Facility Risk-Assessment and Security Guide

...for Grain Elevators, Feed/Ingredient Manufacturers, Grain Millers and Oilseed Processors...

National Grain and Feed Association

North American Millers Association

September 2009

Disclaimer: The National Grain and Feed Association and North American Millers Association make no warranties, expressed or implied, concerning the accuracy, application or use of the information contained in this publication. Further, nothing contained herein is intended as legal notice. Competent legal counsel should be consulted on legal issues.

Contents

Introduction

This guide assists grain elevators, feed and feed ingredient manufacturers, flour mills, and other grain and oilseed processors in conducting facility risk assessments, as well as in developing and implementing facility security plans.

This guide was developed initially by the National Grain and Feed Association (NGFA) in 2001. It subsequently was updated and expanded by the NGFA in 2004. In 2008, it was reviewed and further revised by the Joint Agroterrorism/Facility Security Committee comprised of members of the NGFA, North American Export Grain Association (NAEGA), and Grain Elevator and Processing Society (GEAPS) to reflect lessons learned from a series of facility vulnerability assessments in which these organizations participated in partnership with federal and state agencies. In addition, the North American Millers Association (NAMA) participated in reviewing and modifying the draft.

Importantly, this guide provides basic concepts that can be used as a starting point upon which to build facility-specific risk-assessment and security plans. As such, it should be viewed as a foundation – or the base of a pyramid – upon which individual companies can build their own tailored plans specific to their facility operations and personnel; agricultural commodities handled; geographic surroundings; potential threats; and other conditions.

Appendix 2 may be particularly useful. It provides a sample template for developing a facility security plan.

How this Guide is Organized

This document is organized in the following manner:

- **Part I** provides guidance for conducting a facility risk assessment.
- **Part II** provides guidance for developing and implementing a facility security plan.
  - **Part II.A** – Presents a menu of options for addressing the general security of the physical facility and grounds.
  - **Part II.B** – Presents options for addressing operating and personnel procedures.
  - **Part II.C** – Presents options for addressing shipping and receiving procedures.
  - **Part II.D** – Presents options for addressing incident-response procedures.
- **Appendix 1** contains sample forms that can be used for developing: 1) an emergency telephone list; 2) an employee emergency telephone list; and 3) a visitor's log.
- **Appendix 2** contains a Sample Facility Security Plan Template that can be used in conjunction with Part II of this guide to develop a new – or modify an existing – security plan for your facility. Be sure to include other or different facility-security procedures already used at your facility and its operations. This template also is available electronically in a "fill-in-the-blank" format by clicking here. Importantly, this document is designated as "Sensitive Security Information" (SSI) under federal law, and is **not** to be distributed or released to persons not in a "need-to-know" status within your company.
- **Appendix 3** contains generic flow diagrams of various types of facilities to assist in conducting a risk-assessment.
- **Appendix 4** contains links to useful facility security-related information available from various public and private-sector websites.
- **Appendix 5** contains a glossary of commonly used security-related terms.

The topics discussed and guidance provided in this document are **not** formal recommendations. Nor are they a comprehensive compilation of all security issues confronting the grain, feed, milling and processing industry or other agribusinesses. Rather, this document provides a **"menu" of ideas and concepts** that managers can consider when conducting a facility risk assessment and developing a facility security plan.

It is extremely important when conducting a risk assessment and developing or modifying a facility security plan to select those procedures that are effective, practical and realistic for the type, characteristics and operation of the facility for which they are intended, as well as the physical environment in which the plant exists. There is no "one-size-fits-all" approach. Further, different plans may be appropriate for different facilities operated by the same company, based upon the types of processes, circumstances and conditions present. **In addition, it is extremely important that you select facility-security measures that address real, rather than perceived, risks, are achievable and will be implemented.**

Benefits

In addition to the obvious benefit of reducing the risk of an attack from an insider or outsider, there are several major business-related benefits to conduct a facility risk assessment and develop a sound facility security plan:

- It helps facilities comply with government-mandated food/feed-defense requirements.
- It reinforces a facility's standard operating procedures, internal controls, quality-assurance plans and other programs that foster the production of safe food and feed, thereby providing additional assurances to customers.
- It makes management and employees alike more aware of potential "risks" to their operations, as well as mitigation strategies that can help prevent theft and other non-terrorist-related incidents.
- It encourages the development/refinement of human resource policies that increase the awareness of – and address – disgruntled employees or behavioral issues in the workplace.
- It encourages building ongoing relationships with local law enforcement, emergency responders and other key local, state and federal officials who are critical resources in the event of a natural disaster, terrorism event or other emergency.
- It may make facility and product liability insurance more available and affordable.
- It makes management more aware of the other systems upon which their facilities rely, such as suppliers, transporters and other infrastructure.
- It ultimately protects the company's shareholder and brand value, which can be undermined by a food/feed safety incident.

Federal Government Requirements

Several federal government standards and directives pertain to facility security. Some of those that may apply to your facility are explained in this section, and are provided for your awareness. Not all apply to all facilities; for instance, the maritime security requirements apply to grain and other facilities regulated under the Maritime Transportation Security Act (MTSA). This section also may not encompass all requirements that apply to all facilities.

- **Presidential Security Directives:** In the aftermath of Sept. 11, 2001, President Bush issued a host of "Homeland Security Presidential Directives" ordering federal departments and agencies to take specific actions to protect the nation from terrorist acts. For agriculture, the most important of these is Homeland Security Presidential Directive Number 9 (HSPD-9), designed to "harden" the agricultural sector and make it less vulnerable to a terrorism incident or other security-related

breaches that could compromise the safety of the U.S. food supply. HSPD-9 is a sweeping executive order that directs several federal agencies to work cooperatively to develop plans to protect the safety and security of the nation's plant and animal-based food supply.

Among other things, HSPD-9 directs the secretaries of agriculture; health and human services (which includes the Food and Drug Administration), and homeland security to "expand and continue vulnerability assessments of the agriculture and food sectors," and to update those assessments every two years. It also requires USDA and the Departments of Homeland Security, Health and Human Services, and Justice (including the FBI), as well as the Environmental Protection Agency, CIA and other federal agencies, to "prioritize, develop and implement…mitigation strategies to protect vulnerable critical nodes of production or processing from the introduction of diseases, pests or poisonous agents." And it calls on federal agencies to expand on the development of "common screening and inspection procedures" for agriculture and food products imported into the United States, and to "maximize effective domestic inspection activities" for domestic shipments of food products.

- **USDA's Uniform Grain and Rice Storage Agreement (UGRSA) Contract:** The U.S. Department of Agriculture (USDA) since Sept. 1, 2004 has required that grain elevators entering into a Uniform Grain and Rice Storage Agreement (UGRSA) contract with the Commodity Credit Corp. (CCC) conduct a facility vulnerability assessment and implement a facility security plan. UGRSA contracts are required for grain elevators that store or handle CCC-owned grain, or that offer marketing assistance loans to producers under the U.S. farm programs. Among other things, Part III of the UGRSA contract – which addresses the warehouse operator's contractual responsibilities – specifically requires facilities to implement a security plan that "includes measures to protect grain handled and stored" under the contract. The facility vulnerability assessment most warehouse operators are required to conduct addresses four major components: 1) The general security of the physical structures and grounds of the grain storage facility; 2) the warehouse's shipping and receiving procedures to ensure grain is "not subject to tampering"; 3) actions to be taken in the event of a "national emergency"; and 4) emergency contact information for local security authorities. For more information from the NGFA, click here.

- **USDA's Requirements for Suppliers of Domestic and International Food Assistance:** Similarly, USDA has indicated its intent to soon require contractually that companies supplying raw or processed agricultural commodities for its domestic or foreign food aid programs (such as the School Lunch Program and P.L. 480 food aid shipments) conduct facility vulnerability assessments and implement facility security plans.

- **Bioterrorism Act Facility Registration:** Under the Bioterrorism Act of 2002, the U.S. Food and Drug Administration (FDA) requires domestic and foreign facilities (and their U.S. agents) that "manufacture, process, pack or hold *(i.e., store)* food" for human or animal consumption in the United States to register with the agency. Among the types of facilities covered by this regulation are grain elevators, commercial feed mills, flour mills, corn and oilseed processing plants, pet food manufacturers, renderers and others. The facility registration requirement took effect on Dec. 12, 2003. Click here for more information.

- **Bioterrorism Act Recordkeeping Regulations:** Under the Bioterrorism Act of 2002, FDA requires those who "manufacture, process, pack, transport, distribute, receive, hold *(i.e., store)* or import food into the United States establish and maintain records sufficient to identify the immediate previous source(s) and immediate subsequent recipient(s) of such food, as well as transporters used to receive and ship such products. Put simply, this regulation requires "one-step-forward, one-step-back" product-tracing recordkeeping. The requirement to maintain such records was phased in based upon the size of the company, with larger firms required to do so starting Dec. 31, 2005, medium-sized companies on June 9, 2006 and small companies on Dec. 11, 2006. Among others, these recordkeeping requirements apply to domestic and export grain elevators, feed and flour mills, dry and wet corn mills, and oilseed processing plants. Click here for a comprehensive NGFA compliance guide on this standard; click here for a comprehensive guide for millers authored by NAMA.

- **Chemical Facility Antiterrorism Standard:** The U.S. Department of Homeland Security (DHS) in April 2007 issued a chemical facility antiterrorism standard (CFATS) regulation, which may apply to grain elevators, commercial feed and feed ingredient manufacturers, flour mills, grain and oilseed processors, farm supply retailers and other food, agricultural and chemical facilities depending upon whether they "possess or plan to possess" any of more than 300 "chemicals of interest" at threshold quantities designated by DHS as potential threats of theft, release or sabotage/contamination. Affected facilities are required to provide information about such chemicals and their operations to DHS using a web-based tool known as "Top Screen," and may be required to implement more stringent facility security plans based upon the result of DHS's analysis. DHS has said it will audit implementation of such security plans. Click here for guidance documents on this standard prepared by the NGFA and NAMA.

- **Hazardous Materials Transportation Law:** Agricultural facilities transporting specific chemicals, such as farm supply businesses, may be covered under the federal hazardous materials transportation law and regulations implemented by the U.S. Department of Transportation (DOT). Importantly, this law and regulations are distinct from the chemical facility antiterrorism standard and regulations cited previously. The hazardous materials transportation law authorizes the secretary of transportation to designate specific materials or groups/classes of materials, such as fertilizers and pesticides, as hazardous when he/she determines that transporting the material in commerce in a particular amount and form may pose unreasonable risk to health, safety or property.

  Regulations issued by DOT's Pipeline and Hazardous Materials Safety Administration require those covered to develop and implement plans to address security risks associated with the transport of such materials in commerce. Substances covered are those, including fertilizers and pesticides, transported in a quantity that require the shipment to be placarded. The security plan is required to be in writing and include an assessment of possible transportation security risks associated with the shipment, as well as appropriate measures to address those risks. At a minimum, the security plan is to contain:

  - **Personnel Security:** Measures to confirm information provided by job applicants hired for positions that involve access to and handling of hazardous materials covered by the security plan. Employers are required to include the measures they have implemented to confirm information provided by applicants in the written security plan, but are not required to document the results of their efforts to confirm information on specific applicants.

  - **Unauthorized Access:** Measures to address the possibility that unauthorized persons may gain access to the hazardous materials covered by the security plan or to transport conveyances being prepared for transport of such materials.

  - **En Route Security:** Measures to address the security risks of shipments of hazardous materials covered by the security plan en route from origin to destination, including shipments stored prior to shipment.

  DOT inspectors are authorized to review these security plans if they conduct a compliance review at the facility. Click here for more information on DOT's hazardous materials regulations.

- **Voluntary Private Sector Preparedness Standards:** A law (P.L. 110-53), enacted in August 2007 to implement recommendations of the Congressional 9/11 Commission, contains a section (Title IX) creating a voluntary private sector preparedness standards program. The law authorizes the U.S. Department of Homeland Security (DHS), in consultation with the private sector, to develop guidance or recommendations, as well as to identify best practices, that assist or foster action by the private sector to: 1) identify potential hazards and assess risks and impacts; 2) mitigate the impact of a "wide variety of hazards, including weapons of mass destruction; 3) manage necessary emergency preparedness and response resources; 4) develop mutual aid agreements; 5) develop and maintain emergency preparedness and response plans, and associated operational procedures; 6) develop and conduct training and exercises to support and evaluate emergency preparedness and response plans, as well as, operations procedures; 7) develop and conduct training programs for security guards to implement emergency preparedness and re-

sponse plans and operations procedures; and 8) develop procedures to respond to requests for information from the media and public. The law also requires DHS to enter into agreement with one or more nongovernmental entities to create an accreditation and certification program for facilities adopting consensus preparedness standards or best practices.

- **Maritime Facility Security:** Under the 2002 Marine Transportation Security Act (MTSA), the U.S. Coast Guard on Oct. 22, 2003 issued final regulations that require facilities that receive commercial vessels greater than 100 gross register tons on international voyages – such as grain export facilities – to develop and implement a facility security plan approved by the Captain of the Port, or a Coast Guard-approved alternative security program meeting specific requirements. Other types of facilities required to develop facility security plans under the Coast Guard regulations are those handling certain explosive or hazardous cargoes (including ammonium nitrate fertilizer or fertilizer mixtures), as well as facilities that load or unload barges with animal fats or vegetable oils. More information is available by clicking here.

  Among the requirements for MTSA-regulated facilities is to comply with the Transportation Worker Identification Credential (TWIC) program, operated jointly by the Coast Guard and Transportation Security Administration. TWICs are tamper-resistant biometric credentials issued following a security background check to persons who require unescorted access to designated secure areas of MTSA-regulated ports, vessels and outer continental shelf facilities, as well as all credentialed merchant mariners. Mandated by Congress under MTSA, all of the nation's ports were required to be in compliance with the TWIC program by April 14, 2009. TWIC requirements and information are available on the U.S. Coast Guard's Homeport web site at: http://homeport.uscg.mil/.

