Facility Vulnerability Assessment and Facility Security Plan

A Guide for Complying with the CCC Uniform Grain and Rice Storage Agreement

USDA

National Grain and Feed Association

Copyright© July 2004
By the National Grain and Feed Association
1250 I St., N.W., Suite 1003
Washington, D.C., 20005-3922
E-Mail: ngfa@ngfa.org
Web Site: www.ngfa.org

All Rights Reserved. No portion of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, without prior permission in writing from the publisher.

Disclaimer: The National Grain and Feed Association makes 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

Preface

This document, developed by the National Grain and Feed Association (NGFA), provides guidance to assist grain warehouse operators in complying with the Uniform Grain and Rice Storage Agreement (UGRSA) requirement to conduct a facility vulnerability assessment and implement a facility security plan to protect CCC-owned or CCC-interest grain.

This document is organized in the following manner:

- **Introduction** provides an overview of Amendment 1 to the UGRSA contract for 2004-05, as well as a clarifying notice to the industry issued by USDA/CCC. The texts of both documents also are provided. Part I also places the UGRSA contract requirements related to facility security into context with the overall U.S. government initiative to protect the agricultural sector and to make it less vulnerable to a terrorism incident or other security-related breaches that could compromise the safety or abundance of the U.S. food supply.

- **Part I** provides guidance for warehouse operators on complying with the UGRSA contract provisions requiring that **facility vulnerability assessments** be conducted.

- **Part II** provides guidance for warehouse operators on complying with the UGRSA contract requirement that a **facility security plan** be developed and implemented. For clarity, this section is divided into four subparts that cover each of the UGRSA contract requirements:

  - **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.

- **Appendix 1** contains a sample form that warehouse operators can use to document that they have conducted a facility vulnerability assessment and implemented a facility security plan, which can be placed into an appropriate file.

- **Appendix 2** contains sample forms that warehouse operators can use for developing: 1) an emergency telephone list; 2) a sample employee emergency telephone list; and 3) a sample visitor's log.

  The topics discussed and guidance provided in this document are **not** formal recommendations. Nor are they designed to be a comprehensive compilation of all security issues confronting grain storage facilities or other agribusinesses. Rather, this document is designed to provide a **"menu" of ideas and concepts** that grain warehouse managers can consider incorporating into a facility security plan so as to comply with the UGRSA requirements.

  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, and different plans may be appropriate for different facilities operated by the same company based upon the circumstances and conditions present. The facility vulnerability assessment can be useful in identifying facility-security steps that may be appropriate for individual situations. **In addition, it is extremely important that you select facility-security measures that are achievable and that will be implemented.**

Two other important points:

- There currently is **no requirement to submit a facility vulnerability assessment or facility security plan to USDA/CCC** for review or approval. In fact, USDA/CCC does not want to receive these documents and returns those it does receive to the warehouse operator. Rather, keep these documents on hand and available in a secured area at the facility in the event a CCC warehouse examiner inquires during the examination whether you have conducted such a vulnerability assessment and prepared a security plan. Be sure the warehouse examiner has proper credentials before providing any such information.

- As explained later in the Introduction, USDA/CCC does **not require that a separate facility security document be developed by warehouse operators to comply with the UGRSA requirement**, so long as the warehouse operator has a preexisting plan that addresses the requirements. Thus, the ideas and concepts presented in Parts I and II of this document can be used as a tool to review and compare your existing plan to ensure it addresses the facility vulnerability assessment and facility security requirements of the UGRSA. Or, it can be used as a starting point for developing your individualized plan. In this regard, be sure to include other or different facility-security procedures already being utilized at your facility and its operations.

The information contained herein largely is derived and adapted from the ***Agribusiness Facility and Operations Security*** document developed by a special task force of the NGFA and published on Nov. 16, 2001. *[See the NGFA's web site at www.ngfa.org for a copy.]* This document also contains information presented during a special "Industry Town Hall Meeting" conducted on March 15, 2004 at the NGFA's 108th annual convention in San Antonio, Texas. Speakers included USDA officials who developed the amendment and industry experts in the field of facility asset security.

Introduction

What the UGRSA Contract Requires
…And What It Doesn't…

Under Amendment 1 to the UGRSA contract for 2004-05 issued by USDA/CCC, grain warehouses are required by Sept. 1, 2004 to conduct a facility vulnerability assessment and implement a facility security plan.

