Baked Goods	Deli-Salads
Imported Product: Spices*	Bottle Water	Distribution Centers
Rice*	Breaded Fish Products	Grocery Store
	Canned Tuna	Imported Product: Spices*
	Chocolate: Candy Bar	Milk Transportation
	Dry Breakfast Cereal	Orange Juice Storage and Transportation
	Fresh Produce*	Restaurants
	Frozen Food	Retail/Distribution
	High Fructose Corn Syrup	Retail Milk
	Ice Cream	
	Infant Formula	
	Imported Product: Spices*	
	Pet Food	
	Ready to Eat Seafood: Surimi	
	Rice*	
	Yogurt	

*These products contain characteristics of more than one subsector

Farm

Due to the geographically isolated, spread out, and open nature of farms, most nodes in the farm subsector exhibited a high degree of accessibility. In addition, the level of human observation in many farm activities may be low and an attacker was found to have ample opportunity to adulterate a product with little chance of being seen or discovered. For these reasons, accessibility is difficult to mitigate and generally high for this subgroup. For example, an attacker would likely have extended time to defeat any physical barrier (locks, gates, fences) and tools to enhance visibility (cameras, lights, mirrors) may not be suitable or effective.

Products within the farm subgroup typically dealt with large quantities of raw, unprocessed product. This served to reduce vulnerability in that it would require a large amount of threat agent, which would be difficult to acquire and problematic to administer to the product. In addition, most agricultural products undergo down-line processing prior to final sale to consumers (washing, pasteurization, etc.). For these reasons, vulnerability is generally low in the farm subgroup and the successful adulteration of a farm process is doubtful.

Manufacturing

Products grouped in the manufacturing subgroup often exhibited complex manufacturing processes in enclosed or controlled facilities. An adulteration event would likely be carried out by an authorized insider such as an employee, contractor, or vendor. Common attributes of critical nodes included manufacturing steps where product was mixed and/or where secondary ingredients are being introduced to the product stream. The vulnerability of these nodes centers on the ability of the threat agent to be evenly mixed within the product and affect all the servings in an adulterated batch. It was determined that since the attacker would likely be an insider, effective mitigation strategies may be staffing or employment procedures that emphasis team working environments or buddy systems. Instituting more secure ingredient storage protocols was also highlighted as an important mitigation strategy. Additionally, installing key card or passcode locks, which maintain a record of individuals entering the storage rooms or other sensitive or critical areas, were also specified as potentially important measures. Lastly, the development and maintenance of comprehensive food defense plans and periodic vulnerability assessments would assist manufacturing facilities to be most aware of specific vulnerabilities in their facility and take appropriate action to address them.

Retail/Distribution

Products grouped in the retail/distribution subgroup typically involved the transportation, preparation, and sale of consumer food items. In retail food service environments, critical nodes focus on the preparation of ready to eat food. The workers in these nodes had open and complete access to unpackaged food and could introduce a threat agent during the course of their normal duties without raising much suspicion from either other workers or customers. Storage of open containers of ingredients in low observation areas also raised concerns of assessment participants. For assessments involving transportation and distribution of products, critical nodes typically focused on the long periods of time where a truck driver would have the opportunity to adulterate the product being transported. Assessment participants believed a dedicated attacker would have enough time to successfully adulterate the product in most cases. Mitigation strategies for retail/distribution facilities centered on employee training, employee awareness and conducting background checks of new employees. For employees working in a teamwork environment like a food service venue, concession stand, etc. more secure and strict ingredient handling protocols should be followed to prevent the adulteration of stored or staged ingredients. For distribution assessments, it was found that, to the extent possible, stopovers and other times where the product is not in motion should be eliminated as an effective mitigation strategy to prevent an attack from either the driver or an outside attacker.

Characteristics of Nodes Commonly Identified as Critical

A detailed analysis of CARVER+Shock results from vulnerability assessment meetings conducted under this, and prior efforts, was performed. This analysis was aimed at determining characteristics of nodes, such as commonalities in activities performed, that could be used to identify nodes of potentially higher risk and enable the FDA to provide mitigation guidance and public health regulation focusing on higher risk nodes. This analysis provided information on how best to develop an integrated national framework to reduce the risks at nodes that

commonly were identified as of highest concern. This analysis will help the FDA and industry to more appropriately institute guidance and standards to improve food defense.

