U.S. ARMY CENTER FOR HEALTH PROMOTION AND PREVENTIVE MEDICINE

Technical Guide 188

U.S. ARMY FOOD AND WATER VULNERABILITY ASSESSMENT GUIDE

July 2008

DISTRIBUTION: This document has been approved for official use within the U.S. Government, and distribution is limited to U.S. Government agencies.

FOR OFFICIAL USE ONLY – RELEASABLE TO NATO. The recipient countries handle this information as NATO RESTRICTED.

Requests for this document from outside of the U.S. Government must be referred to the U.S. Army Center for Health Promotion and Preventive Medicine, Aberdeen Proving Ground, MD 21010-5403

In Coordination With: Department of Defense Veterinary Service Activity

This June 2008 Edition of Technical Guide 188 incorporates current policies and procedures for conducting food vulnerability assessments and food and water defense at special events. The water vulnerability chapter will be updated in future editions.

TABLE OF CONTENTS

CHAPTER 1. INTRODUCTION AND BACKGROUND 1-1
1-1. INTRODUCTION 1-1
1-2. BACKGROUND 1-1
1-3. FOOD DEFENSE OVERVIEW 1-2
1-4. WATER SYSTEM OVERVIEW 1-3
1-5. SPECIAL EVENTS OVERVIEW 1-5

CHAPTER 2. FOOD VULNERABILITY ASSESSMENT 2-1
2-1. INTRODUCTION 2-1
2-2. PLANNING 2-2
2-3. ASSESSMENT PROCESS 2-5
2-4. VULNERABILITY ASSESSMENT 2-6
2-5. SPECIAL EVENTS CONDUCTED ON A MILITARY INSTALLATION 2-30
2-6. COMMUNICATING HEALTH RISKS. 2-33
2-7. RISK MANAGEMENT 2-36
2-8. POINTS OF CONTACT 2-41

CHAPTER 3. WATER SYSTEM VULNERABILITY ASSESSMENTS 3-1
3-1. INTRODUCTION 3-1
3-2. PRE-VISIT 3-6
3-3. ON-SITE ASSESSMENT 3-14
3-4. FINAL REPORT 3-23
3-5. ADDITIONAL INFORMATION 3-26

CHAPTER 4. FOOD AND WATER VULNERABILITY ASSESSMENTS AT SPECIAL EVENTS OFF-INSTALLATION 4-1
4-1. INTRODUCTION 4-1
4-2. RESPONSIBILITIES 4-1
4-3. COMMUNICATING FOOD RISKS 4-2
4-4. FOOD AND WATER DEFENSE TEAM COORDINATION 4-2
4-5. PRE-EVENT MEETINGS 4-3
4-6. TEAM ASSEMBLY 4-9
4-7. EVENT SUPPORT 4-9
4-8. SAMPLING PLAN 4-10
4-9. POST-EVENT 4-13
4-10. TERMS 4-15

APPENDIXES

A – REFERENCES A-1
B – CONDUCTING FOOD VULNERABILITY ASSESSMENTS OVERVIEW B-1
C – WATER SECURITY/DOD SPECIAL EVENTS ADDITIONAL INFORMATION C-1
D – AFTER ACTION REPORT EXAMPLE D-1
E – ADDITIONAL RESOURCES CONTACTS E-1

TABLE LIST

Table 2-1 – Risk Assessment Matrix 2-19
Table 2-2 – Risk Level Definitions 2-19
Table 2-3 – Example Severity Ratings 2-20
Table 2-4 – Analyze Risk Control Measures and Rank Example 2-22
Table 2-5 – Make Control Decision and Implement Risk Controls 2-23
Table 2-6 – Features that Could Increase Physical Security Effectiveness 2-39
Table 2-7 – Features that Might Increase Perception of Protection 2-40

Table 3-1 – SDWA/Army WSVA and ERP Compliance Deadlines 3-3
Table 3-2 – Target Components of Water Systems 3-9
Table 3-3 – Probability Criteria 3-19
Table 3-4 – Severity Criteria 3-20
Table 3-5 – Example Report Recommendations Table 3-25
Table 3-6 – Chemical Hazards and Select Properties 3-30
Table 3-7 – Biological Hazards and Select Properties 3-32
Table 3-8. - Radiological Hazards Summary 3-37
Table 3-9 – Features to Increase Physical Effectiveness 3-40
Table 3-10 – Features to Increase Perception of Protection System 3-41
Table 3-11 – Analyzer Information 3-42

FIGURE LIST

Figure 2-1 – Risk Management Cycle 2-1
Figure 2-2 – Fact Sheet – Summary Joint Staff Integrated Vulnerability Assessment Food Vulnerability Benchmarks 2-3
Figure 2-3 – Asset List Example 2-7
Figure 2-4 – Example Conventional Dining Facility Flow Diagram 2-8
Figure 2-5 - Example Food Service Facilities with Cook-Chill Facilities Flow Diagram 2-9
Figure 2-6 – Example Delivery Subsistence Prime Vendor or Retail Food Distribution Flow Diagram 2-10
Figure 2-7 – Example Retail Store Flow Diagram 2-11
Figure 2-8 – Food Vulnerability Checklist 2-12

FIGURE LIST CONTINUED

Figure 2-9 – Risk Control Measures Worksheet 2-29
Figure 2-10 – Installation Special Events Checklist Example 2-30
Figure 2-11 – Example Risk Communication Checklist 2-35

Figure 3-1 – Risk Management Process 3-4
Figure 3-2 – Water System Overview 3-10
Figure 3-3 – Water System Vulnerability Assessment Worksheet 3-12
Figure 3-4 – Example of Completed WSVA Worksheet 3-13
Figure 3-5 – Example Items For WSVA Worksheet 3-17
Figure 3-6 – Risk Assessment Matrix 3-20
Figure 3-7 – Potable Water System Threat Survey Results 3-28
Figure 3-8 – Chemical Threats to Potable Water Systems 3-29
Figure 3-9 – Example Notification Letter 3-50

Figure 4-1 – Tasking Memo 4-4
Figure 4-2 – Model Contract: Model Contract: Food and Water Security Implementation Language for Incursion in Performance Work Statement 4-5
Figure 4-3 – Food Defense Questionnaire 4-7
Figure 4-4 – DA Form 1594 – Daily Staff Journal or Duty Officer's Log 4-11
Figure 4-5 – Food Sampling Plan 4-12
Figure 4-6 – Anticipated Sample Trays by Event 4-14

Glossary Glossary-1

CHAPTER 1

INTRODUCTION AND BACKGROUND

1-1. INTRODUCTION.

a. This Technical Guide (TG) is designed to assist force protection, security, food service and public health, preventive medicine, and veterinary food personnel in identifying vulnerabilities, assessing the severity and potential for the risks identified and providing a decision matrix that can be used to eliminate, minimize, or control the risk. The evaluation sheets, data collection, and evaluation are designed to be implemented by the installation staff with minimum assistance from outside agencies such as U.S. Army Center for Health Promotion and Preventive Medicine (USACHPPM), Navy and Marine Corps Public Health Center (NMCPHC), Navy Environmental and Preventive Medicine Unit (NEPMU), U.S. Air Force School of Aerospace Medicine (USAFSAM), and U.S. Army Veterinary Command (VETCOM).

b. This guide is divided into four chapters: an introduction chapter and three main chapters. Chapter 2 covers food vulnerability, Chapter 3 covers water system vulnerability, and Chapter 4 covers Food and Water Defense (FAWD) for Special Events held off-installation. The vulnerability assessment chapters were developed as stand-alone chapters because different teams will likely conduct the assessments, and the assessments follow different procedures. That stated, the vulnerability chapters have many common goals and objectives. Numerous forms, figures, tables, and text are repeated in all chapters to make it easier for the users.

1-2. BACKGROUND.

a. General. Chapter 1 contains general overviews and background information relevant to terrorist attacks. It is designed for the installation Commander and staff to assess the vulnerability of the food, including ice and bottled water supply, food preparation, storage and transport operations to terrorist attack to include the intentional contamination or destruction of food.

b. Vision. Enhance public health and force protection by providing Soldiers, Sailors, Marines and Airmen and their Families, civilian workers and other beneficiaries with safe and secure food and water sources and supplies.

Use of trademarked names does not imply endorsement by the U.S. Army but is intended only to assist in identification of a specific product.

c. Strategy. Identify, assess, and mitigate vulnerability of food and water supplies to terrorist attack. This guide is intended for installation Commanders and their staff to counter terrorist threats to military food and water supplies. It is also designed to assist in planning and implementing protective measures to prevent or mitigate attacks against food and water at fixed installations and to assist Commanders in instituting control measures during periods of increasing threat.

d. Assumption. Current procedures and safeguards are adequate to prevent unintentional contamination of food supplies, foodservice operations and water under Department of Defense (DOD) control. Current procedures in conducting a comprehensive food or water safety program can alert the installation staff to potential terrorism. For example, customer complaints of unusual taste, color, and odor in food or water, or complaints of product tampering or defective package seals, if tracked and recorded, can serve as early warnings even before illness is detected. If current practices are not well defined, then it may be impossible to differentiate between a terrorist attack and a naturally occurring event.

e. Scope. The focus of this program is to assess installation vulnerability to intentional contamination or destruction of food and water supplies.

f. References. See Appendix A for a list of references that have been compiled from various Federal agencies and professional associations.

1-3. FOOD DEFENSE OVERVIEW.

a. The Food Vulnerability Assessment (FVA) program is a part of the installation Antiterrorism program as outlined in DOD Instruction (DODI) 2000.16. The Food Defense Assessment Team (FDAT) works with the Commander in meeting the requirements in DODI 2000.16 and other regulatory requirements including the protection of critical assets. The FVA incorporates and works in conjunction with the Force Protection Condition (FPCON) system. Recommendations for elimination or control of identified vulnerabilities are coordinated with the FPCON system. The results for the FVA are used to develop the food vulnerability annex to the installation emergency response plan (ERP).

b. To meet the antiterrorism requirements, each installation/base, activity, or agency must have an initial comprehensive FVA. Support to perform this initial FVA, as well as training of installation/base staff, is normally requested from the USACHPPM and VETCOM. This is a coordinated evaluation. Veterinary service and preventive medicine personnel normally perform the annual FVA.

c. The DOD Veterinary Service Activity is responsible for food safety and defense of subsistence procured and delivered to DOD installations. This guide is primarily limited to food defense under the control of the installation Commander and staff, generally from the time a delivery vehicle enters the installation boundary, during storage, and until the food is either consumed or sold.

d. Additions. This edition of TG 188 incorporates program requirements for food and water vulnerability at special events, which can occur on an installation. Special events taken place outside the installation must be sponsored by the DOD or the individual military Services and include high-risk personnel and high-profile attendees.

NOTE: DODI 2000.12 requires a vulnerability assessment for any event or activity determined to be a special event or other activity involving a gathering of 300 or more DOD personnel.

e. Vulnerability Assessments are also required for off-installation housing areas, schools, daycare centers, transportation systems, and routes used by DOD personnel and their dependent Family members when the Terrorism Threat Level is Significant or higher. While this guide was designed for use in evaluating food operations on the installation, the basic principles can be adapted to off-installation operations such as public and private schools, daycare centers, and other similar operation. Assessment of off-installation, non-DOD operations must be coordinated with the installation security manager. The installation security manager should be responsible for identifying off-installation facilities requiring FVAs and coordination with any local authorities. The results of the FVA can be used in providing the installation guidance in selecting off-installation sites including housing, schools, daycare and locations for special events.

f. The installation FVA should include evaluation of designated high risk personnel (HRP) and Family members as appropriate.

g. The guide includes a summary of the Joint Staff/Defense Threat Reduction Agency Vulnerability Assessment Benchmarks. This is included to assist the installation in evaluating the effectiveness of its program.

h. The guide also includes information which can be used to develop the food vulnerability annex to the installation ERP.

1-4. WATER SYSTEM OVERVIEW.

a. The Water Supply Management Program (WSMP) of the USACHPPM designed this Water System Vulnerability Assessment (WSVA) protocol based upon the best available information from various federal agencies and professional associations. The intended audience

for this protocol is a technically competent engineer with a background in waterworks and a basic knowledge of physical security fundamentals. Such an assessor (a USCHPPM project officer or qualified installation engineer) should be able to execute a WSVA given this protocol and other appropriate references listed in this protocol. We recommend that the assessor also receive a block of instruction from the WSMP that specifically teaches the methodologies and practical considerations of conducting a WSVA.

b. The WSVA is designed to provide installation Commanders and key staff members with a thorough, risk-based assessment of the vulnerabilities of their drinking water systems and to recommend countermeasures to lower the risk by reducing the probability and severity of these vulnerabilities. The WSVA protocol provides for assessment of virtually any Army water system, regardless of size or complexity, including those systems that purchase water from nearby municipal systems. This protocol was developed to counter growing concerns of potential terrorist attacks on critical components of the utility infrastructure. It addresses water system vulnerabilities that, if successfully exploited, could result in—

(1) The physical destruction of water system assets.

(2) The intentional contamination of raw or treated water supplies.

(3) A cyber-attack that could affect the water system's ability to produce, store, or distribute treated drinking water.

c. In July 2002, President Bush signed into law the House of Representatives (H.R.) 3448 - *Public Health Security and Bioterrorism Preparedness and Response Act* (that is, Bioterrorism Act). This act effectively amended the Safe Drinking Water Act (SDWA) to require community water systems serving greater than 3,300 consumers to conduct a WSVA and update or develop their ERP incorporating the findings of the WSVA. In addition to this Federal requirement, both the DOD and Army require military installations to conduct a WSVA and update ERP plans.

d. The current concept for execution of this protocol is summarized below. Additional details are presented later in the sections under Chapter Three.

e. As currently designed, at least two individuals with secret clearances should execute this WSVA protocol for a given water system. The team can consist of installation personnel or third-party persons. There is an advantage to utilizing third-party teams because they can provide an unbiased perspective and, thereby, avoid any potential conflicts of interest.

f. Coordination with the installation should begin at least 3 weeks prior to the on-site assessment. This initial coordination could include a scoping visit if the installation cannot provide detailed information prior to the assessment. The assessment begins with a formal entrance brief followed by a physical inspection of the water system target components (assets).

Next, the assessor reviews key documents and standing operating procedures (SOPs) and interviews various managers and workers. The key to a quality assessment is significant input and coordination with all the key players on the installation. The assessor then assimilates the information gathered using the risk management process to determine the current level of risk for the vulnerabilities detected. The assessor also develops recommendations for the observed vulnerabilities. At the end of the on-site assessment, the assessor out-briefs key personnel and tailors any future actions based on input from the installation Commander. In addition to the final written report that documents assessment findings and proposed corrective actions, other installation entities (such as, Preventive Medicine and the Directorate of Public Works) may also request follow-up assistance in matters relating to the vulnerability assessments or the preparation or revision of the ERPs.

1-5. SPECIAL EVENTS OVERVIEW.

a. Chapter 4 describes the roles of the FAWD team while supporting the security authority at special events, which include a meal or food service provided by commercial activities off DOD installations. The goal of the FAWD team is to reduce the vulnerability of food and drinking water to intentional contamination or disruption that might impact the Army's mission. The team is deployed at the request of, and in support of, the Special Event Security Manager (SESM).

b. The FAWD teams are a targeted resource to prevent deliberate contamination of the food and water supplied to an event. The teams may also ensure that food and water obtained off installation meet public health standards. In Continental United States (CONUS), food and water sanitation requirements are based upon Federal, state or local regulations that are enforced by the municipal public health authorities having jurisdiction over the event venue. Vulnerability assessment of off-installation events are made from the perspective of operational risk management rather than compliance with Department of Army or DOD standards.

CHAPTER 2

FOOD VULNERABILITY ASSESSMENT

2-1. INTRODUCTION.

a. Terrorist threat or actual attacks against the food supply can seriously impact the military's mission, the installations mission, and overall quality of life of the community. This chapter introduces Commanders and their staff to the processes and tools needed to identify, evaluate and manage risks posed by these hazards. It is written to assist personnel responsible for force protection in providing risk assessments of threats against military communities and suggested management strategies to mitigate risks. A general overview is provided on how intentional threats can be evaluated within the context of Field Manual (FM) 5-19, and how to communicate these risks to the Commander, the workforce, and sometimes the public and the media. An effective risk management process includes a risk assessment, as well as risk communication process. See **Figure 2-1**, Risk Management Cycle.

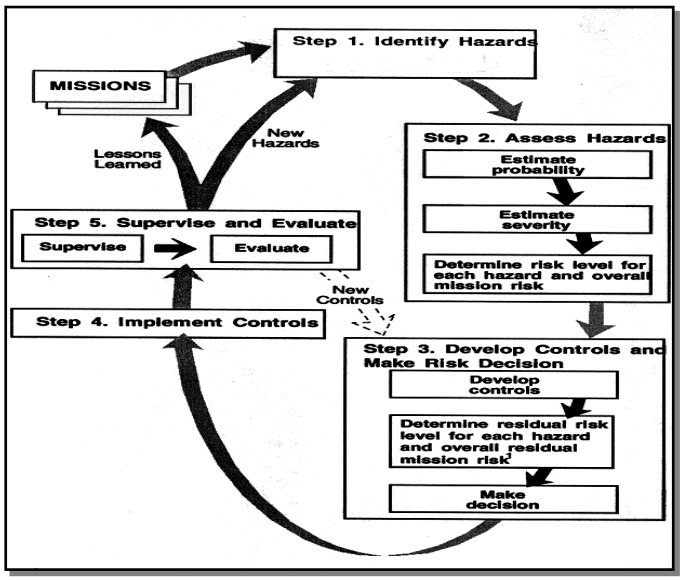


Figure 2-1. Risk Management Cycle

b. Mitigation strategies must be implemented to reduce vulnerability of food from intentional attack. This document focuses on identifying vulnerabilities to intentional attack and employing proactive measures to ultimately prevent any intentional attack. Preventing these incidences from occurring is important in conserving combat power, human resources, and minimizing psychological effects.

c. Personnel can be deliberately exposed to harmful levels of contaminants such as toxic chemicals, radiation, or biological agents. Harmful levels include high-level exposures that result in immediate health effects and/or significant impacts to mission capabilities. Harmful levels also may include low-level exposures that may result in delayed and/or long-term health effects that would not ordinarily have a significant immediate impact on the installation. Why food? Food is an attractive vehicle for poisoning or infecting military personnel, their families and other individuals. Many different physical, chemical, biological and radiological agents can be placed in food without being detected until the food is consumed and symptoms develop. Depending on the population effected, the type of agent and dose, the symptoms can range from mild discomfort to death.

d. The DOD risk management doctrine provides Commanders with methods to evaluate and manage the risks posed by hazards to the military community. This framework is a process that is integrated into planning and decision making at all levels. Leaders manage risk by evaluating hazards and implementing risk management options during course of action (COA) development.

e. The DODI 2000.16 requires at least annual vulnerability assessments. Preventive medicine, veterinary and other food service inspection and supervisory personnel should be trained in food defense requirements and include these in their routine assessments. The FDAT, as designated by the installation Commander, will participate in the risk management process by identifying food hazards, assessing the threat associated with these hazards, characterizing the risks in the context of the proposed COA, effectively transmitting the risk assessments, and recommending appropriate control measure options to the Commander. Commanders will then be able to make informed decisions. Once decisions are made, members of the FDAT will likely be expected or tasked to participate in risk communication efforts to convey information, conduct food defense training and address worker and/or public concern. Participation may range from being a spokesperson, to developing written information, to conducting a risk communication needs assessment. The guide upgrades the definitions for probability, severity, and risk level.

f. For purposes of this guide, the term food includes: food, drinks, food ingredients, ice, and bottled water. Bottled water includes individual size containers as well as bulk water containers supplied to office or for home delivery and water vending. Water in piped systems within the food establishment or food operation is also included in the FVA from the building connection to the installation distribution system, including any internal water storage and treatment, to the point of use. Water in the installation distribution system, prior to the connection to the building, is included in the water vulnerability assessment (WVA).

g. The risk management Cycle is a five-step process. Steps 1 and 2 together comprise the risk assessment. Steps 3 through 5 are the essential follow through actions to effectively manage risk. This approach compliments the military decision-making process (MDMP) described in FM 5-0.

2-2. PLANNING.

a. Recent events and the known threat of intentional contamination of food supplies and food operations highlight the need to enhance force protection activities. Installation Commanders have primary responsibility for ensuring implementation of necessary protective measures to counter terrorist threats to military food supplies. Commanders are encouraged to conduct a systematic review/assessment of installation food supplies and food operations and develop/implement an installation food defense program (**See Figure 2-2**).

FACT SHEET

Summary Joint Staff Integrated Vulnerability Assessment (JSIVA) Food Vulnerability Benchmarks

1. JSIVA requires:

   a. An implemented food defense program.

   b. An office be assigned primary responsibility for installation food defense.

   c. A multi-disciplinary FDAT be established to conduct systematic reviews and assessments.

   d. An annual FVA.

   e. All food operations should be included in the FVA.

   f. The FVA be accomplished according to TG 188.

2. JSIVA also requires that surveillance procedures be linked to the FPCON or threat levels. The Provost Marshall (PM) and veterinary surveillance program as a part of the installation ERP should be linked to the FPCON and threat levels.

Figure 2-2. Fact Sheet - Summary Joint Staff Integrated Vulnerability Assessment (JSIVA) Food Vulnerability Benchmarks

b. To develop an effective food defense program, the Commander should—

(1) Identify an Office of Primary Responsibility (OPR) for the installation.

(2) Establish a multi-disciplinary FDAT that will conduct a systematic review and assessment of installation food systems using the principles of risk management

c. The FDAT should consist of the following core personnel:

(1) Installation Anti-Terrorism/Force Protection Officer (FPO).

(2) Installation Preventive Medicine Officer or Environmental Science Officer.

(3) Installation Veterinary Corps Officer.

(4) Installation Food Advisor/Manager.

(5) U.S. Army Criminal Investigations Division (CID) Agent.

(6) Military Intelligence (MI).

(7) Provost Marshall Office (PMO).

d. Auxiliary (On-call) FDAT members may include:

(1) Environmental Management (Facilities Engineer) Officer.

(2) The PM/Installation Security (if not a core member).

(3) Transportation.

(4) Supply/Logistics.

(5) Contracting Officer(s) for Food Supplies, Operations, Ice, and Bottled Water.

(6) Staff Judge Advocate General (JAG).

(7) Risk Communication specialist or, at a minimum, Public Affairs Officer (PAO).

(8) Emergency Room/Troop Medical Clinic Supervisors.

(9) Hospital Dietitian.

(10) School Food Service Manager.

(11) Army and Air Force Exchange Service/Navy Exchange/Marine Corps Exchange (AAFES/NEX/MCX) Food Service Manager.

(12) Child Development Center/Youth Activities Food Services Manager.

(13) Morale, Welfare, and Recreation (MWR) Food Manager.

(14) Commissary Management Representative.

(15) Others as required or designated by the installation Commander.

e. The core team members must have appropriate security clearances. The auxiliary team members should have appropriate clearances if they are involved in report preparation or similar activities.

f. The installation Commander should appoint a team chief for the FDAT from the core team members. Because the majority of vulnerabilities identified are usually in the area of security, it is recommended that the FDAT team chief be from the force protection, security or PMO. All core members should be appointed on orders.

g. Pre-assessment and exit briefings may be required at the direction of the Commander.

2-3. ASSESSMENT PROCESS.

a. The FDAT should use the following steps to conduct the assessment, after the threat has been evaluated:

(1) STEP 1: Develop a comprehensive list of food assets

(2) STEP 2: Conduct on-site assessment

(3) STEP 3: Identify hazards and vulnerabilities

(4) STEP 4: Assess hazards and vulnerabilities

(5) STEP 5: Recommend controls and determine residual risk

(6) STEP 6: Generate a report for the Commander

NOTE: Implement Controls and Supervise and Evaluate are two processes that are not part of the assessment; they are directed by the Garrison/Installation/ Combatant Command (COCOM) Commander after the FDAT's report is completed. However, they still form a part of the operational risk management process.

b. Format for installation food safety and defense programs will vary depending on installation type, location, size, distribution chain, personnel involved, etc. Unique conditions of each food system should be considered during development of a program. Food supply and distribution systems should be examined for current safety and security operations. After initial procedures are developed, periodic reviews should be accomplished to ensure that vulnerabilities are correctly characterized and to verify and update the program and all its assumptions, guidelines, and restrictions.

2-4. VULNERABILITY ASSESSMENT.

a. **Step 1**: Develop a comprehensive list of food assets. Direct coordination with all food activities is required. This will assist in developing the list of food assets. This list should include personnel, transportation systems, contracting, storage facilities, and preparation and serving resources, supply systems, contractors and businesses approved for selling or delivering food and bottled water onto the installation, etc. See **Figure 2-3**, for assistance in identifying these assets.

b. **Step 2**: Conduct On-site Assessment.

(1) Describe the installation food procurement sources and the distribution from their sources. Develop flow diagrams that describe the processes for each asset (see **Figures 2-4** through **2-7** for examples of flow diagrams). The purpose of a flow diagram is to provide a clear, simple outline of the steps involved in the process. The scope of the flow diagram must cover all steps in the process. A schematic of the facilities involved is useful in understanding and evaluating process flow. If a process flow diagram does not already exist in documents contained in the Veterinary Installation Support Plan (ISP), the FDAT must construct one based on their knowledge of the process. Each food asset, to include supply, distribution, storage, retail sale or preparation and serving should be studied to provide the insight to comprehensively understand the actual process and identify vulnerable areas. This flow chart will provide the foundation for the hazard analysis and must be detailed and complete. It must depict all of the steps in the process.

(2) With appropriate security classifications applied (as directed by the Anti-Terrorism Officer (ATO), video cameras or digital cameras may be useful in gathering and conveying information to the team as assessments are carried out. Potential threats are systematically identified, located, and assessed based on the information provided by other team members and an analysis of the current threat situation (see **Figure 2-8**. Prior installation Commander/ATO authorization must be obtained prior to use.

#	NAME OF ASSET or ESTABLISHMENT	Location	POC & Telephone
1	Troop Issue Subsistence Officer/Installation Food Advisor/Food Service Officer Hospital Nutrition Care Division All OPRATS Storage Locations		
2	Defense Commissary Agency (DeCA) activities		
3	NAF/MWR Contracting Officer Child Development Center Youth Services Officer/NCO Clubs Sports Clubs Gymnasiums Civilian Welfare Fund		
4	AAFES/NEX/MCX Post Exchange All Shoppettes Service Stations Food Court Facilities Fast Food Restaurants Mobile Food Services		
5	Fast Food Delivery (from off-installation)		
6	Office and home bottled water delivery		
7	Home food delivery contracts and vendors		
8	Non-AAFES mobile food operations		
9	DOD Dining Facilities (DFACs)		
10	Hospital food service operations.		
11	Vending machines, including water vending		
12	Temporary and Special Event Food Operations, Chapels, etc.		
13	Off installation food operations supporting High-risk personnel including schools and child care facilities.		
14	DOD Dependant Schools (DODDS) Cafeterias		
15	OCONUS Local National Food Service		
16	Donated Food Operations		
17	Other Food Activities not listed above		

Figure 2-3. Asset List Example

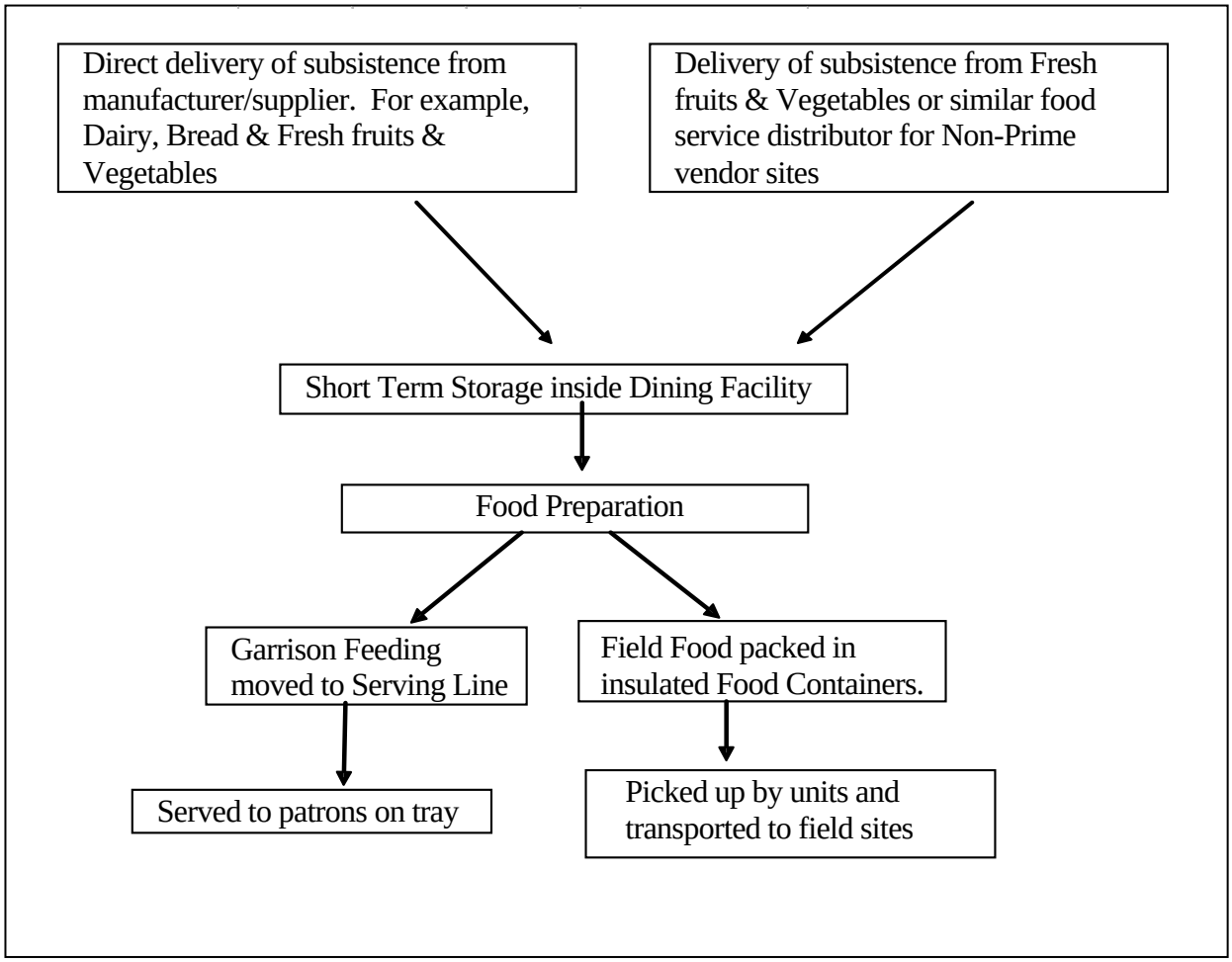


Figure 2-4. Example Conventional Dining Facility (DFAC) Flow Diagram

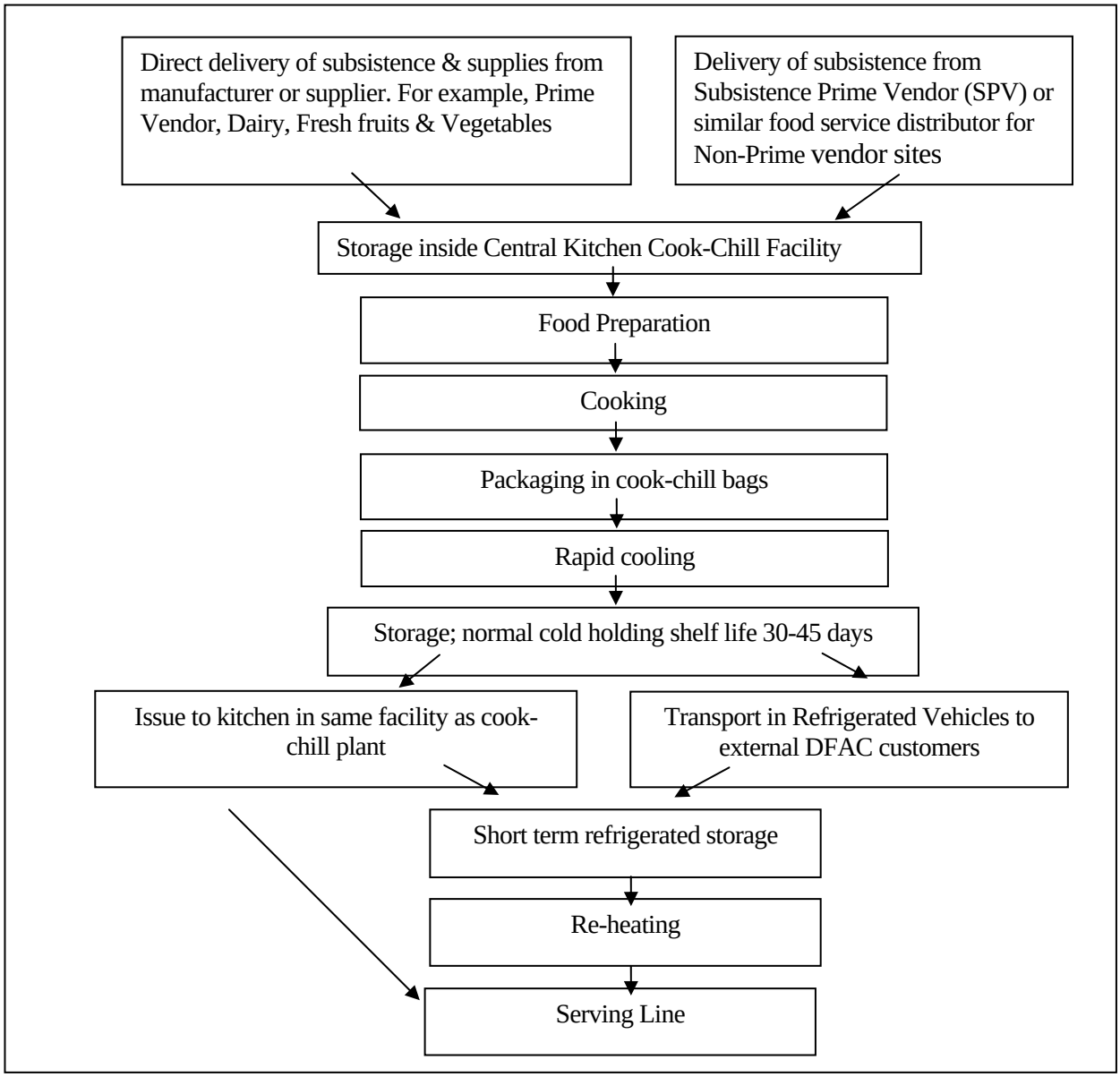


Figure 2-5. Example Food Service Facilities with Cook-Chill Facilities Flow Diagram

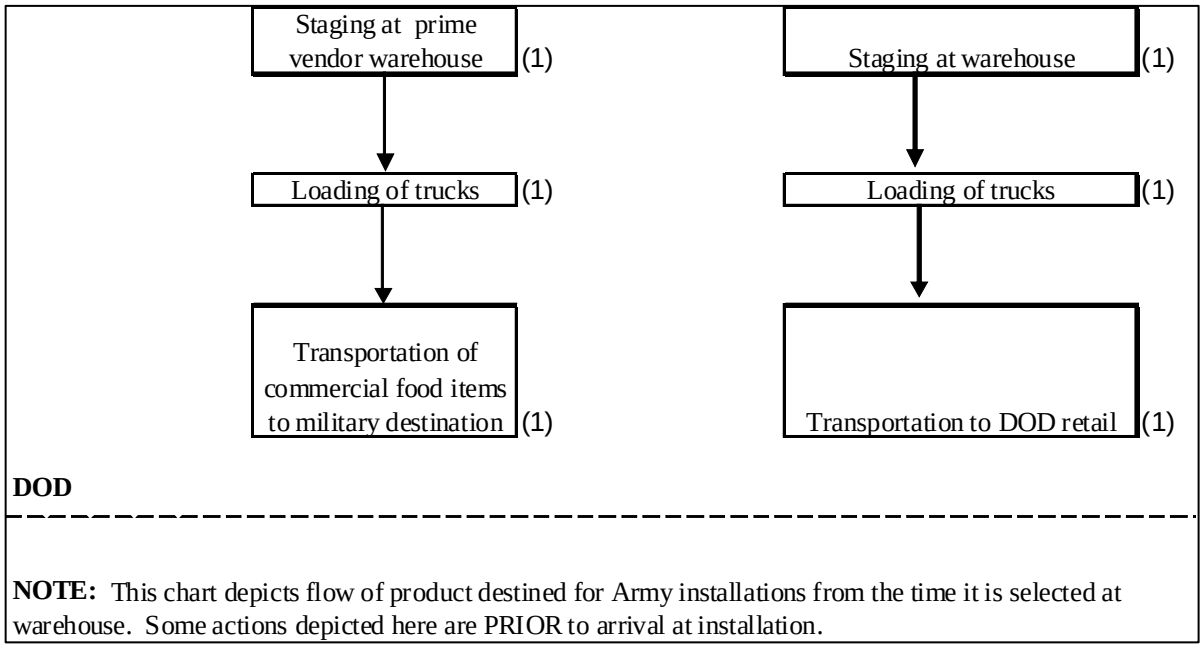


Figure 2-6. Example Delivery Subsistence Prime Vendor or Retail Food Distributor Flow Diagram.