- **Customs-Trade Partnership Against Terrorism (C-TPAT):** Implemented by the U.S. Department of Homeland Security Customs and Border Protection (CBP) division, this voluntary program is designed to provide tiered benefits to importers of cargo, including expedited entry, depending upon the degree to which such importers have implemented security measures within their international supply chain. Program benefits are minimal until after CBP conducts an on-site validation of the user's security measures. C-TPAT participants receiving CBP certification are given access to several potential benefits, including a reduced number of inspections and priority processing when inspections do occur. In addition, C-TPAT-certified importers have access to "free and secure trade" (FAST) designated lanes at border-crossing points for C-TPAT-compliant imports into the United States from either Canada or Mexico. C-TPAT also offers a "stratified exam" for import line items that are subjected to inspection that allows the importer to move all but the container that has the actual line item in question to their premises, thereby avoiding storage costs at the border. Containers that are moved are required to remain sealed and available for inspection in the event CBP decides to examine them. Click here for more information on C-TPAT.

Conclusion

We trust you find this guidance useful, and welcome your ideas and comments on additional information that would be helpful in further protecting facility security and the safety of the U.S. food and feed supply. Comments may be directed to:

Randy Gordon
Vice President, Communications
and Government Relations
National Grain and Feed Association
1250 I St., N.W., Suite 1003
Washington, D.C., 20005
Phone: 202-289-0873
Email: rgordon@ngfa.org

Jess McCluer
Director of Regulatory Affairs
National Grain and Feed Association
1250 I St., N.W., Suite 1003
Washington, D.C., 20005
Phone: 202-289-0873
Email: jmccluer@ngfa.org

Jane DeMarchi
Director of Government Relations
North American Millers Association
600 Maryland Ave., S.W.
Suite 825 West
Washington, D.C., 20024
Phone: 202-484-2200
Email: jdemarchi@namamillers.org

Part I

Guidance for Conducting a Facility Risk Assessment

The starting point in developing a rational and prudent security plan is to conduct a risk assessment of the facility and its surroundings.

The risk-assessment process involves "out-of-the-box" thinking using an "all-hazards, total-risk approach." Identify the assets, products and operations that constitute the most realistic source of risk at the facility, such as natural disasters (e.g., hurricanes, tornadoes, etc.), unintentional human or mechanical events or errors, and intentional human actions. All aspects of the facility's operation need to be considered, including receiving of inbound commodities, ingredients, products and materials; storage, handling and processing; shipping and distribution; and other areas. Further, it requires making these determinations subjectively from the perspective of an attacker (whether an outsider or insider), since risk is present whenever an attacker has the ability, opportunity and desire to do harm.

It involves thinking about:

- How likely is an attack on the facility or one of its key assets?
- How harmful will such an attack be if it does occur and succeeds?
- What impact will an attack on other key assets (e.g., transportation, power sources) have on the facility's ability to recover and resume operations?

Think about this from a triad approach: Is there a desire or motive of an individual to do harm to the facility? Does the individual have the physical or mental capability to carry out an incident? And does the individual have an opportunity to carry out an incident?

Importantly, one of the major goals of the risk-assessment process is to **differentiate between real, versus perceived, risks**, so that scarce human and financial resources can be put to the best use. It is this risk-assessment process that provides the basis from which all other security issues can be addressed, including how many resources and what type of security infrastructure or procedures will be committed to mitigate the potential for such an incident to occur.

The following is a step-by-step approach for conducting a facility risk assessment.

Step 1: Plan for Conducting a Risk Assessment

While many grain-handling, feed-manufacturing, flour and grain-processing facilities have certain similarities, there frequently are unique characteristics or considerations that deserve individual attention and thought when conducting a facility risk assessment.

Generally, grain, feed, feed ingredients, flour and other grain-based products may be contaminated by:

- biological agents *(such as toxins, bacteria, viruses, parasites, etc.)*;
- chemical agents *(such as nerve gas and toxic industrial chemicals – pesticides, rodenticides and heavy metals)*;
- radiological agents *(such as those that can be delivered in liquid or solid form)*; and/or
- physical agents *(such as ferrous and non-ferrous metal, glass and plastic)*.

- **Consider Who to Designate to Conduct the Risk Assessment:** Consider designating an experienced company individual to be the "security coordinator" at the facility. In many cases, this may be the person already responsible for safety, health and environmental compliance. In other cases, it may be the manager. For facilities engaged in multiple operations, such as grain handling, feed manufacturing, grain milling and farm supplies, consider a "team" approach consisting of cross-functional representation from the different types of operations in which the facility is engaged.

  The person(s) designated with this responsibility should be objective and empowered to make a thor-

ough, honest and realistic assessment of the facility's security given the type of commodities handled, type of operation(s), location and surroundings (neighborhood).

- **Identify Critical Physical Assets:** Knowing and identifying the facility's most valuable physical assets are essential to any security plan. This allows limited security resources to be used most efficiently. Examples of potential critical assets include:

    - Receiving areas (rail/truck; liquid and dry) – potential contamination points.
    - Energy sources (transformers, gas service, fuel tanks, boilers, air compressor equipment) – potential critical infrastructure targets.
    - Control rooms and motor control rooms – potential critical infrastructure targets.
    - Information technology *(e.g., computer)* system – potential critical infrastructure target.
    - Production processes *(e.g., mixers)* – potential contamination point.
    - Bulk trucks/delivery – potential contamination points.
    - Access to product storage to finished and product materials – potential contamination points.
    - Hazardous chemicals – potential threat agent.

- **Consider Most Likely Types of Risk and Who May Pose Them:** Before conducting a facility risk assessment, consider the type(s) of risk (sabotage, threat or attack) and whether it most likely could originate from an internal source (such as from a disgruntled employee) or external entity (such as an activist, terrorist or disgruntled neighbor). Your facility's location – urban or rural – and the type of operations in which it's engaged (such as strictly grain handling, or also feed manufacturing, flour milling and/or farm supply enterprise) may have a bearing on the types of vulnerabilities to which attention should be paid.

- **Consider the Degree to which Risks May Exist:** For instance, consider the:

    - types and capacity of storage at the facility;
    - effectiveness of controls on access to the facility and grounds;
    - history of previous incidents or "close calls";
    - number of employees;
    - satisfaction level of employees and the degree to which some of them bring personal problems into the workplace; and
    - surroundings and characteristics of the neighborhood in which the facility is located.

Other factors to consider include:

- Potential threat intentions *[for instance, are there or have there been any threat(s) to the company or facility, or a history of troublesome activity in the area]*.
- Specific targeting *[does the company name, its notoriety or the nature of the facility's activity make it a likely target?]*.
- Visibility and recognizability of the facility and its operations within the community.
- Potential on-site hazards *[such as the presence of hazardous materials, biologics or chemicals that potentially could be used as a threat or weapon]*.
- The security environment and overall vulnerability of the facility to attack *[e.g., the effectiveness of security procedures used at the facility; public accessibility to facility; nature of facility assets; degree of law enforcement presence in area; etc.]*.
- Critical nature of the facility's products and services *[e.g., nature of the facility's assets (hazardous materials, uniqueness and potential danger); importance of the facility to the infrastructure and continuity of basic services to the community, state or nation; etc.]*.
- The "cascading" impact an attack could have on the facility or on the supply chain/infrastructure upon which the facility depends.
- The presence of large numbers of people at the facility who could be harmed.
- The potential for mass casualties within a one-mile radius based upon the types of materials stored or used at the facility.

The degree to which risks exist may be affected or mitigated by the existence and effectiveness of potential countermeasures, such as

- Organizational communications *[e.g., mass notification systems are in place in the event of emergency; crisis response team; awareness of local/regional emergency responders about the facility and its operations; linkage of alarm systems to local law enforcement authorities]*.

- Security and response *[e.g., disaster-response teams trained and available; hazard-monitoring devices on-hand and operational; etc.]*.

- Policy, procedures and plans *[crisis response/ disaster plans in effect that address the most likely threats (e.g., fires, explosions, chemical release, etc.)]*.

- Security equipment *[e.g., existence of a security/alarm monitoring and maintenance system; availability of functioning personnel protective equipment appropriate for hazardous materials that may exist at facility; etc.]*.

- Security of information systems, networks and hardware *(e.g., computer system)*, as well as mail and telecommunications.

- Workplace violence policy in effect and functioning well.

- Programs implemented to train employees on how to recognize risks and threats, and how to report them.

- Implementation of employee health and awareness programs *[e.g., list of employee contact information; employees aware of duties in event of an emergency; etc.]*.

Step 2: Assemble Risk-Assessment Team

Identify those persons within your facility who are responsible for facility security and operations, as well as any outside subject matter experts you may wish to utilize, for conducting the vulnerability assessment. At a minimum, the team should consist of trusted individuals knowledgeable about the facility's physical operation, type(s) of products being handled or manufactured, and product flow – from receiving to outbound shipment.

Step 3: Conduct a Facility Risk Assessment

Next, conduct a risk assessment of the facility and its surroundings, assessing different points of vulnerability. This will enable management to make prudent security decisions that distinguish between "real" versus "perceived" risks.

In addition, developing a schematic diagram of the facility that traces the flow of commodities and ingredients from receiving to loadout allows the risk-assessment team to focus on specific nodes at the facility or in the commodity/ product stream where the product could be contaminated. *[See Appendix 3 for sample generic flow diagrams of various types of facilities.]*

This risk-assessment process also assists in identifying potential mitigation methods and strategies that may be appropriate for the facility.

These are some of the questions that should be considered during the risk assessment:

1. If you wanted to intentionally introduce an agent that would contaminate the safety of commodities or products handled or manufactured at this facility, how and where would you do it?

- Identify and develop a list of the type(s) of threat or attack *(e.g., intentional contamination incident)* most likely to occur at this facility that would pose a danger to product safety or damage ongoing facility operations.

- How likely is an attack of that manner to occur at this facility?

- What plan of attack would an "outsider" use? What plan of attack would be used if it was done by an "insider?"

- Are there measures currently in place at this facility that would mitigate or help reduce the impact of such an attack? What are those measures? And why would they be effective?

- Identify the most serious risks that should receive priority attention based upon: 1) your evaluation of which type of attack(s) would be most likely to occur at this facility; and 2) the measures in place to mitigate against such risks.

2. What would the impact be to this facility and to the company as a whole if these type(s) of attack were to occur?

3. An adversary may seek to harm something or someone other than the facility itself. If you wanted to use the assets of this facility to intentionally harm someone or something else, what would you choose to perpetuate an attack *(e.g., fumigants, release of chemicals, trucks containing hazardous materials, etc.)*? How would you accomplish such an attack?

- How likely is it that an attacker (insider or outsider) could gain access or control of the assets you identified above to perpetrate this kind of attack?

- What attack plan would the person use to intentionally harm someone using these assets?

- Are there measures currently in place at this facility that would prevent an assailant from gaining access to the assets you identified to perpetrate each of these kinds of attacks? What are those measures? And why would they be effective?

- Based upon your evaluation of the preceding questions, list the most significant assets that, if used improperly, would cause the most negative impact on the facility, the community in which the facility operates and the company as a whole.

4. What infrastructure interdependencies or systems – such as access to electrical power, raw materials, roads/bridges, transportation conveyances (rail/barge/truck), etc. – does this facility have? Specifically identify what they are.

- How likely is it that there could be an intentional or unintentional disruption of the supply chain/infrastructure system that is critical to this facility's continuing operations? Examples include roads, bridges, locks and dams, power stations, critical suppliers, etc. Rank each in terms of criticality and likelihood of disruption.

- Are there alternatives or options in the supply chain/infrastructure that could be used to allow this facility to continue operating at full capacity if any of the systems identified above were disrupted?

- What impact would a disruption – either intentional or unintentional – cause, both to this facility and to the company as a whole, if it were to occur to the critical supply chain/infrastructure systems on which this facility depends upon to operate? Rank the impact to the various entities, both internal and external, if a disruption were to occur.

Conclude by evaluating and prioritizing the overall risks and vulnerabilities that would have the greatest impact upon the facility, the surrounding community and the company as a whole.

Note: A Word About CARVER+Shock Vulnerability Assessment Tool: One risk-assessment tool that the reader may hear about is "CARVER+Shock," which originally was developed by the U.S. military and later adapted by FDA for tabletop exercises involving a wide range of food and agricultural products and facilities. CARVER is an acronym for the terms "criticality," "accessibility," "recuperability," "vulnerability," "effect" and "recognizability." "Shock" refers to the combined physical, public health, psychological and economic effects of an attack. While certain concepts of this tool are of value, it also has inherent limitations for practical use by facilities within the grain, feed, milling, grain-processing and export sectors. You may learn more about this vulnerability-assessment tool from the NGFA/GEAPS Facility Security Website at: http://www.ngfa.org/security/home.html.

Step 4: Identify and Implement Mitigation Strategies to Address Results of Risk Assessment

Once the risk assessment has been completed, a plan should be developed to identify and implement specific mitigation methods and strategies *(i.e., countermeasures)* to minimize the vulnerability of those aspects that may pose a "high risk."

Such mitigation may include enhancements to physical, as well as personnel and operational security, training and education, to reduce the potential access of an outside or inside attacker to the facility, product or manufacturing process. Many of those potential risk-mitigation concepts are presented in Part II of this guide.

Recognize, though, that not all risks can be mitigated because of feasibility, costs and other constraints.

Step 5: Document Completion of the Facility Risk Assessment

Document that the facility risk assessment has been conducted and a facility security plan implemented. File the document in an appropriate, secure location at the facility.

Classify the security plan and any accompanying risk-assessment documents as "Sensitive Security Information." Include that statement ("Sensitive Security Information") and the following warning statement on each page of the document: *"**Warning:** This document contains Sensitive Security Information protected from unauthorized disclosure or distribution under Federal Law. No part of this document may be disclosed or distributed to persons without a "need-to-know," unless specific written permission is granted in advance by management." See Appendix 2 for an example.*

Part II

Guidance for Developing and Implementing a Facility Security Plan

Introduction

As noted in Part 1 (Step 4 on page 10), which addressed mitigation strategies *(countermeasures)*, this section contains a **"menu" of ideas and concepts** that managers can consider incorporating into a new or existing facility security plan.

Utilize the "learnings" that come from the risk assessment (Part 1) when devising the security plan.

It is extremely important when developing or modifying a facility security plan to select those procedures that are effective, cost-effective, practical and realistic for the type and characteristics of the facility for which they are intended, as well as the physical surroundings in which the plant operates. There is no "one-size-fits-all" approach when it comes to facility security, and the facility vulnerability assessment is useful in identifying facility-security steps and other mitigation strategies that may be warranted for individual situations. Address real versus perceived risks.