Nodes which contained steps where ingredients were mixed or added to a mixture frequently were identified high risk. The potential to add an agent to these types of processing steps and have that agent homogeneously mixed within the food product caused high levels of concern. More stringent mitigation steps may need to be employed at these areas to mitigate the risk at these nodes. Likewise, nodes where liquid ingredients were handled or stored were also commonly identified as high risk. The potential for a threat agent to mix within a liquid ingredient is high, even if no active agitation or mixing is conducted. Liquid storage tanks and other types of handling of liquid ingredients (such as loading or receiving) should be a focus for mitigation measures. Nodes where ingredients are open and accessible also were of higher concern. Ingredient staging or rework areas may provide an attacker with easier access to open ingredients and increase the risk of adulteration. Mitigation measure focused on securing or observing of these areas should be considered.

Commonalities of Mitigation Strategies and Good Security Practices

Over the course of the vulnerability assessments, participants discussed but did not always come to consensus on numerous mitigation strategies, and good security practices. Mitigation recommendations may not, and are not expected to apply universally to all sites, industries, or processes. The application of mitigation recommendations, even very general recommendations, must be based on a comprehensive determination of risk for a specific site. Where feasible, this report generalized the suggested mitigation strategies in order to show potentially broader applicability across industries.

The following mitigation strategies or good security practices were the most common suggestions brought up throughout the Vulnerability Assessments:

Site-Specific Vulnerability Assessments

Conduct site-specific assessments to learn of vulnerabilities unique to that site. This activity can build upon assessments conducted under this effort as well as the SPPA, which were general in nature (focused on product or commodity instead of a specific site). All vulnerability assessments should be periodically revisited and modified as necessary. As new tools become available, industry should experiment to find the most useful tool for their specific product, commodity, or process. The FDA provides free CARVER + Shock assessment software to facilitate site-specific assessments at www.fda.gov/Food/FoodDefense/CARVER/. In 2011, the FDA released the Food Defense Mitigation Strategies Database available for public use at www.accessdata.fda.gov/scripts/fooddefensemitigationstrategies/. The Food Defense Mitigation Strategies Database contains an extensive listing of mitigation measures that may be useful to industry in reducing their food defense vulnerabilities.

Agricultural Security and Food Defense Plans

A common recommendation was to develop or continue to employ dedicated agricultural security or food defense plans, or incorporate these plans into other security procedures or safety plans. Several trade organizations have developed plan templates for their constituents. Industry members can tailor these templates for their own specific processes/facilities or integrate the template with existing security and safety plans. Additionally, the FDA and USDA have developed model food defense plans and guidance: www.fda.gov/Food/FoodDefense/FoodSecurity/ and www.fsis.usda.gov/Food_Defense_&_Emergency_Response/Guidance_Materials/index.asp. In response to the passage of the Food Safety Modernization Act (FSMA) on January 4, 2011, the FDA is currently developing a Food Defense Plan Builder Tool.

Physical Security and Access Control Measures Based On Site-Specific Vulnerability Assessments

Within food processing industries, where possible, deterrents should be imposed or bolstered at highly accessible or vulnerable nodes. This may vary by site and depends on the production process point, but may include cameras, mirrors, door alarms, door logs, additional supervision, restricted access areas, color-coded uniforms or bump caps to designate work area, and limiting personal items on the production floor. This typically would include increasing the visibility of commodities during production and training the industry to be aware of suspicious activity.

Process Design Changes

Process design changes, such as altering the time/temperature of a food-processing step, may be useful to eliminate certain threat-agents. This would require valid, reliable, and scientifically supported information regarding the stability characteristics of all possible threat-agents and any changes must provide sufficient benefit to outweigh any adverse affects on final product quality. Process design changes could also include the physical layout of a production facility (i.e., place critical nodes where employee traffic can be controlled or monitored.)

Penetration Audits

Penetration audits may be a useful tool to assess or validate security procedures. They may also be useful to validate the results of risk assessments. Penetration audits may include having an outsider attempt to access the facility or may be conducted by having a current employee attempt to access another location within the facility to see if they are challenged or their activity is noticed and communicated to superiors.