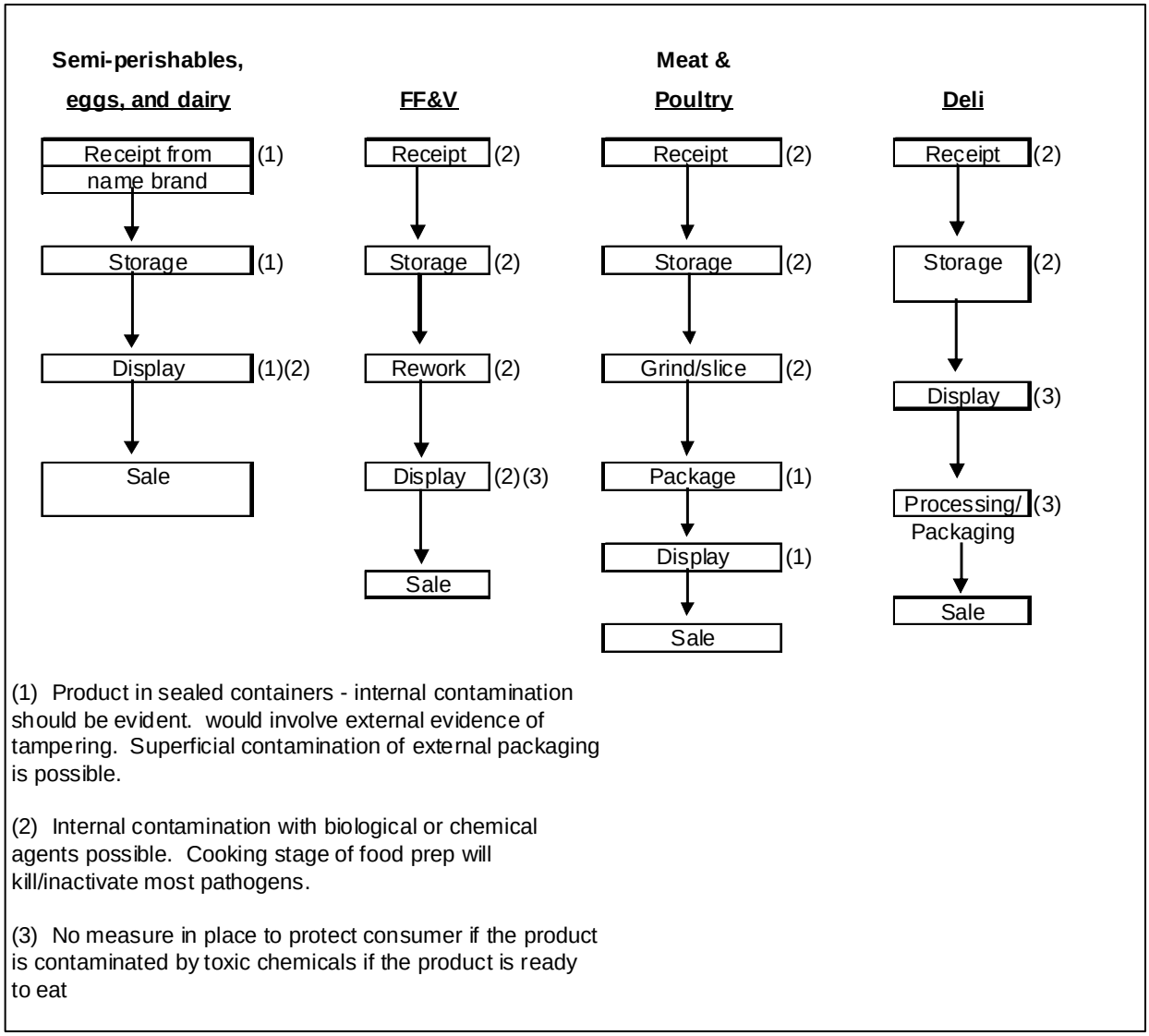


Figure 2-7. Example Retail Store Flow Diagram

FOOD VULNERABILITY CHECKLIST

Facility/(Suppliers)	Max # patrons/ meal	Food Type Served	Notes

Potential Hazard	Assess Risk/Discussion	Risk Level	Options/ Recommendations
1. Facility security			
a. Was an individual assigned responsibility for security? (FS-FF-01) (Std. 14, 16)			
b. Are there procedures for investigating unusual activity? (FS-FF-01) (Std. 14, 16)			
c. Was there unrestricted access into building? (FS-FF-02) (Std. 10, 16)			
d. Is access to building monitored? (FS-FF-02) (Std. 10, 16)			
e. Were contractors (cleaning, maintenance, construction, etc.) or visitors (tours, sales, auditors, truck drivers, regulators, mail delivery, concessionaires, vendor stockers, etc.) recorded, limited to their activity and supervised? Are contractors, equipment maintenance and custodial personnel positively identified and as appropriate compared against work order request? Are visitor passes collected upon departure? (FS-FF-04) (Std 10)			
f. Were contractor tools, equipment, vehicles inspected prior to entering facility? (FS-FF-04) (Std. 10)			

Figure 2-8. Food Vulnerability Checklist (Food Service or Retail Establishment)

Potential Hazard	Assess Risk/Discussion	Risk Level	Options/ Recommendations
g. Is the area around the facility adequately illuminated for nighttime security monitoring? Are facilities periodically inspected by security personnel during non duty hours? Std 14, 16			
h. Was hazardous chemical (such as, cleaning/sanitizing agents, pesticides) storage access restricted? Is application monitored? (FS-FF-05) (Std. 10)			
2. Employees			
a. Are employee criminal background checks performed? (FS-FF-06) (Std. 18, 10, 14)			
b. Are employees made aware of potential for food contamination and need for vigilance?			
c. Is current list of employees maintained? Are authorized entry restrictions in place (keys/photocell badges, etc)? Are control procedures in place in the event of lost keys/badges, etc.			
d. If badges or other forms of ID are used, are they difficult to counterfeit?			
e. Are personal items excluded from preparation and storage areas?			
3. Food Receiving			
a. Was food accepted from un-approved sources? (FS-FF-07) (Std. 10)			
b. Are AT measures included in subsistence contracts? DOD Std 18			

Figure 2-8. Food Vulnerability Checklist (Food Service or Retail Establishment) (continued)

Potential Hazard	Assess Risk/Discussion	Risk Level	Options/ Recommendations
c. Was verification of truck locks and unique seals on receipt performed according to current FPCON level? Is vehicle resealed or escorted between multiple delivery points? (FS-FF-08, FS-TR-01) (Std. 10)			
d. Was delivery and driver verified by the distributor? (FS-TR-04) (Std. 10, 14)			
e. Was incoming food inspected for evidence of tampering? (FS-FF-09) (Std. 10)			
f. Was a trace back system in place to document possible contaminated foods? (FS-FF-10) (Std. 17, 18)			
g. Was the delivery door secure, when the storage room was not occupied by staff personnel? (FS-FF-02) (Std. 10, 16)			
h. Was staff available for review/receipt of food items at the time of delivery? (FF-FS-04) (Std. 10)			
i. Were delivery personnel allowed unescorted access to facility food areas? (FS-FF-04) (Std. 10)			
4. Serving Food			
a. Do food preparation operations inhibit/deter the intentional contamination of food items? (Std. 10)			
b. Did customers have un-restricted access to food/drink/ice at service or sale? Are customer self-service operations monitored? (FS-FF-11) (Std. 10, 16)			

Figure 2-8. Food Vulnerability Checklist (Food Service or Retail Establishment) (continued)

NOTE ABOUT FIGURE 2-8:

The employees of an organization have access to most, if not all areas of an operation. This means that if an individual, or group of individuals wanted to have a detrimental impact on an organization or service it would not be difficult. Therefore, it is very important that the identity and trustworthiness of personnel be investigated.

The local procurement contracting authority can specify additional security measures in contract awards to mandate extra measures that can be taken by local vendors to assist in the safeguarding of food destined to the military community. The DOD Standard 18 requires that antiterrorism performance be considered as an evaluation factor.

At heightened threat levels, all deliveries must be identified as being authorized. The attending security personnel should record delivery vehicles entering the installation at the gate. This information should include, as a minimum, truck driver's name, and state driver's license number, truck license number, time at entry and exit, and destination. The vehicle container should be resealed after inspection by military police (MP) or security personnel or escorted to the first delivery site. The installation veterinary activity must have a food delivery vehicle inspection program which is coordinated with the installation security and with the threat level.

Access to storage areas should be limited to authorized employees of the organization. Other personnel (such as drivers, contract stock persons, etc.) should be limited to their area of responsibility or need. This may require increased monitoring, restricted area badges, or escorts, as needed.

Access to preparation/sale areas may not be limited to authorized employees of the organization. Other personnel (such as drivers, contract stock persons, etc.) should be limited to their area of responsibility, or need. This may require increased monitoring, restricted area badges, or escorts, as needed. If a threat is anticipated, pre-emptive measures might be considered at this stage to preclude intentional contamination from occurring. (This may include using only canned or field rations in facilities, removing all self serve food bars to preclude a possible intentional contamination, etc.) This is not an inclusive list, but it is designed to provide ideas on areas to consider safeguarding that are especially vulnerable.

Figure 2-8. Food Service or Retail Establishment (continued)

c. **Step 3**: Identify Hazards and Vulnerabilities.

(1) Background. Personnel may be exposed to harmful agents from the intentional actions of perpetrators. Exposure can occur from intentional contamination of food, bottled water, ice, physical destruction or disruption of equipment including storage facilities, or a combination of these sources.

(2) The degree with which exposure to one or more materials will result in harm to military personnel and/or the mission will depend on many things, but primary considerations include—

(a) Types of hazard.

(b) Sources of exposure.

(c) Concentration, toxicity or virulence of the chemical, biological or physical agents or other hazards.

(d) Frequency and duration of exposure.

(e) Natural human variability in susceptibility to these conditions.

d. **Step 4**: Assess Hazards and Vulnerabilities.

(1) Within Step 4, evaluation of probabilities, severities, risk characterization, and confidence determination also takes place.

(2) In terms of food systems surveillance and risk assessment, this risk management step examines each hazard in terms of probability and severity to characterize risks of health threats and medical threats posed by intentional food contamination hazards. Risk characterization estimates risk levels and describes their role in the context with installation activities. Three steps are involved during the assessment phase—

(a) Evaluate Hazard Probabilities. Determine the hazard probabilities for all selected hazards.

i. Hazard probabilities for all selected hazards must be determined. Probability levels estimated for each hazard may be based on the current threat or frequency of a similar event, or for food-specific hazards, the magnitude, frequency and duration of exposure of community personnel to health threats integrated with the expected incidence of exposure within the installation relative to guideline levels.

ii. Determining food hazard probability is an evaluation where food asset data are assessed to determine the degree of exposure to the hazard. The estimation of hazard probability involves the following primary considerations:

- Comparability of the installation's exposure profile (exposure factors, frequencies, and durations) to the standard exposure profile used in the derivation of the exposure guideline(s) of concern.

- Proportion of the installation that is likely to experience exposures relative to the specific exposure guidelines.

- Developing procedures to receive credible threat assessments from intelligence personnel (such as, MI, CID, Federal Bureau of Investigations (FBI), etc.). The threat assessments would be based on availability of agents (biologic, chemical, radiological and physical) and aggressor's (terrorists, criminals, subversives, disgruntled employees, etc.) ability to carry out an attack.

- Confidence in the available data, given the sources of uncertainty and variability. When these determinations are made, a hazard probability category must be selected for each food hazard. The general categories of hazard probability are—

  - FREQUENT - occurs very often, continuously experienced.

  - LIKELY - occurs several times.

  - OCCASIONAL - occurs sporadically.

  - SELDOM - remotely possible; could occur at some time.

  - UNLIKELY - can assume will not occur but not impossible.

(b) Evaluate Hazard Severities.

i. Hazard severities for all selected food hazards must be determined. Hazard severity is a function of the consequence of exposure (such as, nature of probable effect) and the predicted distribution of that impact on the installation. The estimation of hazard severity involves three primary judgments:

- Proportion of the installation population or food operations that are likely to exhibit effects.

- Nature of the health effect(s) associated with exposures.

- Confidence in the available data, given the sources of uncertainty and variability.

ii. When these determinations are made, a hazard severity category must be selected for each food hazard.

- **CATASTROPHIC** - loss of ability to accomplish the mission or mission failure. Example indicators: Death or widespread severe illness.

- **CRITICAL** - significantly (severely) degraded mission capability or readiness. Example indicators: Multiple foodborne illness incidences.

- **MARGINAL** - degraded mission capability or readiness. Example indicators: Sporadic foodborne illness, loss of confidence in food supply safety.

- **NEGLIGIBLE** - little or no adverse impact on mission capability or readiness.

iii. Severity can also be affected by—

- Location of incident. For example, attacks against a food establishment supporting mobilization or deployments, DFACs, ships, galleys, child development center (CDC), youth services, dependent school or hospital.

- Population affected. For example, rapid deployment forces or combat units, command and control and emergency response personnel, HRP, very important people (VIP) and guests, personnel responsible for operation of critical infrastructure, dependants including school age children and nursery.

(c) Risk Characterization. Synthesize the estimates of hazard probabilities and severities. Initial Risk levels for all food hazards and the overall mission are determined and described in a public health context.

i. Once the food hazard probability and severity estimates are determined, they are synthesized in this step. Risk levels for all selected hazards are described in the context of the current threat situation. The risk level is defined using the probability and severity information from the previous sections combined with command judgments regarding acceptable risk levels for the installation.

ii. The primary objective is to apply the Risk Assessment Matrix (**Table 2-1**) in a way that is consistent with command guidance so that these risks can be put in the same context with other identified risks. This idea must remain central to the planning perspective—food threats must be clearly communicated to the Commander and the staff. This must occur so that the Commander can make decisions based on credible information.

Table 2-1. Risk Assessment Matrix

	HAZARD PROBABILITY				
HAZARD SEVERITY	**Frequent (A)**	**Likely (B)**	**Occasional (C)**	**Seldom (D)**	**Unlikely (E)**
Catastrophic (I)	Extremely High	Extremely High	High	High	Moderate
Critical (II)	Extremely High	High	High	Moderate	Low
Marginal (III)	High	Moderate	Moderate	Low	Low
Negligible (IV)	Moderate	Low	Low	Low	Low
	RISK ESTIMATE				

iii. Risk characterization should be designed to facilitate the selection of risk control strategies that are associated with risk levels that are greater than an installation-specified rate (as determined by the Commander). **Table 2-2** presents the risk management risk levels, and **Table 2-3** is an example of Severity Ratings.

Table 2-2. Risk Level Definitions

RISK LEVEL	CONSEQUENCE
Extremely High	Expected loss of ability to accomplish the mission, or serious workforce or community impact (either on- or off-post).*
High	Expected significant degradation of mission capabilities in terms of the required mission standard, inability to accomplish all parts of the mission, or inability to complete the mission to standard if hazards occur during the mission, or significant workforce or community impact (either on- or off-post).*
Moderate	Expected degraded mission capabilities in terms of the required mission standard will reduce mission capability if hazards occur during mission, or minor workforce or community impact (either on- or off-post).*
Low	Expected losses have little or no impact on accomplishing the mission, and little or no impact on the community (either on- or off-post).*
*To assess the mission, workforce, or community impact, the FDAT should consider the psychological consequences of a terrorist event.	

Table 2-3. Example Severity Ratings

Anticipated Result of Event	Severity
Loss of ability to provide food to all consumers for an unacceptable period of time.	Catastrophic
Loss of ability to provide food to a critical customer (such as, a hospital or rapid TOE unit) for an unacceptable period of time.	Catastrophic
Intentional contamination of food causing immediate serious health threat to the most vulnerable population, (such as, children in school or day care, hospitalized patients).	Catastrophic
Intentional contamination of food with an unmonitored substance that would cause serious illness or death. Destruction of major refrigeration units, (such as, at commissaries or cold storage). No back-up system or plan available.	Catastrophic
Loss of ability to provide food to one area or portion of the installation for an unacceptable period of time.	Critical
Intentional contamination of food with any substances causing delayed serious health problems.	Critical
Intentional contamination of food served or sold to any consumers with an unmonitored substance that is suspected to cause serious illness or death.	Critical
Loss of ability to provide food to remote personnel for an unacceptable period of time, (such as, delayed shipment; loss of refrigeration equipment). Back-up systems or back-up menu available.	Marginal
Destruction of limited menu items or food service equipment for which substitutions are available.	Marginal
Intentional contamination of food by substances affecting taste, color, or odor but not causing serious illness or death.	Marginal
Property damage except damage to critical refrigeration or cooking equipment.	Marginal

iv. Following a food terrorism event, fear and panic can be expected. Psychological responses following the event may breed unrealistic concerns for personal safety and for the safety of Family members. A terrorism event that affects Family members, especially infants and children, may affect the soldier's psychological stability and ability to perform his/her mission. For this reason, CDCs, schools and other community accessible food operations and retail stores will be given a higher rating of hazard severity even if there is minimum illness or death. A threat or an attack against these populations can adversely affect unit readiness without causing any casualties. Force protection plans should include the availability of mental health support personnel to assist in the event of a terrorist attack.

Appropriate risk communications information should be developed as questions and answers and coordinated with the PAO. There should be a single point of contact to relay information and answer personal and press inquiries.

(d) Determine Confidence in Risk Estimate.

i. A confidence level should be assigned following the derivation of the risk estimate. The degree of confidence in the risk estimate will be particularly important when determining a COA. Confidence levels should be simple categories that can be rationally explained (such as, high, medium, low). The confidence level assigned to a risk estimate should integrate uncertainty associated with each of the elements of the risk assessment. Key areas of uncertainty that should be considered include:

- Sampling or field data quality.
- Actual exposures of installation personnel.
- Installation attributes (such as, demographics, activity patterns).
- Comparability of standard guideline assumptions (such as, exposure duration and frequency) to expected installation exposure patterns.
- Expected symptoms of exposure (that is, hazard severity), including consideration of exposure to multiple hazards.
- Other uncertain, or missing, information relevant to the process.
- Whether the predicted health outcome is plausible, given weight of evidence or real-world experiences.

ii. The final determination of confidence must be based on the well-reasoned judgment of the FDAT members conducting the risk assessment.

e. **Step 5**: Recommend Controls and Determine Residual Risk.

(1) Implementing this risk management task involves developing one or more controls to minimize or eliminate the risks of the evaluated vulnerabilities posed by food and water. Determinations are made whether developed controls are sufficient and acceptable. (See **Table 2-4** and **Table 2-5**.)

Table 2-4. Analyze Risk Control Measures and Rank Example

Hazard	Rank	Risk Control Measures	Remarks
Large food retail facility is destroyed.	1	1. Install locks on all gates and entry areas 2. Place 24-hour security at food storage. 3. Obtain guard dogs 4. Install surveillance cameras 5. Post a DO NOT ENTER Sign	
Food, in on post storage facility, troop issue subsistence activity (TISA) or commissary, is intentionally contaminated.	2	1. Install locks on all gates and entry areas. 2. Provide employees with picture identification (ID) cards. 3. Place 24-hour military security with guard dogs at food storage facilities. 4. Install surveillance cameras around and inside the storage building. 5. Lock all refrigeration units 6. Post a "Do Not Enter" sign	

NOTE: Risk control measures are identified through conducting what if scenarios and brainstorming with personnel responsible for controlling the hazard. In conducting the risk control analysis and ranking the benefits of the control, remember effective control measures reduce the probability, severity, or exposure of a hazard or risk of occurrence.

Table 2-5. Make Control Decisions and Implement Risk Controls

Hazard	Risk	Preventive Measure	Control Decision	Residual Risk (To be completed by team)
Large food retail facility is destroyed.	1	1. Install locks on all gates and entry areas 2. Place 24-hour security at food storage. 3. Obtain guard dogs 4. Install surveillance cameras 5. Post "DO NOT ENTER" signs	Implement 1, the installation of locks on all gates and entry areas. Implement 3, obtaining guard dogs Implement. 5, post "DO NOT ENTER" signs.	
Food in on post storage facility, TISA or commissary, is contaminated.	2	1. Install locks on all gates and entry areas. 2. Provide background checks and picture ID cards. 3. Place 24-hour military security with guard dogs at food storage facilities. 4. Install surveillance cameras around and inside the storage building. 5. Lock all refrigeration units 6. Post " DO NOT ENTER" signs	Implement 1, the installation of locks on all gates and entry areas. Implement 2; provide employees with photo ID badges. Implement 3, place 24-hour military security with guard dogs at the TISA and commissary warehouse. Implement. 6, post "DO NOT ENTER" signs.	

NOTE: For each identified hazard, select those risk controls that will reduce the risk to an acceptable level. The best controls will be consistent with the mission objective and the use of resources. Determine if the cost versus benefit involved in the decision is recorded if the control is not in place or risk is assumed because other controls cannot be put in place. The objective is to select the best possible combination of risk controls from the options. Once it is selected, the individual in charge must make the final decision for implementation and implementing the risk control action. There should be clear implementation guidelines with accountability and appropriate command support. The residual risk is determined after the decision in made to implement controls.

(2) Hazard controls for food vulnerabilities can be divided into three basic categories.

(a) Education and Training. To fully implement food defense measures, the following areas of education and training should be implemented:

1. Educate food service personnel and their supervisors on the importance of basic housekeeping practices. and good personal hygiene standards in reducing the risk of possible contamination (either intentional or unintentional) of food and water supplies.

2. Inform all personnel, including the general public, to report anything out of the ordinary or suspicious regarding food safety and potential contamination to either military police or medical personnel as appropriate. In addition, concerns with the safety of any food product and illnesses potentially associated with it should be reported to medical personnel.

3. Train all personnel on the dangers of intentional contamination of food.

4. Train Commanders, medical and food service personnel, environmental and contracting representatives, CID, and force protection personnel in proper food defense techniques and protection principles.

5. Train contracting officials to write protective measure guidelines into contracts. As an example, products are produced under quality assurance programs such as the Food and Drug Administration (FDA) guidelines, for microbial quality in fresh cut produce, shell egg quality assurance program, and other quality assurance plans.

6. All food service personnel, preventive medicine and veterinary food inspectors should receive specific threat recognition and response training including recognition of tampering with food products and food containers, appropriate to their duties.

7. Train medical, preventive medicine, veterinary, and food service personnel on monitoring for signs of tampering during the inspection of food, ice, and bottled water. Train clinic staff to include emergency room, troop, and occupational health staffs to recognize early signs of foodborne illness as well as symptoms associated with the intentional contamination of food.

8. Increase the general population's awareness of possible indicators of intentionally contaminated food.

9. At the installation level, designate a central point of contact to which personnel would report possible terrorist activity as well as other concerns with food safety and security. Install a local Hot Line if possible.

10. Provide training for all personnel on the dangers of intentional contamination of food.

11. Provide training for security personnel, including MPs and civilian guards in identifying deliberate contamination of foods.

(b) Physical Controls.

1. Limit access to facility through fencing, locks, etc.

2. Illuminate building exteriors or exterior sites where food is stored or food service operations are conducted.

3. Restrict access to food preparation and storage areas to authorized personnel only.

4. Maintain current list of employees including contract food service, janitorial and maintenance personnel.

5. Validate ID for all service personnel against all service requests. Compare worker to valid work requests. Verify ID of all outside personnel. For example, pest control, chemical salesman, equipment maintenance personnel, and delivery personnel, maintenance, insect, and rodent control personnel.

6. Provide food service personnel with difficult to duplicate photo ID cards that contain their employer and/or place of employment. Cardboard or non-photo ID cards and name plates are unacceptable.

7. Conduct periodic inventory of ID cards and keys.

8. Install surveillance equipment (such as, cameras) to assist in monitoring the activities, facilities, and food preparation areas, as well as any in-house water storage, softeners, filters, or distribution systems to include water softeners or filters where a contaminant could be temporarily placed before introduction.

9. Prohibit personal items brought into the facility (such as purses, gym bags, thermoses, and drink containers) from food preparation and storage areas.

10. Food service operations including retail stores and storage facilities should provide lockers for employees' personal belongings.

11. Use closed (preferably locked or sealed) trucks for transporting food, ice, and bottled water to food establishments, offices, and private on-post residence.

12. Require food suppliers and transportation companies to provide a list of drivers and delivery personnel as well as photo ID cards for authorized personnel.

13. Require backflow prevention on vehicles that connect to potable water supplies (such as fill hoses for water tanks for mobile food units).

14. Use serially numbered seals on vehicles; annotate numbers on shipping papers.

15. Verify shipping seals with shipping papers.

16. Keep parking truck waiting areas away from food operation and storage facilities until the delivery is verified.

17. Minimize number of gates in perimeter fencing and keep locked at all times.

18. All entrances to food operation and storage facilities must be secured. This includes exhaust vents, entrance to crawl spaces, equipment and mechanical rooms, air-handling units, and the roof of the facility.

19. Ensure a 100 percent check of all facilities prior to end of shift to ensure personnel are not hiding in the facility. This check must include a complete walk-through check of bathrooms (both male and female), storage areas, and utility closets. A person should also be identified to check all entry points to make sure they are secured at the end of each duty day.

20. Ensure locks are changed, badges inactivated, etc. when keys/access badges are lost and a key control is maintained.

21. Ensure all food operations including ice machines are secured or visible to facility personnel.

(c) Avoidance—

i. Personnel.

- Conduct work reference checks on all employees (to include concessionaires, drivers, contractors, temporaries and volunteers, or other personnel that may enter a food facility) and random criminal background checks.

- Require background checks for all contract food employees and housekeeping employees who have access to food operations.

- Require transportation companies to conduct criminal background checks on all drivers.

- Perform DNA archiving or fingerprinting on all personnel.

ii. Food.

- Salads, desserts and similar items should be in individually wrapped or packaged single service portions. Desserts and salads should be commercially wrapped or wrapped in food-grade plastic wrap.

- All cooked foods should be brought to a minimum internal temperature of 165 degrees Fahrenheit (°F). This provides some protection against intentional contamination with biological hazards.

- Increase inspection of all food items for signs of tampering, according to current ATO Plan.

- All food items including canned and packaged foods should be checked for tampering both at receipt and upon removal from storage prior to preparation or serving.

iii. Menu.

- During periods of increased threat—

- Evaluate menu to eliminate most easily contaminated food items during periods of increased threat.

  - Eliminate customer self-service buffet and serving areas or post food employee attendants in these areas.

  - Do not publish menu in advance.

  - Have a back-up menu and adequately protected food supplies in the event contamination is suspected.

- In event of significant threat, switch to protected food items (such as, Unitized Group Rations (UGR) Heat and Serve rations, other B Rations, commercially canned foods and Meal Ready-To-Eat (MREs).

f. **Step 6**: Determine Residual Risk and Submit Written Report to the Commander.

(1) Document all results on the risk management worksheets. A final consolidated report should be provided to the Commander (Vulnerability Assessment Management Matrix).

(2) These following (last 2) steps are implemented and managed by the Commander. The FDAT team should be prepared to answer questions, conduct follow-up, and reassess implemented controls and potential new hazards at the Commander's request.

(3) Residual risk is risk remaining after the recommended controls are implemented. The information is communicated to the Commander, and risk decisions are made. These tasks are completed during the MDMP: COA development, COA analysis, COA comparison, and COA approval. Risks are managed by incorporating risk management controls into normal operations.

(4) A key element of risk decision is determining if the risk is justified. The Commander must compare and balance the risk against community expectations. He/she alone decides if controls are sufficient and acceptable and whether to accept the resulting residual risk. If he/she determines the risk level is too high, he/she directs the development of additional controls or alternate controls, or he/she can modify, change, or reject the recommended control measures.

g. The following two processes are not part of the assessment; they are directed by the Garrison/Installation/COCOM Commander after the FDAT's report is completed. However, these two processes still form a part of the overall assessment program.

(1) Implement Controls.