Also consider other measures that may be appropriate for your specific facility and its surroundings. Be sure to include other or different facility-security procedures already being utilized effectively at your facility and its operations.

In addition, it is extremely important that you select facility-security measures that are achievable and that will be implemented.

This section is organized in the following manner**:**

- **Part II.A** – Presents a menu of options for addressing the general security of the physical facility and grounds.
- **Part II.B** – Presents options for addressing operating and personnel procedures.
- **Part II.C** – Presents options for addressing shipping and receiving procedures.
- **Part II.D** – Presents options for addressing emergency response procedures.

Part II.A

General Security of Physical Facility Operations and Grounds

Assess the feasibility of implementing the following procedures to enhance the **general security of the facility and grounds**:

1. **Control Access:** Use "layers" of security appropriate to the threat level to prevent unauthorized persons from having access to critical assets or areas of the facility, as identified in the risk assessment.

   A "layered" security approach to control access to the facility and its critical assets involves implementing a combination of physical and operational measures.

   Physical security options may include, but are not limited to, **one or a combination** of the following options:

   - Installing security lighting in high-risk or dimly lit areas. Consider using high-low ballast lighting, in which high-beam light is activated by physical movement of intruders in the area(s) subject to surveillance.
   - Conducting periodic walk-arounds by company personnel of the facility and grain storage and product loading/unloading areas.
   - Conducting drive-by surveillance patrols by local law-enforcement on a regular, but unpredictable, basis.
   - Installing electronic security devices, such as door alarms *(e.g., horns, bells, etc.)*, motion-detection devices and alarms monitored by an off-site security system or contractor.
   - Installing appropriate signage for:
     - "No trespassing."
     - "Private property."
     - "Visitor Parking."
     - "All visitors must check in with front office."
     - "All visitors must be escorted."
     - "No vehicles beyond this point."
     - "Patrolled" *(if appropriate)*.
     - "Closed-Circuit TV surveillance" *(if appropriate)*.
   - Installing video surveillance.
   - Retaining guard service from contract security firms.
   - Installing physical barriers, such as virtual or visible perimeter fencing and locked gates. *[Note: This may not be necessary, practical or cost-effective because of the configuration of the facility, its surroundings or the relative risk identified.]*
   - Enrolling in a local business or community "crime-watcher's" program.

   Operational measures include:

   - Designating specific access points to the facility, and posting appropriate signage.
   - Screening persons and vehicles prior to entry.
   - Requiring acceptable identification, such as a valid driver's license or government issued identification card, for individuals prior to entry.
   - Designating restricted areas of the facility and grounds, and posting appropriate signage, to prevent or deter unauthorized access. Consider the presence of unauthorized persons in restricted areas to be a breach of security that requires immediate notification of management.
   - Limiting employee access to critical areas or assets of a facility based upon their job functions.
   - Updating employee shift rosters *(e.g., noting absences, replacements, etc.)* for supervisors at the start of each shift so they know who is expected to be on site.
   - Imposing increasingly stringent measures for accessing critical areas or assets of the facility.

2. **Establish Procedures for Access to Facility and Grounds by Visitors, Outside Contractors, Vendors:**

Limit access of the facility to non-company personnel, such as farmer-customers, outside contractors, vendors, truck drivers and others.

- **Designate specific areas for parking** for visitors, outside contractors and vendors.
- **Require visitors to check-in** with a designated company representative upon arrival; consider **posting signs** informing visitors of where to report in.
- **Maintain a visitor's log book** that requires sign-in upon entry, along with required identification, company name and purpose of the visit, and sign-out when departing. *(A sample form is provided in Appendix 1).*
- Consider using **name badges/tags, identification cards or other means** *(such as a special hat, etc.)* to identify visitors.
- **Restrict access** to grain storage, feed manufacturing, milling and grain processing areas. Do not allow visitors, including delivery personnel, contractors and vendors, to wander the premises.
- Consider adopting policies that **require visitors to be accompanied/escorted** by a company employee before being granted access.

3. **Secure the Facility's Handling/Processing Operations and Conveyances:** Based upon the results of the risk assessment, evaluate the physical operation of the facility, such as grain and product flows, and intervention points where human access could occur. Consider using one or a combination of the following:

- Consider developing and implementing a **pre-opening/start-up and closing security checklist** in which key employees are assigned to check critical security areas for signs of tampering, burglary, vandalism or suspicious activities. Such checks may include visual inspections of the perimeter of buildings and secured areas (such as dump pits; control rooms; inventory storage areas, doors and windows; equipment; power sources and electrical boxes; grain augers; and openings to exterior-located aeration fans, particularly if they are located in insecure areas or where lighting is insufficient). Note and rectify any discrepancies.
- Consider installing **locked gates on exterior ladders** to protect from unauthorized use and to prevent access to the top of storage tanks.
- **Cover and secure the receiving pit**.
- **Secure access doors to enclosed receiving pits and tunnels**.
- **Secure grain discharge spouts** (especially those used infrequently)**.**
- **Secure outside storage bins and containers holding finished products**. Alternatively, relocate containers to inside secure areas.
- **Consider additional surveillance** *(e.g., CCTV surveillance, periodic human observation, etc.)* **for outside grain piles, as well as grain and feed ingredient receiving pits**.
- For facilities storing liquids for application to grain or in further blending into feed or other grain products *(e.g., mineral, vegetable oil, animal fats, etc.)*, **consider securing the access points to the liquid storage tank, as well as controls and valves** *(both above and below ground level)* when not in use. These points may include manhole covers and valves used to fill and discharge the tank. If the tank is located outside of a building, consider what additional security methods, such as lighting, fencing or CCTV surveillance cameras, may be needed to minimize the potential for unauthorized access to the tank.
- **Secure doors to shop and tool storage areas**.
- **Restrict access to the facility's control room**, as well as computer process-control and data systems.
- **Safeguard information *(e.g., computer)* systems** with up-to-date anti-virus protection on computer server and individual operating units. Store back-up data offsite.
- **Secure access to power sources**, such as power rooms and electrical panels, to prevent unauthorized entry and power disruption or sabotage.
- Maintain current and accurate **inventory records** of grains, ingredients, finished feed and flour production, and animal drugs.
- If manufacturing feed and/or handling feed ingredients, **keep bagged ingredients, feed, flour and animal drugs in secured storage areas**. Similarly, flour or dry corn mills should consider storing enrichment and other minor ingredients in secure storage areas.
- For facilities performing mixing operations, **consider establishing controls to secure the points of entrance into the mixer**. These controls may include locking the mixer inlets during off-hours and/or performing a visual inspection of the interior

of the mixer prior to start-up. During operation, monitor the addition of ingredients and materials into the mixer.

- **Keep warehouse receipts, scale tickets, weight certificates, bills of lading, seals and other critical items in secured, locked storage** when not in use.

- **Establish a system for dispensing keys** to limit access to authorized personnel.

- **Consider changing door locks periodically**, especially in high-security areas or in secure areas at facilities with frequent employee turnover. Consider changing combinations and re-key these secure areas after employee terminations.

- **Lock all vehicles** parked outside the facility at night or during non-business hours. Remove keys from ignition switches when vehicle not in use.

- **Secure gates of vehicles** *(truck, rail)* during hours when facility is not operating or unattended.

4. **Review Security of Hazardous Substance Storage:** For areas used to store hazardous substances, such as fumigants, fertilizers, chemicals, fuel, ammonia, chlorine, flammable liquids, acids and other substances:

   - Conduct regular **inventory checks**.

   - Consider installing **industrial-design door hardware, such as higher-level locks and chains (case-hardened metal, if available), for areas where hazardous materials are stored**. Restrict access and availability of keys to authorized employees only.

5. **Periodically Meet with Police, Fire Departments and Emergency Responders:**

   - **Notify local law enforcement** authorities and emergency responders about the steps taken to enhance the **security of your facility and grounds**. Use a plant tour to familiarize them with the facility and its operations. Acquaint them with the: 1) types of products handled; 2) the location of all potentially hazardous materials; 3) exits and assemblage areas for employees and visitors in the event of an emergency; 4) service shut-off points for utilities or hazardous materials; and 5) hazard communication/documents; and 6) food defense regulatory requirements.

   - **Provide** law enforcement dispatchers with **current emergency contact information** for the facility.

   - **Post emergency contact information** in a conspicuous locations *(e.g. employee bulletin board, main entrance doors, outer office doors, etc.)* where it can be seen readily. Communicate this information and its posting location to employees.

   - Immediately **report unusual or suspicious persons, vehicles or activities** to local law enforcement.

6. **Restrict Access to Sensitive Information:** Be cautious about requests for information received by telephone or email. Do not provide information if the request appears suspicious or is from an unfamiliar person or organization.

   - Ask for such **requests** to be submitted **in writing**. Obtain as much information as possible from requestors with whom you are unfamiliar, including name, address, telephone number, references and reason for the request. Any reluctance by the requestor to provide such information should serve as a warning flag – don't cooperate further.

   - If there is any doubt about the appropriateness of releasing information – particularly information that might compromise security – refuse to provide it.

   - Companies with web sites should be cautious not to post sensitive, security-related information about the company, its operations, or facility layout or ingredient/product lines. **Do not display sensitive (such as facility diagrams) or private company information on company web site**.

   - Be discreet about sharing any information contained in the facility security plan or accompanying documents.

   - Control access to all information – including, but not limited to, documents, notes, photographs, diagrams and/or other work products – that contain sensitive, security-related information. Make sure such information is never left unattended by the originator or other authorized recipient. At the end of each workday, secure any such formation in a locked and controlled environment.

   - Sensitive, security-related information that is stored in electronic form should be maintained in a password-protected environment that is sufficiently secure from access by any unauthorized source. No sensitive, security-related information should be transmitted through unsecure email.

   - Verbal communication of sensitive, security-related information should occur in environments where only those with a legitimate "need to know" may hear it.

Part II.B

Operating and Personnel Procedures

Assess the feasibility of implementing the following steps to enhance the **security of the facility's operating and personnel procedures**:

1. **Employee-Hiring Practices:** When hiring:

   - **Request resumes** from applicants specifying their qualifications and references. Be cautious of applicants who offer incomplete information on employment applications.[1]

   - **Verify** that all employees and applicants are **U.S. citizens or have appropriate legal alien status and work authorization documents** issued by the U.S. Department of Homeland Security.

   - Depending upon the nature and sensitivity of the applicant's job function, **check with multiple references** for background checks to establish a prospective employee's qualifications and demeanor. Consider using commercial services to conduct pre-placement background security checks, which involve checks of police and motor vehicle records. Make sure the third-party service is reputable and uses procedures designed to protect against unlawful discrimination. *[Note: Under some state laws, applicants may need to sign an agreement to grant permission for such security checks.]*

   - For employees granted **access to secure areas, maintain higher requirements** for references, length of employment and other safeguards. Validate the authenticity of certificates issued to employees handling hazardous chemicals.

   - Be **wary of transient or seasonal employees**. Do not issue keys or access codes to employees who are seasonal or expected to be short-term. Consider immediately re-keying locks that secure sensitive areas if employees lose or leave with keys or were in a position to have copies made.

   - Check to **ensure that truck drivers**, if required, **have valid commercial driver's licenses** and other forms of identification *(e.g., current medical qualification certificates, etc.)*. Consider annually reviewing truck driver's driving records.

2. **Employee Training:** The most important threat-reduction measure is vigilance on the part of employees, their awareness of anything out-of-the-ordinary, and their prompt communication of that information to facility management or law enforcement personnel. Instill security awareness in all employees so that security becomes part of their job when communicating and interacting with visitors, customers, vendors, truck drivers and fellow employees.

   - Conduct **regular training** to discuss the facility's security policies and procedures, the areas of potential risk, and the location of emergency exit routes and service shut-off points for utilities, fuel, pipelines, fuel tank pumps, anhydrous ammonia, etc. Conduct refresher training periodically *(annually, etc.)* for existing employees; when hiring new employees; and whenever substantive changes to security policies or procedures are made.

   - Instill in employees their **responsibility for the safety of themselves and fellow employees in protecting the facility and equipment** from unauthorized persons.

   - Train employees to **recognize and report to management immediately any suspicious individuals** or abnormal behavior/activities, security breaches, suspicious materials or devices, and misplaced equipment.

   - Implement procedures to identify and address disgruntled employees or suspicious-acting outsiders. Encourage employees to report such incidents promptly.

---

[1] *From a legal perspective, employers should be mindful that the Equal Employment Opportunity Commission (EEOC) has a heightened sensitivity to discrimination made on the basis of religion and/or national origin, and is more likely to make probable-cause findings in response to allegations of this type. In hiring or disciplinary action, consistency in treatment and thorough documentation of actions taken are extremely important. Always treat similarly situated applicants or employees in the same, consistent manner, and always document the reasons for disciplinary actions or employment decisions.*

3. **Employee-Identification Practices:** Consider establishing an **employee identification system** through the use of name/photo badges, uniforms, hard hats with logos and names, or other methods – particularly in situations where the facility has a high employee turnover rate or uses temporary labor.

4. **Resignation/Termination of Employees:** Upon resignation or termination of the employee:

   - **Collect the departing employee's identification** cards, photos or other items that demonstrate employment with the company.

   - **Collect all keys** to vehicles, secured buildings and other secured areas that may have been issued to the departing employee.

   - **Collect cell phones, two-way radios and other company electronic devices** that may have been issued to the employee.

   - **Suspend access to information/computer systems** to prevent former employees from gaining access to sensitive information. This may involve changing passwords or other access codes for the facility's computer system.

   - **Inform customers when there is a change in the name of the employee servicing those accounts** to prevent unauthorized access to the customer's property.

   - **Update company records**, telephone lists, web sites and other materials that list employee names or authorize access to company facilities, shipments, records or other information.

5. **Outside Contractor/Vendor Policies:** When using outside contractors and vendors, consider the following procedures:

   - **Check background, references and insurance coverage** for outside contractors or other outside groups before granting access to the facility. In the contract with such parties, outline the parameters and conditions that apply to those assigned to the site.

   - **Inform** outside contractors **about established company safety and security procedures**. Conduct annual training/orientation for regular contractors to reinforce the facility's safety and security policies.