Agricultural Security and Food Defense Incorporated into Procurement Selection Process

Agricultural security and food defense-related parameters and Standard Operating Procedures (SOPs) could be applied to procurement selection processes and vendor assurance programs. The goal is to assure the security and defense of raw ingredients and other inputs. This action

may also cause a trickle-down effect, where security or defense measures are implemented throughout the agriculture and food industries. For instance, food processors may require that their suppliers have a food defense plan and conduct food defense training. Likewise, the food retailers may require that the food processors have a food defense plan and conduct food defense training.

Raw Materials Inspection

Raw materials inspection procedures should be enhanced to include an emphasis on the detection of tampering or adulteration. This could include SOPs for rejecting opened, damaged, or altered goods, and quarantine and investigation procedures. The use of tamper resistant labels on packaging, and containers should also be encouraged.

Employee Peer Monitoring Programs

Companies should create or further develop employee peer monitoring programs to include an emphasis on agricultural security and food defense activities. Employees can be utilized to increase security for little or no additional cost to a company. Examples would include "badge challenges" - questioning anyone without a visible and valid company identification badge, and "location challenges" - questioning peers that are found in areas not associated with their job function. Another option is to team individuals together (buddy system) at nodes of higher concern. The addition of another individual that verifies and oversees the production process provides dual control during a critical step.

Awareness Training

Awareness training should be implemented to educate employees about the importance of agricultural security and food defense. These activities would need to be tailored to the appropriate audience at each level within an organization. Awareness training could include information regarding the implications of a terrorist attack on the U.S. food supply. To further this goal, the FDA and USDA offer a free web-based course, *An Introduction to Food Security Awareness*, at www.fda.gov/Training/ForStateLocalTribalRegulators/ucm120951.htm. The FDA's ALERT program is intended to raise the awareness of state and local government agency and industry representatives regarding food defense issues and preparedness: www.fda.gov/Food/FoodDefense/Training?ALERT/ucm110258.htm. In addition, Employees FIRST is an FDA initiative that food industry managers can include in their employee food defense training programs. Employees FIRST educates front-line food industry workers from farm to table about the risk of intentional food contamination and the actions they can take to identify and reduce these risks: www.fda.gov/Food/FoodDefense/Training/ucm135038.htm

Trade/Industry Group Best Practices Guidance

Trade industry groups can encourage their members to adopt uniform food defense and agriculture security practices through guidance documents and good security practices developed by industry and trade associations. Many industry groups and trade associations currently have existing components of agricultural security or food defense plans, e.g., emergency contact lists, biosecurity procedures, physical security programs, and recall procedures. Companies should evaluate existing programs to see if they compliment or strengthen security or defense plans. The evaluation findings may justify the financial commitments necessary to make changes within a system or process design. Industry, in general, would prefer for trade organizations to promote the adoption of good security practices.

Commonalities of Identified Research Gaps and Needs

Throughout the Vulnerability Assessments and subsequent discussions, participants identified numerous research gaps and needs. For this report, research gaps and needs that were specific for a single product or commodity have been omitted or generalized so that they are more broadly applicable.

Threat-Agent and Agent/Matrix Research:

Industry participants expressed a need for more specific threat-agent information. Participants identified the following agent or agent/matrix research needs as priorities:

- Could a list of biological and chemical agents be prioritized for their potential risk to specific products or commodities and can this list be provided to industry?
- Is information regarding threat-agent inactivation temperatures, effects of environmental conditions, agent persistence, etc. known and readily available to the food industry? Although it is not feasible to research the stability of all potential threat-agents against all scenarios, general threat-agent stability information in a representative variety of conditions and matrices would be useful.
- What oral dose is toxic or infectious for each threat-agent (biological and chemical)? The minimum toxic or infective dose may be useful during threat assessments.
- What are possible or feasible ranges of terrorist capabilities for threat-agent production or acquisition?

Incident Detection:

Industry participants noted a need for information concerning detection methods currently available for threat-agents (biological and chemical) applicable to each industry. They also asked which detection methods have been validated against products or commodities within their industry. The following questions were asked:

- What detection methods are currently available?
- Are the methods rapid?
- What methods have been validated against particular products, commodities, or processes?
- To whom are the methods/materials available (industry, emergency responders, etc.)?