(a) Controls are implemented at all levels, and as a result, must be clear and simple enough to be understood and executed by all affected activities. The other key component of Risk Management—Risk Communication—will play a crucial role in this step because in order for controls to be implemented as directed, they must be communicated in a clear and concise manner to the food workers and consumers. Add to that the likelihood that military personnel, Family members, civilian employees, contractors, media, and the general public may be highly concerned and interested in the safety of the food. Risk communication skills may be as important as the controls being implemented.

(b) Leaders and their staff ensure that controls are integrated into contracts, SOPs, written and verbal directives, and briefings. The critical check for this step, with oversight, is to ensure that controls are converted into clear, simple instructions that can be understood at all levels. Leaders must explain how supervisors will implement controls.

(2) Supervise and Evaluate.

(a) Controls are monitored and surveillance continues for new hazards. All staff must ensure that the risk management process was effective.

NOTE: All levels of the command must understand the information and controls. Constant surveillance of the situation ensures that hazards that may have been missed and new hazards are identified and controlled during the operation.

(b) As the directives or operations are executed, responsible personnel observe and evaluate the risk management procedures set in place. This information further provides data on the effectiveness of current procedures and assists in future planning. This allows for constant evaluation of the risk level and the efficacy of the controls in place.

(c) During preparation and execution, facility managers must ensure that their subordinates understand how to execute risk controls. Managers continuously assess risks during daily operations. Managers maintain situational awareness and guard against complacency to ensure risk control standards are not relaxed or violated. To gain insight into areas needing improvement, managers must continuously evaluate their subordinates and facility's effectiveness in managing risks. (See **Figure 2-9**, Risk Measures Worksheet.)

Risk Control Measures Worksheet

Hazard	Risk	Control Measures*	Control Decision	Residual Risk

***NOTE:** Risk control measures are identified through conducting what if scenarios and brainstorming with personnel responsible for controlling the hazard. In conducting the risk control analysis and ranking the benefits of the control, remember effective control measures reduce the probability, severity, or exposure of a hazard or risk of occurrence.

Figure 2-9. Risk Control Measures Worksheet Sample

2-5. SPECIAL EVENTS CONDUCTED ON A MILITARY INSTALLATION.

The FDAT may be tasked to perform a vulnerability assessment at special event functions conducted on an Installation. When this occurs, the *Installation Special Events* Checklist is utilized. (See **Figure 2-10**, Installation Special Events Checklist Example.)

INSTALLATION SPECIAL EVENTS CHECKLIST EXAMPLE

Facility/(Suppliers)	Max # patrons/ meal	Food Type Served	Notes

Potential Hazard	Assess Risk/Discussion	Risk Level	Options/ Recommendations
1. Event security			
a. Is an individual or group assigned responsibility for security? (FS-FF-01) (Std. 14, 16)			
b. Are there procedures for investigating unusual activity? (FS-FF-01) (Std. 14, 16)			
c. Is there unrestricted access into food preparation and storage areas? (FS-FF-02) (Std. 10, 16)			
d. Is access to event monitored? (FS-FF-02) (Std. 10, 16)			
e. Are contractors (cleaning, maintenance, construction, etc.) or visitors (tours, sales, auditors, truck drivers, regulators, mail delivery, concessionaires, vendors, etc.) recorded, limited to their activity and supervised? Are contractors, equipment maintenance and custodial personnel positively identified and as appropriate compared against work order request? Are visitor passes collected upon departure? (FS-FF-04) (Std. 10)			

Figure 2-10. Installation Special Event Checklist Example (continued)

Potential Hazard	Assess Risk/Discussion	Risk Level	Options/ Recommendations
f. Are contractor tools, equipment, vehicles inspected prior to entering event? (FS-FF-04) (Std. 10)			
g. Is the area around the event adequately illuminated for nighttime security monitoring? Is the event area periodically inspected by security personnel during non-duty hours? Std 14, 16			
h. Are hazardous chemical (such as, cleaning/sanitizing agents, pesticides) storage access restricted? Is application monitored? (FS-FF-05) (Std. 10)			
2. Employees			
a. Are employee criminal background checks performed? (FS-FF-06) (Std. 18, 10, 14)			
b. Are employees made aware of potential for food contamination and need for vigilance?			
c. Is current list of employees maintained? Are authorized entry restrictions in place (keys/photocell badges, etc)? Are control procedures in place in the event of lost keys/badges, etc.			
d. If badges or other forms of ID are used, are they difficult to counterfeit?			
e. Are personal items excluded from preparation and storage areas?			
3. Food Receiving			
a. Is food accepted from approved sources? (FS-FF-07) (Std. 10)			

Figure 2-10. Installation Special Event Checklist Example (continued)

Potential Hazard	Assess Risk/Discussion	Risk Level	Options/ Recommendations
b. Are AT measures included in contracts? Do they address food operations? DOD Std 18			
c. Are delivery and driver verified by the event coordinator? (FS-TR-04) (Std. 10, 14)			
d. Is incoming food inspected for evidence of tampering? (FS-FF-09) (Std. 10)			
e. Is a trace back system in place to document possible contaminated foods? (FS-FF-10) (Std. 17, 18)			
f. Is subsistence secure during transport to event area? (Locked, positive control, seals, etc.)			
g. Is event area secure, when not occupied by food operation personnel? (FS-FF-02) (Std. 10, 16)			
h. Is staff available for review/receipt of food items at the time of delivery? (FF-FS-04) (Std. 10)			
i. Are delivery personnel allowed unescorted access to food areas? (FS-FF-04) (Std. 10)			
4. Serving Food			
a. Do food preparation operations inhibit/deter the intentional contamination of food items? (Std. 10)			
b. Do customers have un-restricted access to food/drink/ice at service or sale? Are customer self-service operations monitored? (FS-FF-11) (Std. 10, 16)			

Figure 2-10. Installation Special Event Checklist Example (continued)

2-6. COMMUNICATING HEALTH RISKS.

a. The FDAT will need to communicate the food risks accurately, objectively and clearly in a credible manner to the Commander. The FDAT will need to prepare to explain the basis for significant assumptions, data, models, and inferences used or relied upon. The FDAT should be prepared to describe the sources, extent, and magnitude of significant uncertainties associated with the assessment. The FDAT must be prepared to assist the Commander in making appropriate comparisons of food risk(s) to other risks.

b. The FDAT may also be requested by the Commander to communicate food risks to the installation/community, although FDAT personnel will not normally lead the risk communication effort. Trained communications personnel should be requested. The following concepts should be followed if required.

(1) Risk Communication.

(a) As with all aspects of the installation food safety program, the installation Commander has the ultimate responsibility for determining if/when information about the program is shared with people outside the FDAT. Although a risk communication specialist/PAO should be a member of this team, no information about any phase of this effort (planning, vulnerability assessment/ findings/selected controls) is to be shared without specific prior approval of the installation Commander.

(b) At the same time, academic research has found that implementing a risk communication process before the ‘unexpected’ occurs helps minimize public concerns and garners public support in the event of a crisis. Including risk communication experts early in the planning process of any project, to include food safety, is as important as the technical work that needs to be accomplished.

(c) In any situation where the potential for concern is high, (such as with food and water safety), risk communication efforts are essential in the overall risk management process. If information is not provided clearly without raising alarm, the information itself is useless.

(d) Within the scientific study of the risk communication process, there are three basic types:

i. Care communication: generally applies to situations where risks are known and accepted by most people, and the dangers are generally recognized. This phase involves providing very general information for a specific purpose.

ii. Consensus communication: applies to situations where groups are encouraged to work together to reach a decision or encouraged to learn how to access, manage, or reduce/prevent risk. This phase involves bringing people together to collaborate on a specific issue/project.

iii. Crisis communication: applies to situations where there is extreme or sudden danger (real or perceived). This phase involves telling people very specific information in a way that addresses concerns while maintaining an appropriate level of vigilance.

(2) For the purposes of this guide, care and crisis communication skills should be incorporated into the overall risk management process for a food safety program. **Figure 2-11**. Example Risk Communication "Checklist".

c. Crisis Communication.

(1) If or when a crisis occurs within the food safety program, the risk communication team members must take the lead in implementing a crisis risk communication plan. This will occur only after the installation Commander makes the decision that the crisis communication plan should be implemented. Applying basic risk communication principles throughout the crisis response phase will increase the likelihood that panic and concern will be kept to a minimum.

(2) Research and evaluation of crisis communication efforts, especially since the September 2001 terrorist events, have identified four key steps in any crisis risk communication plan—

(a) Tell people what you know. People will be concerned and will expect to hear all the facts about the situation— both good and bad. They need this information in order to make personal choices as to what actions they will take in response to the threat. Your key messages must address underlying concerns; be short, as positive as possible, clear and understandable (no jargon or acronyms), and be simple (communicate at the 6th-8th grade level).

RISK COMMUNICATION CHECKLIST

As with any long-term effort, the risk communication process involves a logical sequence of events:

1. Identify the goal/purpose of the risk communication program

   a. Get their attention?

   b. Increase their understanding? Or

   c. Change behavior in some way?

2. Identify stakeholder groups, prioritize them. Stakeholders are those that are or could be influenced by the overall risk communication process. For the purpose of this guide, stakeholder groups might include (but are not limited to):

   a. Workforce (military, civilian, contract).

   b. On-post residents.

   c. Management.

   d. Local officials (local, state, federal).

   e. Military dependents and retirees.

   f. Nearby off-post residents.

   g, Media.

3. Develop communication methods appropriate to each stakeholder group. Be aware of the pros and cons of each when developing the appropriate methods:

   a. Visual.

   b. Written.

   c. Oral.

   d. Computer-based.

   e. Audience-interaction.

4. Develop an overall risk communication plan, to include a crisis communication plan. This plan should include messages/tools appropriate for each stakeholder group. Communication avenues depend on the stakeholder group affected, as well as the time allowed to get the communication out. Some communication avenues include:

   a. Fact sheets.

   b. Press releases.

   c. Press briefings/updates.

   d. Flyers.

   e. Web pages/e-mail updates.

   f. Meetings with those most directly affected.

   g. Town hall meetings.

   h. Brochures.

   i. Public Service announcements.

5. Evaluate the effectiveness of the overall risk communication effort. This ensures that future crisis communication efforts will be better, allows for improvements/corrections to be made, and can be incorporated to make future risk communication programs more effective.

RISK COMMUNICATION CHECKLIST

Figure 2-11. Risk Communication Checklist Example

(b) Tell people what you don't know. In crisis scenarios, research indicates that people understand and accept that you don't know everything right away. By sharing information about what you don't know, you demonstrate that your crisis risk communication process is transparent and that you're being as open as possible with details. At the same time, telling them what you don't know provides the opportunity to share your plan of action, which demonstrates your commitment to their continued health and safety.

(c) Tell people what you're planning to do to find out and when you'll provide that information. This step is critical to reaffirm that you're "in it for the long haul," and that you are committed to keeping people informed as new information is developed. This step also demonstrates your commitment to follow through on promises and that you recognize that when you provide the information is just as important as the information itself.

(d) Tell people what they need to do to protect themselves and what you need from them. Again, these messages should follow basic risk communication principles (see (c) above) so that your goal of changing behavior (such as, practice certain safety measures) is accomplished, and that people recognize the importance of providing you with the information you deem critical.

2-7. RISK MANAGEMENT.

a. Develop Controls and Make Risk Decisions. This section of the guide identifies controls, or countermeasures, to mitigate risk and counter the terrorist threat against installation food and drinking water systems. Controls are grouped in educational, physical, and avoidance based on the risk management guidelines.

(1) Educational Controls. Educational controls are based on individual and organizational knowledge and skills. There are several generic educational controls that can be implemented to protect any food operation. These include improving management practices, increasing routine monitoring and preventive medicine or Veterinary inspections, implementing better communication systems between the installation and the population it serves.

(a) Emergency Contingency Plans. Well-prepared emergency contingency plans can enable a utility to effectively respond to emergencies. Emergency planning should protect food operations personnel, the consumer, the food supply, and food system components. The plans must address weaknesses that were identified in the vulnerability assessment but not mitigated. The plans address both preparation and response to emergency conditions leading to the restoration of full service. These plans should, at a minimum, identify system vulnerabilities and contingencies for addressing those vulnerabilities, individual and organizational responsibilities, ID, and response to emergency warnings and alerts, procedures for recognizing sudden emergencies, procedures to promote effective internal communication, contingency contracts and agreements, emergency response procedures and recovery, the distribution list of

the plan, and plans for individual and organizational training. This plan will mitigate the risk associated with the threat of biological, chemical, and radiological contamination of food. A guide to developing an emergency contingency plan is provided as a file on the accompanying compact disc. Response actions must first protect consumers and then address/resolve the terrorist problem. Appropriate notifications must be made, safe emergency food supplies be made available, necessary expert assistance be obtained as terrorist acts may be preceded by threats. The effectiveness of counter-terrorism responses depends on the care with which the emergency plan has been prepared.

(b) Bacteriological Monitoring Programs. Bacteriological monitoring programs for food are very difficult. The tests available identify specific microorganisms. If the wrong microbe(s) are tested for, a negative test could lead to a false sense of food safety. Only trained veterinary food safety or preventive medicine personnel should conduct any bacteriological monitoring.

(c) Early Warning Complaint Systems. A formal complaint system enables the preventive medicine service and the installation veterinarian to be rapidly notified by consumers of any suspected tampering of the food supply. The early warning complaint system database should track complaints by location and time of complaint. There should also be a response action plan based on the type and frequency of complaints. This system will mitigate the risk associated with the threat of biological and chemical contamination.

i. Short-term Examples.

- Require a sign-in sheet for all personnel, contractors, equipment repair personnel, inspection personnel, etc., who enter food facilities.
- Create a worksheet to simplify note taking on telephone threats.
- Limit access to facilities. Indicate restricted areas by posting “Employees Only” signs.
- Increase lighting in parking lots, loading docks, and other areas that seldom have people present.
- Invite military police and other guards and law enforcement to become familiar with your facilities; establish a protocol for reporting and responding to threats.
- Establish a chain of command, an emergency call list, and a specific spokesperson to be used in emergency situations.

- Provide copies of your operational procedures to local force protection office, law enforcement and emergency management personnel.

ii. Long-term Examples.

- Install motion sensors and video cameras to monitor, detect, and record events. They can be tied into a supervisory control and data acquisition (SCADA) system for remote monitoring.

- Install intrusion alarms that cover remote buildings and grounds.

- Limit access to food operations (such as food courts, clubs, DFACs, and hospital DFAC) especially if self-service salad or desert bars are used.

- Move personnel checking ID to the main entrance of the Post Exchange (PX) and the food court to limit access to authorized personnel.

- Provide stand-alone food operation facility (ies) for contractors and other personnel who are not Army or DOD beneficiaries.

- Develop a clear policy so all employees know how to deal with trespassers.

- Install pass-code locks instead of keyed locks so access numbers can be changed as necessary (such as, when an employee is terminated). (Make sure, however, that emergency response personnel and law enforcement personnel receive the updated assess codes.)

- Fence and lock vulnerable areas (such as, out-of-doors refrigeration equipment, troop issue subsistence (TISA), commissary, and food operation storage areas and loading docks)

- Know your employees and whom it is you are hiring. Conduct background checks, fingerprint, and drug test all new employees. Conduct background checks on any existing non-U.S. citizens.

- Develop and conduct training activities to prepare your staff to detect, delay, and respond appropriately to terrorist attacks and requests for information from the public or media.

(2) Physical Controls/Security. Physical controls are barriers to control hazards. They include physical security and a variety of treatment technologies. Physical security is intended to control the ease of access by a saboteur to food systems. The goal to improve physical security

should be to prevent the undesired event, to reduce the consequences of the undesired event occurring, and to deter the adversary attack.

(a) Physical security will mitigate the risk associated with the threat of biological, chemical, and radiological contamination.

(b) System Upgrades to Reduce Risk of Attack. Specific physical security vulnerabilities identified earlier provide suggestions for measures to reduce risk. Enhancing the existing physical security plan with upgrades should address detection; delay, and response, as well as mitigation features that are intended to prevent the undesired event from occurring. Vulnerabilities that are common to all undesired events should be addressed first. Further, a system feature common to many scenarios is a good candidate for upgrade because upgrading this single feature can usually result in a higher level of protection for many scenarios. Other guidance for placement of specific features includes where it is desirable to have the first detection point and where added delay affects most scenarios. In general, the first detection point must be as early as possible, whereas placing the delay and response and mitigation features closer to the distribution and storage systems will also provide a benefit. Protection-in-depth means that an adversary should be required to avoid or defeat a number of security devices in sequence to accomplish the goal. Layers of features cause difficulty for the adversary to include: increased uncertainty about the system, more extensive preparations prior to the attack, and additional steps where failure could occur. **Table 2-6** presents example options to enhance security based on the "detect, delay, respond and mitigate" approach. For areas such as warehouse and storage areas, which can be accessed by the public, minimize directional signs that would facilitate access to critical areas (such as, storage rooms and hazardous chemical containers).

Table 2-6. Features that Could Increase Physical Security Effectiveness

Increase Physical Security Effectiveness			
Detection	Delay	Response	Mitigation
Add sensors— Doors Windows Gates Add assessment Closed-circuit television (CCTV) Alarm Control Center Add entry control measures Badges Key cards Positive ID	Harden doors Harden gates Harden locks Add barriers— cages vaults	Shorten law enforcement response time Add on-site response officers	Sensors/ equipment to cause system to shut down if contamination detected

(c) System Upgrades to Reduce Consequences. In the event that it is deemed impossible to prevent the adversary from succeeding, the security objective may be to reduce the consequences caused by the attack. Mitigation features or consequence reduction features should then be considered for each undesired event. Some mitigation features might include: redundancy, contingency plans, early-warning systems, stockpiling of back-up food supplies, or identifying critical equipment.

(d) System Upgrades To Deter Adversary. Deterrence is an attempt to increase the actual or perceived level of the security system. This may be accomplished by adding visible security features (such as, warning signage, fences, cameras, or security officers) or by adding surveillance equipment or features that provide ID for prosecution evidence. The effectiveness of deterrence is difficult to measure. It would be a mistake to assume that because an adversary has not challenged a system that the effectiveness of the system has deterred such challenges. Further, note that not all threats are going to be deterred, and some level of prevention or mitigation are still required. **Table 2-7** provides examples of features that might increase the perception of the protection system.

Table 2-7. Features that Might Increase Perception of Protection

Deterrence
Add visible features - Warning signage - Locked doors - Cameras for surveillance and recording devices for prosecution data - Patrols - Barriers for critical assets - Sirens and lighting systems

(3) Avoidance. Avoidance is not using the contaminated food and instead seeking other sources. Avoidance will mitigate the risk associated with the threat of biological, chemical, and radiological contamination.

(a) Alternative Food Supplies. Alternate supplies of food, ice, and bottled water could be provided if terrorists threaten the installation food supply. Alternate foods supplies include MREs, UGR (Heat and Serve) providing bottled water or ice from alternative sources, on post-secure operations and transporting food from another installation. The installation should stockpile bottled water and non-perishable food in the event terrorist attack or disable critical food storage or food operations. This should be part of the emergency contingency plan.

(b) Conservation Programs. If an adequate supply of food water is not available or if critical food equipment has been damaged or destroyed, it may be necessary to limit consumption or move food products from one facility to another.

b. Implement Controls and Supervise and Evaluate. Steps 3 through 5 of the Risk Management Cycle are illustrated in the example presented earlier in this guide. The Installation FDAT should now continue to apply the risk management principles based on their site-specific assessment.

2-8. POINTS OF CONTACT. Some useful addresses and websites are provided in Appendix E.

CHAPTER 3

WATER SYSTEM VULNERABILITY ASSESSMENTS

3-1. INTRODUCTION.

a. Use of this Protocol. The WSMP of USACHPPM designed this WSVA protocol based upon the best available information from various Federal agencies and professional associations. The intended audience for this protocol is a technically competent engineer with a background in waterworks and a basic knowledge of physical security fundamentals. Such an assessor (a USCHPPM project officer or qualified installation engineer) should be able to execute a WSVA given this protocol and other collected references. We recommend that the assessor also receive a block of instruction from the WSMP that specifically teaches the methodologies and practical considerations of conducting a WSVA.

b. Background. The growing threat of international and domestic terrorism has generated heightened concern over public safety and the vulnerability of our national infrastructure. Because the American military serves as a symbol of our country's strength, military installations present an ideal target for terrorists who wish to create fear and attract sensational media coverage. Of particular concern is the vulnerability of drinking water systems that serve U.S. Forces and their Families. Although essential to human life, the delivery of quality drinking water has been generally taken for granted. Complacency with regard to security measures can provide a terrorist with opportunistic targets. With relatively little effort, it may be possible to bring about catastrophic effects by attacking a water system. Fortunately, steps can be taken to significantly reduce the probability or severity of terrorist attacks. This protocol addresses water system vulnerabilities that, if successfully exploited, could result in—

(1) Physical Destruction of Water System Assets. This is generally defined as damage to or destruction of the physical components of a water system in order to interrupt the water system's ability to supply treated potable water to its consumers.

(2) Intentional Contamination of Raw or Treated Water Supplies. This primarily involves the addition of foreign or harmful substances to the water supply. The public health implications and loss of consumer confidence associated with a successful attack of this nature can be catastrophic. This protocol presents the latest facts regarding chemical, biological, and nuclear (radiological) contamination of water systems.

(3) Cyber Attack. This category is broadly defined as the electronic disruption of control, monitoring, or communication systems in order to cause harm. As the use of technology increases to improve efficiency and productivity, so does the vulnerability to a cyber attack. In particular, SCADA systems are now becoming key elements in the production and distribution of quality drinking water. Unlike the other two categories of threat, cyber attacks do not require physical access to water system components and could be performed at great distances from the installation.

c. Regulatory Drivers. In June 2002, the Public Health Security and Bioterrorism Response Act was signed into law. This act effectively amended the SDWA requiring community water systems serving more than 3,300 consumers to conduct a WSVA and update or develop their ERP. A WSVA is defined as a mechanism for evaluating a water system's susceptibility to adversarial actions and provides a prioritize approach for reducing or mitigating the risks associated with those identified adverse actions. As required in the SDWA, a WSVA must include "a review of pipes and constructed conveyances; physical barriers; water collection, pretreatment, treatment, storage and distribution facilities; electronic, computer or other automated systems which are utilized by the public water systems; the use, storage, or handling of various chemicals; and the operation and maintenance of such system." In addition to the Federal WSVA requirement, both DOD and Army have developed policy memorandums requiring WSVA be conducted at various military installations. The DOD Policy on Drinking Water Vulnerability Assessments and Emergency Response Plans, released 3 July 2003 requires all CONUS and OCONUS public water systems (that is, water systems serving greater than 25 DOD consumers) to conduct a WSVA and update/develop their ERP. This includes overseas systems that produce water or are provided water by a local supplier, consecutive and unregulated water systems in the United States, and all small community and non-community public water systems in the United States. The Army has also developed a Policy Memorandum, Food Operations and Water System Vulnerability Assessments and Emergency Response Plans dated 30 September 2002, requiring all Army community water system to conduct WSVAs and update/develop ERPs. Since the release of the 3 July 2003 DOD policy, the Army will likely update its existing policy to more specifically address DOD policy requirements.

(1) Compliance Timetable. Under the SDWA WSVA requirements, depending on a water system's size, a copy of the WSVA must be provided to Environmental Protection Agency (EPA) by a certain date, outlined below. In addition, the water system must update/develop their ERP and provide certification to the EPA within 6 months of submitting their WSVA to EPA. The Army is requiring those systems meeting the SDWA requirements to provide HQDA their WSVA and ERP prior to submitting to EPA. **Table 3-1** provides the compliance timetable for meeting Federal and DOD/Army deadlines.

Table 3-1. SDWA/Army WSVA and ERP Compliance Deadlines

Population Served by Community Water System	Number of Army Installations Affected	HQDA Deadline– Water System Vulnerability Assessment & Certification	EPA Deadline– Water System Vulnerability Assessment & Certification	EPA Deadline– ERP Preparation or Update Certification
100,000 or more	None	N/A	By 31 mar 03	By 30 Sep 03
50,000 to 100,000	2	By 1 Dec 03	By 31 Dec 03	By 30 Jun 04
3,301 to 50,000	44	By 31 May 04	By 30 Jun 04	By 31 Dec 04
3,300 or less	50-100 (est'd)	By 31 Dec 04	N/A	By 31 Dec 04 to HQDA (No report to EPA required)

(2) ERPs. The same systems would have to prepare or revise ERPs that incorporate vulnerability assessment results and certify to EPA no later than 6 months after completing the assessments. The bill would have ERPs include "plans, procedures and identification of equipment that can be implemented or utilized in the event of a terrorist or other intentional attack" as well as "actions, procedures, and identification of equipment which can obviate or significantly lessen the impact of terrorist attacks or other intentional actions." Also, water systems would be required to coordinate such plans with local emergency planning committees to the extent possible.

d. Methodology. A risk-based methodology developed by the Sandia National Laboratory (SNL) for the Department of Energy (DOE) Nuclear Surety Program has recently been adapted for use by the water utility industry. The WSMP engineers have attended EPA-sponsored seminars and workshops given by SNL in order to apply aspects of the DOE methodology to the DOD. Since the Army already has a published and widely used risk management process (FM 5-19), this protocol uses the established Army methodology as its basis. The Army risk management process has also been adapted and modified by USACHPPM to address health risk management (TG 248). This WSVA protocol tailors these two Army risk management processes with specific definitions for the water utility industry.

(1) As seen in **Figure 3-1** below, the focus for the WSVA team is steps 1, 2, and the first two functions of step 3. The assessed installation performs the last function in step 3 (make decisions) and continues the process with steps 4 and 5. The process, as illustrated, is circular with opportunities to re-evaluate risk based on new threat information or new countermeasures employed. The WSVA provides only an initial starting "snapshot" of risks based on the current practices at the time of the assessment.

RISK MANAGEMENT PROCESS

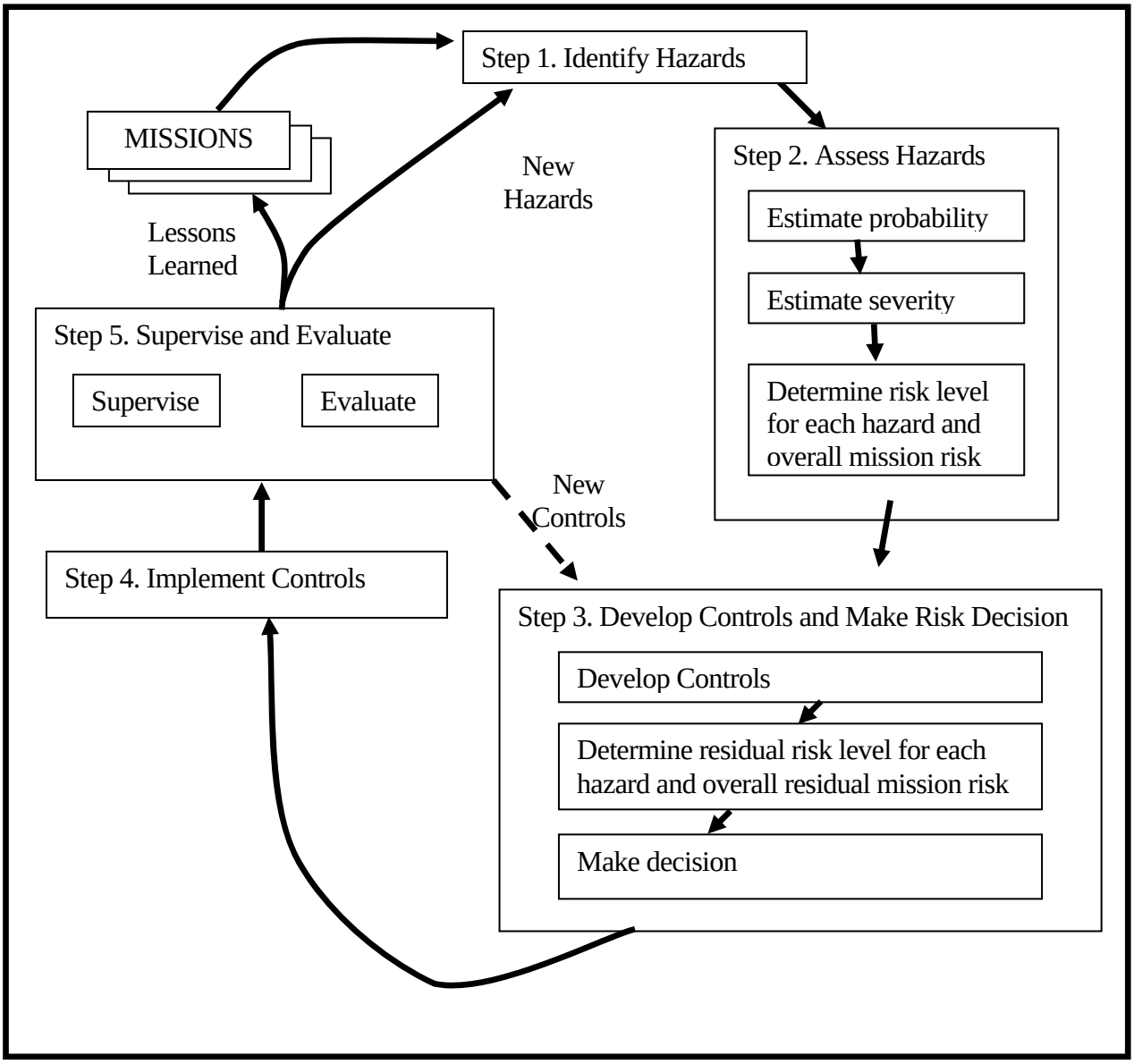


Figure 3-1. Risk Management Process

(2) In the first step of the process (Identify Hazards), team members inventory the water system assets (viewed through the eyes of an aggressor these are "target components"). This process begins well before the on-site portion of the assessment with a review of past technical reports and distribution system maps. In the next step, team members identify and evaluate the current levels of protection at each target component during the on-site survey. This information is then used to estimate: (1) the probability that a terrorist could successfully exploit this vulnerability, and (2) the severity of the ensuing consequence. Together these two factors are used to determine the risk level at each target component or a related vulnerability attack scenario. Team members present these preliminary risk determinations to installation personnel during the out-briefing and facilitate discussion to address any changes in the ratings. The installation Commander should be presented a summarized vulnerability matrix at this out-briefing.

(3) The final step for WSVA team members is to provide recommendations (specific countermeasures) that will reduce the risk (by lowering the probability or severity) at the target components and related vulnerability attack scenarios. This information will help the installation Commander make informed decisions on where to focus limited manpower and monetary resources. More detailed recommendations can be developed later (off-site) upon request from the installation Commander based on his prioritization determination (how he ranks the risks). Other installation entities (such as preventive medicine and the Directorate of Public Works) may also request follow-up assistance in matters relating to the vulnerability assessment, preparation or revision of their ERPs.

(4) There are no existing requirements calling for specific certified personnel (that is, a licensed professional engineer (PE) — or certified protection professional— to conduct a WSVA. The installation may choose to hire a contractor or choose to conduct the WSVA internally. However, there is an advantage for having an assessment team outside the Installation conduct the WSVA. The rationale is that an external third party is preferred to provide an unbiased perspective and, thereby, avoid any potential conflicts of interest.

e. Classification Guidance. As a general guideline, all information collected during the WSVA will be handled as For Official Use Only (FOUO) and maintained with positive control while in the field environment. A reasonable effort for maintaining positive control is keeping information within an arm's reach. At the installation, the assessment team will discuss security classification of collected information with appropriate installation security personnel and will default to the authority of the installation security officer, who will determine the classification of documents and establish daily security procedures. The final written report will be classified as SECRET based on DOD security classification guidance.