   - Consider whether to use **a pre-work checklist with individual contractors** to ensure they understand the facility's safety rules *(e.g., hot work permits, lock-out/tag-out procedures, etc.)*; areas of the plant where they are allowed access; and the need to actively manage their own personnel and the security of all materials and tools used at the worksite.

   - **Inform outside contractors about areas of the facility to which they are allowed access**.

   - **Require** outside contractors to sign in and be issued company credentials so they can be identified easily prior to being granted access to the facility.

   - **Consider requiring an employee escort for contractors using hazardous or dangerous materials** on site (such as chemicals or items that could be used as a weapon).

   - Consider stipulating that contractors use **only fresh, unopened containers when delivering pesticides and other agricultural chemicals** to the facility to minimize tampering risk.

6. Companies should work with suppliers of hazardous substances *(e.g., chemicals, fumigants, etc.)* to establish protocols to ensure that their orders cannot be diverted to another location or entity. This could consist of a procedure that requires official written notification from management to the supplier before changes to the delivery location is authorized for any hazardous materials.

Part II.C

Receiving and Shipping Procedures

The most frequent access to property and grounds by persons other than employees is during the unloading or loading of grains, feed, feed ingredients, flour and other products at the facility. The potential for intentional contamination of either inbound or outbound products also warrants attention. At other times – based upon the type of product being received or shipped – the security of loads in transit may need to be addressed.

Consider adopting one or a combination of the following procedures to secure the facility's receiving and load-out operations:

Receiving Procedures:

- **Know your suppliers**. Periodically obtain certificates of analysis from new suppliers or those from which inferior product has been received. Consider visiting new suppliers, particularly those providing significant types or quantities of ingredients/products. Request samples and review their security procedures for product handling and transport.

- **Know your farmer-customers:** Become familiar with the identity of your customers and their representatives/ employees to minimize unauthorized access or delivery of suspect products or ingredients.

- If the delivery is not from an established supplier or farmer-customer, **consider formalizing a customer-interview process before unloading and commingling commodities**.

- As part of the facility's standard start-up procedures, consider **checking outside receiving pits for evidence of tampering** prior to opening for business and before unloading product.

- **Sample, grade and weigh inbound** grains, oilseeds, feed ingredients and other agricultural commodities upon arrival/unloading; retain file samples for an appropriate period of time.

- It usually is advisable to **visually inspect** grain, ingredients or other products **upon receipt and prior to unloading**. For ingredients, check for uniform color and texture, as well as for odor, excess moisture, foreign objects and excessive heat. In addition, be aware that some of the substances that might be intentionally used to contaminate inbound grain or grain products are not easily detectable through visual examination, objectionable odors, etc.

- **Inspect inbound bagged ingredients** for tears, tampering, excess moisture and insect activity.

- **Be cognizant of relevant regulations** of the U.S. Department of Agriculture, Food and Drug Administration, Environmental Protection Agency, U.S. Department of Homeland Security and other federal/state agencies pertinent to inbound ingredients *(e.g., mycotoxins, prohibited mammalian protein, etc.)*.

- If seals are utilized on inbound shipments, check to make sure the seals have not been tampered with and verify that seal numbers are consistent with load numbers on bills of lading.

Load-Out Procedures:

- For **outbound shipments**, establish a system for **retaining file samples** for an appropriate, specified time period.

- Develop **standard operating procedures for inspecting the integrity and cleanliness** of truck trailers, railcars and barges before loading.

- If and when using seals, **record the seal numbers** on the bills of lading. Consider whether to utilize tamper-evident, tamper-proof or tamper-resistant plastic seals, or high-security cable seals. The decision on whether to utilize seals, as well as which seal to use, will depend upon the product being hauled, the mode of transport used and customer requirements. Each type of seal performs a different security function and varies in cost. If and when using seals, establish procedures for placing and verifying the placement of seals on conveyance openings. If receiving sealed conveyances, upon receipt check to ensure that the seals are intact and verify the seal numbers. *[**Note:** Shippers that have qualified for expedited entry across the Canadian or Mexican borders utilizing the U.S. Department of Homeland Security's Customs Trade Partnership Against Terrorism (C-TPAT) Program are required to affix high-security seals in conformance with International Standards Organization (ISO) guidelines (ISO/ PSA 17712)]*.

- For **managing the security of loads in transit**, the shipper has limited control, depending upon the mode *(truck, rail or barge)*, length of haul and the carrier involved:

  - For **truck shipments**, if operating your own fleet and hiring drivers, incorporate into regular training their responsibility to maintain load security and integrity during transit. Include recommended procedures to safeguard employees and cargo while unloading at a customer's location, such as precautions to minimize exposure to potential biosecurity hazards. If contracting with an outside trucking firm, consider including specific security language as part of the contract.

    Consider the following procedures, regardless of whether using your own truck fleet and crew of drivers, or using contract carriers:

    - **Restrict access to delivery schedules, routes and destinations** to employees on a need-to-know basis.

    - Instruct drivers picking up or delivering grain, feed or processed products **not to talk to unauthorized persons** about the delivery route, delivery schedule or ultimate destination of shipments. Instruct drivers to refer such questions to appropriate facility management for response.

    - Instruct drivers **not to allow unauthorized persons in the truck cab**.

    - Instruct drivers not **to deviate from planned routes or delivery schedules** unless notifying the dispatcher or office in advance.

    - Instruct drivers when parking delivery vehicles for other than loading or unloading operations to **park in well-lit and safe areas** where visibility with the vehicle can be maintained, and to **secure/lock** the vehicle. Do not allow driver schedules and delivery locations to be visible on dashboards or seats when vehicle parked and unattended.

    - Instruct drivers to be **alert to, and to report, suspicious activity** that may endanger the shipment.

  - For **rail shipments**, discuss the need for additional security measures during transit with the receiver or shipper. While there are physical mechanisms available to reduce the potential for – or to discourage – tampering, they may not provide complete control against willful acts of terrorism. In the case of rail shipments that might be in-transit for a lengthy time and subject to delays or stoppages, the shipper and receiver may wish to consider asking the carrier to provide additional monitoring of the load.

  - For **barge shipments**, in-transit security may be needed when barges are waiting to be loaded or unloaded. Shippers and receivers of barge products need to carefully evaluate the vulnerability of such loads to intentional contamination methods to enhance security.

Part II.D
Emergency Response Procedures

To protect employees and the facility, it's a good business practice – as well as a requirement under Occupational Safety and Health Administration regulations – to implement a written emergency action/response plan.

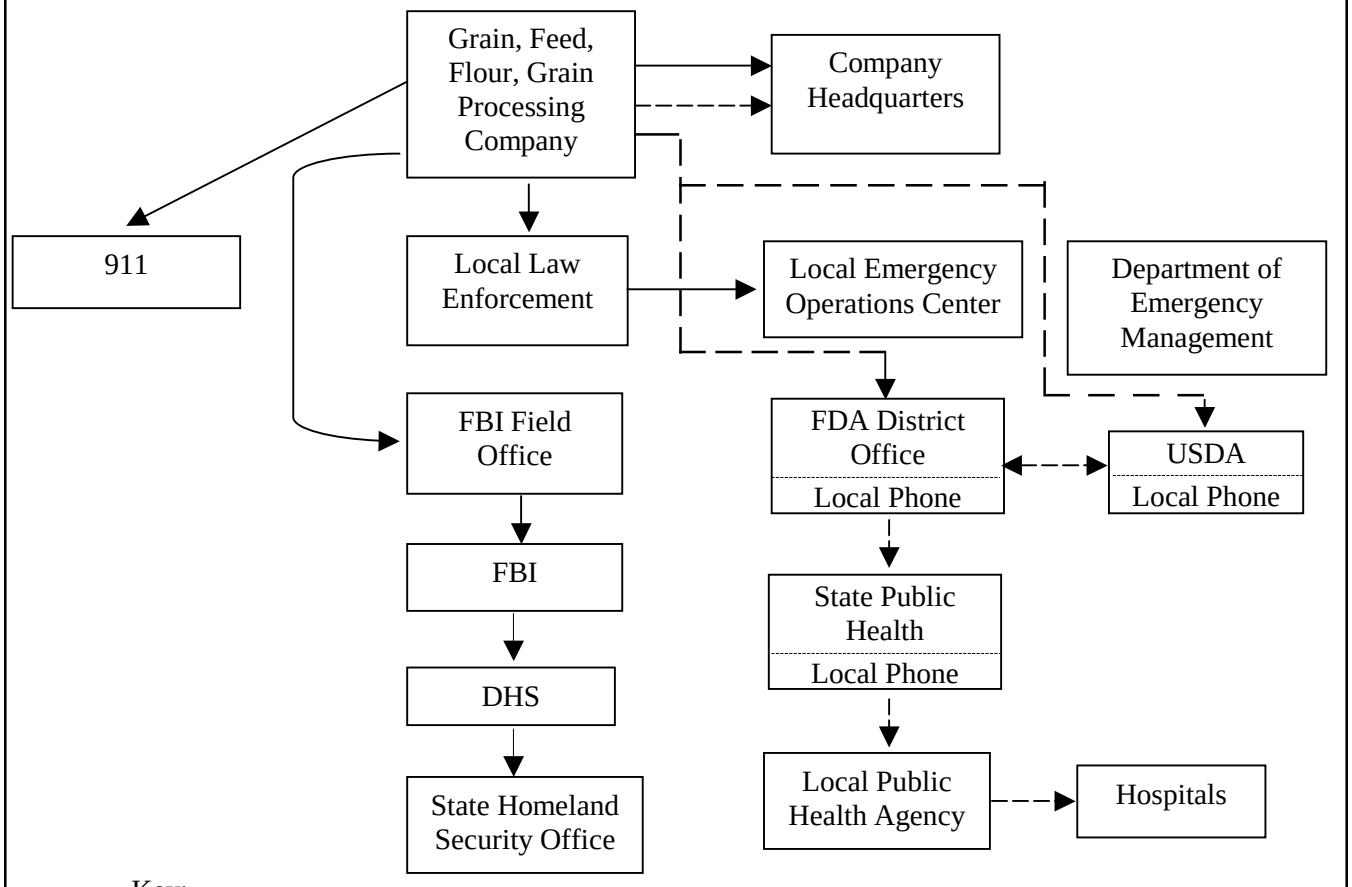
An emergency action/response plan identifies the specific responsibilities of employees in the event of a fire, explosion or other emergency at grain-handling, feed, milling and other grain-processing facilities. It also provides specific procedures for evacuating the working areas of the facility, contacting law enforcement and emergency responders, securing the scene and identifying witnesses in the event of suspicious circumstances.

The following elements should be considered as part of an emergency action plan:

- **Develop 'Decision Tree' and List of Emergency Contacts:** Consider developing a "decision tree" *(see accompanying schematic)* that maps out the list of law enforcement agencies, emergency responders, and local, state and federal government agencies that will be contacted in the event of an incident. Whom you contact may vary, depending upon whether the incident involves a deliberate or unintentional contamination of an agricultural commodity, feed or food product; a natural disaster (hurricane, flood, tornado, etc.); fire, explosion or other safety incident; or other type of emergency.

  Generally, the first point of contact for most incidents will be your local law enforcement agency (police, sheriff, etc.). Rescue/ambulance services, hospitals and

Sample Decision Tree in Event of Emergencies



utilities also may be high on the list of contacts in the event of a natural disaster or safety-related incident. The local FBI office and state police should be contacted — after local law enforcement is notified — if the incident is believed to be a criminal act, regardless of whether it involves an alleged terrorist or disgruntled "insider."

In the event of an unintentional contamination incident involving grain, feed, flour, processed commodities or food products, the local FDA office, USDA and state public health officials may require notification, particularly if the contamination rises to the level of a Class I recall. *[**Note:** FDA's recordkeeping regulations implementing the Bioterrorism Act of 2002 require that facilities be able to trace products one-step back to the previous immediate source and one-step forward to the next subsequent recipient.]*

In the event of an intentional contamination incident, local law enforcement agencies, in addition to the aforementioned government entities, should be notified. Contact information on insurance providers also is useful.

Be sure to keep the information current. Place the list at or near all phones in the facility, and consider laminating it to protect its durability. *[A sample form of Emergency Contacts is included in Appendix 1.]*

- **Develop List of Employee Telephone Numbers:** This is useful in the event of an emergency, and also should be kept current. *(A sample form is found in Appendix 1).*

- **Specify Type of Alarm System Used:** Specify the type of alarm system used at the facility *(standard fire alarm, visual alarm with flashing lights, etc.)* and the types of signals used for various emergencies *(fire or explosion, tornado, general evacuation, etc.).*

- **Develop/Use Visitor Log:** As noted previously, maintain a visitor log to facilitate evacuation in the event of an emergency. *[A sample form is included in Appendix 1.]*

- **Specify Employee Assignments:** Specify the assignments for each employee responsible for performing essential facility shut-down procedures prior to exiting the property based upon their job functions. Include any actions needed to address suspected contamination, tampering or other food-security concerns.

- **Establish and Specify Emergency Escape Routes:** Escape routes from all working areas of the facility should be established and communicated to all employees, outside contractors or visitors who may be located at the plant.

- **Designate Rendezvous/Assemblage Areas:** Consider posting a site plan designating escape routes, rendezvous/assemblage areas, and firefighting and rescue equipment. Designated company officials should be assigned the responsibility for escorting any visitors to designated assemblage areas in the event of an emergency.

- **Conduct Employee Training:** As part of the emergency action/response plan, specify the type and frequency of training for each of the following: 1) hazard detection and recognition; 2) fire detection and reporting; 3) recognizing suspicious activity and reporting to management; 4) location of alarm and firefighting equipment; 5) use of self-contained breathing apparatus and first-aid kits; 6) emergency exit routes and assemblage areas; and 7) assignment of individual employee responsibilities. Periodic drills and exercises can assist in ensuring adequate knowledge on how the emergency action/response plan is to operate.

  Also keep employees informed about the nation's color-coded threat level as determined by the U.S. Department of Homeland Security (DHS), as well as when changes to the threat level are made. Higher threat levels may require enhanced security measures commensurate with the increased risk posed.

Conclusion

The aforementioned guidance does **not** constitute formal recommendations. Nor is it designed to be a comprehensive compilation of all security issues confronting grain storage facilities, feed mills, flour mills, grain-processing plants or other agribusinesses. Rather, it provides a "menu" of ideas and concepts that can be considered as part of a facility risk-assessment and security plan.