Incident Magnitude and Response:

Industry participants expressed interest in the development or availability of economic models or studies on the consequences of terrorist attacks on certain food products or agricultural commodities. The interdependencies and supply chain complexities of the food and agriculture industry make the impact of an attack on a single item or commodity difficult to determine. Additionally, the participants sought information regarding the time or method to restore consumer confidence following an attack.

To assist the industry, and State and local government officials responding to a terrorist attack against foods where threat agents are used, the USDA has published the *Guidelines for the Disposal of Intentionally Adulterated Food Products and the Decontamination of Food Processing Facilities*: http://www.fsis.usda.gov/Food_Defense_&_Emergency_Response/Guidance_Materials/index.asp.

Similarly, the U.S. Environmental Protection Agency (EPA) has published the "Federal Food and Agriculture Decontamination and Disposal Roles and Responsibilities": http://www.epa.gov/homelandsecurity/portal/pdf/Final_Food_and_Ag_CONOPS.pdf.

Improved Communication Channels:

There is an abundance of food defense and agriculture security information available from government websites, trade organizations, State and local health or agriculture departments, etc. The participants at several assessments suggested creating a single resource by consolidating these materials. The FBI sponsored "InfraGard" website, which includes a Food and Agriculture Special Interest Group is an information sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members within the government, academia and the private sector. InfraGard is an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States. For more information, please visit: www.infragard.net

Another possible resource is the Critical Sectors Community within the Homeland Security Information Network (HSIN), a web portal for information sharing. For more information about this portal, please visit:
www.dhs.gov/files/programs/gc_1156888108137.shtm

An additional communication issue was the need for simplified and uniform point-of-contact lists and procedures for suspicious incidents. Many participants requested clear protocols for whom to contact (besides local law enforcement) following a suspected contamination or terrorist event. One such resource is FoodSHIELD, a communication tool hosted by the National Center for Food Protection and Defense (NCFPD) – A DHS Center of Excellence: www.foodshield.org. The "one-stop" website provides the emergency contact information sought by the participants.

Commonalities of Identified Threat Indicators

Threat indicators, early warnings of a possible suspicious event or planning for an attack, have been discussed at all assessments. Participants have focused upon very general threat indicators dealing with employee vigilance and awareness. These indicators include:

- Observing employees, visitors, vendors, and contractors in areas where they have no legitimate reason to be.
- Someone expressing an unusual interest in the production process.
- Employee health patterns such as unusual absence or attendance patterns and illnesses related to particular job functions or work areas.
- Delays in deliveries, deviations from delivery schedules or evidence of product tampering.

V. CARVER + Shock Vulnerability Assessment Tool

The CARVER+Shock vulnerability assessment tool and methodology has been used to conduct vulnerability assessments for the FDA since 2005.

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

CRITICALITY CRITERIA	SCALE
Loss of over 10,000 lives OR loss of more than $100 billion. (Note: if looking on a company level, loss of >90 % of the total economic value for which you are concerned*)	9 – 10
Loss of life is between 1,000 – 10,000 OR loss of between of between $10 billion and $100 billion. (Note: if looking on a company level, loss of between 61% and 90 % of the total economic value for which you are concerned*)	7 – 8
Loss of life between 100 – 1000 OR loss of between $1 and $10 billion (Note: if looking on a company level, loss of between 31% and 60% of the total economic value for which you are concerned*)	5 – 6
Loss of life less than 100 OR loss of between $100 million and $1 billion (Note: if looking on a company level, loss of between 10% and 30% of the total economic value for which you are concerned*)	3 – 4
No loss of life OR loss of less than $100 million (Note: if looking on a company level, loss of <10% of the total economic value for which you are concerned*)	1 – 2
*The total economic value for which you are concerned depends on your perspective. For example, for a company this could be the percent of a single facility's gross revenues, or percentage of a company's gross revenues lost from the effect on a single product line. Likewise, a state could evaluate the effect of the economic loss caused by an attack of a facility or farm by the proportion of the state's economy contributed by that commodity.	

Criticality attempts to capture the public health impact in terms of deaths or economic impact associated with an adulteration event. Criticality is most commonly based on number of deaths, which is calculated from batch size, distribution units produced and number of consumers per distribution unit produced at the node in question. Assessment participants expressed concern that the scoring criteria for criticality, in terms of a public health impact, are based solely on the number of resulting deaths. Large food borne illness outbreaks with no deaths can still severely affect a food company and the product market and result in a significant public response. Illnesses attributed to a particular product or commodity can currently be scored based on economic impact alone, but economic impact is difficult to define and there is frequently not agreement among the assessment group on the scope of economic cost.