3-2. PRE-VISIT.

a. Authority. Before beginning work on a WSVA, the team must acquire authority from the host installation. This authority provides justification when requesting access to facilities and information on the installation. The "customer" for this WSVA is the installation Commander (or garrison Commander), and the team should ensure contact and coordination with the installation Commander. Additionally, the team should have clear coordination with the installation FPO prior to the visit. A formal notification letter should be sent to the installation at least 2 weeks prior to the visit, preferably earlier to ensure all necessary installation personnel can accommodate the assessment team. This letter provides official notification of the project, states the dates of the assessment, addresses security/access issues, and describes assistance required. The letter must stress that installation involvement throughout the process is essential to the effectiveness of the WSVA. See **Figure 3-9** for an example notification letter.

b. Assessment Team. As currently designed, at least two individuals should execute this WSVA protocol for a given water system. More team members may be desirable given the complexity of a system or time constraints. The team should coordinate with available physical security assets on the installation (that is, FPO, provost marshal, and military police) to augment the physical security and cyber-attack portion of the assessment. Additionally, USACHPPM has partnered with the U.S. Army Reserve Information Operations Center (USAR IOC) to assist in the cyber-attack portion of the assessment. When requested by USACHPPM, the USAR IOC will conduct a non-intrusive network vulnerability assessment of any local area network operated by the drinking water system, and the SCADA system. This will include locating any external connections to the internet to ensure there is proper firewall and intrusion detection systems (IDS) in place, as well as checking any internal connections to other DOD or Department of the Army (DA) co-located facilities to ensure proper firewall, IDS, and permission systems are in place. The assessment will also cover any radio frequency or wireless connections to remote wells, pumps, etc., to ensure the proper security protocols are used and updated. Finally a thorough scan of all desktop computers will be conducted to identify critical patches for operating systems, and a review of SOPs regarding passwords and access permissions. Contact the WSMP at USACHPPM-Headquarters for assistance in requesting support from USAR IOC.

c. Research. Team members should gather as much historical information as possible on the water system to be evaluated. The best sources of information are past reports (completed by USACHPPM or other agencies). These reports should provide information on water system assets and known problem areas. Team members should also review the installation's cross-connection control (backflow prevention), emergency/contingency, and flushing plans. If sufficient information does not become available, a scoping visit by the team leader may be warranted. The information gathered will prove valuable in determining the team size and daily work plan required during the site visit. The team leader should develop an initial plan for conducting the WSVA that focuses on division of work among team members during the site visit and a rough time schedule to manage activities.

d. Coordination. In addition to the force protection personnel mentioned above, the team leader should identify and coordinate with points of contact within the Directorate of Public Works (or other agency that oversees water utilities), the installation medical authority, and the supporting preventive medicine assets. The installation intelligence office (Military Intelligence unit or Division/Corps G2) and local law enforcement may be able to assist in providing more specific local threat information. The type of information and assistance that may be required from the various installation personnel are summarized below.

(1) Installation Commander. Grant access to water system components (either escorted or unescorted), and permission to photograph and videotape waterworks structures.

(2) Installation FPO. Copy of Installation Force Protection/Physical Security plan (list of Mission Essential Vulnerable Areas (MEVAs) and actions to take at different FPCON levels) as well as any recently completed security evaluations of the waterworks.

(3) Preventive Medicine (Environmental Science Officer). Information on drinking water sampling plans, other related SOPs, and disease surveillance SOPs. Several installations will have preventive medicine assets in various field units as well as the hospital. Each may have a unique role in detection (monitoring) and response.

(4) Provost Marshal (or Contracted Installation Security Personnel). Information on any security checks/patrols of water system areas and roles in emergency response. They will also need input when developing physical security recommendations. A physical security officer can also accompany the team during the physical inspection of water system assets.

(5) Installation Security/Military Intelligence Office. Local threat information and guidance on classification of vulnerability assessment findings.

(6) Director of Public Works and Installation Environmental Staff. Drawings and descriptions of water system components, distribution system maps, copies of past waterworks evaluations, SCADA information, policy on access to water system information, water management plans and records (such as, emergency/contingency, cross-connection control, conservation, flushing, tank maintenance, regulatory sampling plans; source-water protection plans), and information on alternate power and communications sources, and information about employee job descriptions, performance evaluations, criteria relating to security, as well as award/reprimand policy concerning security.

(7) Water Treatment Plant Operators. Type of monitoring done (that is, parameters, frequency, location), information on currently used on-line monitors, copies of security SOPs/visitor policies/release of information policies, and list of problem areas in the plant.

(8) Water System Operations and Maintenance Personnel. Locations of access points to distribution components (such as, valve pits/boxes), replacement parts availability, and problem areas in the distribution system. Provide information on hydrant access for construction crews and street cleaning operations.

(9) Fire Chief and Hazardous Material (HAZMAT) Supervisor. Information on roles in emergency response and any problems encountered with fire-hydrant operation (contractors and access experiences). Contracting Officer for Chemical Shipments/Deliveries: Information on practices that ensure security of deliveries (Are vehicles always inspected, drivers checked? Any security provisions in contract?, etc.).

(10) Information Management Office. Information on water system internet connections, firewalls, and telemetry systems.

(11) Public Affairs Officer (PAO). Information on public notification plans in event of emergency, including hoax scenarios. Information about neighborhood watch programs, housing area newsletters, and town meetings.

e. Equipment and Supplies. In addition to the usual items planned for a 2-week survey, include a digital camera (with cables, software, and extra batteries) and a cell phone to double check appointments and coordinate access for restricted sites. Other equipment that may be useful include a video camcorder (and tapes), a TV/VCR combination (to allow editing of video footage), and a portable shredder.

f. Identify Target Components. With some minor variations, water systems contain eight major components, each of which includes sub-elements. Team members must review current design plans and maps in order to identify the specific elements for a given waterworks. (See **Table 3-2** and **Figure 3-2**.) The major components and their related considerations are briefly described below.

(1) Water Source. Installations utilize water from either ground or surface water sources (or a combination of both). Some installations purchase their treated water from a local municipal system. Consider that primary and emergency water sources, as well as the actual treatment facility, may be located off the installation boundary.

Table 3-2. Target Components of Water Systems

Target Component	Specific Elements
Water Source	Wells, aquifers, watersheds, reservoirs, dams, rivers, connections to another system
Intakes and Pumping Stations	Intake structures, transmission lines, valves. Pumping and booster stations
Treatment	Bar racks, screens, chemical feeds, aerators, rapid mixers, flocculators, sedimentation basins, filters, chlorine feeds, other chemical feeds (fluoride, corrosion control, etc.), chemical storage areas, other supply storage areas (spare parts, etc.), administrative offices, laboratories, physical plant compound, chlorine monitors, pH monitors, turbidity monitors, other water quality monitors, flow meters, water pressure gauges
Monitoring and Control Systems	SCADA, other system controls and monitors
Distribution Systems	Fire hydrants, manholes/access shafts, water mains, service pipes, valves, filling points, replacement parts storage
Water Storage Areas	Elevated tanks, standpipes, underground tanks, other reservoirs, valves
Power Supply	Transmission lines, transformers, generators, other alternate sources including substations
Communications Systems	Telephones, radios, telemetry

Water System Overview

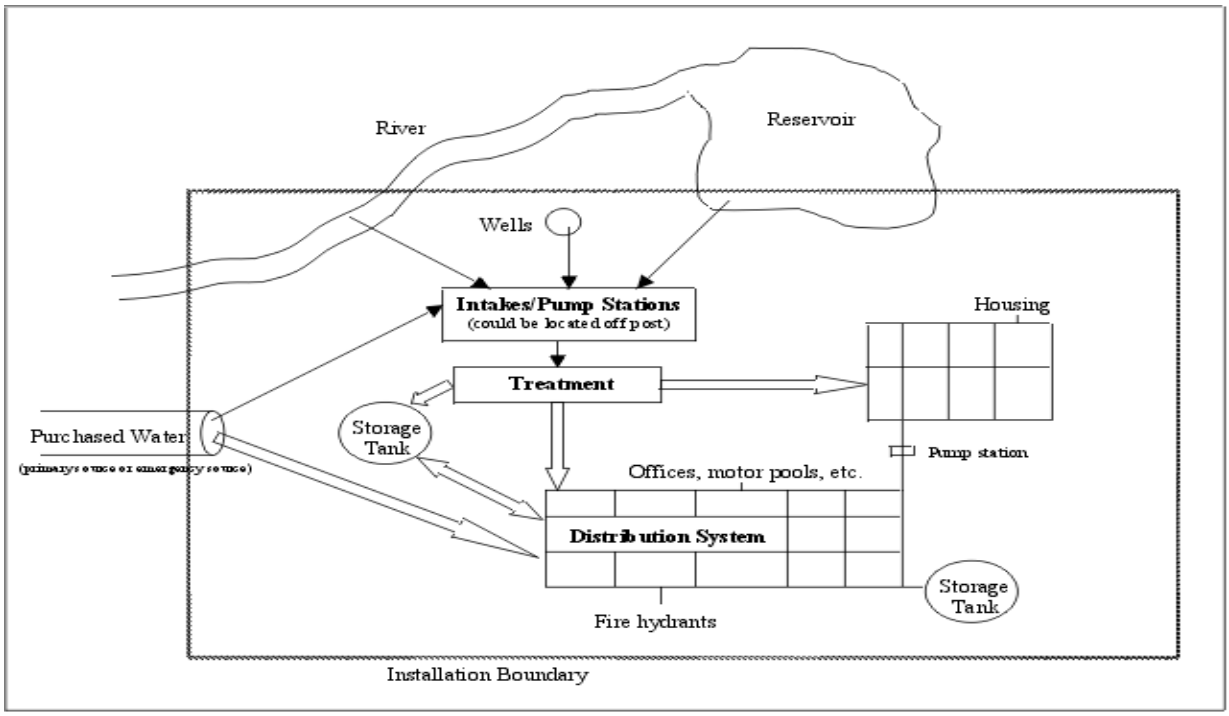


Figure 3-2. Water System Overview

(2) Intakes and Pumping Stations. Intakes are structures built in a body of water for the purpose of drawing water for human use. Water may flow from the intake by gravity or mechanical pumps may be used to move the water from the intake to the water treatment plant. Pumping stations move the water through the pipe distribution system (pressurizing the system) and can be located before and after the treatment plant.

(3) Treatment. Treatment is performed to make the water safe and palatable for the consumers. Treatment processes can vary greatly in size and complexity. This component also includes any physical or chemical pretreatment mechanisms. In the assessment, consider the treatment facility and related structures as the "treatment compound" to evaluate physical security vulnerabilities.

(4) Monitoring and Control Systems. All water systems have some method of controlling and monitoring the quantity and quality of the water, as well as the performance of the unit processes. The complexity of systems may range from operators manually grabbing samples periodically and testing with hand-held equipment to advanced automated systems. Some automated systems allow control from a central location, while others have a restricted range of influence.

(5) Distribution System. Every water system has a distribution system that carries treated water to the consumer. While usually buried, some pipes and valves may also be above ground due to permanent frost conditions or general ease of access.

(6) Water Storage Areas. Clearwells are typically located at the water treatment plant and provide sufficient treated water supplies to support various plant operations as well as providing necessary contact time for disinfection. Water storage tanks (below ground, ground level, and elevated), typically located in the distribution system, serve to balance the hydraulic pressure of the water system and provide bulk supplies of water for peak demand and fire fighting.

(7) Power Supply. Many components of the water system rely on electricity to function. Back-up sources (generators) may or may not be available. The back-up generator may also be located directly to the side of the critical machinery. While this has been desirable for ease of operation, it is possible that an aggressor could now destroy both primary and back-up power sources with one well-placed charge. A fuel tank for the back-up generator is also likely to be present and can be used to accelerate an explosion.

(8) Communication Systems. A functioning communication system is critical to the proper operation of a water system and timely response to emergencies. Not all remote pump houses and storage tanks may be equipped with telephones. Employees accessing these portions of the system should have a way to communicate back to the treatment plant and be able to contact law enforcement if needed.

(a) After identifying the target components and their specific elements for the water system, customize the assessment worksheet template shown as **Figure 3-3** by filling in the first column (Specific Elements). These worksheets will serve as guides during the on-site visit.

(b) An example of a completed worksheet is presented as **Figure 3-4**.

WATER SYSTEM VULNERABILITY ASSESSMENT WORKSHEET

Target Component: _____

Specific Element	Type of Threat	Security (Accessibility)	Redundancy (Backups)	Other Existing Protection Measures	Current Practices that Monitor Protection Measures	Known Deficiencies
	Physical					
	Contamination					
	Cyber					
	Physical					
	Contamination					
	Cyber					

Figure 3-3. Water System Vulnerability Assessment Worksheet Example

EXAMPLE OF COMPLETED WSVA WORKSHEET

Target Component: Water Storage Areas

Specific Element	Type of Threat	Security (Accessibility)	Redundancy (Backups)	Other Existing Protection Measures	Current Practices that Monitor Protection Measures	Known Deficiencies	Probability	Severity	Risk
Storage tank 1 (1.5 MG elevated tank)	Physical	6 ft chain link fence with lock, signage, lights, pump house has locked door, anti-climb device on ladder	Small storage tank 2	Screens on vents	Weekly inspections	None	Questionable	Catastrophic. Destruction of tank would severely alter pressure of entire system and reduce fire fighting capabilities	High
	Contamination	Same as above	Same as above	Same as above	Same as above	None	Unlikely	Catastrophic. Toxic agent could be delivered to entire distribution system	Moderate
	Cyber	Same as above	Water level can be monitored and controlled at tank or at plant control room	Automatic shutoff and automatic fill, overflow drains	Systems checked annually	None	Unlikely	Marginal. Automatic shutoff and overflow drains prevent tank destruction.	Low
Storage tank 2 (50,000 gal standpipe)	Physical	6 ft chain link fence with lock, signage, lights	Storage tank 1	Screens on vents	Weekly inspections	None	Questionable	Critical. Tank serves remote area of distribution system	Moderate

Figure 3-4. Example of Completed WSVA Worksheet Example

3-3. ON-SITE ASSESSMENT.

a. Entrance Briefing. Attendees should include all the key personnel who play a role in providing safe drinking water to the installation. The core personnel who should be present are: Installation Commander, Installation FPO, the installation Preventive Medicine/Environmental Science Officer, Provost Marshal (or contracted installation security personnel), installation Security Officer, and Director of Public Works with representatives from water, power, communications, and wastewater. Other personnel to be invited include: environmental staff that maintain water management plans and records, treatment plant operators, Fire Chief and HAZMAT supervisor, contracting officer for chemical shipments/deliveries, the PAO, and other water system operations and maintenance personnel (such as, plumbing shop).

(1) The purpose of the briefing is to make introductions and explain the purpose and scope of the project. Emphasize that success in reducing vulnerability depends on the active involvement of all the key personnel mentioned above. Distribute handouts to each attendee that briefly describes the assistance needed from each office (listed in section 3-2d). The American Water Works Association (AWWA) "New Horizons" videotape could be shown following the brief to generate early discussion (contact WSMP to borrow the videotape or order from AWWA bookstore at www.awwa.org). The team leader can also use this time to make additional appointments with the key personnel. Following presentation of the videotape, the team leader may wish to read several questions from the interviewing questionnaire (provided in section 3-5c) to spur discussion and give the personnel more time to think about the questions and locate requested documents. The team leader should also provide all personnel present with the team contact information (phone numbers and e-mail addresses).

(2) The team leader should discuss the final report security classification guidance and recommend personnel to review the report during the entrance brief. Because the final report will be classified as secret based on DOD security classification guidance, installation personnel who will review the report must have at least secret clearances. At a minimum, the team leader should recommend representatives for the installation Commander, the Department of Public Works (DPW), Director of Force Protection, and water system operation and maintenance (that is, water plant/distribution system supervisors) review the final report. It has been USACHPPM's experience that key water system personnel do not typically have secret clearances. Water system personnel should be actively involved in the WSVA process to include reviewing the final report for two main reasons: (1) they are typically the most knowledgeable people on the installation water system; and (2) they should be actively involved in incorporating the WSVA findings into the Installation ERP. Discussing this as early on in the WSVA process as possible will allow key personnel without secret clearances to begin the process of obtaining at least an interim secret clearance through their installation.

b. Physical Inspection of Assets. Much of the time during the on-site visit is devoted to physically examining the target components and their specific elements. Team members should review their list of elements with water system operators to ensure accuracy and completeness. Someone knowledgeable of the water system should then escort team members to each target component (desirable for speed and ease of access). Digital photos should be taken of all specific elements for easy reference, and as reminders when analyzing at a later date (ensure the Installation Commander grants authority prior to taking pictures).

(1) Video Footage. The use of the video camcorder is highly recommended. When footage is later edited and presented at the exit briefing, the video can present most of the highest vulnerabilities. This is also an excellent tool to allow the team to "look through the eyes of the aggressor" and show an attack scenario. The video can easily demonstrate terrorist avenues of approach, poor lighting at target components, and poor physical security features. If possible, consider incorporating digital footage into the slide presentation. This keeps the video in context with the briefing and presents a very professional brief. In order to make an effective video, several tips are offered.

(a) When the team first arrives at the site of a target component, walk around to note deficiencies before turning on the camera. Avoid "discovering" items while walking around (shaky, disjointed unprofessional footage).

(b) After the site is assessed and discussed among team members, film one person standing still, who then orients the audience to the site and summarizes the vulnerabilities noted. Use "sound bites" and remember the audience is the installation Commander. Practice once before recording.

(c) When filming a structure, use your finger (or a pointer) in the camera's field of vision to point out the focus of the shot. Don't focus on the same thing too long. Make use of the "fade" function to transition between sites (target components). This also helps in editing the footage.

(d) Do not say the installation name or identifying marks that give away exactly where you are. This tape could be very dangerous in the wrong hands; keep the location details to a minimum.

(e) Edit the tape to 10-20 minutes. Ensure the edited version for the exit brief covers the Extremely High and High Risk vulnerabilities at a minimum. The tape may be classified by the security officer and not returned to the team after the exit brief.

(f) Do not intentionally embarrass anyone at the installation or ambush him or her with footage at the exit brief. The assessment should be frank, but trust and cooperation is essential for a good working relationship. If in doubt, show the person the footage ahead of time and discuss your plans.

(2) WSVA Worksheets. Use the customized WSVA worksheets to evaluate each area of concern for each type of threat (physical, contamination, cyber). It will most likely be necessary to take notes in a field notebook and actually fill in the worksheets electronically at a later date. Instructions for completing columns 3 through 7 of the worksheets are as follows:

(a) Security. This column should address existing security measures that control the accessibility of each specific element. Identify current physical and operational barriers to an attack. Examples are given in **Figure 3-5** and discussed in more detail in section 3-5b. Army's FM 3-19.30 also provides excellent examples. Most security measures apply to all three forms of attack. Team members should put themselves in the "shoes of the attacker," and consider primary and alternate routes of entry/access to the specific elements. Look at all potential entry points (such as gates, doors, windows, vents, and skylights).

(b) Redundancy. Indicate in this column any existing back-up or redundant systems that could be used should the specific element become disabled. Ask the question: "What are the available options if this element is taken out of action?" Maintenance and operation personnel will be the most valuable sources of this information since this issue is addressed during routine maintenance and repairs.

(c) Other Existing Protection Measures. Identify any other measures that provide protection against attack.

(d) Current Practices that Monitor Protection Measures. Specify any means of ensuring that the existing protection measures (identified in steps 3-3b(2)(a)-(c)) are functioning properly. These are the "status checks" of the specific elements and usually fall under a routine inspection schedule. For example, if a pump house is protected with an alarm, how do you know the alarm works? Who, if anyone, does it notify? If the treatment plant uses a continuous chlorine residual monitor, how do you know the readings are accurate? Is it calibrated routinely? Again, solicit input from operators.

Security Measure	Examples	
Security (Accessibility)	- Fences - Locks - Signage - Bars on windows - Lighting - Anti-climb devices on ladders - Screens on vents/drains/overflow outlets - Vehicle barriers	- Security patrols/inspections - Required ID badges - Security cameras - IDS - Passwords on computer systems - Parking policy - Set-back distance
Other Existing Protection Measures	- Continuous water quality monitors - Chlorine residual - Filters - Routine sampling	- Backflow prevention devices - Supply of replacement parts - Isolation mechanisms (shut-off valves) - Fire suppression equipment
Current Practices that Monitor Protection Measures	- Equipment calibration - Routine quality control checks - Verifying automated sensor results with manual procedures - Active maintenance/cleaning program - Ensuring adequate backwashing of filters - Testing backflow prevention devices - Routine flushing of mains - Daily inspections	- ID checks - Testing of alarms - Incident response rehearsals - Functional checks of emergency/ back-up equipment - Routine pass code/password changes - Close tracking of consumer complaints - Monitoring hospital illness trends

Figure 3-5. Example Items for WSVA Worksheet

(e) Known Deficiencies. Annotate any known deficiencies in the operation or structure of the specific elements. Some deficiencies may be obvious, like a broken gate or leaking pipe, but others require the knowledge of maintenance/operations staff. Also, consider past acts of vandalism.

> **NOTE**: If water is purchased from an outside agency, it may not be possible to visit off-post facilities. In this case, team members should gather as much information as possible from the provider concerning efforts to protect their portion of the water system. Prior coordination with the state health department and/or off-post facility may allow the team to conduct some level of assessment at the off-post facility. Extend invitations to the off-post facility representatives, with the approval of the installation Commander, to attend the inbrief and outbrief.

c. Document Review. Finish reviewing any existing water system plans to include facility drawings/maps, operations and maintenance plans, emergency/contingency plans, cross-connection control plans, flushing plans, SOPs, and water quality monitoring plans.

d. Interviews. When interviewing the identified installation personnel, managers should be interviewed individually. Workers (due to time constraints) may be interviewed in a group as long as their supervisor is not present. In many cases, the greatest insights about vulnerabilities are gained by talking with personnel who have the daily maintenance responsibilities for the distribution system or work the night shift at the treatment plant. The interviewing questionnaire is found in section 3-5c. Not every question will apply to each individual given their job description.

e. Data Assimilation and Risk Assessment. The risk management process is used to determine the overall risk posed by terrorist threats to each target component. Survey team members and installation personnel decide on the level of risk based upon the probability and severity of each event according to the definitions presented below (derived from the FM 5-19 and TG 248).

(1) Probability and Severity. The team leader must assign a probability and severity ranking to each identified vulnerability. A probability and severity can also be assigned to likely attack scenarios as more about the water system is learned. This may crystallize to the installation Commander the impact of having multiple vulnerabilities at one target component. The term probability is defined as the likelihood that an aggressor could successfully exploit the vulnerability. This probability also takes into account a rough estimation of the effort required to

man, train, equip, and supply a terrorist to carry out such an attack. The question of whether or not such a terrorist exists and is trained and equipped and is actually targeting the installation is the hardest unknown factor to evaluate. Members of the intelligence community and law enforcement/security personnel can best make this determination.

(a) The probability assigned will change, however, if specific threats are made against the system or similar attacks occur at other locations. Probabilities are Highly Likely, Likely, Probable, Questionable, and Unlikely (**Table 3-3**). The criteria for each ranking are defined as follows:

Table 3-3. Probability Criteria

Probability	Criteria
Highly Likely	Easy to execute. No existing safeguards. No specialized training and very little equipment required (80-100% success rate).
Likely	Does not require high level of training and supplies are easily obtained. Minimal protective measures in place (60-80% success rate).
Probable	Reasonable that capability exists and existing measures inadequate to deter. Collusion with an insider could provide a terrorist access and the necessary training and equipment (40-60% success rate).
Questionable	Remotely possible. Specialized knowledge, training, and equipment required. Information may be obtained by an outsider from generic sources (20-40% success rate).
Unlikely	Can assume would not attempt or would not be successful due to lack of capability and existing control measures. Relies on facts not easily obtained by an installation outsider (0-20% success rate).

(b) Severity refers to the extent of loss that would result if a successful attack occurs, and is expressed as Catastrophic, Critical, Marginal, or Negligible. The criteria for each ranking are defined as follows in **Table 3-4**:

Table 3-4. Severity Criteria

Severity	Criteria
Catastrophic	Causes deaths or widespread severe illness, complete loss of ability to provide safe drinking water to entire water system—will take more than 2 days to restore service.
Critical	Causes minor illness, severely damages ability to provide safe drinking water—service can be restored in 2 days, major property damage.
Marginal	Degrades ability to provide safe drinking water, appreciable property damage, requiring a construction project to repair.
Negligible	Little or no adverse impact on ability to provide safe drinking water, little property damage—does not affect normal equipment operation.

(2) Level of Risk. Determine the overall risk posed to each specific element using Figure 3-6. Risk is expressed in terms of Extremely High, High, Moderate, and Low. Discussion among team members is necessary to ensure consensus. If necessary, discuss the determined risks with water system personnel to get their feedback and agreement. Be prepared to explain the reasoning and logic behind the determination of risk.

	HAZARD PROBABILITY				
HAZARD SEVERITY	Highly Likely	Likely	Probable	Questionable	Unlikely
Catastrophic	Extremely High	Extremely High	High	High	Moderate
Critical	Extremely High	High	High	Moderate	Low
Marginal	High	Moderate	Moderate	Low	Low
Negligible	Moderate	Low	Low	Low	Low
	RISK ESTIMATE				

Figure 3-6. Risk Assessment Matrix

f. Develop Recommendations. Upon completion of the risk assessment, the final step in the WSVA process is to develop means of reducing the risk to the most vulnerable areas. The major methods of increasing protection are as follows:

(1) Improve Physical Security. Emphasis should be placed on restricting access to the water system components at highest risk. Upgrading or installing physical barriers, especially fences and locks, reduces the likelihood of an attack. A stringent key control program is essential to the success of many physical barriers. Improved lighting, signage, motion detectors, and alarms also serve as effective deterrents. Frequent security inspections and camera surveillance increase the chance of early detection of an intrusion. While cameras may act as a deterrent (perception of tight security), their primary purpose should be to evaluate (assess) an intrusion alarm. Also, consider employee background checks and reviewing the local policy regarding release of water system design/operation information. More aspects of physical security measures are discussed in section 3-5b.

(2) Increase Water Quality Monitoring. The frequency and location of water sampling may change in response to the threat conditions (FPCON levels). Monitoring of the basic water quality indicators of chlorine residual, pH, turbidity, temperature, and conductivity is essential to early detection of an attack. Continuous in-line monitors for these normal parameters are widely available and in use today. Similar monitors for chemical and biological contaminants are expensive and rarely used but are becoming more available for increased water quality surveillance. Environmental staff and preventive medicine personnel may also be available to assist and provide resources for water system monitoring in response to increased FPCON levels. See monitoring discussion in section 3-5b, for more details.

(3) Improve ERPs. Written plans should be rehearsed and revise, and should address terrorist threats. Of particular importance are effective plans to isolate affected sections of the distribution system; obtain alternate water and power sources; and notify local, state, and Federal agencies of emergency conditions. Accurate maps and plans of the water system are also critical.

(4) Repair Observed Deficiencies. One of the easiest methods of reducing vulnerabilities is to fix any known deficiencies in existing protection measures. These deficiencies are identified during the vulnerability assessment. Corrective action can be as simple as repairing a hole in a fence or replacing a light bulb.

(5) Improve Consumer Communication. Since consumers may be the first to detect problems in the distribution system (such as, odor, taste, color, or pressure loss) an effective means of receiving complaints must be established. A formal early warning complaint system enables the installation to react quickly to problems in the distribution system. The complaint collection system should include a database that tracks complaints by location and time. Technology such as geographic informational system (GIS) incorporating water distribution

plans and real property overlays can be leveraged to better track complaints. Equally important is a means to alert consumers and provide guidance in the event of an emergency condition. Planners and the installation PAO should consider procedures for notifying local radio, television, and newspaper agencies, as well as going door-to-door to ensure information is disseminated as quickly and effectively as possible.

(6) Increase Medical Surveillance. Interaction with local medical authorities is important in identifying potential water quality problems, especially biological agent contamination. Since there is a delayed onset of symptoms for many diseases, increased hospitalizations may be the first sign of trouble. Preventive medicine personnel need to actively monitor admissions and sick-call visits for illness trends or spikes. The GIS technology mentioned above could also incorporate this into a tracking database.

(7) Ensure Optimization of the Treatment Process. A properly operated water treatment plant is a countermeasure against contamination of the source (raw) water. This maximizes the capability of the plant to serve as a treatment barrier. The performance potential of the unit processes of the treatment plant should be optimized. Consider upgrades to provide redundancy or enhanced treatment capabilities (such as, addition of activated carbon to improve chemical contaminant removal). The USACHPPM Water Supply Management Program can provide specific assistance in this area.

g. Exit Briefing. Prior to the exit briefing, have a 10-minute desk-top executive summary version prepared for the installation Commander. The installation Commander may not have the time to attend the exit briefing but wants a quick brief from the team. Generally, those present for the entrance briefing should also be present for the exit brief. If possible, those personnel responsible for corrective actions should be present so that they can become aware of recommendations. Provide your slides (with speaker's notes), videotape, and summary vulnerability matrix to the FPO or security officer prior to the exit brief to determine classification markings. Attendance at the briefing may be restricted based on the content classification.

(1) The team leader should thank everyone that provided assistance and give a summary statement or two on the overall perceptions of the installation's water system vulnerabilities. Next, present the video (if a video was shot) and afterwards highlight any additional details about the vulnerabilities with the highest risk. Since some vulnerabilities concerning management procedures and policy documents are not suited for inclusion in the videotape, the team leader can brief these separately. As time permits, facilitate discussion and present additional moderate- and low-risk vulnerabilities. The team leader should try to gain consensus of the probability and severity ranking if opinions vary among the installation personnel. Next, present some of the recommended countermeasures that will lower risk to the observed vulnerabilities. Appoint a team member to write down any specific requests from the audience for additional follow-up information. Allow for questions at the end of the brief.

(2) The time invested in the exit brief will greatly aid the generation of the final report. Most of the attendees at the brief should only receive the "three-pack" of slides for their reference, while the key personnel get the detailed "speaker's notes" version. Ask the installation Commander and the installation Security Officer (or their representatives) for guidance on final report distribution and report reviewers. The team leader should leave the installation with a clear sense of what further work is required and the timeline for delivering the final report or other service.

3-4. FINAL REPORT.

a. The format of the final report is flexible but should include the sections below. Overall, the report should be brief being no longer than a total of 20-30 pages.

(1) Classification. The final report will be classified 'SECRET" based on DOD security classification guidance. The team may be allowed to travel from the installation with assessment materials. This should be coordinated with installation security personnel. Classified material could be sent via the Secured Internet Protocol Network (SIPRNET) or authorized courier.

(2) Executive Summary. Provides the "bottom line up front," quickly conveying the most important information. The executive summary states the purpose and presents the Extremely High and High vulnerabilities in a summarized matrix along with the corresponding recommended countermeasures.

(3) Authority. This is the first section of the full report and states the source of authorization to conduct the WSVA. Example: Telephonic conversation between COL XXXX, Garrison Commander, Fort Bragg, and CPT XXXX, USACHPPM on 1 November 2001.

(4) Purpose. The purpose explains why the WSVA is being conducted and the assessment goals. Example: To identify the most vulnerable areas of the Fort Polk water system, and to provide recommendations to reduce these vulnerabilities. The goal is to enhance force health protection by hardening the water system to reduce the probability and severity of a terrorist attack. This assessment will satisfy the SDWA water system vulnerability requirements as well as DOD and Army requirements

(5) Methodology. The methodology describes the steps followed in conducting the assessment. This is an important step to document the thoroughness of the assessment. Example: The WSVA began with a comprehensive review of past evaluations of the Fort Polk water system and current management plans and system maps. Using this information, the assessment team identified target components of the water. The installation security office was also contacted to gather local threat information.

(a) A member of the DPW utility crew then escorted team members to each target component. The survey team determined the current levels of protection of each specific element using the WSVA worksheets (Appendix C). Areas addressed during the on-site visits included: existing security measures (ease of access), redundancy (available back-ups in the event of failure), actions or devices that monitor status of protection measures, and known deficiencies.

(b) The gathered information was then used to assess the risk posed by terrorist attacks against the water system components based on the methodology presented in FM 5-19 and USACHPPM TG 248. Risk levels were assigned based upon the probability and severity of intentional attacks against each specific target components and elements of the water system.

(6) Assessment Team. This section states the names, ranks/grades, duty positions, and security clearances of survey team members.

(7) Water System Overview. This section briefly discusses the route water follows from source to tap. It includes a simple description of water system components, supported with a map or graphic depiction.

(a) Example: Fort Dusty receives raw water from the Giambone well field. The water is of good quality and only requires the addition of chlorine and fluoride to meet Federal and state standards. Maintaining a residual level of chlorine helps ensure high water quality and provides protection against chemical and biological contaminants. Fluoride provides a measure of cavity protection in children. Chemical feeders deliver metered amounts of chlorine, fluoride, and corrosion-control chemicals to the water as it is pumped into the distribution system.

(b) There are eight aboveground storage tanks throughout the system. These tanks balance the hydraulic pressure of the water system and provide bulk supplies of water for peak demand and fire fighting. Each storage tank has a pump that automatically maintains a pre-set water level. The pumps can also be manually operated, and have emergency generators in the event of a power failure.

(c) There is no centralized control and monitoring station; however, storage tank water levels are checked daily. Water is also tested daily for pH, turbidity, and chlorine residual at sample locations throughout the system. (Include a sketch of water system, showing location of wells, storage tanks, pumps, and sample locations.)