The UGRSA contract amendment is part of an overall government initiative, embodied in Homeland Security Presidential Directive Number 9 (HSPD-9), 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. The directive is expected to have significant implications for grain elevators, feed mills, processors and other sectors of the U.S. agriculture and food system. For instance, in addition to the UGRSA, HSPD-9 is expected to result in USDA issuing vulnerability assessment and security planning requirements for entities operating under other government contracts, including those used by CCC to procure products for domestic and foreign food assistance programs. As the sequential number would indicate, similar homeland security presidential directives already have been issued for several sectors of the U.S. economy, including the financial services and transportation sectors.

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 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. In implementing its provisions, the directive also states that federal agencies are to "ensure that homeland security programs do not diminish the overall economic security of the United States."

Amendment 1 to the UGRSA added a new "Security Plan" section to Part III of the contract, which addresses the warehouse operator's contractual responsibilities. Specifically, UGRSA Amendment 1 requires warehouse operators to **implement a security plan that "includes measures to protect grain handled and stored" under the contract**. It also requires warehouse operators to **conduct a facility vulnerability assessment that addresses four major components**:

- The **general security of the physical structures and grounds** of the grain storage facility;
- The warehouse's **shipping and receiving procedures** to ensure grain is "not subject to tampering";
- Specifying **actions to be taken in the event of a "national emergency"**; and
- **Emergency contact information** for local security authorities.

In response to input submitted by the NGFA, USDA on Jan. 14, 2004 issued a "Notice to the Industry" *[BCD-65]* in which it clarified several important aspects of Amendment 1.

Importantly, USDA clarified in its notice that it does **not intend to specify minimum standards** for what should be included in a UGRSA warehouse's facility security plan. Instead, the notice states that CCC intends to provide flexibility for the warehouse operator to make a "good-faith effort" to address the requirements contained in Amendment 1. "The security plan required…is general in nature because of the diversity of the warehouse industry and the need for warehouse operators to determine the extent of risk that exists at individual locations and to devise appropriate risk-mitigation measures," the notice adds. "Thus, it is not USDA's intent to prescribe the specifics to be included in the warehouse's facility security plan."

During a presentation at the NGFA's 108th annual convention in March 2004, USDA officials elaborated that the "minimum standard" for a specific warehouse facility will vary, but will be "what is required to keep stored and handled commodities safe." They noted that the requirement "is a work in progress," and that USDA will continue to evaluate whether further guidance is needed in future years.

USDA's notice to the industry also attempts to clarify several of the most troubling and confusing aspects of the UGRSA amendment. Specifically, USDA elaborated on the following requirements:

- The requirement to have shipping and receiving procedures in place to protect against tampering of grain means that the operator is to have procedures that provide "**adequate security at the receiving and load-out areas** at the UGRSA facility that are within the "**physical control of the warehouse operator**." In essence, this means that the warehouse operator's obligation does **not** extend to those delivering grain to the facility. Further, currently this provision does **not** impose obligations on UGRSA warehouse operators concerning security of outbound conveyances; instead, those matters are between the shipper and receiver/customer.

- The requirement to take action in the event of a "national emergency" means that the warehouse operator is to have a contingency plan that includes **emergency steps that would be activated if there is a "credible threat to the safety or security of those commodities stored or handled at the UGRSA facility**." Under the federal Bioterrorism-Preparedness Law, declarations of credible threats to various sectors of the food and feed chain are the responsibility of the U.S. Department of Homeland Security and FDA. Enabling those agencies to convey such alerts was one of the principal purposes of the facility registration requirement mandated under the law and implemented by FDA effective Dec. 12.

- The requirement to have contact information for local security authorities means that the warehouse operator is to **include in the security plan the names and telephone numbers for local emergency responders**, such as the local police and fire departments, as contact points if a terrorist or other incident occurs that could compromise the safety of commodities stored or handled under the UGRSA. In addition, USDA's notice to the trade recommends that the warehouse operator include contact information for the local FBI office, if available, so that the FBI can be contacted in the event of a terrorism incident.