A reminder: It is extremely important when developing or modifying a facility security plan to select those procedures that are effective, practical and realistic for the type and characteristics of the facility for which they are intended, as well as the physical surroundings in which the plant operates. There is no "one-size-fits-all" approach when it comes to facility security; different plans may be appropriate for different facilities operated by the same company based upon the circumstances and conditions present. In addition, it is extremely important that you select facility-security measures that are achievable and that will be implemented.

Appendix 1

SAMPLE FORMS

- **Sample Emergency Responder Telephone List**
- **Sample Employee Emergency Telephone List**
- **Sample Visitors' Log**

Sample Emergency Responder Telephone List

Company Manager _____
Assistant Manager _____
Superintendent _____
Other _____

Agency	Phone Number	Contact Person
Police/Law Enforcement		
Local Police:	_____	_____
Sheriff:	_____	_____
Local FBI Office:	_____	_____
State Police/State Patrol:	_____	_____
Fire Department:	_____	_____
FBI Headquarters	202-FBI-3000	
Rescue Squads / Medical Personnel		
Ambulance:	_____	_____
Physician:	_____	_____
Hospital:	_____	_____
Trauma:	_____	_____
Local Poison Control Center:	_____	_____
National Poison Control Center:	1-800-441-8080	
Food and Drug Administration		
Local Office:	_____	_____
Regional Office:	_____	_____
FDA Information Hotline:	1-888-723-3366	
Centers for Disease Control:	1-800-311-3435	
U.S. Department of Agriculture		
Kansas City Commodity Office:	_____	_____
Chemical		
Chemical Transportation Emergency Center (Chemtrec):	1-800-424-9300	
Toxic Substances Control Hotline Number:	_____	_____
Poison Control Center:	_____	_____
CropLife America:	202-296-1585	
Agricultural Retailers Association:	202-457-0825	
Utilities		
Gas:	_____	_____
Water:	_____	_____
Electricity:	_____	_____
Specialty Contractors		
Inert Gas Suppliers:	_____	_____
Cranes:	_____	_____
Helicopters:	_____	_____
Cutting Equipment:	_____	_____
Excavation Equipment:	_____	_____
Salvage Operators:	_____	_____
Insurance Company:	_____	_____
U.S. Coast Guard:	_____	_____

Employee Emergency Telephone List

Employee Name	Home Telephone Number	Cell Phone	Name of Person to Contact in Emergency	Emergency Contact's Telephone Number (if different than home)

Visitors' Log

Visitor's Name	Company Name	Telephone Number	Purpose of Visit	Area of Facility to be Visited	Time In	Time Out
(Print Name) *(Signature)*						
(Print Name) *(Signature)*						
(Print Name) *(Signature)*						
(Print Name) *(Signature)*						
(Print Name) *(Signature)*						
(Print Name) *(Signature)*						
(Print Name) *(Signature)*						

Appendix 2

Facility Security Plan Template

Facility Security Plan

for the

Name of Company

Address

City, State

Important Notes for Managers

This appendix contains a sample Facility Security Plan Template. It is designed to provide a starting framework managers can use to develop a Facility Security Plan tailored to their specific facilities and operations. This template is designed to be used in conjunction with this guide – particularly the ideas and concepts presented in Part II – as well as the facility's existing standard operating procedures and any facility security plan that already may be in place.

The design is intended to be adaptable to new security regulations or programming so that one document will allow for compliance with all regulations or programs (understanding that some, like those issued by the Maritime Transportation Security Administration, require a regulation-specific plan).

In this template, draft examples of various policies and procedures are shown that reflect the concepts contained in Part II of this guide. This draft language is for sample purposes only, and should be modified or expanded upon to reflect the specific security policies and practices implemented at your specific facility. As noted below, such policies and procedures should be developed only after a security survey and risk assessment of the facility is conducted.

Also importantly, this template is designated as "Sensitive Security Information" (SSI) under federal law, and is **not** to be distributed or released to persons who are not in a "need-to-know" status within your company. This template also is available electronically in a "fill-in-the-blank" format by clicking here.

Helpful Steps in Developing a Facility Security Plan

There are several important steps in developing a facility security plan:

- **Step 1:** Conduct a risk assessment of the facility.
- **Step 2:** Do a "gap analysis." That is, use the results of your facility risk assessment to identify vulnerabilities or "high-risk" threats that may exist. See Part I of this document for guidance on how to perform a risk assessment.
- **Step 3:** Develop mitigation strategies to reduce "real" risks identified through the risk assessment. Make sure these mitigation strategies are practical and effective, cost-effective, and sustainable over time.
- **Step 4:** Develop a policy on how the facility's security infrastructure will be monitored and maintained.
- **Step 5:** Put the security plan in writing. Specify the policy that will govern periodic reviews and updates to the policy, as well as how and where it is to be retained and to whom it is to be distributed.

- **Step 6:** Purchase and install any security devices or equipment deemed to be necessary, cost-effective and prudent that have been identified through the risk assessment.

- **Step 7:** Train and educate facility personnel on the security plan. It is suggested that refresher training occur annually, as well as whenever the security plan is updated or changed. Consider maintaining a record of training, indicating the date, employees trained and subject matter covered.

- **Step 8:** Develop an audit system for monitoring the security plan, and the specific components applicable to each person's job function and responsibilities.

Section 1
Facility Description and Location

Address of Facility: _____

GPS Coordinates for Facility: _____

Site Plan of the Facility and Grounds: Site plan, including photos of key areas, is attached to this section.

Flow Diagram of Facility: A flow diagram of the facility's handling, processing operation is attached to this section. *[See sample flow diagrams in Appendix 3 of this guide.]*

Brief Description of Facility Location: _____
_____
_____
_____
_____
_____

[Draft Example: XYZ Grain Co. occupies a two-acre lot located at the intersection of ___ St. and ____ Ave. Primary facets of the operation consist of: 1) an office housing administrative personnel and grain sampling and weighing equipment, 2) six grain bins with a combined storage capacity of xxx million bushels; 3) a xx-bushel flat storage structure located across the road from the main facility; 4) emergency storage of raw grain located approximately 1 mile from facility; and 4) a feed mill with a capacity to manufacture xxx tons of feed a year. Facility also consists of a truck dump pit for receiving raw ingredients that include corn, soybeans and ingredients (potassium chloride, 18% dical phosphate and zinc phosphate); warehouse storage (30,000 sq. ft.); outside-located liquid storage tank; motor control room; visitor parking lot; employee parking lot.]

Description of Operation/Activities of Facility: _____
_____
_____
_____
_____
_____

[Draft Example: This facility is a country elevator and feed mill. The country elevator operation receives grains and oilseeds from farmers from a six-county region in the state of _____. The facility's annual average throughput is XXX million bushels. The feed mill operation is a premix facility that manufactures swine feed for commercial integrators. The facility receives commodities and ingredients by truck, and ships outbound products by truck using contract carriers and by rail unit trains. This facility sources all of its ingredients from domestic suppliers, with the exception of vitamins used in premix feed, which are imported.]

Section 2
Facility Risk Assessment Outcomes

Description of Method Used to Conduct Risk Assessment: _____
_____
_____
_____
_____

[Draft Example: Facility management convened a team consisting of the plant superintendent, feed mill operator, dump pit/scale operator and truck driver on (insert date) to identify and evaluate potential risks to the facility that could be posed by an outside attacker or disgruntled employee. This team also conducted a security survey of the facility. The team subsequently met and reached consensus on critical assets and significant risks/threats identified below.]

Critical Assets Identified: _____
_____
_____
_____

[Draft Example: Through the risk assessment process, the following key assets were identified that are critical to this facility's operation: 1) electrical generation station located at _____; 2) grain/ingredient receiving area; and 3) batch mixer. Through this risk-assessment process, the team also identified several factors that reduce the risk to this facility, including: 1) the facility's limited size; 2) a small number of employees; 3) the facility's location in a rural town of less than 50,000 people; 4) there are no businesses in close proximity to the facility that present a viable target for physical attack; 5) the facility is located in an area relatively free of crime; and 6) the facility has a good, ongoing working relationship with local law enforcement authorities.]

Significant Risks/Threats Identified: _____
_____
_____
_____
_____

[Draft Example: As a result of this risk assessment, the following potential risks/threats to the facility were identified: 1) unsecured/uncovered grain dump pit during overnight hours when facility not in operation; 2) uncovered emergency storage for raw grain; 3) unsecured liquid feed storage tank; and 4) the on-site storage of hazardous chemicals.]

Section 3
Personnel Security Procedures

Employee-Selection Policy: The following policies apply when selecting prospective employees to work at this facility: *[See Part II.B., page 15-16 of this guide.]*

_____
_____
_____
_____

[Draft Example: All potential employees are required to submit resumes prior to job interviews. Management verifies that all employees and applicants are U.S. citizens. Depending upon the nature and sensitivity of the job function, facility management checks with multiple references and conducts background checks.]

Contractor/Vendor Selection Policy: The following policies apply to contractors and vendors used at this facility: *[See Part II.B., page 15-16 of this guide.]*

_____
_____
_____
_____

[Draft Example: Background, references and insurance coverage for outside contractors are checked prior to granting access to the facility. Outside contractors and vendors are informed about established company safety and security procedures, including the areas of the facility to which they are allowed access. Outside contractors are required to use only fresh, unopened containers when delivering pesticides or other agricultural chemicals to minimize the risk of tampering. Outside contractors and vendors are required to arrive during normal working hours, are subject to screening and are required to sign in. Such persons are required to wear company-issued badges so they can be recognized while on site.]

Employee Training: The following policies apply to employee training on security-related matters at this facility: *[See Part II.B, pages 15-16; and Part II.D., pages 19-21 of this guide.]*

_____
_____
_____
_____

[Draft Example: All employees are trained annually on the security measures in effect at this facility, as well as whenever substantive revisions to the security plan are made that affect the specific area(s) to which individual employees have access. Such training includes the facility's security policies and procedures, the areas of potential risk, the location of emergency exit routes and service shut-off points for utilities, fuel, pipelines, fuel tank pumps and anhydrous ammonia, etc. Employees also are trained to be vigilant and to report any unauthorized or suspicious person or activity, including disgruntled colleagues, to management immediately.]

Employee Resignation/Termination Policies: _____

_____

_____

_____

_____

[Draft Example: Upon resignation or termination of employees, management collects all employee identification badges, keys, cell phones and two-way pagers that may have been issued to the employee. In addition, the passwords previously used by the employee to access the company's information/computer network are changed. Company employee rosters are updated to reflect the change, and customers previously served by the employee are notified about the name of the newly assigned employee who will be servicing the account.]

Section 4
Computer/Information Technology Security

Description of Computer/Information Technology/Security System: The following computer system and security technology is used at this facility: _____
_____
_____
_____

[Draft Example: This facility uses (describe nature of the information/computer system or network used at the facility). All employees utilizing computers have individual personal computers with individual accounts, and use individualized sign-on passwords to access the system. All passwords are changed on a _____ (e.g., quarterly, semi-annual) basis. Violations of the facility's computer policy and unauthorized access are investigated.

The company also maintains a publicly accessible website. But no sensitive, security-related information is posted about the company, its operations, the facility layout or operations, or ingredients or product lines that are received, stored or manufactured.]

Document/Records Control, Retention and Destruction Policy: The following policies apply to the control, retention and destruction of different kinds of documents and records at this facility: _____
_____
_____
_____

[Draft Example: All information – including, but not limited to, documents, notes, photographs, diagrams and/or other work products – that contain sensitive, security-related information are never left unattended by the originator or other authorized recipient. At the end of each workday, any such information is to be secured in a locked and controlled environment. Such information that is stored in electronic form is maintained in a password-protected environment that is sufficiently secure from access by any unauthorized source. No sensitive, security-related information may be transmitted through unsecured email. In addition, verbal communication of sensitive, security-related information is to occur in environments where only those with a legitimate "need to know" may hear it.]

Section 5
Physical Security Systems/Infrastructure

The following measures and procedures protect the physical security of this facility *[See Part II.A., pages 12-14 of this guide]*:

Locks/Key Control: _____

[Draft Example: The facility manager is responsible for the issuance of, and accountability for, all keys. A master key that opens all facility doors is issued only to designated supervisors. A total of ___ (insert number) keys is issued, based upon necessity. Keys to parts of the facility that have been designated secure areas are issued only to employees authorized to work in such spaces. A sign-out log is used for issuance of temporary keys. Upon resignation or termination of employees, management collects all keys issued to employees. If keys are lost or stolen, attempts are made to recover such keys before locks are changed. All external and internal windows, gates and fences are secured with locking devices.]

Fence and Gates: _____

[Draft Example: This facility is equipped with a fence, X-feet high. Two main mechanical (roll-away) gates, each equipped with an outrigger and barbed wire, constitute the main access gates (one in front and the other at the rear of the facility). The two gates are activated electronically from the office or a key pad near the gate. All fence and gates are in excellent condition, and are monitored periodically to protect against security breaches at designated security areas.]

Or

[Draft Example: This facility does not utilize fencing as part of its layered approach to security. The risk assessment revealed that such a step would not enhance security or be cost-effective at this location.]

Security Lighting: _____

[Draft Example: The facility has sufficient lighting, comprised of metal halide, mercury vapor and high-pressure sodium industrial lights mounted 360-degrees on poles throughout the parking lot, and on the walls of the building.]

Electronic Access Control and Alarm Monitoring: _____

[Draft Example: Electronic access cards are required for entry to petroleum-storage area.]

Intrusion-Detection Systems: _____

[Draft Example: Motion-detection devices are installed at the entry and in portions of the facility designated as secure areas. These devices are activated during non-working hours.]

Contract Alarm Monitoring Service: _____

[Draft Example: This facility has contracted with _____ (insert name of outside security firm) to monitor its intrusion-detection system during non-working hours. If the alarm is triggered, it notifies the outside security service.]

Video Surveillance: _____

[Draft Example: There are two CCTV cameras mounted at the facility. One monitors the entrance, while the other monitors the exit. The cameras are overtly mounted on poles, and provide a digital feed direct to the office. There is a backup power supply to prevent outages. The CCTV system is monitored and maintained by company officials. If an incident occurs during non-working hours, recordings are used to retrieve evidence.]