(8) Findings. This section discusses in detail the highest areas of vulnerability (those with a risk ranking of Extremely High, High, or Moderate). It explains where these components are located and why they are at highest risk. Findings should be supported with digital photos. Example: Elevated Storage Tank 1. This tank is located on the western boundary of the installation near the motor pool. This structure is at high risk of a physical attack. Destruction of

this elevated tank would flood surrounding areas with 1.5 million gallons of water of tremendous force. This sudden loss of water would cause pressure changes in the distribution system. Availability of water for peak demand and fire fighting would also be depleted. The tank is at moderate risk of intentional contamination. A toxic agent entering the tank could eventually be delivered to the entire system. Existing protection measures include a 6-foot chain link fence, warning signs, lights, screens on vents, and an anti-climb device on the service ladder. Weekly inspections check the status of the tank. Because of the current protection measures, and since no specific threats have been made against the system, an attack on this component is considered only remotely possible.

(9) Recommendations. This section provides feasible recommendations for reducing vulnerability of the water system from intentional attack. Recommendations should be more detailed and refined than those presented at the exit briefing. This section should also contain the summarized vulnerability matrix, starting with the most vulnerable, and corresponding recommended countermeasures that address the specific vulnerabilities. This table will aid the installation Commander in determining where to focus attention and resources (**Table 3-5**).

(a) Example: Improve physical security. Have military police increase visual checks of water storage tanks and wellheads on their daily patrols of the installation. Consider installing additional lighting around elevated storage tank 1. Install fencing around well 2B. Institute a formal key control system to ensure accountability.

(b) Improve ERPs. Update current response plan to address specific emergency actions to take in the event of the physical destruction of elevated storage tank 1. Update the list of key points of contact.

Table 3-5. Example Report Recommendations Table

Most Vulnerable Areas (Highest Risk)	Recommended Countermeasures
Storage tank 1	Increase MP patrols, install additional lighting, key control, address destruction of storage tank in ERP
Well 2B	Install fencing, increase MP patrols, key control
Chlorine tank at Well 4A	Place vehicle barriers around tank, install fencing

(10) Distribution. The installation security office or FPO will specify the distribution policy and authorized recipients of the final report. Remember that the report will be classified SECRET containing sensitive information regarding installation vulnerabilities, and distribution should be limited. Authorized recipients should be discussed at the entrance brief. At a minimum, the installation Commander (or representative), DPW Director, installation Security

Officer, and water system supervisor(s) should be authorized recipients. Some of these individuals may not have secret clearances and should pursue a clearance through their respective organization or installation as early on in the WSVA process as possible. Once a draft final report is completed and authorized recipients are known, send the report via SIPRNET if the installation has SIPRNET capability and/or send a hardcopy of the report. You must follow proper security procedures for sending hardcopies of classified materials. Your installation security personnel can assist with properly sending hardcopies of classified material.

(11) Appendices. Include any additional information, data, or photos as appendices. Appendix A should include typed versions of the completed WSVA worksheets. These worksheets are important because they document information on the low-risk areas that were not discussed in the body of the report.

3-5. ADDITIONAL INFORMATION.

a. Threats to Drinking Water Systems. Gay Porter Denileon examined the threats to drinking water systems in the May 2001 Journal of the AWWA article "The Who, What, Why, and How of Counter-terrorism Issues". According to Denileon, three attributes are crucial to water supply users. Water suppliers must be able to ensure that adequate supplies of water are delivered to satisfy consumer demand at sufficient pressure and be safe and acceptable for consumer use. Actions that affect any of the three factors can be debilitating to the infrastructure. A variety of methods could be employed to undermine any of these three essential functions including physical destruction, intentional contamination, and cyber attack.

(1) Physical Destruction.

(a) Denileon notes that "many observers believe that physical destruction of a water system's components or the disruption of a water supply is a much more likely scenario than a contamination event." Physical destruction of water system components could result in loss of flow, pressure, and ability to satisfy consumer demand. Loss of adequate flow and pressure could reduce or eliminate fire-fighting capabilities. Physical destruction could also result in a reduction of water quality, placing consumer health at risk.

(b) Examples of physical destruction include: damage to equipment or infrastructure using explosives, damage to interdependent infrastructure, such as power supplies and communications, arson, and attacks aimed at personnel. Damage of a physical nature includes disruption or destruction of—

i. Raw water reservoirs, dams, intake structures, transmission lines, valves, and pumps;

ii. Water treatment chemical containers, mechanical equipment, monitoring equipment, chemical feed pumps, and high-pressure pumps.

iii. Distribution system valves, storage tanks, and water mains.

iv. Power source or other interdependent infrastructure, such as telecommunications.

v. The SCADA systems.

(c) Physical attack could focus upon chlorine and other hazardous chemicals used in the water treatment process, particularly during transport or at an unsecured site. The release of chlorine gas into a housing area or critical operational area could be catastrophic. Eliminating the supply of chlorine or other essential chemical, such as a primary coagulant (aluminum sulfate) could undermine the treatment process and create a situation where the treatment plant can no longer produce potable water.

(2) Intentional Contamination.

(a) Overview. Another class of threats potentially aimed at drinking water systems is the introduction of a harmful contaminant into the water supply system. The public health implications of such actions are obvious. Historically, water suppliers have rarely been targeted by intentional contamination. Water systems are most often contaminated incidentally rather than intentionally. Of a reported 84 terrorist incidents since 1942, only six concerned water at any significant level. Of these 84 reports, only one, involving cholera contamination in Italy, may have achieved a degree of success. Effective disinfection can mitigate the effect of similar incidents. The most probable scenario is the contamination of a storage tank with a highly toxic chemical or biological agent. The fact that such storage tanks are located after the treatment plant, afford relatively easy access, and are one of the few parts of the distribution system that are not under positive pressure, make them ideal targets. The harmful health effects upon consumers may not manifest until days after exposure—when it may be too late. Fortunately, the shear size of drinking water sources and distribution systems (both in terms of water volume and detention time) and the presence of existing treatment processes significantly reduce the effectiveness of such an attack on a water source or treatment plant. Intentional contamination of a raw water supply using a known or potential biological warfare agent, for example, would require at least 30,000 times the toxic dose for each individual placed at risk, even neglecting natural attenuation and ordinary treatment efficacy. This is not an effective point to contaminate the supply unless massive amounts of contaminant are applied. This type of attack, in order to be effective, would likely be aimed at a storage tank or a part of the distribution system serving a specific high-profile building. Installations that purchase water from an outside supplier may be

targeted just outside of the gate as water crosses the fence line. Contamination threats can be further categorized into threats from chemical contaminants, biological contaminants, and radiological (nuclear) contaminants.

i. The USACHPPM WSMP searched published newspaper and Internet sources, as well as published journal literature in an effort to determine the most commonly mentioned water supply threats. This study was initiated because no historical water system threat information is available. More than 55 media reports, published journal papers, and Internet sites were reviewed. As shown in **Figure 3-7**, 57 percent of the potable water system threats/attacks mentioned in the surveyed literature and Internet sites were chemical in nature. This finding is analogous to the common belief that chemicals are the most likely intentional contaminants because they are widely used and easily acquirable. Biological contaminants were the next frequently mentioned threat (19 percent), followed by trespassing, vandalism, and sabotage (11 percent). Surprisingly the use of explosives was the least mentioned type of threat/attack against water systems. This finding contradicts previous Department of Justice reports that indicate the most likely terrorist event would involve explosives. One reason for the less frequent focus on explosives could be because many published reports are focusing on the less understood intentional contamination event. Radiological contaminants were not referred to in any of the reports reviewed and may be because radiological contaminants are extremely difficult to obtain and transport.

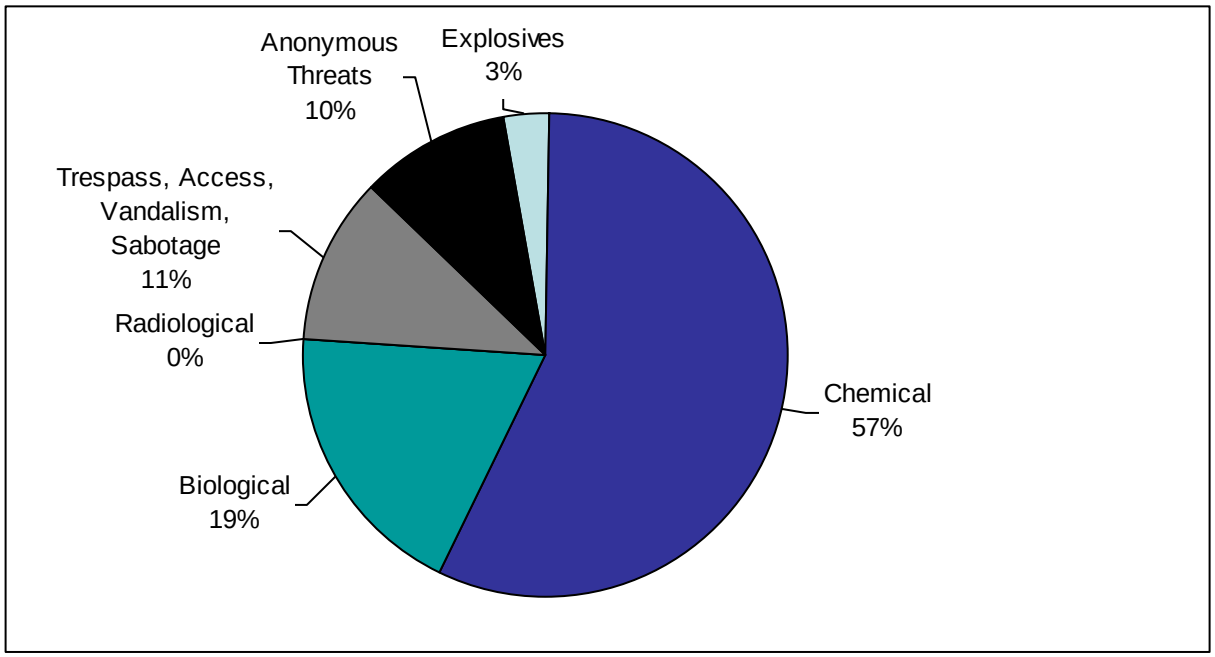


Figure 3-7. Potable Water System Threat Survey Results

ii. By far, the most often mentioned chemical threat was cyanide (59 percent, 26 of 45 responses) as shown in **Figure 3-8**. This is not surprising since cyanides have been identified as a notable threat to water systems (See Whelton et al.) and have long been used by rogue individuals and organizations to carry villainous acts. Other chemical threats that were identified were common in nature such as solvents, paints, gasoline, oil, and industrial chemicals. These common chemicals comprise 22 percent of the total chemical threats identified.

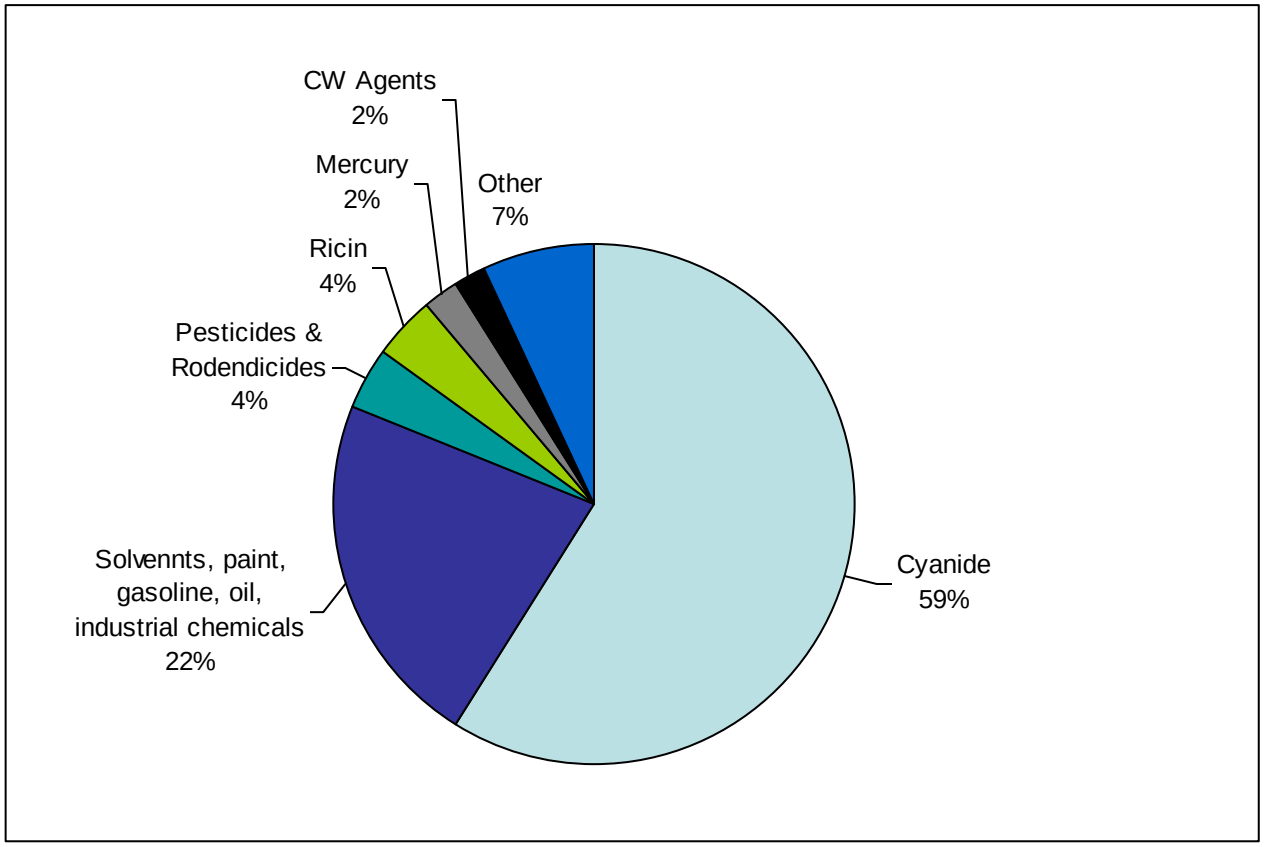


Figure 3-8. Chemical Threats to Potable Water Systems

(b) Chemical Hazards. While toxic chemicals (such as nerve agents, arsenic, cyanide, mercury, and cadmium) pose great health risks, many common constituents of water treatment systems are also potential sources of contamination. For example, chlorine, fluoride, or other chemical feed systems could be sabotaged in order to dispense harmful quantities into the treated water supply system. Insecticides, rat poisons, weed killers, fertilizers, solvents, petroleum products, and paints are also routinely used in or near water systems. **Table 3-6** lists the various chemical hazards as well as some basic properties of each (such as, stability in water and chlorine reactivity). The chemicals identified were selected because they are considered to cause acute health effects. The early detection of sabotage by chemical contamination will likely

come from the customer due to a dramatic change in taste, color, as well as odor, through some other change in basic water parameters, such as a drop in chlorine residual, or change in pH or conductivity depending upon the specific contaminant and its respective concentration. The chemicals most likely to be employed are those chemicals that are commercially available, relatively stable in water, and have the potential to significantly degrade the mission. Although, historically, these chemicals have not been utilized to contaminate drinking water, it is possible that a saboteur could employ them. The likelihood of the employment of a chemical agent, such as the nerve agent VX, is not as likely because availability is more limited. Even though use of the chemical agent may be more effective than the commercially available chemical, contaminating drinking water may not be the best use of a terrorist's supply of chemical agent. The use of the hallucinogens and other cited nerve agents are even less likely. The use of hallucinogens to impact the water supply will cause marginal impact on mission capabilities. The nerve agents cited, other than VX, are relatively unstable in water where they form innocuous products.

Table 3-6. Chemical Hazards and Select Properties

Hazard	Type	Stable in Water*	Chlorine Reactivity
Insecticides	Arsenic, Parathion	Yes	Most insecticides - No Arsenic -yes, forms inorganic compound
Herbicides	Atrazine, Alachlor	Yes	No
Rodenticides	Sodium Fluoroacetate	Yes	No
Fertilizers	Nitrogen Compounds	Yes	No
Nerve agents	GA (Tabun), GB (Sarin), GD (Soman)	No	No
Nerve agents	VX methylphosphonothioic acid	Yes	Yes - forms more toxic chemical
Hallucinogens	LSD (lysergic acid diethylamide) BZ (3-Quinuclidinyl benzilate)	Yes	No
Cyanide	K (Potassium)& Na (Sodium) Cyanide Salts HCN (Hydrogen Cyanide)	K & Na Salts Yes HCN No	No
* Stability within a water distribution system. Organic compounds above will volatilize when exposed to air			

(c) Biological Hazards. Of the various contamination hazards, biological hazards are the most effective means for a saboteur to debilitate a drinking water system. The incubation period for these hazards allows the terrorist to vacate the area before the effects manifest themselves. Additionally, until symptoms begin to appear and medical facilities begin to see the large numbers of patients, detection will be very slow. Adding to the difficulty in detection of a biological contaminant is the fact that symptoms of exposure may be interpreted as a natural outbreak of a communicable disease. Therefore, it is critically important to have an active medical surveillance program in place with effective reporting procedures to facilitate early detection. Burrows and Renner have reported extensively on biological hazards in water. **Table 3-7** lists the various biological agents of concern, some associated properties, and outbreak information. Common water-borne pathogens such as *Vibrio cholera*, *Salmonella* spp., and *Cryptosporidium parvum* are credible biological warfare agents. They are readily available, highly infectious, and cause gastrointestinal distress or even death. Some are even highly resistant to chlorine. Viruses are less likely water-borne threat agents but should not be discounted. Biotoxins, although lethally toxic, are not generally available and are not credible threat agents unless applied to a minor water supply, such as one serving a single building. Nine known or potential biological agents were determined to be the most likely to be employed. There is also a high risk associated with those bacteria, protozoan or biotoxins that are commonly found in the environment or easily prepared, stable in water, and have the potential to significantly degrade the a public water system. The remaining biological hazards are less likely to be employed primarily because the probability of obtaining or synthesizing them is very low.

Table 3-7. Biological Hazards and Select Properties

Hazard	Type	Water Threat	Stable in Water	Chlorine Tolerance	Possible Means of Contamination	Level in drinking H2O that causes illness, drinking 15L H_2O per day (5L per day) for 7 days	Historical Outbreaks (1971-1996)*
C. Perfringens	Bacteria	Probable	Common in sewage	Resistant	Cooked Beans allowed to ferment then dumped into water supply/secondary sewage effluent	106 organism/L (107 organism/L)	None found
Anthrax	Bacteria	Yes	2 years (spores)	Spores resistant	Soil contamination, animal hides	57 spores/L (171 spores/L)	None found
Shigellosis	Bacteria	Yes	2-3 days	Inactivated, 0.05 ppm, 10min	Human fecal contamination	100 organism/L (300 organism/L)	42 outbreaks/ 9,055 sick
Salmonella	Bacteria	Yes	8 days (fresh water)	Inactivated	Dump raw poultry, eggs, raw milk, feces from poultry into water supply	100 organism/L (300 organism/L)	13 outbreaks/ 2,995 sick
Campylobacteriosis	Bacteria	Yes	Stable	Easily killed with chlorine	Dead birds, especially pigeons, in a water tank	No threshold determined in literature	17 outbreaks/ 5,487 sick

Table 3-7. Biological Hazards and Select Properties (continued)

Hazard	Type	Water Threat	Stable in Water	Chlorine Tolerance	Possible Means of Contamination	Level in drinking H2O that causes illness, drinking 15L H_2O per day (5L per day) for 7 days	Historical Outbreaks (1971-1996)*
Escherichia Coli	Bacteria	Yes	Stable	Easily killed with chlorine	Feces contamination	No threshold determined in literature	5 outbreaks/ 1,305 sick
Botulinum toxins	Biotoxin	Yes	Stable	Inactivated, 6 ppm, 20 min	Home canned foods dumped into the water supply. Only killed through steam heat/boiling	0.0004 µg/L	None found
Cryptosporidiosis	Protozoan	Yes	Stable days or more	Oocysts resistant	Cattle fecal contamination, people with compromised immune systems are most susceptible (hospitals, CDC)	1 oocyst/L (3 oocysts/L)	11 outbreaks/ 420,016 sick
Balanatidiasis	Protozoan	Yes	Probably stable	Unknown	Swine fecal contamination	No threshold determined in literature	1979 outbreak in Ecuador
Cholera	Bacteria	Yes	"Survives well"	"Easily killed"	Dump feces, raw meat into water	10 organisms/L (30 organism/L)	2 outbreaks/ 28 sick

Table 3-7. Biological Hazards and Select Properties (continued)

Hazard	Type	Water Threat	Stable in Water	Chlorine Tolerance	Possible Means of Contamination	Level in drinking H2O that causes illness, drinking 15L H_2O per day (5L per day) for 7 days	Historical Outbreaks (1971-1996)*
Giardiasis	Protozoan	Yes	Stable	Chlorine does not kill it however it is easily filtered	Feces with a known giardia contamination placed into the system after filtering.	No threshold determined in literature	115 outbreaks/28,129 sick
Plague (*Yersinia pestis*)	Bacteria	Yes	Stable	Unknown	Disease of rodents; bubonic, septicemic and pneumonic	0.67 organism/L (2 organism/L)	None found
Hepatitis A	Virus	Yes	Unknown	Inactivated, 0.4 ppm, 30 min	Human fecal contamination	No threshold determined in literature	28 outbreaks/827 sick
Brucellosis	Bacteria	Probable	20-72 days	Unknown	Unpasturized milk or milk products dumped into the water supply	100 organism/L (300 organism/L)	None found

Table 3-7. Biological Hazards and Select Properties (continued)

Hazard	Type	Water Threat	Stable in Water	Chlorine Tolerance	Possible Means of Contamination	Level in drinking H2O that causes illness, drinking 15L H_2O per day (5L per day) for 7 days	Historical Outbreaks (1971-1996)*
Tularemia	Bacteria	Yes	Up to 90 days	Inactivated, 1 ppm, 5 min	Uncooked rabbits or hare meat dumped into the water system.	106 organism/L (3 x 106 organism/L)	None found
T-2 mycotoxin	Biotoxin	Yes	Stable	Resistant	Trichothecene mycotoxin isolated from cereal grains infected with fusarium spp. of fungi	65 µg/L	None found
Aflatoxin	Biotoxin	Yes	Probably stable	Probably tolerant	Metabolites of the mold Aspergillus flavus that infects peanuts.	75 µg/L	None found
Ricin	Biotoxin	Yes	Unknown	Resistant at 10 ppm	Waste product of castor oil production.	15 µg/L	None found

Table 3-7. Biological Hazards and Select Properties (continued)

Hazard	Type	Water Threat	Stable in Water	Chlorine Tolerance	Possible Means of Contamination	Level in drinking H2O that causes illness, drinking 15L H_2O per day (5L per day) for 7 days	Historical Outbreaks (1971-1996)*
Staph enterotoxins	Biotoxin	Yes	Probably stable	Unknown	Protein toxins produced by Staphylococcus aureus.	0.1 μg/L	None found
Microcystins	Biotoxin	Yes	Probably stable	Resistant at 100 ppm	Hepatoxic products of freshwater blooms of cyanobacteria of Microcystis spp. And M. aeruginosa.	1 μg/L	None found
Saxitoxin	Biotoxin	Yes	Stable	Resistant at 10 ppm	Paralytic shellfish poisoning (PSP) produced by the Gonyaulax (marine dinoflagellate)	0.4 μg/L	None found
* AWWA Manual of Water Supply Practices Waterborne Pathogens							

Notes:
ppm = parts per million
min = minute
L = liter
ug/L = microgram per liter

(d) Radiological Hazards. The third category of intentional contamination is the use of a radiological hazard. **Table 3-8** summarizes various sources of radiological hazards and some additional comments for each. Generally, the likelihood that a terrorist would employ a radiological hazard to contaminate a water supply is low because it would be difficult to obtain sufficient quantity, in the correct form, at adequate strength to be effective.

Table 3-8. Radiological Hazards Summary (continued)

Locations and Materials	Radiation Sources	Source Strength	Comments	Likely Means to Contaminate
Gauges, Sources, Static Eliminators	Iridium-192, Cesium-137, Cobalt-60, Radium -226, neutrons, Americium-241, Plonium-210	Greater than about 4TBq	Sealed sources	Deposit in water system
X-ray Machine Sterilizers, Processors, and Particle Accelerators	X-ray, protons, deuterons, electrons, gammas, Cesium-137, Cobalt-60	4 TBq to 40 PBq	Anywhere in an industrial area Be aware of possible activation products.	Deposit in water system
Mineral Extra ion and Processing - including phosphate fertilizers, oil, natural gas and coal	Naturally Occurring Radioactive Materials- Uranium, thorium, and progeny	General Low level with external exposures from background to about 0.01 mSv (1 mrem)	Discovered low-level material and scale buildup in piping It is possible for radon to be of concern	Deposit in water system
Power Sources	Plutonium-238, Strontium-90	Plutonium-238: up to 4 GBq, Strontium-90: up to 1 TBq	In equipment in isolated areas	Deposit in water system
Radioluminescent Material	Promethium-147, Tritium, Radium-226	Up to tens of TBq	Various areas, and if leaking, surface contamination	Deposit in water system

Table 3-8. Radiological Hazards Summary (continued)

Locations and Materials	Radiation Sources	Source Strength	Comments	Likely Means to Contaminate
Cancer Treatment Areas	Cobalt -60 and Cesium-137	1 to several 10 Gy over several hours at about one meter if the source is exposed	Found in therapy rooms.	Deposit in water system
Medical Sources and Applicators	Cesium-137, Iridium-192, Radium-226, Phosphorous-32, Strontium-90, Iodine-125	Tens of MBq	Therapy and nuclear medicine areas	Deposit in water system
Radio pharmaceuticals	Iodine-131, Iodine-123, Technetium-99m, Thalium-201, Xenon-133	Tens of MBq	Storage, nuclear medicine areas and transportation	Deposit in water system
Various medical Sources and Devices	Tritium, Carvon-14, Sodium-22, Sodium-24, Sulfur-35, Calcium-45, Cobalt-60	Tens of MBq	Laboratories, nuclear medicine	Deposit in water system
Experimental Reactors and critical Assemblies	Activated Products, Fission products, transuranics	Tens of MBq	Universities, laboratories	Deposit in water system

Notes:
1. 1Bq = 1 disintegration of an atom/second.
2. 1 Curie = 3.7 x 1010 bQ

Tba = Tera Becquerele
PBq = Peta Becquerel
GBq = Giga Becquerel
mSv = millisievert
mrem = millirem
Gy = gray

ii. Optimally, the best radioactive material (RAM) would be easily attainable and water-soluble, have high activity, toxicity, and half-life, and be easily shielded or concealed during transportation. To be effective, the RAM would have to be introduced into the water system continuously over an extended period. These characteristics would ensure the greatest health impact to the intended population. If the water treatment facility can be contaminated with RAM either in a dust, liquid, or solid form, it will be an effective tool to shut down operations. Operations will not be able to resume until the RAM contamination or sources are removed. The RAM does not have to be present in a large amount or have a long half-life to work on a psychological level. Federal or state governments license RAM based on radioactivity amount and the health risk associated with various RAM.

iii. The greater the amount/activity or type (alpha vs. beta/gamma producer or high toxicity) of the radioisotope, the more difficult it is to procure due to the increased health risk to the general population. The health risk from RAM is limited because the majority of the water in the system goes to toilets, washing, bathing, etc. This would cause a potential external radiation exposure/contamination to beta/gamma radiation. The greater concern is the amount of water used for drinking. Alpha-producing RAM is the greater exposure risk internally, but large amounts of alpha-producing RAM are very difficult to procure. The RAM exposure from a source would come in a bolus or a single acute exposure except for the residual contamination. A more effective delivery system would introduce a periodic drip delivery of RAM to give a long-term hazardous chronic exposure. The chemical and physical form is very important. The majority of the sources are solid RAM sources. The solid source would sink to the bottom of the well or water system and not cause any significant contamination. The source could start to oxidize or produce limited contamination from erosion in the water, but the dilution factor would make the contamination negligible. If a high activity industrial source were introduced to the system, an external exposure hazard from the close proximity may be of concern.

(3) Cyber Attack. The final classification of threats aimed at water systems is the cyber attack. A cyber attack can affect an entire infrastructure network knocking out power, communications, and water systems. As the use of technology increases to improve efficiency and productivity, so does the vulnerability to a cyber attack. In particular, SCADA systems are now becoming key elements in the production and distribution of quality drinking water. These technologies have, for a longer period of time, been employed in power and communications networks. Electronic disruption of control, monitoring, or communications systems can have a dramatic effect on the proper operation of a water system, placing consumer health at risk to being exposed to inadequately treated drinking water. A SCADA system infected with a computer virus could result in the shutdown of an automatic chlorine feeder and evade detection by displaying false readings to the operator and inactivate any associated alarm system. Automated systems, such as SCADA systems that are accessible through the Internet, are vulnerable to hacking. However, because many SCADA systems are not connected to the Internet, the threat of a cyber attack is most likely to come from a disgruntled employee with access to the system.

b. General Recommendations.

(1) Physical Security. Efforts to enhance the existing physical security plan with upgrades should address detection; delay, and response, as well as mitigation features that are intended to prevent the undesired event from occurring. Vulnerabilities that are common to all types of attacks should be addressed first. Furthermore, a system feature common to many specific elements (such as, fence around treatment plant protects all of the treatment equipment inside) is a good candidate for upgrade because upgrading this single feature can usually result in a higher level of protection for many elements of the water system. Protection-in-depth means that an adversary should be required to avoid or defeat a number of security devices in sequence to accomplish the goal. Layers of features cause difficulty for the adversary, including: increased uncertainty about the system, more extensive preparations prior to the attack, and additional steps where failure could occur. **Table 3-9** presents example options to enhance security based on the detect, delay, respond, and mitigate approach.

Table 3-9. Features to Increase Physical Security Effectiveness

Approach	Security Feature
Detection	Sensors on doors, windows, and gates Camera surveillance (primarily to evaluate (assess) an alarm) Entry control measures like badges, key cards, guards
Delay	Harden doors, gates, and locks Add barriers like cages and vaults
Response	Shorten law enforcement response time Add on-site response officers
Mitigation	Install sensors/equipment that shut down system if contamination detected

(a) System Upgrades to Reduce Consequences. In the event that it is deemed impossible to prevent the adversary from succeeding, the security objective may become to reduce the consequences caused by the attack. Mitigation features or consequence reduction features should then be considered for each undesired event. Some mitigation features might include redundancy, contingency plans, early warning systems, or stockpiling of critical equipment.

(b) System Upgrades to Deter Adversary. Deterrence is an attempt to increase the perception level of the security system. This may be accomplished by adding visible security features (such as, warning signage, fences, cameras, or security officers) or by adding surveillance equipment or features that provide identification for prosecution evidence. The effectiveness of deterrence is difficult to measure. It would be a mistake to assume that because an adversary has not challenged a system the effectiveness of the system has deterred such

challenges. Further, note that not all threats are going to be deterred and some level of prevention or mitigation are still required. **Table 3-10** provides examples of features that might increase the perception of the protection system.

Table 3-10. Features to Increase Perception of Protection System

Deterrence
Add visible features Warning signage Locked doors Cameras for surveillance and recording devices for prosecution data Patrols Barriers for critical assets Sirens and lighting systems

(2) Monitoring. While monitoring itself cannot deter a determined terrorist, early detection of a contaminant should activate the response procedures and mitigate the severity of the consequences. Installations should consider a surveillance matrix that shows the personnel responsible for monitoring certain parameters at certain locations and the frequency of the monitoring. The GIS capabilities available at most installations should be used to provide a consolidated monitoring surveillance plan.

(a) Continuous Monitoring. Continuous monitoring is the in-line measurement of various parameters on a continuous basis. Ideal locations for continuous water monitors are inlets and outlets of treatment plants, as well as storage tanks throughout the distribution system. Monitors should measure pH, free available chlorine, turbidity, temperature, conductivity, and pressure. The AWWA Sourcebook provides vendor information. (See American Water Works Association, Sourcebook 08, http://www.awwa.org/awwa/sourcebook/.)

(b) Daily Monitoring. Daily monitoring should be conducted for pH, free available chlorine, turbidity, temperature, and conductivity by DPW. This monitoring should be conducted at multiple locations in the distribution system based on system-unique requirements. This could include sensitive locations such as Child Development Centers, hospitals, schools, and Command and Control centers. The DPW should closely monitor the results as an early warning system of potential contamination. This monitoring will mitigate the risk associated with the threat of biological and chemical contamination.