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. The measure is independent of the probability of successful introduction of threat agents.

ACCESSIBILITY CRITERIA	SCALE
Easily Accessible (e.g., target is outside building and no perimeter fence). 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.	9 – 10
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

Accessibility, along with Vulnerability, was one of the most useful CARVER + Shock factors for differentiating nodes of higher and lower concern and typically provided excellent discussion points regarding physical security, observation levels, and equipment design. Accessibility became less relevant in assessment where public access to the facility is inherent to its operation (i.e. a retail environment) or at assessments where plants are growing in open fields (i.e. Imported Products: Spices). It is not possible to enclose and monitor every field used for growing plants and therefore accessibility was consistently high and not helpful in the differentiation of higher and lower concern nodes within the process.

Accessibility was often difficult to differentiate from Vulnerability, which attempts to measure the ease with which threat-agents can be introduced in quantities sufficient to achieve the attacker's purpose once the target has been reached. There is an overlap of parameters such

as “volumes of contaminant” and “time available” between the Accessibility and Vulnerability definitions and criteria. Additionally, the Accessibility definition includes the statement, “This measure is independent of the probability of successful introduction of threat-agents,” but the criteria/score table states “Attack can be carried out using medium or large volumes of contaminant without undue concern of detection”. A revision to the definition of Accessibility may improve the ease of assigning Accessibility scores at future assessments.

The Accessibility factor was also highly dependent on the terrorist scenario selected and how the terrorist scenario was interpreted. Prior to each assessment, a terrorist profile was selected. This profile included attributes such as expertise, funding, and the ability to acquire threat-agents. In addition, the profile included whether the terrorist was an outsider or insider. An insider was considered someone with legitimate access to the facility or location and was typically selected over an outsider. The insider scenario assumes that the terrorist works in a facility or industry (or is present in the facility through authorized means) and therefore already has some level of access. It was assumed that if a facility could be hardened against the possibility of an attack by an insider, the same defenses should apply to an attack by an outsider (someone that has not been granted access). If the insider scenario was selected *and* assessment participants assumed that the insider could only be the legitimate worker assigned at each node in the process flow, then Accessibility (and Recognizability, and possibly Vulnerability) became irrelevant in most cases because building entrance security and other personnel access control measures may not apply. At the majority of assessments, it was assumed that the insider terrorist was not necessarily the person assigned to work at a particular node. With this caveat to the insider profile, participants could evaluate factors such as “Would someone who doesn’t normally work at this node appear out of place?”

The Accessibility factor is scored on equal weight with other factors, although Accessibility can be viewed as a pass/fail factor in the scoring process. Without Accessibility, there will be no event. Weighting the value of the Accessibility score may highlight its importance to facility managers and help to make nodes with high Accessibility scores rise higher in the relative risk ranking of nodes.

Recuperability: Recuperability is measured in the time it will take the specific system to recover productivity. The effect of a possible decrease in demand is also considered.

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

Recuperability was difficult to score in many cases due to the ambiguity of the scoring guidance and the unfamiliarity industry members typically have with this factor. The term "system" is intended to refer to the production or processing of a particular product or commodity, such as apple juice production, but a consistent interpretation of "system" was not applied across all assessments, as it was often difficult to determine if "system" referred to a specific company or the entire product, commodity, or industry. A clearer definition of "system" may clarify this factor and may need to be adapted for each sub-sector

Additionally, the current Recuperability scale lists periods ranging from less than one month to over one year. Thankfully, the US has not experienced a large-scale terrorist attack to the Food and Agriculture Sector, but this lack of historical data made it difficult for participants to estimate the time to recover from such an event. The scores attributed to this factor were typically either very high or very low, which may indicate that the scale is too restricted. By expanding this scale to cover a two or three year period, participants may be more comfortable with estimating the time to recover. Attendees also questioned if regulatory or investigative activity would be included in the time calculation for a facility to resume production.