Monitoring and Maintenance Procedures: _____

[Draft Example: The company's maintenance crew conducts scheduled maintenance of the security system and its components.]

Other Measures: _____

Section 6
Access-Control Procedures

The following procedures have been implemented at this facility to allow entry only to authorized personnel, as well as to designate specific sensitive areas of this facility that are to be accessed only by authorized personnel. *[See Part II.A., pages 12-14 of this guide]*:

Signage: _____

[Draft Example: Appropriate signage has been posted at the facility, including those indicating "no trespassing," "private property," "visitor parking," "no vehicles beyond this point," and "close-circuit TV surveillance."]

Access Procedures Governing Personnel:

- Employees: _____
- Outside Contractors: _____
- Vendors: _____
- Visitors: _____

[Draft Example: The manager and employees are granted access to the facility; photo identification does not need to be displayed, but must be on their person. Personnel from outside contractors and vendors are required to arrive during working hours, must notify management upon arrival, display valid photo identification, sign in on a company log book and be issued a company hard hat. Contractors and vendors are subject to screening. Visitors are required to arrive during working hours, display valid photo identification, sign in on the company log book and must be escorted by company personnel at all times. In addition, facility employees are trained about the plant's access-control procedures.]

Access Procedures Governing Vehicles (parking location, tags):

- Employees: _____
- Outside Contractors: _____
- Vendors: _____
- Visitors: _____

[Draft Example: Employees and visitors are required to park in designated spaces marked for their use with signage.]

Restricted Access Areas: _____

[Draft Example: This facility designates specific areas as restricted-access areas to prevent or deter unauthorized access, protect persons present at the facility, protect the facility itself, protect the safety of products handled, manufactured and shipped, and prevent unauthorized access to product storage areas. All restricted-access areas are clearly marked by signage. Unauthorized personnel found in restricted-access areas constitute a breach of security, requiring immediate notification of management.

The following areas at this facility have been designated as restricted access areas (list):
_____
_____
_____
_____*.]*

Section 7
Grain, Feed, Food Product Defense-Specific Measures

The following practices and procedures are in effect to protect grain, grain products, feed and food from contamination incidents that could endanger human or animal health. *[See Part II.C., pages 17-18 of this guide]*:

Supply Chain Procedures: _____

_____

_____

[Draft Example: This facility maintains a list of approved suppliers. Certificates of analysis are requested from new suppliers of ingredients, as well as from those whose products have been found to be inferior in the past. New suppliers are visited, during which time they are briefed on the facility's security procedures for product handling and transport. This facility also has a policy of becoming familiar with farmer-customers and those who may deliver grain on their behalf at harvest, so as to minimize unauthorized deliveries.]

Product-Receiving Procedures: _____

_____

_____

[Draft Example: Inbound grains, oilseeds and ingredients are sampled, graded and weighed upon arrival. These products also are inspected visually prior to unloading, checking for uniform color and texture, as well as odor, excess moisture, foreign objects and excessive heat that may indicate contamination. File samples are retained for an appropriate time. All inbound bagged ingredients are inspected for tears, tampering, excess moisture and insect activity. If seals are used on inbound shipments, the seals are checked prior to unloading to ensure they have not been tampered with and that the seal numbers are consistent with the load numbers on the bill of lading.

Further, at the start of the first work shift following a period during which the facility has been closed, the outside receiving pits are checked for evidence of tampering prior to opening for business.]

Product Load-Out Procedures: _____

_____

_____

[Draft Example: For outbound shipments, the integrity and cleanliness of the conveyance is checked before loading. If seals are used, the seal numbers are recorded on the bill of lading. This facility operates its own truck fleet, and its drivers are trained about their responsibility to maintain the security and integrity of the load during transit. Access to delivery schedules,

routes and destinations is restricted to employees on a need-to-know basis. Drivers also are trained not to talk to unauthorized persons about the delivery route, delivery schedule or ultimate destination of shipments, and are prohibited from allowing unauthorized persons to enter the truck cab. They also are instructed not to deviate from planned routes or delivery schedules; to park in well-lit and safe areas; to lock the truck cab and secure the cargo if the truck will be unattended for a period of time; and to report any suspicious activity to management.]

Policies on Compromised Conveyances, Containers, Seals: _____

_____

[Draft Example: Seals are to be removed utilizing bolt-cutters or snips only by an authorized facility employee. If the employee suspects that a sealed conveyance or container, or the seal itself, has been compromised or tampered with, he/she is to notify management and await further instructions before unloading or loading the conveyance or container.]

Section 8
Emergency Contact Information

Note the names and emergency contact information for the each of the following. *[See Appendix 1, pages 22-25 of this guide]*:

Key Personnel and Contact Information:

_____
_____
_____
_____

24-Hour Contact at this Facility: _____
_____
_____

Emergency-Responder Contacts: *[See sample form in Appendix 1]*

_____
_____
_____
_____
_____
_____
_____

Key Regulatory Agency Contacts: *[See sample form in Appendix 1]*

_____
_____
_____
_____
_____
_____
_____

Contacts for Reporting Suspicious Activity/Incident: _____
_____
_____
_____

Section 9
Emergency Response Procedures

The following emergency-response procedures apply to incidents that may occur at this facility *[See Part II.D., pages 19-21 of this guide]*:

Suspicious Activity: _____

[Draft Example: Employees at this facility are trained to be alert to suspicious activity, and are directed to report any such activity to management immediately. Particular focus for such awareness is at shipping and receiving areas; mail processing; and parts of the facility designated as secure areas.]

Phone/Internet Threats: _____
_____
_____

[Draft Example: Employees are to report threatening communications receive via telephone, email or other electronic means to management immediately for possible referral to law enforcement authorities.]

Breach of Security *(instances involving persons bypassing security or being detected in a restricted-access area of the facility with the intent to do harm)*:
_____
_____
_____
_____

[Draft Example: Employees who detect unauthorized persons at the facility are directed to report such incidents to management immediately. In the event of unauthorized access, management will investigate the nature of the event and determine whether to report the incident to local law enforcement personnel.]

Workplace Violence: _____
_____
_____
_____

[Draft Example: Employees are to report any suspected incidents of workplace violence or harassment to management immediately for action.]

Violent Intruder/Event:

_____

_____

_____

_____

[Draft Example: Employees should immediately notify 911 and contact management if detecting a violent intruder. To protect personal safety, do not attempt to detain such an intruder.]

Food/Feed Defense Incident:

- Response to Report of Threat to Facility that Could Compromise Food/Feed Product Safety:

  _____

  _____

  _____

- Response to Actual Product Contamination Incident that Could Endanger Human or Animal Health:

  _____

  _____

  _____

[Draft Example: Employees who detect an actual or suspected contamination of the grains/oilseeds handled or stored, or the products manufactured, at this facility are to alert management immediately. Management will determine next steps, which may include, but not be limited to, sampling and testing of the suspect product, alerting local law enforcement and appropriate state and federal regulatory agencies, and conducting a product recall if any of the suspect product has been distributed in commerce.]

Other Issues *(identify other critical high-risk issues identified during the risk assessment)***:**

_____

_____

_____

Section 10
Facility Security Plan Audit/Review

The following procedures apply to auditing and reviewing the facility security plan periodically:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

[Draft Example: Management is responsible for ensuring that the security plan is maintained, and reflects the actual conditions of the facility and its operations. An annual review of the security plan is required. The annual review consists of an assessment of the plan and a site security check. The review is documented using an audit form, a copy of which is maintained in a secure area of the facility. Plant managers are required to evaluate the results of the security review to determine what, if any, changes need to be made to the plan.]

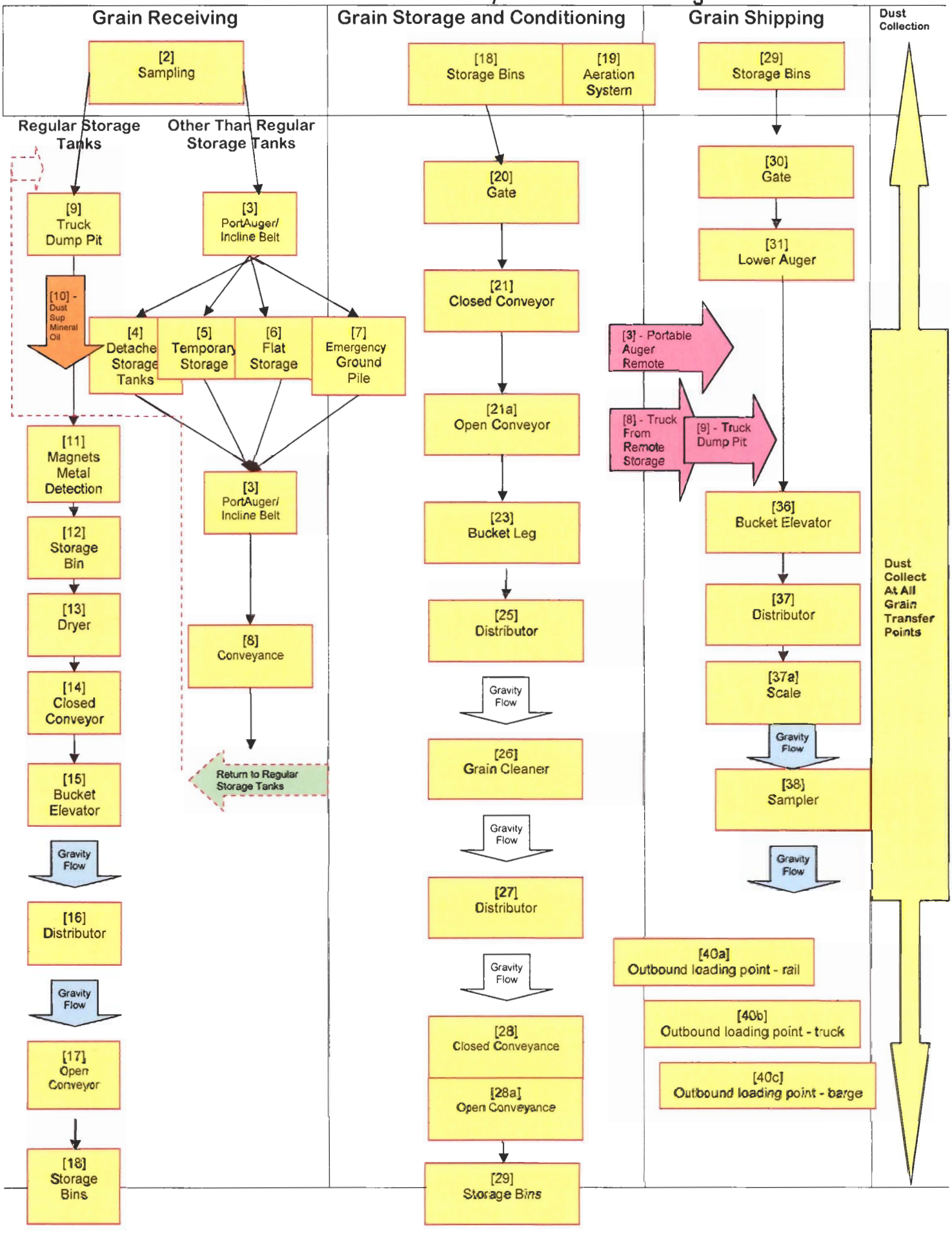
Sample Security Plan Audit Form

Subject	Date	Initials
Section 1: Sensitive Security Information *(Reacquaint with confidential nature of plan)*	_____	_____
Section 2: Facility Description and Location *(Verify information correct; update photos/ flow diagram, description if necessary)*	_____	_____
Section 3: Facility Risk Assessment *(Reacquaint with method used; update any critical assets/significant threats)*	_____	_____
Section 4: Personnel Security *(Review employee selection, training and termination policies; contractor/vendor policies)*	_____	_____
Section 5: Computer/Information Technology Security *(Reacquaint with information technology and and document control, retention and destruction procedures)*	_____	_____
Section 6: Access-Control Procedures *(Reacquaint and verify policies regarding locks/key control; security lighting/fencing; and security systems)*	_____	_____
Section 7: Product-Defense Measures *(Review and reacquaint with procedures applying to suppliers, receiving and load-out, and conveyances/seals)*	_____	_____
Section 8: Emergency Contact Information *(Review and update list of personnel and emergency responders, regulatory agencies and local, state and federal law enforcement officials)*	_____	_____
Section 9: Emergency Response Procedures *(Review and reacquaint with procedures for identifying and reporting suspicious activity, security breaches and workplace violence)*	_____	_____