USDA's notice also clarifies that USDA will **not** require UGRSA warehouse operators to have a separate and distinct facility security plan solely for USDA's purposes. Instead, existing plans developed for other government or private entities (such as emergency action plans, hazardous material response plans, spill prevention, control and countermeasure plans or other similar programs) will suffice as long as they address the four broad requirements contained in the UGRSA amendment. In addition to the three requirements cited previously, the fourth is for the facility security plan to address the general security of the physical structures and grounds of the warehouse.

CCC-25 (Amend. 1)
(11-21-03)

U.S. DEPARTMENT OF AGRICULTURE
Commodity Credit Corporation

AMENDMENT 1 TO CCC-25, UNIFORM GRAIN AND RICE STORAGE AGREEMENT (UGRSA)

(1) **No. A _____ -3-CCC _____**

NOTE: *The authority for collecting the following information is Pub. L. 107-171. This authority allows for the collection of information without prior OMB approval mandated by the Paperwork Reduction Act of 1995. The time required to complete this information collection is estimated to average 15 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information.*

The following statement is made in accordance with the Privacy Act of 1974 (5 USC 552a). The authority for requesting the following information is 15 U.S.C. 714 and regulations promulgated thereunder (7 CFR Parts 1421 and 1403). The information will be used to complete the terms of an agreement between the warehouse operator and CCC. Furnishing the requested information is voluntary, however, without it, eligibility to enter into an agreement with CCC cannot be determined. This information may be provided to other agencies, IRS, Department of Justice, or other State and Federal law enforcement agencies, and in response to a court magistrate or administrative tribunal. The provisions of criminal and civil fraud statutes, including 18 USC 286, 287, 371, 641, 1001; 1014, 15 USC 714m: and 31 USC 3729, may be applicable to the information provided. ***RETURN THIS COMPLETED FORM TO THE KANSAS CITY COMMODITY OFFICE, Mail Stop 8748,***

The Commodity Credit Corporation (CCC) and *(2)* _____ (warehouse operator or contractor) hereby agree to amend the UGRSA as follows:

PART III, O., Security Plan, is added to read as follows:

PART III. WAREHOUSE OPERATOR'S RESPONSIBILITIES

* * * * *

O. Security Plan

The warehouse operator must:

1. Have a security plan that includes measures to protect grain handled and stored under this Agreement.
2. Conduct a facility vulnerability assessment and establish procedures that address:
   a. General security of the physical structures and grounds of the warehouse,
   b. Shipping and receiving procedures to ensure that grain is not subject to tampering,
   c. Action to be taken in the event of a national emergency, and
   d. Contact information for local security authorities.

3. WAREHOUSE OPERATOR:	**4. COMMODITY CREDIT CORPORATION:**
3A. _____ (COMPANY NAME)	
3B. By _____ (SIGNATURE)	4A. By _____ (CONTRACTING OFFICER)
3C. Title _____	4B. Effective Date: _____

The U.S. Department of Agriculture (USDA) prohibits discrimination in all its programs and activities on the basis of race, color, national origin, gender, religion, age, disability, political beliefs, sexual orientation, and marital or family status. (Not all prohibited bases apply to all programs.) Persons with disabilities who require alternative means for communication of program information (Braille, large print, audiotape, etc.) should contact USDA's TARGET Center at (202) 720-2600 (voice and TDD). To file a complaint of discrimination, write USDA, Director, Office of Civil Rights, Room 326-W, Whitten Building, 1400 Independence Avenue, SW, Washington, D.C. 20250-9410 or call (202) 720-5964 (voice or TDD). USDA is an equal opportunity provider and employer.

United States Department of Agriculture

Farm and Foreign Agricultural Services

Farm Service Agency

Kansas City Commodity Office
P.O. Box 419205
Kansas City, Missouri
64141-6205

NOTICE TO THE INDUSTRY – BCD - 65

DATE: January 14, 2004

TO: All Warehouse Operators Seeking Approval Under The Uniform Grain and Rice Storage Agreement (UGRSA)

SUBJECT: Amendment 1 to CCC-25, Part III, O., Security Plan

Background

The events of September 11, 2001, highlighted the need to enhance the security of the infrastructure of the United States, including those facilities engaged in storing and handling the nation's grain supply. Congress responded by enacting the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (Act), providing the Food and Drug Administration (FDA) new authority to protect the nation's food supply against actual or threatened terrorist acts and other food-related emergencies that pose a threat of serious adverse health consequences or death for humans or animals. Among other things, FDA's regulations require domestic and foreign facilities that manufacture, process, pack, or hold food for consumption in the United States to have registered with the FDA by December 12, 2003. In support of this Act and other initiatives by the U.S. Department of Homeland Security, the U.S. Department of Agriculture/Farm Service Agency (USDA/FSA) has started the process of implementing security plan requirements into Commodity Credit Corporation (CCC) commodity storage agreements, including the UGRSA.