(c) Monthly Monitoring. State regulations mandate that water systems be monitored monthly for indicators of biological contamination and chlorine residual. The installation preventive medicine office should continue this schedule and possibly increase monitoring to weekly for selected locations based on the development or revision of the bacteriological monitoring program. The DPW is responsible for developing the bacteriological

monitoring program and taking appropriate action based on findings and recommendations by the preventive medicine office. This monitoring will mitigate the risk associated with the threat of biological contamination.

(d) Enhanced Monitoring. During times of increased threat, measurement of routine parameters such as pH, turbidity, conductivity, and chlorine residual (location, frequency) should be expanded; on-line measurements along with alarm capability are considerations. An unexplained drop of chlorine residual could indicate contamination by a crude agent preparation. Specialized analyses (example for chemical agents) may be warranted. Consumer complaints concerning discoloration, unusual taste, or objectionable odor may provide early warning, as well as an increase in illnesses at emergency medical-care facilities. Continuous monitoring of water pressure has value in evaluating the potential for contamination by cross-connections. Any off-line and continuous on-line monitors are currently available for chemical detection as shown in **Table 3-11** below—

Table 3-11. Analyzer Information

Analyzer	Parameters detected	Average Price
Gas chromatographs (GC)	Volatiles, oil, hydrocarbons	$20,000
GC coupled with mass spectrophotometers (GC/MS)	Identifies specific compounds	$200,000
Atomic absorption spectrophotometers	Metals	$20,000
Inductively coupled plasma spectrometers (ICP)	Metals	$200,000
Ultraviolet/Visible spectrophotometer	Polar organics	$1000

Technology for online monitoring of biological parameters is still in the developmental stage in the United States. One current methodology for general screening is the use of particle counters. Many existing counters, (such as the Hach® 2200 PCX ($8000)), are able to detect particles in a range of 2 to 750 microns. These counters could be used as surrogate indicators for contaminants, such as cryptosporidium and anthrax spores. Online biomonitors that measure biological responses of bacteria (Microtox-OS©), invertebrates (water fleas), or vertebrates (fish) to toxic chemicals are probably the next logical step in detection. Such devices are used in Europe but are still being tested in the United States. All of the current monitors are designed to indicate the presence of toxic compounds, but not their identity. The U.S. Army Research, Development, and Engineering Command (RDECOM) is currently evaluating advanced water monitoring systems. Hach® is a registered tradmark of the Hach Company. Microtox-OS© is a copyright of International Life Sciences Institute.

(3) Other Recommendations.

(a) Operations and Maintenance Practices. Operations and maintenance practices that mitigate the risks to drinking water systems include routine line flushing, exercising hydrants and appurtenances to ensure they are functional and in good repair, repair or replacement of distribution lines with disinfection and bacteriological testing, proper functioning of treatment systems, and maintenance of storage systems. These operations and maintenance practices should be systematically performed on a regular schedule for all installation water systems. The hydrant access policy (for contractors primarily but others as well) must be clearly stated and enforced. A permitting system can be used so that a person hooking up to a hydrant must display the signed authorization. The installation may want to explore options to tamper-proof hydrants near critical buildings (cost-prohibitive for every hydrant). Under terrorist threat conditions, increased emphasis should be placed on ensuring that these practices are conducted and improved as necessary. These practices will mitigate the risk associated with the threat of biological, chemical, and radiological contamination.

(b) Sanitary Surveys. Sanitary surveys are a physical survey of the water supply, treatment, and distribution system for the purpose of evaluating their adequacy for producing and distributing safe drinking water. They should include a review of selected management practices and monitoring efforts. These surveys should include host nation support facilities. This survey will mitigate the risk associated with the threat of biological, chemical, and radiological contamination.

(c) Cross-Connection and Backflow Prevention Programs. Cross-connection and backflow prevention programs mitigate the risk from contamination to the water supply from cross connections or pressure changes. The program should include an inspection program to ensure adequate protection of the drinking water system. An unprotected system could provide an easy means of access to a terrorist with knowledge of a specific system. This program will mitigate the risk associated with the threat of biological, chemical, and radiological contamination.

(d) Potable Water Master Plans. The purpose of potable water master plan is to develop and maintain an operations plan for the successful delivery of a sufficient quantity and quality of drinking water to the faucet. The various plans, assessments, surveys, operations and maintenance practices, physical security, and monitoring are all subordinate to the master plan. These plans should include current and accurate water distribution maps, drawings of pertinent system components, quantificating water demands under routine and non-routine conditions, and assessment of current and future water supply capabilities. They should also address training of personnel that are responsible for the operation of the water systems. This plan will mitigate the risk associated with the threat of biological, chemical, and radiological contamination.

(e) Chemical Deliveries. Ensure the safety of all chemical deliveries to the water system. Use the following bullets as guidance:

i. Vendors will send the utility photos and names of the drivers making deliveries.

ii. Utility will be notified of the name of the driver before the truck leaves the terminal.

iii. Trucks will be sealed with a security tag, and the serial number will be faxed to the utility after the truck has been loaded and is ready for shipping.

iv. Tanker number will also be faxed to the utility in order to match the numbers, assuring that it is the same tanker that left the terminal.

v. Utility will use two staff members on a regular basis to offload chemicals. This way they will become familiar with procedures, drivers, manifests, etc.

vi. Manifests will contain all of the same information along with the serial numbers and tanker numbers.

vii. Operators will notify the supervisors of any discrepancies before proceeding with the off-loading process. Discrepancies will result in delay of chemicals being off-loaded until problems are resolved.

viii. Notify police in the event of significant differences.

(f) General Short- and Long-term Examples. The AWWA provides a list of short- and long-term actions that the installation can take to harden the water treatment plant, distribution system, and storage tanks. These examples are provided to assist the installation staff and water plant operators with actions to take now and concepts to incorporate into management policy to reduce vulnerability to terrorist attack.

i. Short-Term Examples.

- At your office, well houses, treatment plants, and vaults, make it a rule that doors are locked and alarms are set.
- Make security a priority, and emphasize it at employee and safety meetings.
- Tell employees to ask questions and make note of strangers who are in your facilities or call in threats.

- Limit access to facilities. Indicate restricted areas by posting "Employees Only" signs.

- Increase lighting in parking lots, treatment bays, and other areas that seldom have people present.

- DO NOT leave keys in equipment or vehicles.

- Invite local law enforcement to become familiar with your facilities, and establish a protocol for reporting and responding to threats.

- Discuss detection, response, and notification issues with public health officials; establish protocols with them.

- Establish a chain of command and an emergency call list to be used in emergency situations.

- Provide copies of your operational procedures to local law enforcement and emergency management personnel.

ii. Long-Term Examples.

- Install motion sensors and video cameras to monitor, detect, and record events. They can be tied into a SCADA system for remote monitoring.

- Install intrusion alarms that cover remote buildings and grounds.

- Limit access to water supply reservoirs.

- Develop a clear policy to ensure all employees know how to deal with trespassers.

- Fit hydrants and valve boxes with tamperproof caps and lids.

- Install pass-code locks instead of keyed locks so access numbers can be changed as necessary (such as, when an employee is terminated). (Make sure, however, that emergency response personnel and law enforcement personnel receive the updated access codes.)

- Fence and lock vulnerable areas, such as wellheads, reservoir vents, and meter pits (valve boxes).

- Mark equipment with logos and distinctive paint jobs.
- Integrate early warning monitoring systems into water transport, treatment, and distribution systems so that an operator will be notified immediately of changes in chemical characteristics, flows, pressures, and temperature.
- Design and install valves that open and close slowly.
- Know your employees and who it is you are hiring. Make it standard practice to conduct background checks on all new employees.
- Install firewalls in computer systems, and change access codes frequently.
- Conduct and attend training activities to prepare your staff to detect, delay, and respond appropriately.

c. Interviewing Questionnaire. The following list of questions is presented to provide examples of the types of questions to ask installation personnel during the assessment.

(1) What do you think are some of the vulnerabilities of the water system?

(2) What do you think is the biggest vulnerability?

(3) How do you think an aggressor would attack it? How would you attack it based on what you know?

(4) What would be some of your suggestions to harden the water system from these vulnerabilities?

(5) What do you think should be done first (simplest or most critical action to take)?

(6) Are you aware of a security policy or SOP for your job? Yes____ No____

(7) Is it enforced? Yes____ No____

(8) Have you witnessed any problems with security? If so, can you explain?

(9) Have there been any recent events anywhere in the water system such as a threat, suspicious activity or vandalism?

(10) What areas (such as,doors, buildings, and facilities) of the water system do you have access to?

(11) How is the access controlled? How are keys controlled?

(12) What is security like at these locations?

(13) When an employee terminates employment, how is turn in of keys handled?

(14) How are chemical deliveries to the water treatment plant handled? What are the vehicle inspection procedures? Do you test chemicals upon delivery?

(15) Is conformance to security procedures and SOPs part of job description and/or performance objectives?

(16) When was the last time someone was rewarded for coming up with a security improvement?

(17) When was the last time someone was punished for not following proper security procedures?

(18) Are you aware of any specific threats (such as, disgruntled former employee, union issues, concerns with privatization)?

(19) Are background checks done on employees (are positions sensitive)? Are clearances required of any? Is your position considered "sensitive"?

(20) What is the policy concerning background checks on contractors and access control for contractors?

(21) How many operators per shift and working schedule?

(22) Is there any guard coverage? If so, where and describe coverage (such as, 2 guards at WTP each 8-hour shift, 24-hours per day).

(23) Have the MPs ever visited this site? Did they recommend any security improvements? Are they linked into the different aspects of the water system with roving patrols?

(24) Do you think security is tough enough at this water system? Yes___ No___ (if no, describe how so)

(25) Have the MPs ever been called for an incident? If so, what was the response like? Do you know their response time to the various locations of the water system?

(26) Are there any concerns with protestors?

(27) Do you receive any alerts from law enforcement (state or local police, MPs, or FBI)?

(28) What is your role in the monitoring program for source, treatment, and distribution of water?

(29) What monitoring equipment do you use? Is it calibrated and maintained?

(30) What are the laboratory capabilities in the area? Where do you go for non-regulatory parameters?

(31) Do you have an emergency/contingency plan and response plan?

(32) Have you practiced the plan and when was the last time it was updated?

(33) Do you have a memorandum of understanding (MOU) with the hospital (for early detection, investigations, response)?

(34) How are consumer complaints handled? By whom? Is there a central point of contact? Are complaints tracked both temporally and spatially?

(35) How are emergency room visits and sick calls tracked and assessed for incidence of waterborne illness?

(36) Do you have a cross-connection control program? How is it enacted?

(37) Who conducts flushing? Who has access to hydrants? Are they equipped with tamper control devices?

(38) Is there an off-post supplier? Has any coordination been done with them to see what type of vulnerabilities they might have?

(39) Are there any industrial activities in the watershed or within the wellhead area that could impact water quality?

(40) Have you coordinated with the State Emergency Management, EPA, and FBI etc? Do you participate in InfraGuard®? WaterISAC? InfraGuard® of the Federal Bureau of Invesitgation. (http://www.infragurad.net/)

(41) Have you coordinated with other local municipalities?

(42) What other studies or reports about water plant security might have been done (FPO, CID, MPs)?

(43) Has the installation prioritized activities, buildings, zones, etc.?

(44) Have you engaged in any type of neighborhood watch program, educated consumers of the threats and what to look for?

(45) How is parking controlled at key facilities?

(46) How are new employees trained with respect to security?

d. Example Notification Letter. **Figure 3-9**, is an example notification letter presented as a template for use by the assessment team.

e. Additional Resources. See Appendix E.

DEPARTMENT OF THE ARMY
US ARMY CENTER FOR HEALTH PROMOTION AND PREVENTIVE MEDICINE
5158 BLACKHAWK ROAD
ABERDEEN PROVING GROUND MD 21010-5403

MCHB-TS-EWS (40) 8 November 2001

MEMORANDUM FOR Commander, XVIII Airborne Corps and Fort Bragg, Directorate of Public Works, ATTN: APZA-PW (COL Smith), Fort Bragg, NC 28307-5000

SUBJECT: Notification of Visit - Water System Vulnerability Assessment (WSVA)

1. The scheduling of this WSVA visit is based on the telephone conversation between COL Jones, Director, Directorate of Environmental Health Engineering, U.S. Army Center for Health Promotion and Preventive Medicine (USACHPPM) and COL Smith, Garrison Commander, Fort Bragg, Insert date concerning the conduct of and the scheduling of the WSVA.

2. Our purpose in performing this assessment of the Fort Bragg drinking water system is to assess its vulnerability from and to provide recommendations to harden the system against intentional attacks. The assessment will assist in ensuring that the system is providing safe, good quality drinking water that is protective of consumer health.

3. The WSVA visit is scheduled for two weeks, 26 Nov – 7 Dec 2001. An inbrief is scheduled for insert time, 26 Nov 2001 in insert location. A tentative outbrief is scheduled for insert time, 7 Dec 2001 in insert location.

4. The Project Team will consist of the following members:

a. Mr. Mike Virizlay, P.E., Civil Engineer, Water Supply Management Program (WSMP), USACHPPM. Secret clearance granted insert date by OPM, based on NACI.

b. CPT Joel Bachman, P.E., Environmental Engineer, WSMP, USACHPPM. Secret clearance granted insert date by OPM, based on NACI.

5. It is essential to have key installation personnel available and involved in this process to ensure a thorough assessment and to prioritize any risk control measures. In order to facilitate the survey objectives, please provide the following assistance and materials starting at the beginning of the visit and continuing through the end of the onsite evaluation:

a. The following personnel or their representative attend the entrance brief and be available to the maximum extent possible to the team throughout the duration of the assessment:

(1) Installation Commander,

(2) Installation Force Protection Officer

Readiness thru Health

Figure 3-9. Notification Letter Example

MCHB-TS-EWS
SUBJECT: Notification of Visit – Water System Vulnerability Assessment

(3) Director, Directorate of Public Works (DPW)

(4) Chief, Facilities Management Division, DPW (with representatives for water, power, communications, and wastewater systems)

(5) Chief, Environmental and Natural Resources Division, DPW (with staff responsible for water resource management plans, cross-connection control programs, and regulatory monitoring)

(6) Water Treatment Plant and Distribution System Manager (and other operations and maintenance staff as deemed necessary by management)

(7) Plumbing Shop Foreman (and other staff as necessary)

(8) Fire Chief (and HAZMAT supervisor)

(9) Provost Marshal

(10) Criminal Investigation Division (CID)

(11) Military Intelligence (MI)

(12) Chief, Preventive Medicine

(13) Installation Preventive Medicine Environmental Science Officer

(14) Contracting officer for chemical shipments/deliveries

(15) Judge Advocate General

(16) Public Affairs Officers or Risk Communication specialist

(17) Emergency Room/Troop Medical Clinic Supervisors

b. Access to personnel familiar with and involved in water supply, treatment, distribution, and monitoring activities (to include personnel from the DPW, Preventive Medicine, plumbing shop, and the water treatment plant).

2

Figure 3-9. Notification Letter Example (continued)

MCHB-TS-EWS
SUBJECT: Notification of Visit – Water System Vulnerability Assessment

c. Access to all physical components of the water system, either escorted or unescorted, including secure areas of the post. Written documentation from the appropriate authority providing the necessary authority to access system components, to photograph equipment, videotape the survey, and to provide to law enforcement activities should our activities come in question

d. As-built drawings and an operational description of the water supply and treatment systems (surface water and groundwater systems).

e. Water distribution system maps showing major water mains, and storage reservoir locations and capacities.

f. Copy of installation drinking water emergency/contingency plan, related response plans, and any recent security evaluation reports.

g. System Control and Data Acquisition (SCADA) system design and operation documents.

h. Water system operational monitoring and control reports, plans, and records.

i. Copies of security policies and procedures and system visitor policies and procedure SOPs related to the drinking water system.

j. Copies of documents outlining policies and procedures related to any contract operation affecting the water system (e.g., chemical supplier).

k. Existing security system design and operation plans.

l. Records of recently completed, ongoing, and planned construction projects affecting water treatment, storage, and distribution systems.

m. A convenient work area with access to a DSN telephone for use during the onsite evaluation.

6. Due to the classified nature of the final report (secret), it is recommended that key installation personnel responsible for reviewing, implementing, and utilizing the final report be identified as authorized recipients of the final report. Those people should have, at a minimum, a secret clearance. In addition to security personnel, the Installation Commander, and DPW Director (or their representatives), we recommend that the water system supervisor or an individual(s) with detailed installation water system knowledge be an authorized recipient and therefore have a secret clearance. We recommend authorized recipients without a secret clearance to contact their

3

Figure 3-9. Notification Letter Example (continued)

MCHB-TS-EWS
SUBJECT: Notification of Visit – Water System Vulnerability Assessment

installation security office and begin the process of obtaining a secret clearance as soon as possible. .

7. Please refer any questions regarding this WSVA to Mr. Virizlay at commercial 410-439-3919/7747, DSN 584-3919/7747, or e-mail: mike.virizlay@apg.amedd.army.mil.

FOR THE COMMANDER:

NAME
Program Manager
Water Supply Management

4

Figure 3-9. Notification Letter Example (continued)

CHAPTER 4

FOOD AND WATER VULNERABILITY ASSESSMENTS AT SPECIAL EVENTS OFF-INSTALLATION

4-1. INTRODUCTION.

a. The purpose of the FAWD team is to reduce the vulnerability of food and beverage service to intentional contamination or disruption by terrorists or criminals at special events off-installation where DOD personnel may present an attractive target. The FAWD team is deployed at the request of the SESM to provide expertise in assessing and mitigating food and water risk. The SESM uses FAWD team recommendations to make decisions about overall event security.

b. Unique risks associated with special events include—

(1) Terrorism or Criminal Actions. Special events may be attractive to terrorists due to the strategic, symbolic, or patriotic nature of military events and because they may include access by the media and the general public. Criminals will normally have financial and other motivating factors. Special events can be soft targets because they are often located off base with varying potential levels of security. Special events are a potentially attractive target based on the large numbers (or high value) DOD personnel. Further, they are also well publicized well in advance.

(2) Temporary or Unusual Food Service Venues. Risks can include abrupt changes in food service practices by inexperienced or overwhelmed food service providers, use of temporary (surge) staff, and insufficient oversight by the local health authority.

(3) Lack of Jurisdiction. Unless included in the food service contract, off-installation facilities are not required to meet DOD public health standards, such as purchasing raw materials from DOD-approved sources and oversight by military sanitation inspectors. Contractor employees may not be required to meet Federal security or training criteria.

4-2. RESPONSIBILITIES.

a. The installation Commander is responsible for anti-terrorism and physical security on the installation. The next higher Commander, generally the MACOM Commander, is responsible for policy outside the installations within their geographic areas of responsibility.

b. The MACOM Commanders appoint an AT0 and/or physical security officer to manage and coordinate anti-terrorism and physical security program, generally from within the Provost Marshal's office. This official determines the requirement for the FAWD team.

c. The VETCOM is the MEDCOM lead agent for the FAWD program and coordinates resource programming with MEDCOM Resource Management based upon SESM requirement estimates. The VETCOM Commander will designate a Regional Veterinary Commander with responsibility for FAWD team formation, training, and deployment. The USACHPPM will support the lead agent.

d. The DOD Food Analysis and Diagnostic Laboratory (FADL) provides technical oversight of laboratory support to special events. This includes sampling procedures, oversight of the FAWD team's laboratory practices, and providing advice to the RVC Commander on laboratory results.

e. Once a specific mission is identified, the regional Commander will appoint a FAWD team chief and team members. The FAWD team chief is responsible for mission planning, coordination with food and water suppliers and municipal public health authorities, completing all reporting requirements and is the primary contact for the SESM. The Regional Commander must approve of any information released outside of the FAWD team (for example, laboratory results, vulnerability assessment, and after-action reports).

4-3. COMMUNICATING FOOD RISKS.

a. The FAWD team chief should communicate risks identified by the vulnerability assessment or any identified hazard to the SESM in the context of the FM 5-19 composite risk management process. Risks should be communicated accurately, objectively, and in a credible manner. The FAWD team chief should explain the basis of the risk and the sources, extent, and magnitude of significant concerns/risks associated with the assessment.

b. The FAWD team recommendations should be based upon accepted science, industry/regulatory practices, the growing body of literature regarding food defense, and military intelligence assessment of threats. Consultation with other military and federal public health officials and local public health officials is essential. When considering food security concerns, it is essential to use a team approach and view potential targets and vulnerabilities through the eyes of a potential terrorist/criminal.

4-4. THE FOOD AND WATER DEFENSE TEAM COORDINATION.

a. The SESM and VETCOM should coordinate with the MACOM protocol officer on an ongoing basis to encourage them to provide an early copy of a model performance work standard to the project officer for each event. The performance work standards in the food service contract create the authority for the FAWD team to require compliance with security requirements.

b. The SESM requests FAWD team support through the MACOM G3 to OTSG/MEDCOM operations using a tasking memo (**Figure 4-1**). The MEDCOM creates an OPORD tasking VETCOM for the mission.

c. The team chief contacts the event project officer to establish communication from the FAWD team through the SESM. The team chief confirms that the model performance work statement (PWS) has been included in the food and beverage contract and obtains an estimate of the number of attendees, the venue location, date and time, and food and beverage supplier(s) points of contact. If the Regional Veterinary Commander has not yet done so, the team chief coordinates with USCHPPM for preventive medicine personnel and equipment. See **Figure 4-2** for an example of a Model Contract: Food and Water Security Implementation Language for Inclusion in PWS.

d. If the performance standards are not included in the food service contract, the FAWD team has no authority to require compliance with security measures. Despite this large disadvantage, the team can still monitor the food and beverage service, work with the local public health and water authorities and provide recommendations to the SESM.

4-5. PRE-EVENT MEETINGS.

a. Face-to-Face Meetings. These meetings should take place as soon as practical with the food service contractor, the local water authority, and the local public health authority. It is critical to establish a good working relationship from the very beginning and to explain the significance of the special event and the "attractiveness" for terrorists. Be prepared to provide identification and/or security clearance information prior to a face-to-face meeting. Transfer of security clearance information should be done through your security office.

b. Food and Beverage Supplier. The team chief should meet with the supplier's senior staff include the event planner, security personnel, food and beverage director and facility engineer. The output from the meeting includes a team assembly plan and a date to walk through the facility; an initial estimate of personnel and equipment requirements; an initial estimate of timeline for coverage; a schedule and agenda for meeting with municipal health authorities; and initial estimates for expenses, travel and per diem, and identifying potential lodging which will meet team requirements. Subjects which should be covered during this initial meeting include—

(1) The purpose, structure, and capabilities of the FAWD team.

(2) The FAWD team priority for preventing intentional contamination over supplementing the local public health authority.

(3) Contractual performance work standards (if included in the contract) to include the security requirement to oversee food service from raw ingredient receipt to consumption.

DEPARTMENT OF THE ARMY
Office of the Deputy Chief of Staff, G-3
400 Army Pentagon
Washington, D.C. 20310-0400

REPLY TO
ATTENTION OF:

OPMG-OPS 30 October 2003

MEMORANDUM THRU: G3 Operations, HQDA, Army Pentagon,
Washington DC 20310

MEMORANDUM FOR: Health Care Operations, Office of the Surgeon General,
5111 Leesburg Pike, Suite 400, Falls Church, VA 22041

SUBJECT: Food and Water Defense (FAWD) Team support for the 2003 Holiday Reception which will be held at the National Museum for Women in the Arts, 1250 New York Avenue, NW., Washington, D.C. 20005-3970 on 10 December 2003

1. This memorandum is to inform you that the Secretary of the Army and the Chief of Staff of the Army, Under Secretary of the Army, and Chief of Staff of the Army are hosting this event. OPMG-SESM will initiate Vulnerability Assessment and provide a Security Plan for this event being held at the National Museum for Women in the Arts. POCs for this event is Mr. John Doe, John.Doe@hqda.army.mil. (703) 642-4406. Venue/Museum POC: Ms. Jane Doe, Director of Specail Events, 1650 New Hampshire Avenut, N.W. Washington, DC 20005-3970, (202) 784-5555, Jdoe@nwa.org.

2. Currently, the expected attendee list includes Secretary of the Army, Secretary of the Navy, Chief of Staff of the Army, Vice Chief of Staff for the Army, Sergeant Major of the Army, and other high ranking military and civilian personnel.

3. Request the assistance of your Food and Water Defense (FAWD) Team to provide pre-event vulnerability assessment at the above listed location NLT 15 Nov 03, and oversight of food and beverage service at the event scheduled for 10 December 2003. Your assistance is a necessity in performing a combined security operation given current threat conditions and conference attendees.

4. The POC for this event is Special Agent Max Smart, OPMG-OPS (703) 614-3210.

///Signed///
Max Smart
CID Special Agent

Figure 4-1. Tasking Memo

The Army requires safe and secure food service and drinking water supply. The food service contractor shall implement procedures to mitigate risk and provide reasonable assurance that the food and water supply chain for the event is safe and secure from intentional or unintentional contamination.

The contractor shall comply with the current food code. The contractor shall make a food safety plan (such as, Hazard Analysis and Critical Control Point (HACCP) plan) and a current list of food distributors that will support the event available to the Contracting Officer for review. The contractor will provide the Contracting Officer a list of its full part-time and intermittent employees and subcontractors providing services under the contract. The contractor will also provide the Contracting Officer documentary evidence of a completed favorable local law enforcement agency or equivalent background check in the form required by the Contracting Officer for all subcontractors, full-time, part-time, or intermittent employees employed for less than 2 years, who would under normal circumstances be allowed access to the food service or food preparation areas.

The contractor shall not identify or obtain food or beverage ingredients in any unique manner or specify them as being purchased for the specific event. To the maximum extent practicable, food for the event will be from common-use stock and randomly selected just prior to the event from generally available stocks.

The contractor shall use only unopened, untampered containers (including condiments, liquor and beverages) for event food service including open bars, morning and/or afternoon conference snacks, and room service, if provided for conference guests.

The contractor shall physically secure all food and beverage storage, preparation, and access points against improper entry just prior to and during the event. The contractor shall physically secure all water distribution points that are vulnerable to terrorist attack, including any distribution points identified by the FAWD team as being vulnerable to terrorist attack.

Food samples from each meal may be collected just prior to or just after the meal by the FAWD team for laboratory testing by the Army. The contractor shall provide in the manner specified by the Contracting Officer an extra serving of each food or beverage item from each meal and each snack provided under the contract for this purpose. The contractor will provide a secure refrigerated storage area for these food samples for the duration of the event.

The Contracting Officer may, at his/her option, assess food and water safety and security procedures several weeks in advance of the event or during whatever other time period

Figure 4-2. Model Contract: Food and Water Security Implementation Language for Inclusion in PWS

(4) Jurisdictional issues and the team's coordination with local heath department and water authority.

(5) Review of the food defense questionnaire (**Figure 4-3**).

(6) Review of event menu, supplier list for food, bottled water, bulk beverages and ice, and timeline for receipt of food items through cooking, and serving.

(7) Response planning. Define situations that food service personnel should be alert for, and discuss the role of food and water supplier personnel in reporting events to the FAWD team. Describe ERPs when contamination is suspected.

c. Regulated Drinking Water Supplier. Typically the preventive medicine representatives assigned to the team meets with water authority. For most DOD special events, the regulated drinking water supplier will be a water system owned by a municipality. To find a point-of-contact (POC) for the regulated drinking water supplier, search the web for a municipal website. The majority of municipal water systems, like Army water systems, are operated by a Public Works Department (such as, DPW). In most cases, there is contact information for the water system in the municipality's public works website. Key items to address during this meeting—

(1) A regulated drinking water supplier will have updated, detailed ERP in place to address intentional contamination of their drinking water system. The supplier will know how to respond to an intentional contamination event. Ensure contact information is provided to the FAWD to enable quick activation of the ERP should intentional contamination of the facility's drinking water system be suspected during the special event. Contact information, at the very least, should consist of a 24-hours emergency water system phone number. It is also helpful to have on- and off-duty phone numbers for the POC(s) attending the meeting. Also, provide the FAWD contact information to the supplier.

(2) Extend an invitation, with the approval of the special event facility's POC(s), to the supplier to have representatives attend the conduct of the facility vulnerability assessment. In many cases, the supplier will have and can supply distribution system maps identifying nearby fire hydrants and where the facility's water system connects to the distribution system. The supplier's representatives may also have vulnerability assessment experience and can provide additional input during the vulnerability assessment.

(3) If the FAWD has already coordinated with the regulated drinking water supplier for an earlier DOD special event, then this step may not be necessary. In this case, consider a face-to-face meeting if the location of the special event has changed or is new. Regardless, make sure the contact information for an intentional contamination response is up-to-date and accurate.

Food and Water Defense Team
Special Event Food Defense Questionnaire

PERSONNEL SCREENING
Are employees positively identified for security purposes?
Are unauthorized personnel prevented from entering functional areas?

ACCESS TO PREMISES

Is access to the facility limited? [Physical barriers (fences, locked doors), security personnel]
How is access monitored? [Surveillance equipment (CCTV, alarm system), badges, time cards, sign-in rosters]

SECURITY OF RAW MATERIALS AND PACKAGING

Are raw materials and packaging monitored? [QA program, vehicle security (seals), document verification]

CONTROLS OF MANUFACTURING OPERATIONS

Is food protected during preparation? (Closed/open systems, Control points for open systems, unlabeled containers, Knowledge of product destination, Access control)
Is food protected/monitored during transport if it is moved after preparation?
What procedures are in places to prevent tampering? [Vehicle ownership, Vehicle security (seals), Vehicle tracking systems, Knowledge of product destination]

WAREHOUSING AND DISTRIBUTION

Are products protected during storage? [Access control (authorized personnel), Inventory control, Separation of returned products]

Are products protected during distribution?

RESPONSE TO FOOD DEFENSE VIOLATIONS

Are procedures in place to respond to food defense violations? (Reporting requirements, Segregation & marking of suspect product, Recall program, Corrective action, Method of disposition)

Is training provided on food defense? (Recognition of potential tampering, Reporting procedures, Handling of suspect foods, Frequency and scope of training)

Figure 4-3. Food Defense Questionnaire

d. Local Public Health Authority. Local public health authority with jurisdiction over food service contractor. Subjects covered in this meeting include—

(1) The purpose, structure, and capabilities of the FAWD team.

(2) The FAWD team priority for preventing of intentional contamination over supplementing the local public health authority.

(3) Jurisdictional issues and the team's coordination with the food supplier and water authority.

(4) Describe the event (including size) potential attendance by VIPs, and food service arrangements.

(5) Coordination of responses to intentional and unintentional food or water contamination.

(6) Coordination of information sharing and review of previous food sanitation inspection results for the event venue.

e. Venue Walk-Through. The next meeting should be at the event location and include the FAWD team chief, key FAWD team members, water authority representatives, key food preparation supervisors, facility security, venue engineer and the food service event project officer. The purpose of this meeting is to—

(1) Review food defense checklist responses.

(2) Review menu and attendee count.

(3) Develop food receipt and preparation timelines.

(4) Obtain a list of all food, beverage, ice and bottled water suppliers, as well as review for especially hazardous foods and/or other specific security concerns.

(5) Conduct a walk-through assessment of all food storage, preparation and serving facilities, the public water supply connections to the facility and the internal water supply and distribution system with specific emphasis on water supplied to food operation and dining rooms.

(6) Review and discuss the facilities food operation food safety program.

(7) Review requirements to include access to the facilities and cooperation between the contract hotel, restaurant, and other facility staff with the FAWD.

(8) Determine need for credentials, access lists, and duty uniform for FAWD team members, parking, and meals.

(9) Conduct a water safety vulnerability assessment (see Appendix C). Review water system components vulnerable to intentional contamination (such as, nearby hydrants, facility water tanks, facility booster pumps, facility treatment systems).

(10) Review communication and reporting procedures.

4-6. TEAM ASSEMBLY. Ideally, this meeting occurs 1 week prior to the event. Team members include a mixture of DA civilians, officer and enlisted Army food inspection and preventive medicine personnel. The goals include—

a. Review team purpose; introduce team members, disseminate menu, key timelines, and food and water safety and security assessment.

b. Establish schedule.

c. Discuss individual team member responsibilities, duty uniform, communication, logistics (meals, transportation), communication (cell phones, radios).

d. The team members should tour all facilities, kitchens, storage and receiving areas and dining rooms associated with the event.

e. Preventive medicine team members should also tour water distribution, storage, and treatment at the venue to identify critical sites.

f. Discuss the selection, collection, and testing of food, water, and ice samples.