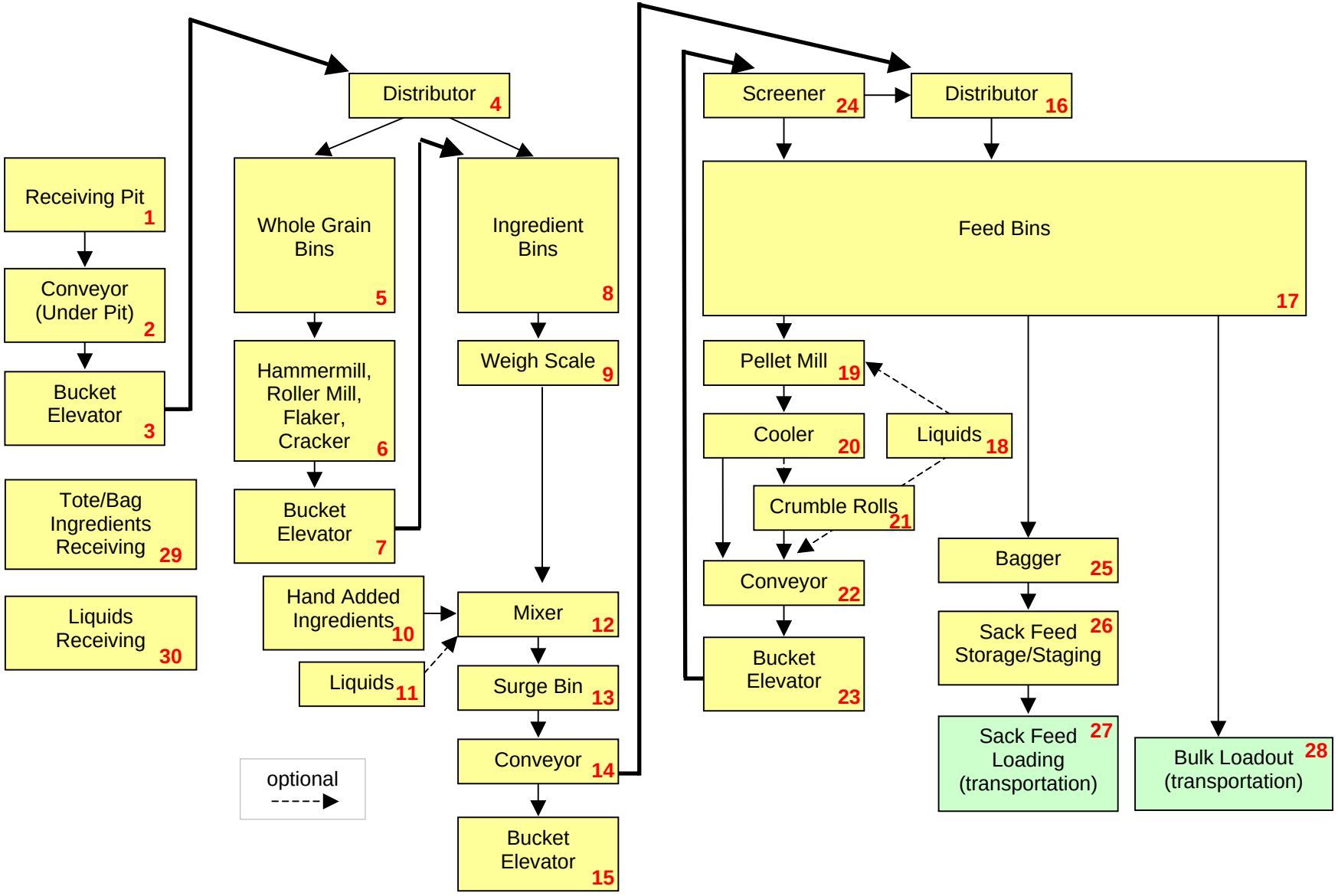
Appendix 3

Sample Generic Facility Flow Diagrams

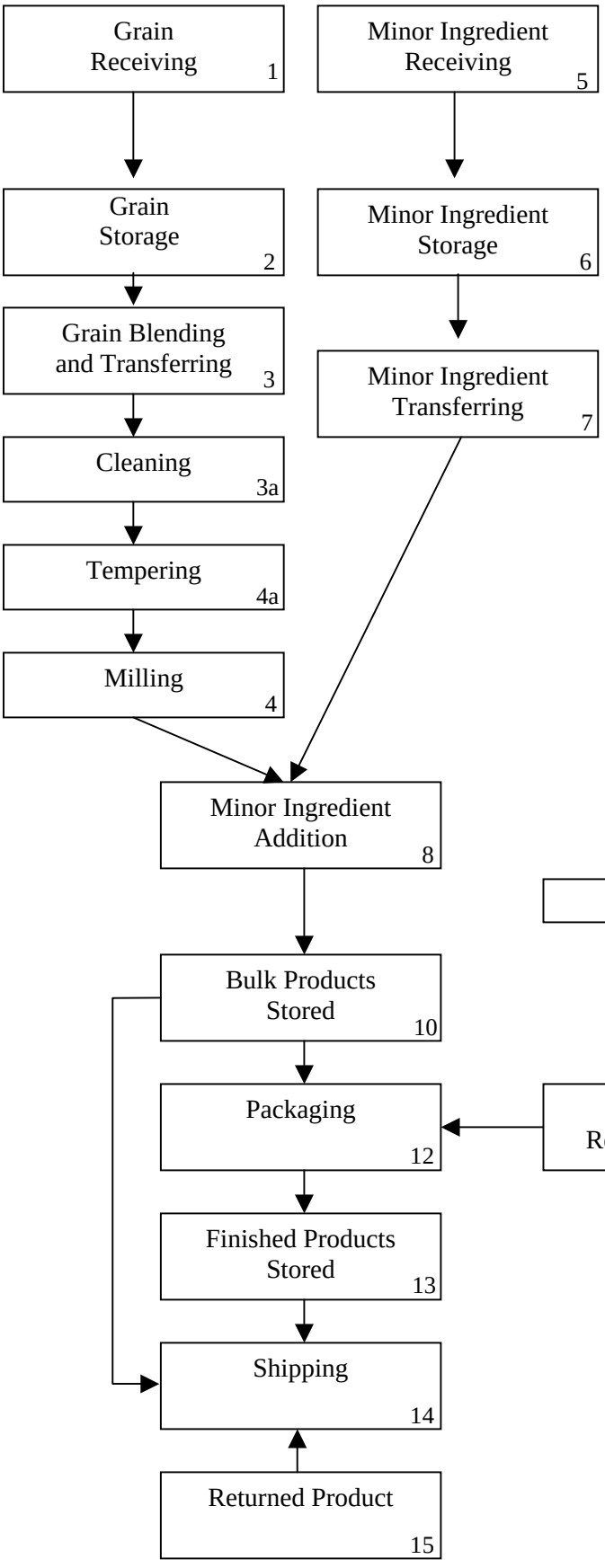
Generic Bulk Grain Country Elevator Flow Diagram



Generic Feed Mill Flow Diagram



Generic Flour Mill Flow Diagram



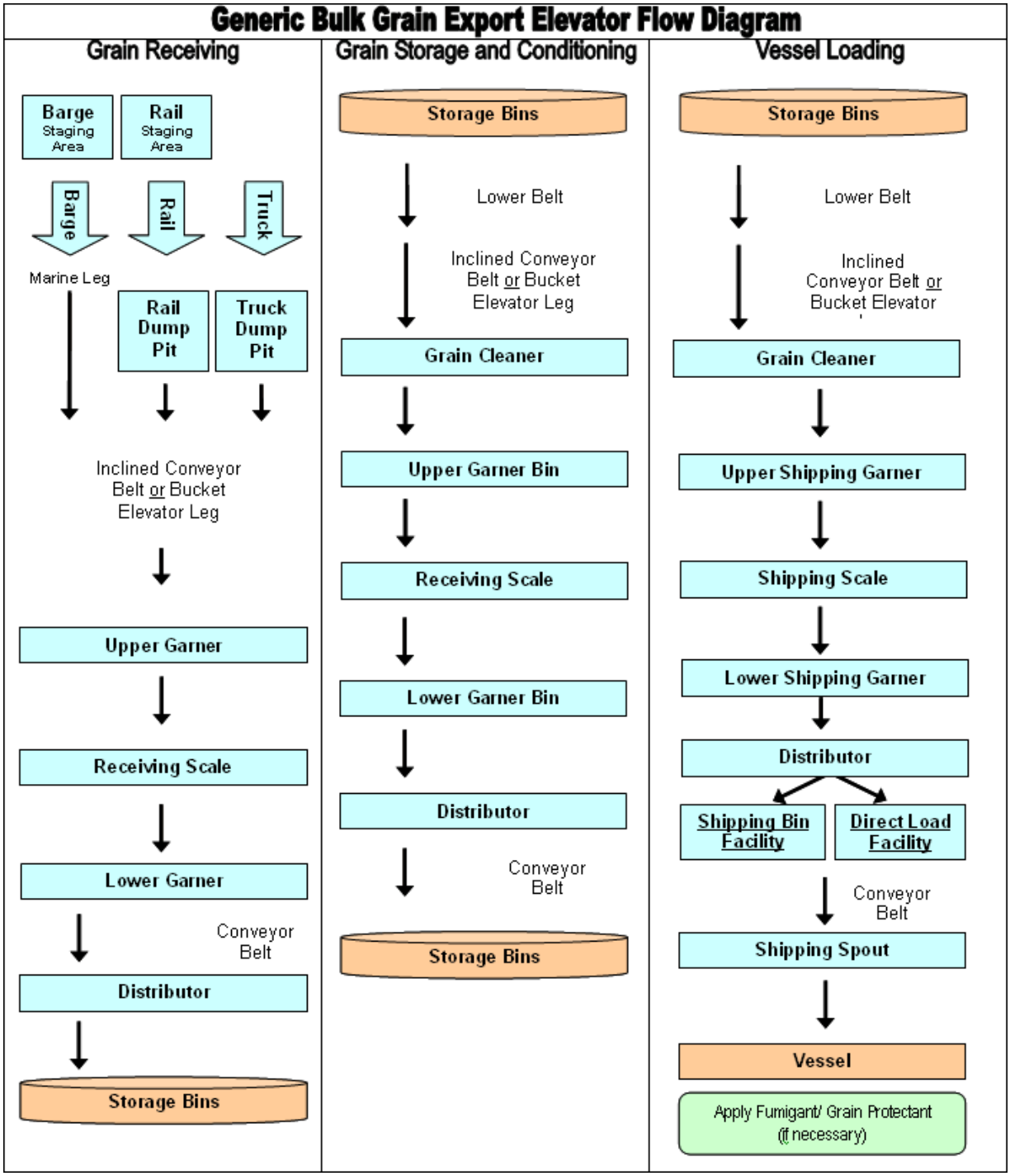
Grain received in barges, rail cars and trucks (usually open top). Additives and packaging received in bulk trucks, common carries, less than load (LTL) trucks and special deliveries (UPS, FedEx etc.)

Grain stored in concrete or metal silos, additives stored palletized in warehouse or main plant.

Grain transferred in both opened and closed conveying systems. Additives conveyed mostly in closed systems or in original packaging.

Bulk Loadout – wheat flour and corn meal; Finished Products – palletized and shipped from warehouse.

Received at the finished products warehouse according to the inspection of incoming shipments procedures. Placed on hold pending final disposition.


Generic Bulk Grain Export Elevator Flow Diagram
Grain Receiving
Barge Staging Area
Rail Staging Area
Barge
Rail
Truck
Marine Leg
Rail Dump Pit
Truck Dump Pit
Inclined Conveyor Belt or Bucket Elevator Leg
Upper Garner
Receiving Scale
Lower Garner
Conveyor Belt
Distributor
Storage Bins
Grain Storage and Conditioning
Storage Bins
Lower Belt
Inclined Conveyor Belt or Bucket Elevator Leg
Grain Cleaner
Upper Garner Bin
Receiving Scale
Lower Garner Bin
Distributor
Conveyor Belt
Storage Bins
Vessel Loading
Storage Bins
Lower Belt
Inclined Conveyor Belt or Bucket Elevator
Grain Cleaner
Upper Shipping Garner
Shipping Scale
Lower Shipping Garner
Distributor
Shipping Bin Facility
Direct Load Facility
Conveyor Belt
Shipping Spout
Vessel
Apply Fumigant/ Grain Protectant (if necessary)

Appendix 4

Links to Facility Security-Related Information

NGFA/GEAPS Facility Security Website: http://www.ngfa.org/security/home.html

- Security Alerts and Notices
- Federal Government Security Regulatory Requirements
- Facility Security Education/Guidance/Training Materials
- What Applies to My Facility?

American Institute of Bakers

- Food Defense Resource Center: www.aibfooddefense.org

Centers for Disease Control: www.cdc.gov

- Search: "Workplace Violence"

U.S. Department of Agriculture: www.usda.gov

- Search for "Security," "Security Inspections," "Model Security Plans

U.S. Department of Labor – Occupational Safety and Health Administration: www.osha.gov

- Search "Workplace Violence"

U.S. Food and Drug Administration:

- Center for Food Safety and Applied Nutrition: www.cfsan.fda.gov

Appendix 5

Glossary of Facility Security Terms

The following are frequently used terms pertaining to facility security:

Access Control(s): One or a combination of procedures or methods that restrict the movement of persons into or within a secure or protected area so as to allow entry only to authorized persons or vehicles. Such methods may include signage, photo identification and badges, sign-in logs, electronic security equipment *(e.g., CCTV cameras or motion-detection devices/alarms)*, hardware *(e.g., locks and keys)*, software *(e.g., electronic card readers or biometric readers)* or physical barriers *(e.g., gates/fences)*. *[See also Biometric Readers, Controlled Perimeters, Perimeter Defenses.]*

Access Control Point: A location at a facility where visitors, vendors, contractors and/or employees are directed to gather to gain authorized access to the facility. Authorized access may be contingent upon identity verification and a screening process through which suspicion over unauthorized entry is reasonably eliminated. *[See also Access Control(s).]*

Agent: A biological or chemical poison that can be used for intentional or terrorist acts.

Asset: A resource of value requiring protection. An asset can be tangible, such as people, equipment, facilities, products, activities, operations and information; or intangible, such as processes or a company's information, reputation and brand value. *[See also Critical Asset.]*

Automated Broker Interface (ABI): A voluntary program available to brokers, importers, carriers, port authorities and others to electronically file with the U.S. Customs Service prior notice import data required under the Bioterrorism Act of 2002. This single electronic portal is one component of Customs' Automated Commercial System (ACS).

Automated Commercial System (ACS): The system used by the U.S. Customs Service to track, control and process all commercial goods imported into the United States.

Biological Attack: The deliberate release of germs or other biological substances that can cause illness.

Bioterrorism Act: The law enacted on June 12, 2002, formally known as the Public Health Security and Bioterrorism Preparedness and Response Act of 2002, that includes requirements for food, feed and other companies handling, processing or exporting agricultural commodities to register facilities with the U.S. Food and Drug Administration, provide prior notice of imported products, and maintain records, including one-step-forward, one-step-back product tracing.

Biometric Reader: An electronic device that evaluates unique physical characteristics *(i.e., fingerprint, eye patterns, voice, etc.)* to determine if a person is authorized to enter a secure or protected area. *[See also Access Control.]*

Bio-Safety Level (BSL): Developed for microbiological and biomedical laboratories dealing with safe working conditions, these designate – in ascending order, from BSL 1 through BSL 4 – the risks associated with various agents (such as foot-and-mouth disease). BSL 3 and BSL 4 laboratories are highly specialized containment facilities for certain rare and dangerous agents.

Card Reader: An electronic device used to read encoded information on a magnetic card or other device.

CARVER: An acronym for six target evaluation criteria used as part of a vulnerability-assessment approach. The acronym stands for "criticality," "accessibility," "recuperability," "vulnerability," "effect" and "recognizability."