Purpose

The purpose of this notice is to clarify USDA/FSA expectations regarding the above-referenced amendment. Under the amendment, warehouse operators entering into a UGRSA agree to conduct a facility-vulnerability assessment and implement a security plan that includes measures to protect grain handled and stored under the UGRSA. It is important that each company evaluate the existing level of security at each of their facilities and develop a plan for managing potential risks. In order to allow warehouse operators time to meet the requirements of Amendment 1, CCC will provide a five-month phase-in starting April 1, 2004, before any actions are taken for non-compliance.

Clarifications to Amendment 1

The security plan required under Amendment 1 is general in nature because of the diversity of the warehouse industry and the need for warehouse operators to determine the extent of risk that exists at individual locations and to devise appropriate risk-mitigation measures. Thus, it is not CCC's intent to prescribe the specifics to be included in the warehouse's facility security plan. However, CCC will expect warehouse operators to make a good faith effort to address each of the four elements contained in Part III, O, 2, as

USDA is an Equal Opportunity Employer

outlined in Amendment 1, so as to mitigate the facility's vulnerability to a potential terrorism incident and to effectively respond if an event occurs. CCC recognizes that UGRSA warehouse operators already may have conducted vulnerability assessments of facilities under the UGRSA, and prepared facility security plans that address the provisions of Amendment 1 in response to requirements imposed by other federal or state government agencies, insurance carriers or other entities. These may include emergency action plans; hazardous material response plans; spill prevention, control and countermeasure plans; or other programs implemented by the warehouse operator. CCC will recognize these plans as meeting the requirements of Part III, O, 2 of the UGRSA, as conveyed in Amendment 1, so long as such plans address the areas specified in Amendment 1.

CCC also wishes to clarify its intent with regard to the components of the facility security plan required under Part III, O, 2:

- In part 2, b, of the amendment, the warehouse operator agrees to have shipping and receiving procedures in place to protect against tampering of grain. This means that warehouse operators are to implement procedures that provide adequate security at the receiving and load-out areas at the UGRSA facility that are within the physical control of the warehouse operator.

- In par 2, c, of the amendment, it states that the warehouse operator is to specify actions to be taken in the event of a national emergency. This means that the warehouse operator should have a contingency plan on emergency steps that would be activated if there is a credible threat to the safety or security of those commodities stored or handled at the UGRSA facility.

- In part 2, d, of the amendment, it states the warehouse operator must have contact information for local security authorities. This means that warehouse operators should include in the security plan the names and telephone numbers of local emergency responders, such as police, fire department and the local FBI office, if available, that the warehouse operator can call in the event of a terrorism incident.

Action

Amendment 1 must be signed and returned with the other documents included in the UGRSA renewal packet by January 23, 2004, in order to be approved. CCC will continue to monitor the progress regarding implementation of security plans; however, no action will be taken for failure to comply with the requirements of Amendment 1 until September 1, 2004.

/s/ Steven P. Miteff

Steven P. Miteff
Acting Director, KCCO

USDA is an Equal Opportunity Employer

Part I

Guidance for Conducting a Facility Vulnerability Assessment

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

Generally, grain, feed, feed ingredients 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 *(such as ferrous and non-ferrous metal, glass and plastic).*

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

Step 1: Plan for the Vulnerability Assessment

- **Consider Who to Designate to Conduct the Vulnerability 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 and farm supplies, consider a "team" approach consisting of cross-functional representation from the different types of operations in which the facility is engaged.

  In any case, the person(s) designated with this responsibility should be objective and empowered to make a thorough, 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 Assets:** Knowing and identifying the facility's most valuable assets is essential to any security plan. Through such identification, limited resources can be used most efficiently.