Recuperability is a CARVER factor that rarely changes after the assessment group scores it at the first processing node. Assuming that an event occurs, the Recuperability score is typically the same for all process nodes whether the event is large or small, and usually does not help to differentiate the overall CARVER + Shock scores between nodes. An exception occurs when the human health impact was estimated to be very small, resulting in two or less deaths. In these cases, it was unclear if the terrorist event would be traced back to the product, commodity or process being assessed and the time to recuperate was reduced accordingly. However, Recuperability is generally node independent. It may be possible to assign a single Recuperability score to all nodes at the beginning of each assessment.

Vulnerability: Vulnerability is 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 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

Vulnerability is determined by both the characteristics of the target (e.g. ease of introducing agents, ability to uniformly mix agents into the target) and the characteristics of the surrounding environment (e.g. ability to work unobserved, time available for introduction of agents). It is important to consider what interventions are already in place that might thwart an attack. Vulnerability was often difficult to differentiate from Accessibility due to the overlap of parameters such as "volumes of contaminant" and "time available" between the Accessibility and Vulnerability definitions and criteria. A revision to the definition of Vulnerability may improve the ease of assigning Vulnerability scores at future assessments

Vulnerability differs from the other CARVER factors in that assessment participants must consider subsequent process nodes. The criteria for scoring Vulnerability require assessment participants to evaluate the "introduction of sufficient agents to achieve aim". The node being evaluated may allow for the easy introduction of the threat-agent, but participants must then consider whether subsequent processing steps such as dilution or heat treatment will diminish or negate the "achieve aim" portion of the Vulnerability definition. In addition, since the scoring guidance for Vulnerability is so broad, it is important that adequate notes be captured to justify a node's Vulnerability score.

Like Accessibility, Vulnerability is scored on equal weight with other factors, although Vulnerability can be viewed as a pass/fail factor in the scoring process. Without Vulnerability, there will be no event. Weighting the value of the Vulnerability score may highlight its importance to facility managers and help to make nodes with high Vulnerability scores rise higher in the relative risk ranking of nodes.

Effect: Effect is a measure of the percentage of system productivity damaged by an attack at a single facility and is inversely related to the number of facilities that produce the same product.

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

This factor is directly related to the facility, product, or commodity under assessment and is typically node independent. The term "system" is intended to refer to the entire industry producing the product – not a specific facility. Clarification in the scoring guidance may reduce confusion between Effect and Recuperability.

Effect is a CARVER factor that rarely changes after the assessment group scores the first processing node. Assuming that an event occurs, the Effect score is typically the same for all process nodes whether the event is large or small, and usually does not help to differentiate the overall CARVER + Shock scores between nodes. It may be possible to assign a single Effect score to all nodes at the beginning of each assessment.

Recognizability: Recognizability is the degree to which the target can be identified by an attacker without confusion with other targets or components.

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

As with Accessibility, Recognizability is highly dependent on the terrorist profile chosen for the assessment scenario. An 'insider" who works at the node being assessed would, by default, be able to recognize the node. Careful consideration of the terrorist scenario prior to scoring individual nodes is necessary. At the majority of assessments, it was assumed that the insider

terrorist was not necessarily the person assigned to work at a particular node. With this caveat to the insider profile, participants could evaluate factors such as "Would someone who doesn't normally work at this node recognize the target. When an exception was made, and the node worker was considered the attacker, adequate notes were captured to reflect this scenario.

Shock: Shock is a 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.

SHOCK CRITERIA	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

Shock typically tracks closely with the Criticality factor, and therefore does little to independently change the overall ranking for a node. It instead simply augments the Criticality score, in essence giving Criticality a double weighting. Additionally, the Shock definition states, "Mass casualties are not required to achieve widespread economic loss or psychological damage", yet the scale includes the same mortality ranges as Criticality. A revision to the definition and/or criteria of Shock may increase the relevance of the Shock factor for the CARVER + Shock tool on future assessments. For example, loss of life and economic impact

could be removed from the definition and criteria statements such that only the target and populations types are considered.

Illnesses attributed to a particular product or commodity can currently be scored based on economic impact alone. In reality, a large illness outbreak with no deaths can still cause an excessive public health impact by overwhelming health care facilities and cause public panic. There have been several requests by assessment participants to modify the Shock (and Criticality) scale to include human illnesses in addition to loss of life.