4-7. EVENT SUPPORT.

a. Event Support. Event support begins when food, specifically identified for the event, is delivered on site. The FAWD personnel arrive on site in phases according to mission needs. For example, initial receiving requires minimal staffing. The FAWD team chief briefs key food service personnel on role of the FAWD team to include specific food defense concerns and what to do if supervisors identify any security issues. As the team begins onsite monitoring of food preparation and serving, they conduct chemical, radiological, and biological sampling for further assessment of food items according to the sampling plan.

b. Team Members. The FAWD team members are expected to work together; the team leader can move or assign members to work in any area of FAWD. This is especially important during high production periods or when preparing and serving food.

c. Record Keeping. Support to DOD special events by FAWD team members must be accurately documented. All activities monitored or observed during DOD special events should be recorded, on a continuous basis, on a DA Form 1594 (Daily Staff Journal or Duty Officer's Log) (**Figure 4-4**). This record should be passed between team members on each shift and used in the final after-action report, which is distributed to the SESM and higher headquarters upon completion of the event support mission.

d. Emergency Response Plans. The ERPs should provide for several possible scenarios—

(1) Unintentional contamination that is unlikely to cause illness or result in a regulatory action by the local public health authority. If authorized by the RVC Commander, communication can go directly from the FAWD team chief to the senior food service representative on site.

(2) Unintentional contamination that is likely to cause illness and would probably result in a regulatory action by the local public health authority. The FAWD team chief informs the RVC Commander, who authorizes communication with the SESM and local public health authority.

(3) Intentional contamination. The FAWD team informs the RVC Commander, who authorizes communication with the SESM.

e. Alcoholic Beverages and Bar Service. To prevent deliberate contamination of alcoholic and non-alcoholic mixers during events where a bar is available, all containers will be sealed and unopened at the start of the event. The FAWD team members will inspect all beverage containers before use and ensure they are held in a locked cabinet or other secure location between uses.

4-8. SAMPLING PLAN. A sampling plan is drafted prior to the event (**Figure 4-5**). Samples will represent all components of the meal such that if intentional contamination occurs, the source of contamination may be identified and defined as much as possible. Visible sampling procedures may also deter actors; often the most practical location to sample is at point of serving (or plate-up). The fewest practical number of team members will be involved in sample selection, preparation, testing and packaging.

a. Microbiological testing. If rapid microbiological sampling technology is available, testing may be added to the protocol according to guidance from DOD FADL. Alternatively, samples for microbiological testing are taken for contingency purposes only. Food samples, consisting of 2 ounces from each component from each serving line, will be taken for each food offered to the customers to include dessert, table water, ice and beverages from a common container. Beverage samples include 16 ounces of hot and iced tea as well as liquid creamers and coffee. Individual drinks from closed containers are not normally sampled.

DAILY STAFF JOURNAL OR DUTY OFFICER'S LOG
For use of this form, see AR 220-15; the proponent agency is Office of The Deputy Chief of Staff for Operations & Plans

PAGE NO.	NO. OF PAGES

ORGANIZATION OR INSTALLATION	LOCATION	PERIOD COVERED			
		FROM		TO	
		HOUR	DATE	HOUR	DATE

ITEM NO.	TIME		INCIDENTS, MESSAGES, ORDERS, ETC.	ACTION TAKEN	INL
	IN	OUT			

TYPED NAME AND GRADE OF OFFICER OR OFFICIAL ON DUTY	SIGNATURE

DA FORM 1594, NOV 1962 PREVIOUS EDITION OF THIS FORM IS OBSOLETE. APD PE v3.00ES

Figure 4-4. DA Form 1594 – Daily Staff Journal or Duty Officer's Log

FAWD Team
Food Sampling Plan

1. Items to Sample. Sample items served as components of a full meal as well as other foods and snacks served between meals. If there are multiple serving lines during a meal, collect a sample of each item from each serving line. Be sure to collect a sample of all items offered, including desserts and beverages from common containers (such as, coffee, tea, etc). If any leftover item from a previous meal or substitute foods are offered, collect a sample of these foods as well.

2. Sampling Procedure. A member of the FAWD team should collect samples in sterile, tamper-evident containers according to guidance from the DOD FADL to ensure proper chain of custody. Food service employees may assist by placing or dispensing food into sample containers with utensils that are used to serve the food during the meal. Collect 2 ounces of each food and 16 ounces of each beverage. Individual drinks from closed containers are not normally sampled.

3. Labeling. A member of the FAWD team will label each container to ensure the following information is available:

   Sample number

   Name of food

   Date of preparation

   Date/time sampled

   When served (such as, breakfast)

   FAWD team member's initials

Figure 4-5. Food Sampling Plan

b. Radiological and Chemical Contamination. Collect 64 ounces of facility water which will normally be tested at USACHPPM. Additional food and water samples may be collected according to guidance from DOD FADL or USACHPPM.

c. Food Service Teams (FSTs). All FSTs are controlled by the FAWD team according to DOD FADL guidance to ensure chain of custody. Temperature sensitive samples should be placed in a chilled cooler with an ice blanket for immediate transport to secure refrigerated storage. The FSTs will be held in this secure storage for at least 5 days after the meal is served. This allows proper microbiological testing in the event of a suspected foodborne illness outbreak. Samples are held until released for destruction by the FAWD team chief.

d. Chain of Custody and Documentation. Chain of custody and other sample submission documentation will be according to specific guidance from the DOD FADL. Information required for each sample includes: sample number, name of food and specific event, date of preparation, date/time of sampling, when food was served (such as, breakfast), initials of person collecting sample, etc. (See **Figure 4-6**.)

e. Sampling Results. Any positive food test result should be immediately repeated. The RVC Commander must authorize information release before the FAWD team chief makes a recommendation to the SESM.

f. Reporting. Pertinent laboratory results are included as an annex to the After-Action Review (AAR). If laboratory results are delayed, the AAR is submitted as an interim report. Laboratory testing, conducted primarily as a laboratory validation exercise, is not included in the report.

4-9. POST-EVENT.

a. The FAWD team chief assembles the team immediately following the event to confirm that the sampling plan is complete, to collect records, and to conduct an AAR.

b. Reporting. The FAWD team chief provides a written AAR through VETCOM Headquarters to Operations Center 21/MEDCOM operations, with a copy to the SESM within 4 days of the event. If laboratory results are pending, a preliminary report may be released. Reports are FOUO (unless further restricted by the SESM) and are not provided to the food service provider.

ANTICIPATED SAMPLE TRAYS BY EVENT

EVENT/Location: _____

(For example, Association of the U.S. Army (AUSA) at Washington, DC Convention Center.)

NAME OF FUNCTION/Date/Room/Time:_____

(for example, Breakfast/ 2 Oct 07/Blue Room/0700 hours

List all menu items and sample numbers. Use event name as prefix for sample number (such as, AUSA-1-001).

ANTICIPATED SAMPLE TRAYS BY EVENT

SAMPLE #	FOOD DESCRIPTION	APPROXIMATE QUANTITY

Figure 4-6. ANTICIPATED SAMPLE TRAYS BY EVENT

4-10. TERMS.

a. Special Event. An event declared by the Special Event Security Manager to require physical security support. Typical criteria are events held off-installation and involving 10 or more Presidential appointees, General Officers, Senior Executive Service or equivalent personnel, or those that have special visibility or significance to potential terrorists. For the purpose of this pamphlet, the special event includes a meal or other food and beverage service.

b. Food and/or Water Defense. Prevention and/or mitigation of intentional contamination of food and/or water.

c. SESM. The physical security authority for special events within a certain geographic or organizational area of responsibility.

APPENDIX A

REFERENCES

REFERENCES

Army

DA Memorandum
Food Operations and Water System Vulnerability Assessments andEmergency Response Plans, 30 September 2002

FM 3-19.30
Physical Security, 8 January 2001.

FM 3-100.12
Risk Management, Multiservice Tactics, Techniques, and Procedures for Risk Management, 15 February 2001.

FM 4-02.7
Health Service Support in a Nuclear, Biological, and Chemical Environment, Tactics, Techniques, and Procedures, Appendix J, Food Contamination and Decontamination, 1 October 2002.

FM 5-0
Army Planning and Orders Production, 20 January 2005.

FM 5-19
Composite Risk Management, 21 August 2006.

FM 8-284
Treatment of Biological Warfare Casualties, 17 July 2000.

FM 10-52-1
Water Supply Point Equipment and Operations, 18 June 1991.

MEDCOM Regulation 40-28
U.S. Army Veterinary Command Policies and Procedures, 13 February 2006.

TB MED 530
Occupational and Environmental Health Food Sanitation, 30 October 2002.

TB MED 577
Sanitary Control and Surveillance of Field Water Supplies, December 2005.

USACHPPM Conference Presentation
"*Natural and Terrorist Threats to Drinking Water Supplies*", Proceedings of the 23rd Environmental Symposium and Exhibition, American Defense Preparedness Association, Arlington, VA., prepared by Burrows, W. Dickinson, Valcik, J.A., and Seitzinger, Alan. (http://chppm-www.apgea.army.mil/)

USACHPPM Information Paper No. IP 31-017
Biological Warfare Agents as Potable Water Threats, Medical Issues, March 1998.

USACHPPM TG 244
The Medical NBC Battlebook, April 1999.

USACHPPM TG 248
Guide for Deployed Preventive Medicine Personnel on Health Risk Management, August 2001.

USACHPPM TG 284
Drinking Water Complaints: Indicators from Distribution System Sentinels, May 2003.

U.S. Army Medical Research Institute of Chemical Defense, Handbook
Medical Management of Chemical Casualties, 1995.

U.S. Army Medical Research Institute of Infectious Diseases, Handbook
Medical Management of Biological Casualties Handbook, 4th Ed., Feb 2001.

Department of Defense

Air Force Handbook 10-222
Volume 4. Environmental Guide for Contingency Operations Overseas, 1 March 2007.

AFOSH Std 48-6
Management of the Air Force Drinking Water Program.

AFOSH Std 48-7
Sanitary Control and Surveillance of Field Water Supplies.

AFOSH Std 48-119
Medical Service Environmental Quality Programs, 25 July 1994

Defense Threat Reduction Agency
Security Classification Guide for Vulnerability Assessments, 6 May 2005.

DOD Memorandum
DOD Policy on Drinking Water Vulnerability Assessments and Emergency Response Plans, 03 July 2003

DODD 2000.12
DOD Antiterrorism (AT) Program, 18 August 2003.

DOD 2000.12-H.
DOD Antiterrorism (AT) Handbook, February 2004. This is an FOUO document. Authroized users may obtain a copy at www.dtic.smil/whs/directives.)

DODI 2000.16
DOD Antiterrorism (AT) Standards, incorporating Change 2, December 8, 2006.

Joint Staff/Defense Threat Reduction Agency
Vulnerability Assessment Benchmarks, 1 January 2007. (www.DTRA.mil)

National Defense University
Bioterrorism and Biocrimes: The Illicit Use of Biological Agents in the 20th Century, W. Seth Carus, Center for Counterproliferation Research, 1998, phone 202-685-2242.

USNORTHCOM
Antiterrorism (AT) Operations Order (U) 05-01, 6 May 2005. (FOUO)

Government Agencies

Title 40, Code of Federal Regulations, Part 141
National Primary Drinking Water Regulations, and Part 143, National Secondary Drinking Water Regulations, 2007.

Food Security Awareness Training
available at http://www.fda.gov/ora/training/orau/FoodSecurity/startpage.html

FDA Industry Guidance Documents
available at: http://www.cfsan.fda.gov/~dms/defguids.html

Food Defense Emergency Guidance for Retail Facilities
http://www.foodprotect.org/pdf/EmergencyGuidanceforRetailFoodEstablishments.pdf

Food Safety Inspection Service
Security Guidelines for the Transportation and Distribution of Meat, Poultry, and Egg Products available at: http://www.fsis.usda.gov/PDF/Transportation_Security_Guidelines.pdf

Food Safety Inspection Service
Security Guidelines for Food Processors, http://www.fsis.usa.gov/OA/topics/SecurityGuide.pdf)

GAO/NSIAD-99-163
Combating Terrorism, Need for Comprehensive Threat and Risk Assessments of Chemical and Biological Attacks, Washington, DC 20548.

GAO/RCED-00-3. FOOD SAFETY
Agencies Should Further Test Plans for Responding to Deliberate Contamination, October 1999. (http://www.gao.gov/new.items/r00003.pdf)

Guidelines For The Disposal Of Intentionally Adulterated Food Products And The Decontamination Of Food Processing Facilities
available at: http://www.fsis.usda.gov/PDF/Disposal_Decontamination_Guidelines.pdf

Public Law (PL) 107-188
Public Health Security and Bioterrorism Preparedness and Response Act, July 2002 (12 June 2002). (http://www.fda.gov/oc/bioterrorism/PL-107-188.html)

U.S. EPA 550-F-01-005
Addressing Terrorist Activities in the Local Emergency Plan. . Office of Solid Waste and Emergency Response, Local Emergency Planning Committees and Deliberate Releases, 2001.

Other Agencies

American Public Health Association, 2000
Control of Communicable Diseases Manual, Edited by James Chin, 17th Edition,Washington DC: American Public Health Association.

ASIS International (ASIS) information
available at: http://www.asisonline.org/, Institute of Medicine, National Research Council, 1998. Ensuring Safe Food–From Production to Consumption, Washington DC, National Academic Press. (http://www.nap.edu/catalog.php?record_id=6163).

Professional Publications

AWWA M19, Fourth Edition, 2001
American Water Works Association Manual of Water Supply Practices, Emergency Planning for Water Utility Management.

AWWA M48, 1999
Manual of Water Supply Practices, Waterborne Pathogens

Burrows, W.D., and Renner, S.E., (1999)
Biological Warfare Agents as Threats to Potable Water, *Environmental Health Perspectives.* 107(12), 975-84.

Craun, G., and R. L. Calderon
Waterborne Outbreaks in the United States, 1971-2000.Frederick Pontius (ed.), Safe Drinking Water Act Compliance Book, 1, Chapter3. John Wiley & Sons Incorporated, New York, NY.

Denileon, G.P., 1999
The Who, What, Why of Counter-terrorism Issues, American Water Works Association.

Haimes, Yacov, *Et Al*. 1998
Reducing Vulnerability of Water Supply Systems to Attack. Journal of Infrastructure Systems.

Rycus, Dr. Mitchell J., 1989.
Strategic Security Planning for Public Drinking Water Systems, University of Michigan, prepared for EPA. Office of Research and Development, Ann Arbor, MI.

University of Michigan, 1989
Strategic Security Planning for Public Drinking Water Systems.

Whelton A.J., Jensen J., Richards T., and Valdivia R., 2003.
Cyanide Concerns in Drinking Water. Proceedings National Defense Industrial Association Converence, Richmond, VA. April 7-10.

APPENDIX B

CONDUCTING FOOD VULNERABILITY ASSESSMENTS

CONDUCTING FOOD VULNERABILITY ASSESSMENTS

B-1. PURPOSE. To provide step-by-step procedures for conducting an FVA on military installations.

B-2. SCOPE. This section applies to food activities, including their transportation systems. All information gathered will be protected until a classification is assigned. All external risk communications shall be conducted only through the authorized FDAT spokesperson. The veterinary FDAT representative is required to brief the veterinary Commander upon completion of the assessment.

B-3. CONCEPT. According to DODI 2000.16, installations will conduct an annual comprehensive AT program review. At least once every 3 years, the heads of DOD components shall ensure that subordinate Commands undergo an external AT program review.

B-4. OVERVIEW. Use the following steps to conduct an installation FVA:

STEP 1. Develop a comprehensive list of food assets.

STEP 2. Conduct on-site assessment, encompassing Steps 3 & 4.

STEP 3. Identify hazards and vulnerabilities.

STEP 4. Assess hazards and vulnerabilities.

STEP 5. Recommend controls and determine residual risk.

STEP 6. Provide final report to the Assessment Team Leader/ATO.

B-5. PROCEDURE.

STEP 1. Develop a comprehensive list of food assets.

This list should include personnel, transportation systems, storage facilities, and preparation and serving resources, supply systems, contractors, and businesses approved for selling or delivering food and bottled water onto the installation, etc. Each FDAT team should generate their own installation unique list (See Figure B-1 example below). The following example is not all inclusive. For further information on this step refer to Chapter 2, Sections 2-1 through 2-4.

#	NAME OF ASSET or ESTABLISHMENT	Location	POC & Telephone
1	Troop Issue Subsistence Officer/Installation Food Advisor/Food Service Officer Hospital Nutrition Care Division All OPRATS Storage Locations		
2	Defense Commissary Agency (DeCA) activities		
3	NAF/MWR Contracting Officer Child Development Center Youth Services Officer/NCO Clubs Sports Clubs Gymnasiums Civilian Welfare Fund		
4	AAFES/NEX/MCX Post Exchange All Shoppettes Service Stations Food Court Facilities Fast Food Restaurants Mobile Food Services		
5	Fast Food Delivery (from off-installation)		
6	Office and home bottled water delivery		
7	Home food delivery contracts and vendors		
8	Non-AAFES mobile food operations		
9	DOD DFACs		
10	Hospital food service operations.		
11	Vending machines, including water vending		
12	Temporary and Special Event Food Operations, Chapels, etc.		
13	Off installation food operations supporting High-risk personnel including schools and child care facilities.		
14	DODDS Cafeterias		
15	OCONUS Local National Food Service		
16	Donated Food Operations		
17	Other Food Activities not listed above		

Figure B-1. Asset List Example

STEP 2: Conduct on-site assessment.

Describe the installation food procurement sources and the distribution from their sources. Develop flow diagrams that describe the processes for each asset (see Figures B-2 through B-5). The purpose of a flow diagram is to provide a clear, simple outline of the steps involved in the process (nodes). The scope of the flow diagram must cover all steps in the process.

If a process flow diagram does not already exist in documents contained in the Veterinary ISP, the FDAT must construct one based on their knowledge of the process. Each node in the system (to include supply, distribution, storage, retail sale, or preparation and serving should be studied to provide the insight to comprehensively understand the actual process and identify vulnerable areas. This flow chart will provide the foundation for the hazard analysis and must be detailed and complete. The interview combined with the flow chart and checklist is intended to help the assessor identify initial risk concerns.

With appropriate security classifications applied (as directed by the ATO), video cameras or digital cameras may be useful in gathering and conveying information to the team as assessments are carried out. Potential threats are systematically identified, located, and assessed based on the information provided by other team members and an analysis of the current threat situation (see Figure B-6). Prior installation Commander/ATO authorization must be obtained prior to use.

Summary of the on-site assessment—

a. The assessor will interview the POC to—

(1) Update or create flow diagram.

(2) Initiate the Food VA checklist; include observations obtained through interview

b. Perform walk thru.

(1) Verify information obtained during the interview.

(2) Verify and collect remaining applicable information to complete the Food VA checklist.

(3) Verify the flow diagram and adjust as necessary; annotate vulnerabilities relating to critical nodes.

c. Complete all forms and discuss feasibility of potential mitigation strategies.

SAMPLE FLOW DIAGRAMS

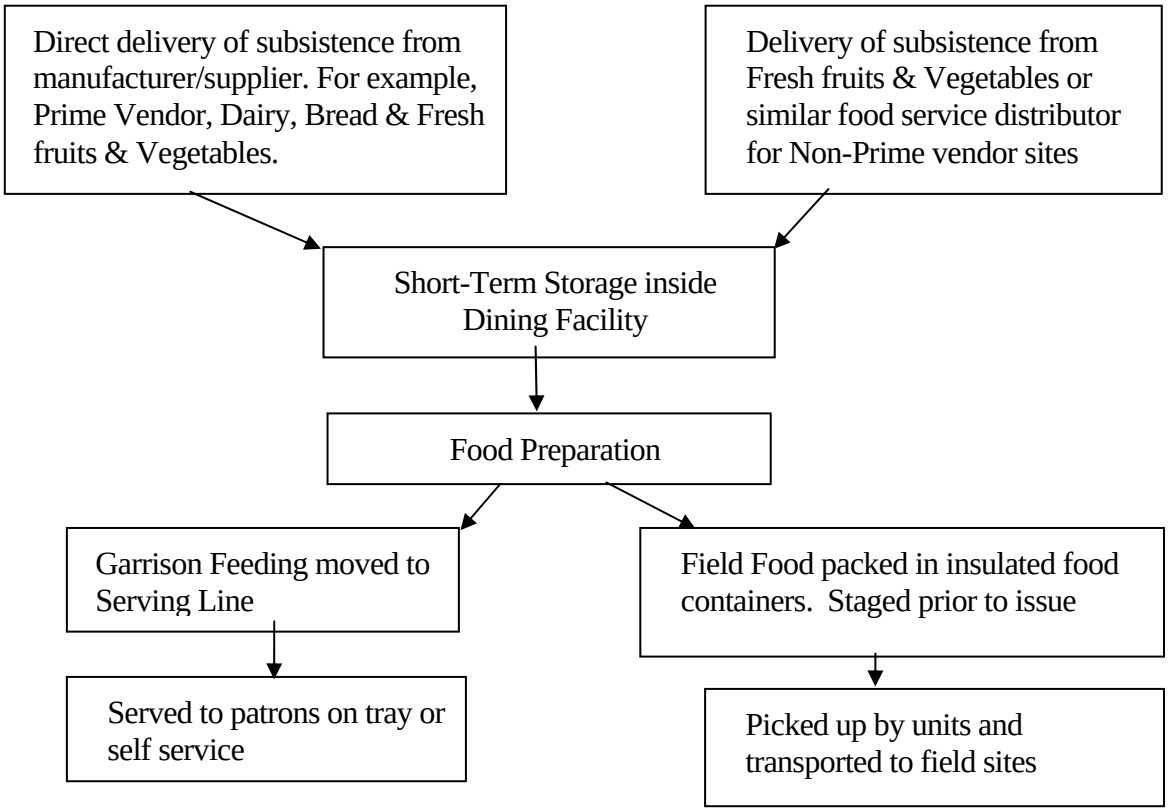


Figure B-2. CONVENTIONAL DINING FACILITY FLOW

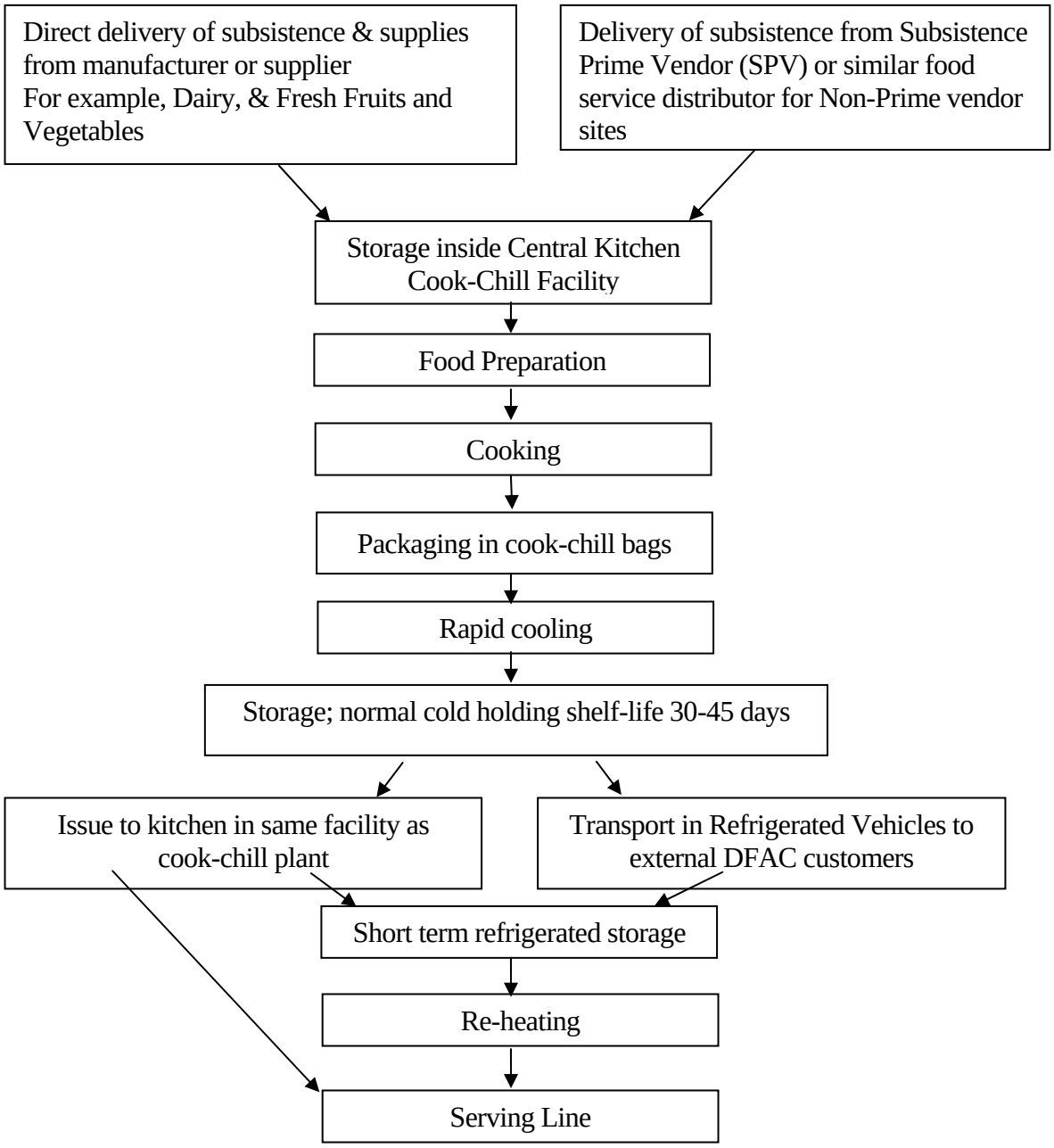


Figure B-3. COOK – CHILL OPERATIONS

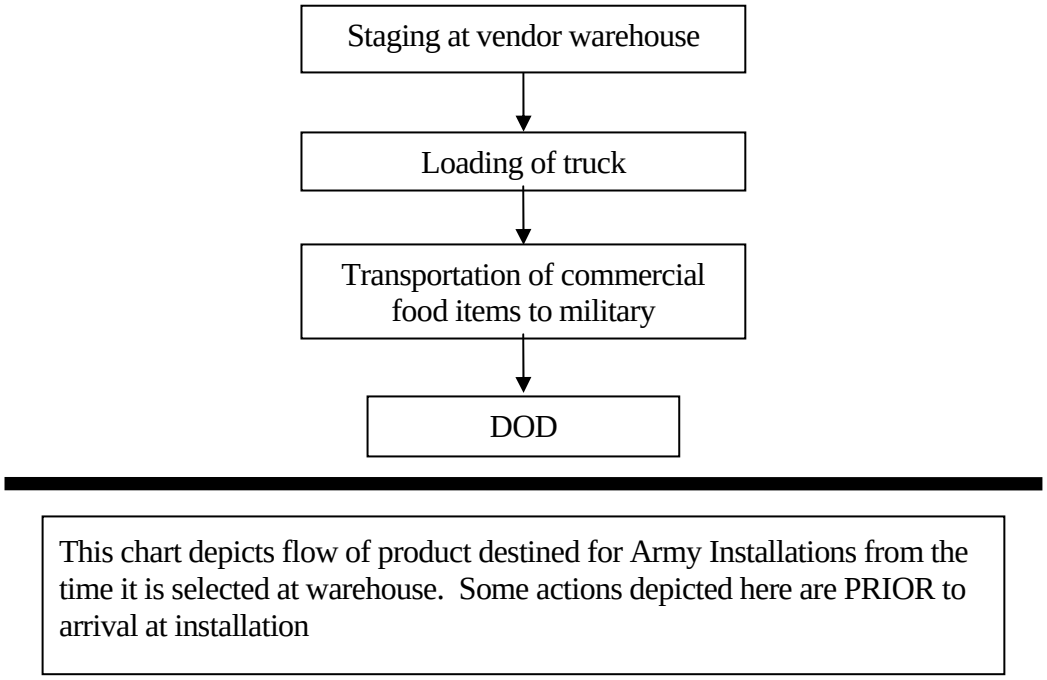
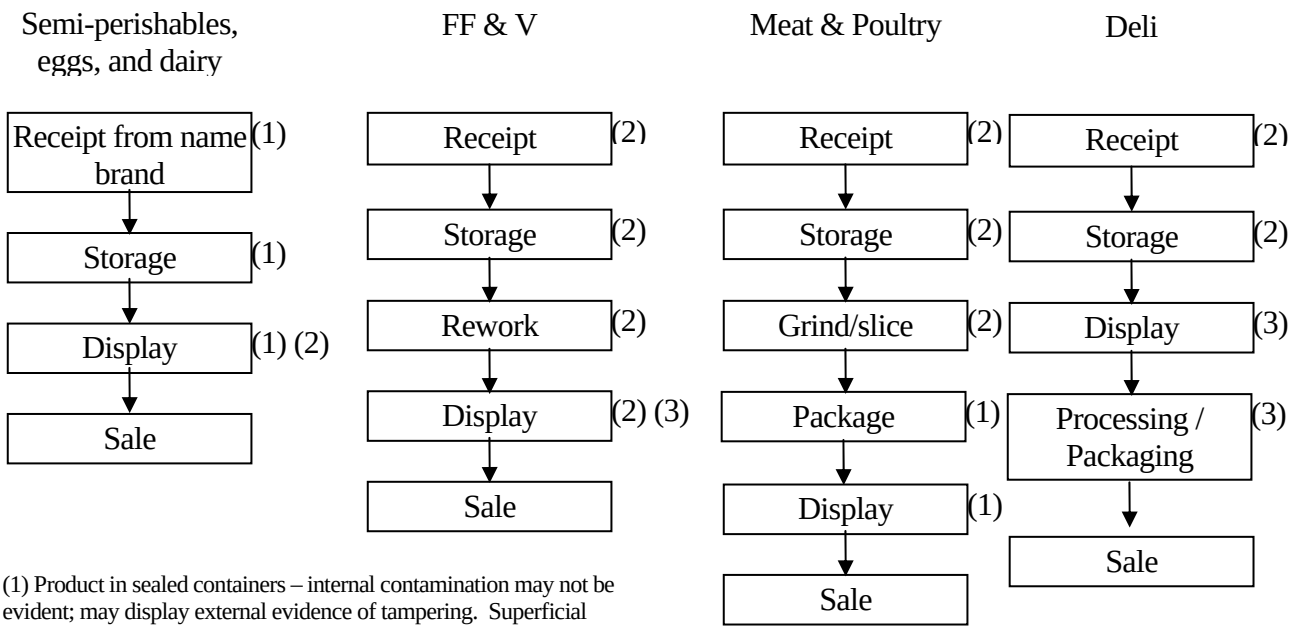


Figure B-4. Delivery Subsistence Prime Vendor or Retail Food Distributor Flow



(1) Product in sealed containers – internal contamination may not be evident; may display external evidence of tampering. Superficial contamination of external packaging is possible.

(2) Internal contamination possible; cooking stage of food prep may kill / inactivate most pathogens.

(3) No measure in place to protect consumer if the product is contaminated, if the product is ready to eat.

Figure B-5. DeCA Retail Establishment

Facility/(Suppliers)/Location/POC	Max # patrons/meal	Food Type Served/Operation Type	Assessor/Date

Potential Hazard	Observations	Risk	Recommended Controls/Residual Risk
1. Facility security			
a. Was an individual assigned responsibility for security? (AF STD: FS-FF-01) (DODI 2000.16, Std. 13)			
b. Are there procedures for investigating unusual activity? (FS-FF-01) (Std. 13)			
c. Was there unrestricted access into building? (FS-FF-02) (Std. 13)			
d. Is access to building monitored? (FS-FF-02) (Std. 13)			

Figure B-6. Food Vulnerability Checklist (continued)

Potential Hazard	Observations	Risk	Recommended Controls/Residual Risk
f. Were contractor tools, equipment, vehicles inspected prior to entering facility? (FS-FF-04) (Std. 13)			
g. Is the area around the facility adequately illuminated for nighttime security monitoring? Are facilities periodically inspected by security personnel during non duty hours? (Std 13)			
h. Was hazardous chemical (such as, cleaning/sanitizing agents, pesticides) storage access restricted? Is application monitored? (FS-FF-05) (Std. 13)			
2. Employees			
a. Are employee criminal background checks performed? (FS-FF-06) (Std. 18)			

Figure B-6. Food Vulnerability Checklist (continued)

Potential Hazard	Observations	Risk	Recommended Controls/Residual Risk
b. Are employees made aware of potential for food contamination and need for vigilance? (Std. 18)			
c. Is current list of employees maintained? Are authorized entry restrictions in place (keys/photocell badges, etc)? Are control procedures in place in the event of lost keys/badges, etc? (Std. 13)			
d. If badges or other forms of ID are used, are they difficult to counterfeit? (Std. 13)			
e. Are personal items excluded from preparation and storage areas? (Std. 13)			
3. Food Receiving			
a. Was food accepted from un-approved sources? (FS-FF-07) (AR 40-657)			
b. Are AT measures included in subsistence contracts? (Std. 18)			

Figure B-6. Food Vulnerability Checklist (continued)

Potential Hazard	Observations	Risk	Recommended Controls/Residual Risk
b. Was verification of truck locks and unique seals on receipt performed according to current FPCON level? Is vehicle resealed or escorted between multiple delivery points? (FS-FF-08, FS-TR-01) (Std. 14)			
c. Was delivery and driver verified by the distributor? (FS-TR-04) (Std. 14)			
d. Was incoming food inspected for evidence of tampering? (FS-FF-09) (Std. 14)			
e. Was a trace back system in place to document possible contaminated foods? (FS-FF-10) (Std. 18)			
f. Was the delivery door secure, when the storage room was not occupied by staff personnel? (FS-FF-02) (Std. 13)			
g. Was staff available for review/receipt of food items at the time of delivery? (FF-FS-04) (Std. 14)			

Figure B-6. Food Vulnerability Checklist (continued)

Potential Hazard	Observations	Risk	Recommended Controls/Residual Risk
h. Were delivery personnel allowed unescorted access to facility food areas? (FS-FF-04) (Std. 13)			
4. Serving Food			
a. Do food preparation operations inhibit/deter the intentional contamination of food items? (Std. 13)			
b. Did customers have un-restricted access to food/drink/ice at service or sale? Are customer self-service operations monitored? (FS-FF-11) (Std. 13)			

Figure B-6. Food Vulnerability Checklist (continued)

STEP 3. Identify hazards and vulnerabilities.