- **Consider Most Likely Types of Threats and Who May Pose Them:** Before conducting a facility vulnerability assessment, consider the type(s) of threat (sabotage, threat or attack) and from whether it most likely is internal (such as from a disgruntled employee) or external (such as from 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, farm supply) may have a bearing on the types of vulnerabilities to which attention should be paid.

- **Consider the Degree to which Threats May Exist:** Consider: 1) the storage capacity of the facility; 2) the number of perimeter entrances and exits; 3) the effectiveness of current access control security measures; 4) the history of previous incidents or "close calls"; 5) the number of employees; 6) the satisfaction level of employees and the degree to which some of them bring personal problems into the workplace; and 7) the surroundings and characteristics of the neighborhood in which the facility is located.

  The North Carolina Department of Agriculture and Consumer Services has developed a sample "Terrorism Threat Vulnerability Self-Assessment Tool" available at http://www.ncagr.com/Industry_self-assessment.doc that agribusinesses can use as a starting place to conduct a vulnerability self-assessment. It is a general tool and can, and should, be customized to your specific facility's activities. Among other things, this vulnerability self-assessment tool advises companies to evaluate:

  - Potential threat intentions from terrorists *[i.e., are there or have there been any terrorist threat(s) to the company or facility, or a history of terrorist activity in the area]*.

- Specific targeting *[does the nature of the facility's activity make it a likely target for a terrorist?]*.

- Visibility of the facility and its operations within the community.

- On-site hazards *[such as the presence of hazardous materials, biologics or chemicals that potentially could be used as a threat or weapon]*.

- The presence of large numbers of people at the facility who could be harmed in a terrorist incident.

- The potential for mass casualties within a one-mile radius based upon the types of materials stored or used at the facility.

- 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); notoriety of the company; importance of the facility to the infrastructure and continuity of basic services to the community, state or nation; etc.]*.

- Organizational communications *[e.g., mass notification systems 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, available; hazard-monitoring devices on-hand and operational; etc.]*.

- Policy, procedures and plans *[e.g., crisis response/disaster plan in effect that addresses most likely threats (fire, explosion, chemical release, etc.)]*.

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

- Security of computers, mail and telecommunications.

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

Step 2: Perform the Vulnerability Assessment

1. Do a general walk-around of your facility and grounds – inside and outside. Assess, **from a criminal or potential terrorist's viewpoint**, the strengths and weaknesses of the facility and grounds. If a person wanted to destroy property or contaminate grain/products, what would he or she find attractive?

2. Determine which areas represent a high probability of security risk. Write them down.

   - A **tiered risk-based approach** probably is the most effective and efficient way to identify, evaluate and prioritize potential vulnerabilities. Consider developing a matrix that contains the most significant vulnerabilities and the frequency with which they could be breached. Special attention should be paid to:

     - Chemicals stored onsite.

     - Location and access of critical areas (facility control rooms, electric rooms, utilities, etc.).

     - Age, type of buildings and accessibility.

     - Whether the perimeter and grounds can be secured adequately.

     - Hours of operation (three shifts versus seasonal operations when the facility is not staffed).

   - Identify method(s) for controlling the highest-risk vulnerability(ies).

   - Evaluate the effectiveness versus costs of various vulnerability-reduction techniques, and weigh the cost-versus-benefits of the control measure in mitigating the vulnerability(ies).

   - Implement the chosen control measure(s) and periodically evaluate its effectiveness in mitigating the vulnerability(ies).

- Develop written procedures for receiving and shipping of product, including all raw materials and finished product *(i.e., grains, oilseeds, feed and feed ingredients, animal drugs, food-grade mineral oil, phosphine and other fumigants, pesticides and grain protectants, packaging, etc.)*

Step 3: Document Completion of the Facility Vulnerability Assessment

For purposes of compliance with the UGRSA contract requirement, warehouse operators may wish to use the sample form provided in Appendix 1, or some variation thereof, to document that the facility vulnerability assessment has been conducted and a facility security plan implemented.

Consider filing the document in an appropriate, secure place at the facility; **there currently is no requirement to submit this document to USDA/CCC or any other government agency**.