Overall, the CARVER+Shock tool is successful in determining relative risk rankings for nodes in a production process. However, as discussed above, Recuperability and Effect are generally assigned constant scores across all nodes within an assessment. This has the effect of negating the scores assigned to these scoring factors in the relative ranking of nodes. It may be more appropriate to remove these factors from the assessment method and simply discuss and capture information relating to Recuperability and Effect prior to an assessment – similar to how a threat agent is selected and a terrorist profile is defined. This information is still valuable to an assessment of the product, but does not benefit the relative risk ranking of nodes. In addition, the potential to weight some of the more critical components (Accessibility and Vulnerability) may serve to make the relative risk ranking of nodes more pronounced. The Shock component currently serves to give double weight to the Criticality factor. Either Shock should be considered for elimination from future assessments or the definition and criteria statements should be revised such that the loss of life and economic impact are removed with only the target and populations types considered. The industry being assessed does not gain any significant insight or benefit from the Shock score and the presence of the Shock score can serve to artificially inflate the overall risk scores of nodes where there are large batch sizes but low accessibility and vulnerability.

Another option would be to use only the Criticality, Accessibility, and Vulnerability (CAV) scores in future assessments. The CAV approach was used for the update assessments under this project and resulted in risk ranking of nodes comparable to the ranking of the same nodes under the original assessment using all of the CARVER + Shock factors. To incorporate the Recognizability factor, the scoring guidance for Accessibility could be modified to incorporate the knowledge and/or training needed to identify the target and know how to properly access the product stream and a particular node. Using this method, Accessibility and Vulnerability (indicative of the ability of an attacker to successfully attack a node) would comprise 2/3^{rds} of a node's total score, with the remaining 1/3rd comprised by Criticality (indicative of the severity of the attack to public health or economic loss). Mitigation steps taken by facilities to reduce either Accessibility or Vulnerability will have a large impact on a node's CAV score and can focus industry attention on these risk factors.

VI. Overall Assessment Observations

Assessment Preparation and Conduct

Each assessment began by the FDA and/or Battelle initiating contact with the relevant trade or industry association to educate the industry on the CARVER + Shock assessment process, its goals, and the data generated. The industry association point of contact would then coordinate attending individuals from various industry members and/or academic experts. Training materials, background information, and a generic process flow diagram were provided to all attendees prior to the assessment. At the assessment, a quick tutorial session on the CARVER+Shock tool was provided to ensure participants understood the assessment method and scoring factors. Following the training, all participants would conduct CARVER+Shock scoring on all process nodes and review the results. Upon reviewing the scoring results, attendees would brainstorm potential mitigation strategies that could be employed to reduce the risk at the highest scoring nodes and highlight any research questions that came up during the course of the meeting.

This schedule and format worked well throughout the vulnerability assessment process. The pre-assessment training materials and tutorial adequately prepared participants for the assessment process and helped participants understand the goal of the assessment meeting and the value of conducting vulnerability assessments. Although the CARVER + Shock training and the tool itself worked well with assessments of the food and agriculture sectors, there were many lessons learned regarding usage of the tool and the software.

Selection of Threat Agent for CARVER + Shock Scenario

The CARVER + Shock assessment tool requires the selection of a threat agent in order to calculate the amount of agent that would be required to successfully adulterate the product at each node. For those processes or commodities that would not result in human health impacts (such as products intended for animal consumption, e.g. pet food and animal by-products), the selection of a threat agent is still important in estimating the potential economic damage and shock following an event.

Prior to the assessment meeting, Battelle's vulnerability assessment team would research the product's characteristics and manufacturing process, and then select a threat agent that would be most suitable for a successful attack on the assessed industry. At the assessment meeting, the agent's characteristics were discussed with industry attendees and its applicability to the product being assessed verified with industry experts.

Participant Perspective

Although much information was exchanged during the course of these assessments, the greatest benefit may have been in the enhanced communication channels that were formed between the Government and the Food Industry. Numerous initiatives such as this, to collaborate on security efforts at the Federal and State levels, are the result of a shift towards working in partnership to address food defense issues. Programs and assessments such as this and preceding vulnerability assessment efforts have further bolstered the trust between industry and their government partners, while also allowing government agencies to tap into the valuable knowledge base found in private industry.