CARVER+Shock: A risk-assessment tool for conducting vulnerability assessments by determining the "critical nodes" that are the vulnerable targets for attack (by outsiders or insiders) that leads to the identification of steps or countermeasures that may reduce the risk to the product or facility. CARVER is an acronym denoting the words "criticality," "accessibility," "recuperability," "vulnerability," "effect," and "recognizability." Meanwhile, "shock" refers to the combined physical, public health, psychological and economic effects of an attack.

CBP: Customs and Border Protection, an agency of the U.S. Department of Homeland Security (DHS) responsible for keeping terrorists and their weapons out of the United States, and for securing and facilitating trade and travel while enforcing U.S. laws and regulations on immigration; plant pests and animal diseases; and drug laws.

CCTV: Closed circuit television, a form of electronic surveillance. *[See also Electronic Surveillance.]*

Center for Food Safety and Applied Nutrition (CFSAN): One of six product-oriented divisions within the U.S. Food and Drug Administration responsible for ensuring the nation's food supply is safe, sanitary, wholesome and honestly labeled, and that cosmetic products are safe and labeled properly.

Center for Veterinary Medicine (CVM): One of six product-oriented divisions within the U.S. Food and Drug Administration that regulates the manufacture and distribution of feed, feed ingredients and drugs intended for use in animals.

Centers for Disease Control (CDC): An agency of the U.S. Department of Health and Human Services whose mission is to promote health and quality of life by preventing and controlling disease, injury and disability.

Central Intelligence Agency (CIA): The federal agency responsible for collecting, correlating, evaluating and disseminating intelligence for national security.

Chemical Attack: The deliberate release of a toxic gas, liquid or solid that can poison people and the environment.

Continuity of Operations: A pre-determined plan for resuming operations following an emergency, natural disaster or terrorist attack, and for maintaining a state of readiness. This term traditionally is used by the federal government and its supporting agencies to describe activities also referred to as disaster recovery, business continuity, business resumption or contingency planning.

Controlled Area: An area into which physical access is restricted or limited through the use of access control(s).

Critical Assets: Those assets of a facility determined to be essential to the minimum operations of the company or organization, and to ensure the health and safety of employees and the public.

Critical Infrastructure/Key Resource (CI/KR): Systems and assets, whether physical or virtual, that are so vital to the United States that the incapacity or destruction of such assets, systems, network or functions would have a debilitating impact on national security, the nation's economy, national public health or safety, or a combination of those matters. As defined under the Homeland Security Act of 2002, a key resource is a publicly or privately controlled resource essential to the minimal operations of the economy and government.

Consequence: The result of a terrorist attack or other incident that reflects the level, duration and nature of the loss resulting from the incident. Loss is measured by four main categories: 1) health; 2) economic; 3) psychological; and 4) governance.

Continuity of Operations Plan: Also referred to as a "crisis management plan," this plan lays out how an organization will maintain operations when a threat or event is detected.

C-TPAT: Customs-Trade Partnership Against Terrorism, a voluntary program implemented by the U.S. Department of Homeland Security Customs and Border Protection (CBP) at border-crossing points between the United States and Canada and Mexico. C-TPAT provides tiered benefits to importers of cargo, including expedited entry and lower cargo inspection frequency at border-crossing points, depending upon the degree to which such importers have implemented CBP-verified security measures within their international supply chains.

DHS: U.S. Department of Homeland Security, a cabinet-level department created in 2002 with the mission of leading a unified national effort to secure the American homeland. The department's mission is to prevent and deter terrorist attacks and protect against and respond to threats and hazards facing the nation, as well as securing U.S. borders while welcoming lawful immigrants, visitors and trade.

Dirty Bomb: The use of non-nuclear explosives to spread radioactive materials over a targeted area. Also known as a "Radiological Dispersion Device (RDD)," a "dirty bomb" is not a nuclear blast, but rather an explosion resulting in localized radioactive contamination.

Electronic Laboratory Exchange Network (eLEXNET): An integrated, web-based information network that allows health officials at multiple government agencies engaged in food/feed safety activities to compare, share and coordinate laboratory analysis findings. eLEXNET provides the infrastructure for an early warning system that identifies potentially hazardous foods/feeds, and enables health officials to assess their risks and analyze trends.

Electronic Security: A security system consisting of sensors, system controls, and an annunciation capability to increase probability that intrusions into secure/protected areas are identified and authorized personnel are notified in a timely manner. Electronic security also may include recording capabilities to allow for subsequent review of intrusion activities.

Environmental Protection Agency (EPA): The federal agency responsible for protecting the environment, as well as public health risks associated with potential environmental hazards.

Federal Bureau of Investigation (FBI): The criminal investigative arm of the U.S. Department of Justice.

FEMA: Federal Emergency Management Agency, part of the U.S. Department of Homeland Security. Its assigned mission is to lead the nation's efforts in preparing, responding to and recovering from disasters.

Food and Drug Administration (FDA): The federal agency responsible for overseeing the safety, efficacy and security of human and veterinary drugs, food and feed, biological products, medical devices and cosmetics.

Food Emergency Response Network (FERN): A network of state and federal laboratories that analyze food samples for contamination. FERN is a partnership involving federal agencies (FDA, USDA, CDC and EPA), states and CDC's Laboratory Response Network.

Food/Feed Defense: The collective term used by the federal government and industry to encompass activities associated with protecting the nation's food and feed supply from deliberate or intentional acts of contamination or tampering.

For Official Use Only (FOUO): The term used to identify unclassified information that is sensitive in nature, the unauthorized disclosure of which could affect adversely an individual or company's privacy or welfare, the conduct of federal programs or other programs or operations essential to the national interest. Information affecting U.S. national security classified "Confidential," "Secret," or "Top Secret" is not considered FOUO.

Gap Analysis: A business resource assessment tool that enables companies to evaluate actual versus desired future performance. At its core are two questions: 1) Where are we?; and 2) Where do we want to be? Gap analysis provides a foundation for measuring investment of time, money and human resources required to achieve a particular outcome. In a facility security context, it involves conducting a risk assessment to identify potential vulnerabilities that

pose a significant risk to the facility, its people or its products, and comparing that risk level against the company's desired level of security. Also referred to as "need-gap analysis," "needs analysis" and "needs assessment."

Hardening Assets: Enhancements, modifications and systems designed to make a facility, object or material more difficult for unauthorized persons to penetrate, and less desirable as a target. Also known as "Target Hardening."

Hazard: A biological, chemical, radiological or physical agent reasonably likely to cause illness or injury.

Hazmat: Hazardous materials, a term used by the U.S. Department of Transportation's regulations to describe chemicals, such as fertilizers, pesticides or other materials, that pose a physical or health hazard.

Homeland Security Advisory System (HSAS): A five-level warning system of color-coded rankings used by the U.S. Department of Homeland Security to provide guidance to law enforcement and other public agencies, citizens and the private sector. Each of the five threat-level conditions is associated with protective measures to be implemented by government agencies. Green represents a "low risk" of terrorist attack. Blue indicates a "general risk." Yellow signifies an "elevated condition" representing a "significant risk" of terrorist attack. Orange represents a "high condition" indicating a "high risk" of terrorist attack. And red represents a "severe condition" indicating a "severe risk" of terrorist attack.

Homeland Security Information Network (HSIN): An interactive, web-based communications system (involving federal, state and private sector partners) that delivers real-time, interactive information among federal and state regulatory and public health agencies and the private sector with the DHS Homeland Security Operations Center. It includes a site specific to the food and agriculture sector that provides information on natural disasters, deliberate or intentional acts of contamination or tampering, and food/feed defense.

Information Sharing and Analysis Center (ISAC): A public/private sector partnership between the food industry and the FBI's National Infrastructure Protection Center. Its purpose is to rapidly and confidentially disseminate information gathered by the federal government's intelligence community to the respective industry sector (e.g., food, rail, etc.) regarding actual or potential threats arising from deliberately malicious or terrorist activity. It also serves as a method for communicating confidential information from industry to the government on any actual, threatened or suspected deliberate malicious attacks so it can be analyzed by DHS.

ISO: The International Standards Organization, which develops voluntary international consensus standards.

ISO 9000: A series of voluntary international standards for product safety and quality. The formal name is the ISO 9000 Series of Standards.

Layered Security: A traditional approach in security engineering that uses concentric circles extending out from an area of a facility to be protected as demarcation points for using different security strategies. An integrated combination of multiple and perhaps redundant physical and operational measures are deployed to control access to the facility and its critical assets. A layered security approach may include such physical security measures as installing security lighting, designated parking, periodic human surveillance, video (CCTV) surveillance and perimeter barriers. Operational measures may include the use of designated access points, limiting access to critical areas or assets, screening of persons and vehicles, and requiring acceptable identification.

MTSA: The Maritime Transportation Security Act of 2002, designed to protect the nation's ports and waterways from a terrorist attack. Requires facility and vessel security plans to be developed, submitted and approved by the U.S. Coast Guard, and incorporated into a National Maritime Security Plan that includes incident-response plans. This law is the U.S. equivalent of the International Ship and Port Facility Security Code (ISPS).

National Incident Management System (NIMS): Establishes standardized incident-management processes, protocols and procedures that all responders – federal, state, tribal and local – use to coordinate and conduct response actions when a homeland security incident occurs. Encompasses both terrorism and natural disaster incidents.

National Infrastructure Protection Plan (NIPP): The federal plan for further developing and implementing protective efforts for national critical infrastructure and key resource (CI/KR) sectors, one of which is food and agriculture. The overarching goals are to: 1) enhance protection of CI/KR assets to prevent, deter, neutralize or mitigate the effects of deliberate attacks to destroy, incapacitate or exploit them; and 2) enable national preparedness, timely response and rapid recovery in the event of an attack, natural disaster or other emergency.

Pathogen or Infectious Agent: A biological agent that causes disease or illness to its host. The term most often is used to describe agents that disrupt the normal physiology of an animal or person.

Perimeter Security: Security measures or systems intended to restrict access to a facility or asset by screening entry at the designated boundaries of the plant or asset.

PPE: Personal protective equipment, such as dust masks, respirators, safety harnesses, etc.

Prevention: Actions taken to avoid an incident or to intervene to stop an incident from occurring.

Recovery: The return-to-service activities that industry and government undertake to ensure consumers that products will be safe and secure following an incident. Involves the development, coordination and execution of service- and site-restoration plans for affected communities and industry sectors, and the reconstitution of government operations and services through individual, private sector, non-governmental and public-assistance programs.

Red Team: A risk-assessment technique that involves using subject-matter experts to view the potential target from the perspective of an attacker to identify a facility's hidden vulnerabilities, and to anticipate possible modes of attack.

Response: Activities that address the short-term, direct effects of an incident. Such activities involve saving and limiting loss of life and property; meeting basic human needs; executing emergency plans; utilizing intelligence to reduce adverse impacts; immunizations; law-enforcement operations; and more.

Risk: The potential for loss of, or damage to, an asset, measured based upon the value of the asset in relation to the threats and vulnerabilities associated with it.

Restricted Area: An area within a facility or its surroundings that has been designated as a high-security area to which access is limited to those with a specific job function or need to know that have proper identification and credentials.

RFID: Radio frequency identification. A method of identifying unique items using radio waves. Typically, a reader communicates with a tag, which holds digital information in a microchip.

Risk Analysis: Determination of the probability of occurrence of an event and the impact or effect if a given loss occurs.

Risk Assessment: A systematic evaluation process that determines the likelihood of an incident occurring at a facility that would result in significant adverse consequences to critical physical and human assets *(e.g., loss of life, injuries, damage to infrastructure, economic loss, loss of shareholder value, etc.)*. The major components of a risk assessment include a hazard identification/analysis and a vulnerability analysis that answer the following questions: What are the hazards that could affect the facility and its surroundings? What can happen as a result of those hazards? How likely is it that such an incident could occur and what are each of the possible outcomes? When the possible outcomes occur, what are the likely consequences and losses?

Screening: A process through which a person or object seeking entry into a controlled area is evalu-

ated, and by which suspicion is reasonably eliminated.

Security Breach: An event which involves an unauthorized entry into a controlled area.

Sensitive Security Information (SSI): A classification for information protected from unauthorized distribution under federal law. No part of such documents may be disclosed or distributed to persons without a "need to know," unless specific written permission is granted in advance by management.

Soft Target: An asset that is unprotected, or inadequately protected.

Strategic Partnership Protection Agroterrorism (SPPA) Initiative: An initiative launched by the FBI that involves federal and state government agencies and private sector volunteers to provide government and industry with a more complete sector-wide perspective of food and agriculture defense. Under this initiative, more than 35 vulnerability assessments were conducted from 2003-09 to help distinguish between real and perceived food-defense risks. The initiative also assisted in identifying mitigation measures and strategies that may be appropriate for the food and agriculture sector. Participants also identified research needs to help prioritize the allocation of food/feed defense research investments.

Terrorism: The "unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives."

- ***Domestic terrorism*** involves groups or individuals based and operating entirely within the United States and Puerto Rico without foreign direction, and whose acts are directed at elements of the U.S. government or population.
- ***International terrorism*** involves groups or individuals that have some connection to a foreign power, or whose activities transcend national boundaries, against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, to further political or social objectives.

Threat: An indicator of possible violence, harm or danger that includes both intent and capabilities.

TWIC: Acronym for "Transportation Worker Identification Credential" program, operated jointly by the U.S. Department of Homeland Security's U.S. Coast Guard and Transportation Security Administration. TWICs are tamper-resistant biometric credentials issued following a security background check to persons who require unescorted access to designated secure areas of MTSA-regulated ports, vessels and outer continental shelf facilities, as well as all credentialed merchant mariners. Mandated by Congress under the Maritime Transportation Security Act. All of the nation's ports were required to be in compliance with the TWIC program by April 14, 2009.

Vulnerability: A weakness in the design, implementation or operation of an asset or system that may be exploited by an adversary or disrupted by a natural disaster.

Water Soluble, Heat Stable Chemicals: One of three types of chemical agents *(e.g., cyanide)*.

Weapon of Mass Destruction (WMD): Any weapon or device that is intended, or has the capability, to cause death or serious bodily injury to a significant number of people through the release, dissemination, or impact of: 1) toxic or poisonous chemicals or their precursors; 2) a disease organism; or 3) radiation or radioactivity.