Part II

Guidance for Implementing a Facility Security Plan

This section contains a **"menu" of ideas and concepts** that grain warehouse managers can consider incorporating into a new or existing facility security plan so as to comply with the UGRSA requirements. Be sure to include other or different facility-security procedures already being utilized at your facility and its operations.

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, and the facility vulnerability assessment is useful in identifying facility-security steps that may be warranted for individual situations.

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

Part II.A

General Security of Physical Facility and Grounds

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

1. **Secure the Perimeter of the Physical Property:** Consider, based upon the perceived threat level, securing the property on which your facility is located to prevent unwelcome visitors from having open access. The configuration of the facility and other factors will determine how much and what type(s) of security are practical for an individual operation.

   In situations where physical barriers, such as perimeter fencing and locked gates, cannot be installed, are impractical or are too costly, consider using **one or a combination** of the following security options:

   - Security lighting.
   - Periodic walk-arounds by company personnel of the facility and grain storage and product loading/unloading areas.
   - Drive-by surveillance patrols by local law-enforcement on a regular, but unpredictable, basis.
   - Electronic security devices, such as door alarms, motion-detection devices and alarms linked to an off-site security system.
   - 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).
   - Security cameras.
   - Off-hours security guard.
   - Contact and request assistance and feedback from neighbors to report suspicious activity to management. Initiate or consider joining a local "crime-watcher's" program.

2. **Secure the Facility:** 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 implementing a standardized, **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, 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.
   - **Lock and secure access doors to enclosed receiving pits and tunnels**.
   - **Lock and secure grain discharge spouts** (especially those used infrequently)**.**
   - **Lock loading and discharge points** of exterior liquid tanks (above and below ground) when not in use.
   - **Lock outside product storage containers**, or relocate containers inside.
   - **Lock and secure doors to shop and tool storage areas**.

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

- When using seals, **record the seal numbers** on the bills of lading. Upon receipt, verify the seal numbers.

- **Restrict access to the facility's control room**, as well as computer process control and data systems.

- **Lock and secure access to power sources**, such as power rooms and electrical panels, to prevent unauthorized product discharges.

- Maintain current and accurate **inventory records** of grains, feed ingredients, finished feed production and animal drugs.

- If manufacturing feed and/or handling feed ingredients, **keep bagged feed ingredients, feed and animal drugs in secured and locked storage areas**.

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

- **Safeguard computer systems** with virus protection. Store back-up data offsite.

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

   - Conduct regular **inventory checks**.

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

   - **Consider changing door locks periodically**, especially in high-security areas or in facilities with frequent employee turnover.

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

   - **Notify local law enforcement** authorities and emergency responders about the steps you are taking to enhance the **security of your facility and grounds**. Use a plant tour to familiarize them with your 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; and 4) service shut-off points for utilities or hazardous materials.

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

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

5. **Establish Procedures for Access to Facility and Grounds by Visitors, Outside Contractors and Vendors:** Limit access to the facility of 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 2)*.

   - Consider using **name badges/tags, identification cards or other means** (such as a special hat, etc.) to identify visitors.

   - **Restrict access** to grain storage and manufacturing/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.

6. **Restrict Access to Sensitive Information:** Be cautious not to provide information over the telephone 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 question 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 information about the company, its operations, or facility layout or product lines. **Do not display sensitive (such as facility diagrams) or private company information on company web site**.

Part II.B

Operating and Personnel Procedures

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

1. **Employee Selection Practices:** When hiring:

   - **Request resumes** from applicants containing 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. Immigration and Naturalization Service.

   - **Check with multiple references** for background checks to establish a prospective employee's qualifications and demeanor. Consider using commercial services to conduct pre-employment 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.

   - 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.

   - Consider establishing an **employee identification system** through badges, uniforms, hard hats with logos and names, or other methods – particularly in situations where the facility has a high employee turnover rate.

   - 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.)*

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. Instill facility security awareness in all employees so that they become assets in monitoring the activities of visitors, customers, vendors, truck drivers and fellow employees.

   - Conduct **regular training** to discuss the facility's security policies and procedures, the areas of potential vulnerability, and the location of emergency exit routes and service shut-off points for utilities, fuel, pipelines, fuel tank pumps, anhydrous ammonia, etc.

   - Instill in employees their **responsibility for protecting the facility and equipment** from intruders.