The comments received from industry participants and trade organizations regarding the vulnerability assessments were generally positive. The structure of these assessments allowed open discussions and questions. This informal atmosphere has further improved the interactions and open communications among the industry and government participants. The fact that multiple industry members were represented has also been a great advantage for industry participants. Often a single question posed by one person/company initiated a robust discussion among all attendees both industry and government. Having all of these voices in the same room at the same time strengthened the perception that government and industry have common goals and that by working in unison they can improve the safety and security of the food and agriculture industry .

International Assessments and Food Defense Workshops

This task also expanded the vulnerability assessment process to include international food sources. Imported Products (Spices) were assessed in Arlington, VA with industry representation from major international spice producers in an effort to understand and assess the process of growing, refining, and then importing this product to the US. Expanding the vulnerability assessment process to include imported products highlights the importance of imported food products to the American consumer.

Battelle also conducted four assessments in Thailand as a follow on to the larger Asian Pacific Economic Cooperation (APEC) Food Defense Pilot Program. During these assessments, Battelle also provided intensive training on the CARVER+Shock Software tool to international attendees and solicited their input and feedback to conduct a software based assessment of three products manufactured in Thailand which are commonly exported to the US. (Canned Fruit, Canned Tuna, and Rice) as well as a Thailand retail food shop. These international assessments enabled the assessment team to understand the production process and environment that exists in other countries. As the US imports a wide variety of food products, assessment of these foreign producers is increasingly important. Additionally, these assessments allowed the assessment team to highlight the importance of food defense and the institution of mitigation measures to an international audience.

Other Observations

During this effort, industry members typically came to the Arlington, VA to conduct the assessment meeting. This generally resulted in fewer industry participants at each assessment meeting than during the SPPA assessments. This was due to travel time, cost, and logistics of coordinating the meetings in Arlington, VA. Having fewer industry participants typically allowed for a shorter assessment meeting, but served to focus the assessment on the process of two or three companies, potentially omitting important information that could be provided by more diverse industry representation. For future assessments, it may be more effective to conduct vulnerability assessment meetings in geographic locations close to industry members and to seek out the participation of small and specialty industry members in addition to large industry members.

Additionally, facility tours were typically not conducted during this task. This resulted in assessment facilitators relying solely on the input of industry members to gain an understanding of the operation, activity, and environment of each process node. Relying solely on discussion to understand an industry rather than touring a facility and witnessing firsthand the production process of an industry resulted in reports that may not include the level of detail obtained during the SPPA assessments where tours were conducted. The absence of facility tours also prevented government experts in food defense and security from being able to make specific inquiries to industry members during the facility tour. The facility tours frequently generated information and initiated important discussion that may not have been gathered without the tour. It is recommended in future assessments that facility tours be conducted.

VII. Conclusion

The size and scale of the American food and agriculture sector is immense and exists as a tempting target for terrorist attack. While it is virtually impossible to guard against all threats, the information generated during this task provides the government with valuable information to enhance food defense initiatives, regulations, and standards; develop resources and guidance; and will assist the industry to take steps to mitigate potential adulteration events.

The ultimate goal of this effort and the FDA's mission as a whole is to ensure to the American people safe food products. In this effort, the FDA's development of valuable software tools and online resources and guidance documentation is critical to support industry members, academia, and the general public. The CARVER+Shock software tool, used extensively during this task was reviewed in detail and a series of suggested improvements were identified and provided back to the tool developers for use in later improvements of the tool. Review and improvement of the CARVER+Shock software tool helps industry members conduct individualized vulnerability assessments and provides helpful mitigation strategies to potentially reduce adulteration risk at identified nodes. The FDA's Mitigation Strategies Database (MSD) also provides many mitigation strategies available for industry review and consideration. The FDA is also currently developing other valuable tools to assist industry to

navigate the food defense requirements and support the development of facility specific food defense plans. These tools should be available for industry use in coming months.

Finally, the participation of industry members and trade associations in the vulnerability assessment process helps to elevate the issue of food defense to one of primary importance to the American food and agriculture sector. The communication and cooperation that was started under the SPPA was continued and expanded under this task to maintain engagement and communication with important industry groups. Food defense measures will be implemented and the costs of those measures will be borne by the industry and it is imperative that industry members understand the importance of food defense to the national security of the United States. This task also expanded the vulnerability assessment process to industries outside of the US, which may become more appealing as a target for terrorists as domestic producers begin incorporating food defense strategies to harden their production processes against intentional contamination.