Continue interview and walk-thru utilizing checklists, flow diagrams, available materials, methodologies and resources to determine the degree with which exposure to one or more materials could result in harm and/or affect the mission. Multiple variables and unknowns will influence your assessment in the next step. However, primary considerations include:

- Types of hazard
- Sources of exposure

STEP 4. Assess hazards and vulnerabilities.

a. **Evaluate probability.**

(1) FREQUENT - occurs very often, continuously experienced.

(2) LIKELY - occurs several times.

(3) OCCASIONAL - occurs sporadically.

(4) SELDOM - remotely possible; could occur at some time.

(5) UNLIKELY - can assume will not occur, but not impossible.

b. **Evaluate severity.**

(1) CATASTROPHIC - loss of ability to accomplish the mission or mission failure. Example indicators: Death or widespread severe illness.

(2) CRITICAL - significantly (severely) degraded mission capability or readiness. Example indicators: Multiple foodborne illness incidences.

(3) MARGINAL - degraded mission capability or readiness. Example indicators: Sporadic foodborne illness, loss of confidence in food supply safety.

(4) NEGLIGIBLE - little or no adverse impact on mission capability or readiness.

c. **Characterize Risk.**

(1) Synthesize the estimates of hazard probabilities and severities. Risk levels for all food hazards and the overall mission are determined and described in a public health context. The primary objective is to apply the Risk Assessment Matrix in a way that is consistent with command guidance so that these risks can be put in the same context with other identified risks. Food threats must be clearly communicated to the Commander and the staff so that the Commander can make decisions based on credible information.

Table B-1. Risk Assessment Matrix

	HAZARD PROBABILITY				
HAZARD SEVERITY	Frequent (A)	Likely (B)	Occasional (C)	Seldom (D)	Unlikely (E)
Catastrophic (I)	Extremely High	Extremely High	High	High	Moderate
Critical (II)	Extremely High	High	High	Moderate	Low
Marginal (III)	High	Moderate	Moderate	Low	Low
Negligible (IV)	Moderate	Low	Low	Low	Low
	RISK ESTIMATE				

(2) Risk characterization should be designed to facilitate the selection of risk control strategies that are associated with risk levels that are greater than an installation-specified rate (as determined by the Commander).

Table B-2. Example Risk Level Definitions

RISK LEVEL	CONSEQUENCE
Extremely High	Expected loss of ability to accomplish the mission, or serious workforce or community impact (either on- or off-post).*
High	Expected significant degradation of mission capabilities in terms of the required mission standard, inability to accomplish all parts of the mission, or inability to complete the mission to standard if hazards occur during the mission, or significant workforce or community impact (either on- or off-post).*
Moderate	Expected degraded mission capabilities in terms of the required mission standard will reduce mission capability if hazards occur during mission, or minor workforce or community impact (either on- or off-post).*
Low	Expected losses have little or no impact on accomplishing the mission, and little or no impact on the community (either on- or off-post).*
* To assess the mission, workforce, or community impact, the FDAT should consider the psychological consequences of a terrorist event.	

d. **Determine Confidence in Risk Estimate**. A confidence level should be assigned following the determination of each risk identified. The degree of confidence in the risk estimate will be particularly important when determining a COA. The final determination of confidence must be based on the well-reasoned judgment of the FDAT. Refer to Chapter 2 of this document for guidance.

STEP 5. Recommend controls and determine residual risk (Food VA Checklist).

a. Hazard controls for food vulnerabilities can be divided into three basic categories.

(1) Education and Training.

(2) Physical Controls

(3) Avoidance

b. Refer to Chapter 2 of this document for control examples.

STEP 6. Final report to the Assessment Team Leader/ATO.

a. Document all results on the FVA Checklist (Figure B-6) risk management worksheets. Report key findings and recommendations from the checklist to the ATO.

b. The implementation of controls, supervision and evaluation of installation food defense programs in support of the antiterrorism plan are all ultimately directed by the Commander based on the FDAT's report.

B-6. SUMMARY. The FDAT veterinary representative will brief the veterinary Commander upon completion of the FVAs. Only secure means will be utilized for communicating CLASSIFIED material. CLASSIFIED material must be stored in approved containers or locations. The FDAT representatives may be directed by the installation command authority to conduct a follow-up FVA.

APPENDIX C

WATER SECURITY

WATER SECURITY CHECKLIST / DOD SPECIAL EVENTS

C-1. Coordination with Regulated Drinking Water Supplier.

a. Establish contact.

b. Hold a face to face meeting.

Note: Set up a meeting to discuss event water security support. Because a regulated supplier for DOD special events will have developed or updated ERPs to address intentional drinking water contamination, it is more effective to "tie into" these existing emergency response resources. Essentially we would want to be able to activate their ERP as soon as possible should a contamination episode occur during the event (such as, call their emergency hotline or specific security/emergency response POC). During the meeting explain that the DOD special event is essentially bringing more risk to their water system – senior DOD leadership outside of their normally secure areas (such as, Pentagon) is an "attractive" target to terrorists. We would like for them to be aware of what is going on in their water system. The key things to secure from this meeting are—

(1) Supplier's awareness of DOD special event.

(2) Emergency response contact information.

(3) Participation in event facility walkthrough.

C-2. Conduct Event Facility Walkthrough.

a. Establish group for walkthrough. Essential personnel—

(1) Event facility Engineer/O&M chief (knowledge of facility plumbing, water treatment)

(2) Regulated supplier distribution system personnel (knowledge and maps of distribution system serving event facility)

(3) Event facility security (knowledge of security procedures)

b. Identify water system components vulnerable to intentional contamination.

c. Evaluate existing water quality consumer complaint handling procedures (if exist).

Note: Focusing on intentional contamination only—physical destruction and cyber attack unlikely.

C-3. Develop Water Security Report (see example, Annex C-1).

a. No longer than 1-2 pages.

b. Components of report:

(1) Purpose

(2) Identified water system vulnerabilities and risks.

(3) Countermeasures to reduce elevated risks.

(4) Consumer complaint handling procedure.

c. Distribution of report:

(1) Food and Water Security Team (FAWD) members.

(2) Drinking water supplier POCs.

(3) Event facility POCs.

Note: Provide countermeasures for vulnerabilities with associated risks greater than "low". Incorporate the FAWD and the supplier's emergency response/consumer complaint personnel into existing procedures. Minimize impact of countermeasures on event facility employees. If a risk can be lowered through more frequent surveillance consider doing the surveillance yourself during the event. For countermeasures and consumer complaint procedures, provide contact information (duty/off-duty/hotline/emergency/cell etc).

C-4. WATER SECURITY STANDARD OPERATING PROCEDURE. (See Annex C-2.)

ANNEX C-1

EXAMPLE DOD SPECIAL EVENT WATER SECURITY REPORT
WATER SECURITY REPORT

RESERVE COMPONENT GENERAL OFFICER CONFERENCE
FOUNDERS INN – VIRGINIA BEACH, VIRGINIA
27 FEBRUARY – 1 MARCH 2006

1. PURPOSE. To reduce identified elevated risks of water system components to intentional contamination prior to and for the duration of the Reserve Component General Officer (RCGO) conference.

2. IDENTIFIED WATER SYSTEM VULNERABILITIES AND RISKS. The facility walkthrough resulted in the identification of three vulnerable water system components and their associated risks as shown in the Table. The level of risk identified for each vulnerable component indicates the likelihood of that water system component being exploited and the severity of the consequences should an intentional contamination event succeed. The low risk vulnerabilities indicate that intentionally contaminating drinking water by exploiting the vulnerable component is very unlikely and/or would result in minimal adverse consequences (that is, adverse health effects, water system shutdown). Vulnerable components at greater risk (such as, moderate, high, and extremely high) indicate a better chance or ability to successfully exploit the component and/or result in greater adverse consequences.

Table 1. Identified Vulnerable Water System Components and Associated Risk

Vulnerable Water System Component	Risk
Virginia Beach DPU-owned hydrant (that is, white-capped hydrant) nearest Founder's Inn potable water connection.	MODERATE
Unprotected connection to pressure gage on exposed water line entering Founder's Inn.	LOW
Softening treatment system in Swan Terrace Kitchen.	LOW

3. COUNTERMEASURES TO REDUCE ELEVATED RISKS. Countermeasures to reduce the risk of Virginia Beach DPU-owned hydrant would lower the overall risk to intentional contamination of the drinking water supply during the RCGO Conference. The following countermeasure should be in place for the duration of the RCGO Conference:

a. The Food and Water Security Team (FAWD) will routinely observe the hydrant for the duration of the conference to ensure there are no illegal connections to the hydrant. Anyone connected to this hydrant should be challenged and the hydrant connection should be verified with DPU. The Virginia Beach DPU 24-Hour hotline is (757) 385-1409. During business hours calls can be made to the Utility Operations Manager at (757) 563-1400.

b. CONSUMER COMPLAINT HANDLING PROCEDURE. Because consumer complaints could be an indicator of possible intentional water system contamination, it is imperative that swift and effective communication between those receiving the complaint and the Virginia Beach DPU, who have the expertise to address complaints, be in place. Any water quality complaints are expected to be directed to the Front Desk Staff. We recommend the Front Desk Staff immediately contact the FAWD as soon as they receive a water quality compliant during the RGCO Conference. The FAWD contact telephone number at USACHPPM is (443) 417-8966. The FAWD will then contact Virginia Beach DPU at the 24-Hour hotline number, (757) 385-1409 or the Utility Operations Manager at (757) 563-1400 during normal business hours.

ANNEX C-2
DEPARTMENT OF DEFENSE
SPECIAL EVENTS

WATER SECURITY STANDING OPERATING PROCEDURE EXAMPLE

1. PURPOSE. To conduct a Water System Vulnerability Assessment (WSVA) of a facility's water system and to ensure a coordinated response to an intentional contamination event with the facility's regulated drinking water supplier.

2. INTRODUCTION.

a. Background. Senior Department of Defense (DOD) leadership in non-routine surroundings can present an attractive target to terrorists. Many DOD and Military specific special events (such as, meetings and conferences) are attended by senior DOD leadership. These events put senior DOD leadership at an increased risk of attack by terrorists. One avenue of attack during these events is intentional contamination of a facility's water system. Intentionally contaminating the drinking water can cause illness and even death. Prior to these DOD special events taking place, a thorough evaluation of the facility's water system must be conducted to reduce the risk of intentional contamination.

b. Food and Water Defense Team Responsibility. The FAWD team must ensure that the drinking water provided during the special event does not pose an unacceptable level of risk of intentional contamination and subsequently provide an attractive target to terrorists. This standing operating procedure (SOP) provides guidance on conducting an evaluation of the facility water system hosting a special event, an evaluation of the municipal water system immediately surrounding the facility, identification of water system components vulnerable to intentional contamination and subsequent determination of risk, and identification and implementation of countermeasures to reduce those risks to acceptable levels. Finally, in the event intentional contamination does occur, the FAWD must coordinate with the municipal drinking water supplier to ensure a quick response and mitigate the consequences of the contamination.

c. Conducting a Facility WSVA. If the FAWD team member responsible for conducting the facility WSVA has little or no experience with drinking water systems or conducting WSVAs, please refer to the U.S. Army Center for Health Promotion and Preventive Medicine Technical Guide (USACHPPM TG) 188, "Food and Water Vulnerability Assessment Guide". The USCHPPM TG-188 provides a comprehensive overview on conducting a WSVA as well as a detailed introduction to drinking water systems. Hardcopies or electronic copies of USACHPPM TG-188 may be obtained by contacting the USACHPPM Water Supply Management Program (WSMP) by phone, (410) 436-3919; or e-mail: water.supply@apg.amedd.army.mil.

d. General Facility Water System Description. The DOD special events are held in hotels, conference halls, resorts, and convention centers. In most cases, these facilities do not have their own water supply. Rather, they purchase treated drinking water from a regulated drinking water supplier, usually a municipal water system. The facility's water system will be connected to the municipal water system's distribution system. Depending on the size of the facility there may be one or several connections. Facility water systems will consist of interior pipes, pumps, water systems (such as, water softener), and possibly storage tanks.

e. Consideration of Intentional Contamination Threat. Water systems are subject to three types of threats—physical destruction (such as, use of explosives); intentional contamination (such as, introduction of a chemical, biological, or radiological contaminant); and cyber attack (such as, remotely changing the operation of a chlorine feed system). For these special events, only intentional contamination is considered a realistic threat. Physical destruction is not likely since a terrorist intent on using explosives or causing physical damage would be inclined to cause damage in the facility where personnel are present and not target the facility's water system. Cyber attack is also not likely since most facility water systems hosting special events consist of only pipes, storage tanks, and pumps that are not remotely operated.

3. PROCEDURES.

a. Overview. To ensure an effective WSVA, FAWD team members should follow this SOP. In addition to conducting a WSVA of the facility's water system, coordination must be made with the regulated supplier, a brief water security report must be developed and provided to all interested parties, and the FAWD team should follow-up after the special event and provide all interested parties with an after action report. Each of these tasked are discussed in detail in this section.

b. Coordination with Regulated Drinking Water Supplier.

(1) Establish Contact. For most DOD special events, the regulated drinking water supplier will be a water system owned by a municipality. To find a POC for the regulated drinking water supplier, search the web for a municipal website. Most municipal water systems, like Army water systems, are operated by a Public Works Department (such as, DPW). In most cases, there is contact information for the water system in the municipality's Public Works website. Call the water system and set up a face-to-face meeting. Tell them who you are and why you are calling. Be prepared to provide identification and/or security clearance information prior to a face-to-face meeting in case the water system wants to verify your identity. Providing security clearance information can be done through your security office.

(2) Hold Face-to-Face Meeting. This step is critical if this is the first meeting between the FAWD and the regulated drinking water supplier. It is very important to establish a good working relationship with the supplier from the very beginning. Three key items must be addressed during this meeting—

(a) the supplier's awareness of the DOD special event;

(b) emergency response contact information; and

(c) supplier's participation in the conduct of the facility WSVA.

i. Explain the significance of the special event for their water system. Essentially, the special event is bringing more risk of attack to their water system due to the presence of DOD senior leadership outside of their usually more secure areas. This presents a more "attractive" target to terrorists.

ii. A regulated drinking water supplier will have updated, detailed ERPs in place to address intentional contamination of their drinking water system. The supplier will know how to respond to an intentional contamination event. Ensure contact information is provided to the FAWD to enable quick activation of the ERP should intentional contamination of the facility's drinking water system be suspected during the special event. Contact information, at the very least, should consist of an emergency water system phone number. It is also helpful to have on- and off-duty phone numbers for the POC(s) attending the meeting. Also, provide the FAWD contact information to the supplier.

iii. Extend an invitation, with the approval of the special event facility's POC(s), to the supplier to have representatives attend the conduct of the facility WSVA. In many cases, the supplier will have and can bring to the facility WSVA distribution system maps identifying nearby fire hydrants and where the facility's water system connects to the distribution system. The supplier's representatives may also have vulnerability assessment experience and can provide additional input during the WSVA.

(d) If the FAWD has already coordinated with the regulated drinking water supplier for an earlier DOD special event, then this step may not be necessary. In this case, consider a face-to-face meeting if the location of the special event has changed or is new. Regardless, make sure the contact information for an intentional contamination response is up-to-date and accurate.

c. Conduct Facility WSVA.

(1) Establish WSVA Team. An effective WSVA depends on a team consisting of individuals with good knowledge of the distribution system supplying the facility and the facility's water system, individuals with WSVA experience, and individuals with good knowledge of the facility's security procedures. A representative WSVA team is comprised of the following individuals:

(a) Facility engineer, or operation and maintenance chief. This person has knowledge of the facility water system components, such as the plumbing, storage tanks, treatment systems, and pumps.

(b) Regulated supplier distribution system personnel. These people have knowledge (and maps) of the distribution system serving the facility's water system.

(c) Facility security personnel. These people have knowledge of security capabilities and procedures and can help in determining the best countermeasures to reduce unacceptable risks for vulnerable water system components.

(2) Conduct the WSVA. Review USACHPPM TG-188, to gain familiarity with conducting WSVAs and water systems. Begin the facility WSVA at the point where the facility's water system connects to the regulated supplier's distribution system. At this location, look for vulnerable facility water system components and supplier's distribution system components such as an unlocked valve pit at the connection or fire hydrants very near the connection. From here, proceed into the facility and view interior water system components that may be vulnerable such as booster pumps, storage tanks, and water treatment systems. Ask questions about routine security procedures near or around water system components (such as, CCTV surveillance, locks), routine maintenance and operation of components, whether contracted or in-house (frequency and next scheduled maintenance). Also, ask questions about potential countermeasures that may be implemented to reduce the risk of intentional contamination. Once vulnerable water system components are identified, determine their risk of intentional contamination. If any risks are determined to be greater than low (according to the low, moderate, high, and extremely high risk scale), then countermeasures must be implemented to reduce the risk to a low level for the duration of the special event. Strongly consider countermeasures that minimize the impact on facility employees and normal business operations. For example, the facility operates a water softener that is located in a remote area of the facility accessible by an unlocked delivery door. The water softener is a vulnerable water system component because it provides an access point to the facility's drinking water. Because it's located in a remote area and near an unlocked delivery door, the probability of a terrorist intending to contaminate the water supply is determined to be likely should this water system component be targeted. The severity, should the attack succeed, is determined to be critical, as a significant amount of contaminant could possibly be introduced into the drinking water at this location before discovery. Therefore, the determined risk using the risk assessment matrix in USACHPPM TG-188 is high. Countermeasures must be implemented to reduce the risk to low. Possible countermeasures to implement during the special event include locking the delivery door if it does not impede normal facility operations, routine surveillance by the FAWD, and ensuring that no maintenance of the water softener occurs during the special event. At least one, if not all of these countermeasures could be implemented and would likely reduce the risk to low.

(3) Evaluate Consumer Complaint Procedures. Investigate how drinking water consumer complaints are handled. Consumer complaints may be the first indicator of intentional contamination. Are complaints called into the help desk and relayed to the facility engineer? Is a water sample collected and analyzed for various parameters (such as, chlorine, turbidity, pH)? Develop a procedure to ensure that during the special event, any water-related consumer

complaints are immediately reported to the FAWD and immediately relayed to the regulated supplier. The regulated supplier can respond to consumer complaints much more efficiently and thoroughly than facility and FAWD members.

d. Develop Water Security Report. After the WSVA is conducted, a water security report must be written. The report should be brief, consisting of no more than 2 pages. The report should include the following components: (1) Purpose; (2) Identified water system vulnerabilities and risks; (3) Countermeasures to reduce elevated risks; and 4) Consumer complaint handling procedure. Once completed the report should be widely distributed to the following groups: (1) FAWD members; (2) Regulated drinking water supplier POCs; and (3) Facility POCs.

e. Provide After Action Report. After completion of the special event, provide an AAR to the regulated supplier POCs and the event facility POCs. The AAR can be a brief e-mail outlining anything noteworthy that occurred during the special event or that the event had no food or water-related issues. Thank the POCs for their support.

4. POINT-OF-CONTACT. The POC for this SOP is USACHPPM WSMP; telephone number (410) 436-3919.

APPENDIX D

AFTER ACTION REPORT EXAMPLE

EXAMPLE AFTER ACTION REPORT TO SUPPLIER AND FACILITY POCs

From: Doe, John Mr USACHPPM
Sent: Thursday, March 02, 2006 8:45 AM
To: Smith, John Mr USACHPPM
Cc: xxxxxx@us.army.mil; xxxxx, xxxxx x Mr USACHPPM
Subject: EXSUM Reserve Component General Officer Conference-Virginia Beach, Virginia

A combined USACHPPM and VETCOM Food and Water Vulnerability Assessment Team (F&WVAT) supported the U.S. Training and Doctrine Command (TRADOC) Reserve Component General Officer Conference, Freedom Inn, Virginia Beach, Virginia, from 27 February to 1 March. The on-site team members were Mr. John Doe, USACHPPM and CW1 xxxxxxxx, Norfolk Branch, Middle Atlantic Division Veterinary Command, Norfolk Branch.

Mr. John Smith from USACHPPM provided the Water Vulnerability Assessment during the team's preliminary assessment 15-17 February. Mr. Doe included the water vulnerability recommendations in the team support to the conference.

The F&WVAT members worked with the CID agents and the Program Manager for the conference. The Freedom Inn guest and food service, security and building engineering staffs implemented the majority of the recommendations from the team's preliminary assessment. No significant problems with either food or water vulnerability were noted during the conference.

John Doe, R.S.
Food Safety and
Environmental Health
DEHE, USACHPPM
APG, MD 21010-5403
(410) 436-5458, FAX -8104, DSN 584-5458
cell phone (443)417-8966
john.doe@us.army.mil

APPENDIX E

ADDITIONAL RESOURCES

American Water Works Association
6666 W. Quincy Ave.,
Denver, CO 80235
Phone: 303-794-7711 or 800-926-7337
FAX: 303-347-0804
Internet: http://www.awwa.org

Association of Metropolitan Water Agencies
1620 I Street, NW
Suite 500
Washington, DC 20006
Phone: (202) 331-2820
FAX: (202) 785-1845
http://www.amwa.net/

Center for Disease Control and Prevention
1600 Clifton Rd.
Atlanta, GA 30333
(404) 498-1515/(800) 311-3435
http://www.cdc.gov

Center for International Security and Cooperation
Encina Hall
616 Serra St E200
Stanford University
Stanford, CA 94305-6165
http://cisac.stanford.edu

Center for Water Security
Director, Center for Water Security
University of Wisconsin-Milwaukee
Great Lakes WATER Institute
600 E. Greenfield Ave.
Milwaukee, WI 53204

The Great Lakes WATER Institute at the University of Wisconsin-Milwaukee (UWM) established a research center focusing on safeguarding the nation's drinking water supply systems. The funds to establish the center were included in the spending bill for the U.S. DOD. Some of the projects the Center will be working on include: Using translucent zebrafish as toxin "sentinels" by genetically altering them to light up like a firefly when the fish encounter small amounts of a particular toxin or class of toxins or bacteria, including an anthrax-type organism, *E. coli and Cryptosporidium*.

Using fiber optics to continually monitor water supplies leaving the treatment plant. Sensors will be placed at various points inside water distribution pipes would be attached to the fibers to report chemical changes in the water.

Using the natural sensing ability of Daphnia, microscopic aquatic animals that have sensory hairs on their bodies to test whether they can distinguish harmful materials in the water.

Using an atmospheric and lake monitoring model to detect and predict the movement of "dirty bomb" materials that could contaminate water.
http://www.uwm.edu/Dept/GLWI/cws/index.html.

FBI InfraGard Program
The InfraGard Program is an FBI/ National Infrastructure Protection Center (NIPC) program that was designed to help identify and coordinate existing infrastructure protection expertise both inside and outside the federal government. The 56 FBI field offices have established local InfraGard chapters with membership rosters that consist of representatives from private industry, the academic community, and the public sector. Local InfraGard chapters can decide how much and what information to share with the NIPC. The InfraGard Program includes an encrypted two-way
e-mail communication system to facilitate the secure sharing of information among InfraGard members.

Contact local FBI field office for more information
http://www.fbi.gov/contact/fo/fo.htm

Federal Emergency Management Agency
500 C Street, SW
Washington, D.C. 20472
http://www.fema.gov/

Infrastructure Analysis, Information Assurance Protection (National Infrastructure Protection Center)
The Infrastructure Analysis, Information Assurance Protection (IAIP) directorate of the Department of Homeland Security, includes the former National Infrastructure Protection Center (NIPC) along with four other government entities and was developed in 1998. The IAIP's current mission is to identify and assess current and future threats to the homeland (including water supply), map those threats against our vulnerabilities, issue timely warnings and take preventive and protective action. Army installations can receive a daily infrastructure threat bulletin (which includes water) by sending an electronic mail request to nipc.watch@fbi.gov. Potential subscribers must include their name, title, organization, telephone number, and reason for the request. A daily-classified threat bulletin can also be sent to Army installation personnel with SIPRINET accounts. Subscribers are not required to pay an access or subscription fee.

International Association of Emergency Managers
201 Park Washington Court
Falls Church, VA 22046-4527
(703) 538-1795
http://www.iaem.com/

International Life Sciences Institute
One Thomas Circle NW, 9th Floor
Washington, D.C. 20005-5802
(202) 659-0074
http://www.ilsi.org

J. Edgar Hoover Building
935 Pennsylvania Avenue, NW
Washington, D.C. 20535-0001
(202) 323-3205
http://www.nipc.gov/

Johns Hopkins University Center for Civilian Biodefense Studies
(410) 223-1667
http://www.hopkins-biodefense.org/

National Domestic Preparedness Office
Rm 5214
935 Pennsylvania Avenue, NW
Washington, DC 20535
(202) 324-9026
http://www.ojp.usdoj.gov/odp/

Coordinates all Federal efforts, including those of the DOD, FBI, Federal Emergency Management Agency, Department of Health and Human Services, DOE, and the Environmental Protection Agency, to assist state and local emergency responders with planning, training, equipment, and exercise needs necessary to respond to a weapon of mass destruction incident.

National League of Cities
1301 Pennsylvania Avenue NW
Suite 550
Washington, DC 20004
(202) 626-3000
http://www.nlc.org/

Sandia National Laboratories
Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the U.S. DOE. With main facilities in Albuquerque, New Mexico, and Livermore, California., Sandia has major research and development responsibilities in national security, energy and environmental technologies, and economic competitiveness.
PO Box 5800
Albuquerque, NM 87185
http://www.sandia.gov/

U.S. Army Center for Health Promotion and Preventive Medicine
5158 Blackhawk Road
Aberdeen Proving Ground, MD 21010-5403
(800) 222-9698
http://chppm-www.apgea.army.mil/

COMMANDER USACHPPM-North ATTN: MCHB AN Fort George G Meade, MD 20755-5225	Phone: Fax:	Commercial: (301) 677-6502 DSN: 622-6200 Commercial: (301) 677-7132 DSN: 622-7132
COMMANDER USACHPPM-South ATTN: MCHB AS 1312 Cobb Street SW Fort McPherson, GA 30330-1075	Phone: Fax:	Commercial: (404) 464-3332 DSN: 367-3332 Commercial: (404) 464-2126 DSN: 367-2126
COMMANDER USACHPPM-West ATTN: MCHB AW Box 339500, MS 115 Fort Lewis, WA 98433-9500	Phone: Fax:	Commercial: (253) 966-0014 DSN: 347-0014 Commercial: (253) 966-0163 DSN: 347-0163
COMMANDER USACHPPM-Pacific ATTN: MCHB AJ Camp Zama, Japan APO AP 96343-5006	Phone: Fax:	DSN: 263-8447 Commercial: 011-81-3117-63-8597 DSN: 263-8597
COMMANDER USACHPPM-Europe ATTN: MCHB AE Landstuhl, Germany CMR 402 APO AE 09180	Phone: Fax:	DSN: 486-8084 Commercial: 011-49-6371-86-7198 DSN: 486-7198

U.S. Army Environmental Center
5179 Hoadley Road
Aberdeen Proving Ground, MD 21010-5401
Telephone: 410-436-2657
Fax: 410-436-1240
http://aec.army.mil/

U.S. Environmental Protection Agency
Ariel Rios Building
1200 Pennsylvania Avenue, N.W.
Washington, DC 20460
http://www.epa.gov/

U.S. Army Corps of Engineers
http://www.usace.army.mil/

U.S. Department of Transportation
1200 New Jersey Ave SE.
Washington DC 20590
(202) 366-4000
http://www.dot.gov

Water Information Sharing & Analysis Center (WaterISAC)
16201 I Street, NW,
Suite 500
Washington, DC 20006
1866-H2OISAC
www.waterisac.org

Glossary

AAFES	Army and Air Force Exchange Service
AAR	After Action Review
AFIOH	Air Force Institute for Operational Health
AT/FPO	Anti-Terrorism/Force Protection Officer
ATO	Anti-Terrorism Officer
AWWA	American Water Works Association
CCTV	closed-circuit television
CDC	Child Development Center
CID	Criminal Investigations Division
COA	course of action
CONUS	Continental United States
DA	Department of the Army
DeCA	Defense Commissary Agency
DFAC	dining facilities
DOD	Department of Defense
DODDS	Department of Defense Dependents Schools
DODI	Department of Defense Instruction
DOE	Department of Energy
DPW	Public Works Department
EPA	Environmental Protection Agency
ERP	emergency response plan
FADL	Food Analysis and Diagnostic Laboratory
FAWD	Food and Water Defense
FBI	Federal Bureau of Investigation
FDA	Food and Drug Administration
FDAT	Food Defense Assessment Team
FM	Field Manual
FOUO	For Official Use Only
FPCON	Force Protection Condition
FPO	Force Protection Officer
FST	Food Service Team
FVA	Food Vulnerability Assessment
GIS	Geographic Informational System

HACCP	Hazard Analysis and Critical Control Point
HAZMAT	Hazardous Material
H.R.	House of Representatives
HRP	high risk personnel
IAIP	Infrastructure Analysis, Information Assurance Protection
IAW	In Accordance With
ID	identification
IDS	intrusion detection systems
ISP	Installation Support Plan
JAG	Judge Advocate General
JSIVA	Joint Staff Integrated Vulnerability Assessment
MACOM	Major Army Command
MCX	Marine Corps Exchange
MDMP	military decision-making process
MEDCOM	U.S. Army Medical Command
MEVA	Mission Essential Vulnerable Area
MI	Military Intelligence
MP	Military Police
MRE	Meal, Ready-To-Eat
MWR	Morale, Welfare, and Recreation
NAF	nonappropriated fund
NCO	Noncommissioned officer
NEPMU	Navy Environmental and Preventive Medicine Unit
NEX	Navy Exchange
NIPC	National Infrastructure Protection Center
NMCPHC	Navy and Marine Corps Public Health Center
OCONUS	Outside the Continental United States
OPR	Office of Primary Responsibility
OPRATS	Operational Rations
OTSG	Office of the Surgeon General
PAO	public affairs officer
P.E.	professional engineer
PM	Provost Marshall
PMO	Provost Marshall Office
POC	point-of-contact
PVNTMED	Preventive Medicine

PWS	Performance Work Statement
PX	Post Exchange
RAM	radioactive material
RCGO	Reserve Component General Officer
RDECOM	U.S. Army Research, Development, and Engineering Command
SCADA	supervisory control and data acquisition
SDWA	Safe Drinking Water Act
SESM	Special Event Security Manager
SIPRNET	Secured Internet Protocol Network
SNL	Sandia National Laboratory
SOP	standing operating procedures
TG	Technical Guide
TISA	troop issue subsistence activity
UGR	Unitized Group Rations
USACHPPM	U.S. Army Center for Health Promotion and Preventive Medicine
USAFSAM	U.S. Air Force School of Aerospace Medicine
USAR IOC	US Army Reserve Information Operations Center
VETCOM	U.S. Army Veterinary Command
VIP	very important person
WSMP	Water Supply Management Program
WSVA	Water System Vulnerability Assessment
WVA	Water Vulnerability Assessment