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

   - Communicate a zero-**tolerance policy for workplace violence** and 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. **Resignation/Termination of Employees:** Upon resignation or termination of the employee:

   - **Collect employee identification** cards, photos or other items that demonstrate employment with the company.
   - **Collect all keys** to vehicles, secured buildings and other secured areas; cell phones; and two-way radios that may have been issued to the employee.
   - **Cancel all computer passwords and other access codes** that would allow former employees to gain access to grains, oilseeds or other agricultural products or hazardous substances.
   - **Consider informing current customers** when a former employee no longer is authorized by the company to have access to company facilities, shipments, records or other information.
   - **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.

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

   - **Check background, references and insurance coverage** for outside contractors or other outside groups.
   - **Inform** outside contractors **about established company safety procedures**.
   - **Inform** outside contractors **about areas of the facility to which they are allowed access**.
   - Consider whether to use **a pre-work checklist with contractors** to ensure they understand the facility's safety rules; 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.
   - **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.

5. **Policies for "Unknown" Customers:** Know your customers and their representatives/employees.

   - For customers whom you do not know, consider formalizing a **customer-interview process** before accepting grain deliveries.
   - **Learn the names of other agribusinesses that unknown customers patronize**, the background and nature of the customer's business, and other products and services that might be of interest to the customer. Consider following up on – and if necessary, alerting local law enforcement officials to – any suspicious information or leads.

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 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 become an issue 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. Visit new suppliers; request samples and review their security procedures for product handling and transport.

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

- If the delivery is not from an established 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 and other agricultural commodities upon arrival/unloading; retain file samples.

- Depending upon individual circumstances, it may be advisable to **visually inspect** grain, ingredients or other products **upon receipt and prior to unloading**. Before implementing such a practice, though, evaluate its net costs and benefits, as it may create additional safety, logistical and other operational/manpower issues. 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.

Load-Out Procedures:

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

- 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 you operate your own fleet and hire drivers, incorporate into regular training the 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 hazards. If you contract with an outside trucking firm, consider including specific security language as part of the contract.

    Consider the need for seals on bulk/tank truck shipments of food-related products intended for human consumption.

    Consider the following procedures if you operate your own truck fleet and crew of drivers:

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

    - Instruct drivers picking up or delivering grain **not to talk to unauthorized persons** about the delivery route, delivery schedule or ultimate destination of grain shipments.

- ❖ 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.

- ❖ Instruct drivers to be **alert to, and to report, suspicious activity** that may endanger the grain 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. When considering the use of seals, become familiar with the differences between "tamper-evident," "tamper-resistant" and "tamper-proof" seals, as each performs a different security function and has varying costs. In the case of rail shipments that might be in-transit for a lengthy period and subject to delays or stoppages, the shipper and receiver may want to consider asking the carrier to provide additional monitoring of the load.

- For **barge shipments**, in-transit security could become an issue 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, as well as methods to enhance security.

Part II.D

Emergency Response Procedures

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

An emergency action plan identifies the specific responsibilities of employees in the event of a fire, explosion or other emergency at grain-handling, feed and 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 included in an emergency action plan:

- **List of Emergency Contact Telephone Numbers:** Include contacts for the fire department, police department, rescue/ ambulance squads, hospitals, utilities and the local FBI office. In addition, in the event of contamination of grain, feed, processed or food products, include contact information for USDA, FDA and state public health officials. Contact information on insurance providers also is useful. Be sure to keep the information current. Place the list at or nearby all phones in the facility. *(A sample form is attached as part of Appendix 2)*.

- **List Employee Telephone Numbers:** This is useful in the event of an emergency, and also should be kept current. *(A sample form is attached as part of Appendix 2)*.

- **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.)*

- **Visitor Log:** As noted previously, maintain a visitor log to facilitate evacuation in the event of an emergency. *(A sample form is attached as part of Appendix 2)*.

- **Employee Assignments:** Specify the assignments for each employee responsible for performing an essential function prior to exiting the property. 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 that may be located at the plant.

- **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.

- **Employee Training:** As part of the emergency action plan, specify the type and frequency of training concerning: 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 assembly areas; and 7) assignment of individual employee responsibilities. Also keep employees informed about the nation's color-coded threat level as determined by the Department of Homeland Security, as well as when changes to the threat level are made.

Conclusion

The aforementioned topics discussed and guidance are **not** formal recommendations. Nor are they designed to be a comprehensive compilation of all security issues confronting grain storage facilities or other agribusinesses. Rather, they provide a "menu" of ideas and concepts that grain warehouse managers can consider incorporating into a facility security plan so as to comply with the UGRSA requirements.

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

Confidential – Not for Public Disclosure

Management Certification of Completion of UGRSA Facility Vulnerability Assessment and Facility Security Plan for the

_____

(Company Name)

_____

(Street or P.O. Box Address)

_____

(City, State, Zip Code)

This is to certify that our company, in accordance with the Uniform Grain and Rice Storage Agreement (UGRSA) contract issued by the U.S. Department of Agriculture's Commodity Credit Corporation, has conducted a facility vulnerability assessment and implemented a facility security plan to protect commodities stored and handled under this contract.

In so doing, management and/or its designated representatives have examined and addressed in the facility security plan potential vulnerabilities associated with:

- The general security of the physical structures and grounds of the grain storage facility.

  As part of this assessment, the following areas or functions were examined and evaluated for their relative vulnerability and degree of risk:

  - Security of the perimeter and physical grounds.
  - Age, type and configuration of buildings.
  - Accessibility of the facility and grounds to visitors, outside contractors and vendors.
  - History of previous incidences of burglary, vandalism, or suspicious activities.

- Location and access of critical areas, such as facility control rooms, electric power rooms and utilities.
- On-site hazards, such as chemicals and other hazardous materials (e.g., pesticides, fumigants, fertilizer, etc.)
- Product flows of grain and other agricultural commodities stored or handled under the UGRSA, as well as other products that could contaminate such commodities (e.g., feed and feed ingredients, grain protectants, animal drugs, etc.)
- Security of computers, mail and telecommunications.
- Practices for outside contractors.
- Practices for dealing with deliveries from "unknown" customers.

➢ Operating and personnel procedures, including:

- Employee hiring, selection and termination.
- Employee training on company security policies and procedures.
- Contractor, vendor and visitor policies.

➢ Receiving and load-out operations to protect against tampering of grains and other agricultural commodities handled under the UGRSA.

➢ Emergency response plan that will be activated if management receives a credible threat to the safety or security of the facility or the commodities stored or handled therein.

➢ Emergency contacts for local emergency responders and law enforcement personnel who will be contacted if management receives a credible threat to the safety or security of the facilities or commodities stored or handled therein.

This plan shall be reviewed periodically _____ to ensure it
(specify annually, biannually, etc.)
continues to meet the security needs of this facility.

This facility security plan represents official company policy.

_____
(Name of Authorized Company Official)

_____
(Signature)

_____ _____
(Title) (Date)

Appendix 2

SAMPLE FORMS

- **Sample Emergency Telephone List**
- **Sample Employee Emergency Telephone List**
- **Sample Visitor's Log**

Sample Emergency Telephone List

Company Manager _____
Assistant Manager _____
Superintendent _____
Other _____
_____

Agency **Phone Number** **Contact Person**

Police/Law Enforcement
- Local Police: _____
- Sheriff: _____
- Local FBI Office: _____
- Fire Department: _____

Rescue Squads / Medical Personnel
- Ambulance: _____
- Physician: _____
- Hospital: _____
- Trauma: _____

Food and Drug Administration
- Local Office: _____
- Regional Office: _____
- Commodity Credit Corporation: (816)-926-2528 Steve Searcy, Chief, Storage Contract Branch, USDA Kansas City Commodity Office

Chemical
- American Crop Protection Association: _____
- Chemical Transportation Emergency Center (Chemtrec): _____
- Toxic Substances Control Hotline Number: _____
- Poison Control Center: _____

Utilities
- Gas: _____
- Water: _____
- Electricity: _____

Specialty Contractors
- Inert Gas Suppliers: _____
- Cranes: _____
- Helicopters: _____
- Cutting Equipment: _____
- Excavation Equipment: _____
- Salvage Operators: _____

Insurance Company: _____

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)

Visitor’s Log

Visitor's Name	Company	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)*						
(Print Name) *(Signature)*						