Implementation Guide for Responsible Care® Security Code of Management Practices

Site Security & Verification

American Chemistry Council

July 2002

This guide necessarily addresses problems of a general nature. Local, state, and federal laws and regulations should be reviewed with respect to particular circumstances.

In publishing this work, the American Chemistry Council is not undertaking to meet the duties of employers, manufacturers, or suppliers to warn and properly train and equip their employees, and others exposed, concerning health and safety risks and precautions, in compliance with local, state, or federal laws.

Information concerning security, safety, and health risks and proper precautions with respect to particular materials and conditions should be obtained from the employer, the manufacturer or supplier of that material, or the material safety data sheet.

This Guide provides sample strategies and resources to assist companies in the implementation of the Responsible Care® Security Code of Management Practices. The sample strategies and implementation resources are intended solely to stimulate thinking and offer helpful ideas on code implementation. They are in no way intended to establish a standard, legal obligation, or preferred option for any practice. Other approaches not described here may be just as effective or even more effective for a particular company. If a company so chooses, it may adopt any of these sample strategies or may modify them to fit the company's unique situation.

Nothing contained in this publication is to be construed as granting any right, by implication or otherwise, for the manufacture, sale, or use of any method, apparatus, or product covered by letters patent. Neither should anything contained in the publication be construed as insuring anyone against liability for infringement of letters patent.

The American Chemistry Council and its employees, subcontractors, consultants, and other assigns make no warranty or representation, either express or implied, with respect to the accuracy, completeness, or utility of the information contained herein, or assume any liability or responsibility for any use, or the results of such use, of any information or process disclosed in this publication, or represent that its use would not infringe upon privately owned rights.

This guide was produced with the assistance of Ohlhausen Research, Inc. Peter E. Ohlhausen, President. (703) 978-7549. info@ohlhausen.com. www.ohlhausen.com.

Contents

I. Introduction

The terrorist attacks of September 11, 2001, forever changed the way Americans live and work. The chemical industry—like every other American industry—is reassessing and enhancing its security measures in the wake of these attacks. We realize that these unprecedented circumstances call for nothing less than the best from our industry—to increase our level of preparedness and solidify our partnerships with law enforcement and security agencies.

In the wake of terrorist attacks against our way of life, chemistry has played an essential role in our nation's first line of defense against terrorism. From the disinfectants and antibiotics used to protect against potential biological warfare agents, to the bulletproof and flame-resistant fibers used to make the helmets and flak jackets that protect our troops in the field and our firefighters at home, to the microprocessors that give the technological intelligence edge to our security forces here and abroad, chemistry is a vital part of our military and public safety operations.

As a backbone industry, the business of chemistry has a rich history of providing products that are essential to America's economy, our way of life, and our national security needs. In the wake of the new security challenges, the industry is committed to doing its part to help protect these values. Our objective is to help ensure the protection of chemical facilities so we can continue—safely—to provide essential, life-saving products, to play a key role in revitalizing the nation's economy, and to secure the protection of our employees and neighbors.

Attention to security is a natural corollary to the chemical industry's safety culture. By reducing the risk of a wide range of threats and mitigating the effects of such incidents as terrorism, vandalism, sabotage, and workplace violence, security measures can serve the goals of process safety management, risk management, and Responsible Care®. Security efforts, like safety efforts, protect the community and company employees while keeping a chemical plant operational and profitable.

The purpose of the Security Code of Management Practices is to help protect people, property, products, processes, information, and information systems by enhancing security throughout the chemical industry value chain. The Code is designed to help companies achieve continuous improvement in security performance using a risk-based approach to identify, assess, and address vulnerabilities, prevent or mitigate incidents, enhance training and response capabilities, and maintain and improve relationships with key stakeholders. The Code must be implemented with the understanding that security is a shared responsibility requiring actions by others such as customers, suppliers, service providers, and government agencies. Everyone in the chemical industry value chain has security responsibilities and must act accordingly to protect the public interest.

Implementation of the Security Code helps achieve several of the Responsible Care® Guiding Principles:

- To seek and incorporate public input regarding our products and operations.
- To make health, safety, the environment, and resource conservation critical considerations for all new and existing products and processes.

- To work with customers, carriers, suppliers, distributors, and contractors to foster the safe use, transport, and disposal of chemicals.
- To operate our facilities in a manner that protects the environment and the health and safety of our employees and the public.
- To lead in the development of responsible laws, regulations, and standards that safeguard the community, workplace, and environment.
- To practice Responsible Care® by encouraging and assisting others to adhere to these principles and practices.

The Security Code complements, and should be implemented in conjunction with, other management practices that demonstrate the industry's commitment to protecting its employees and society. Existing management practices that enhance community awareness and emergency preparedness, pollution prevention, process safety, employee health and safety, product distribution, and product stewardship may relate to security. Companies should regularly reassess these security-related practices in the spirit of continuous performance improvement. Companies also should regularly reassess their participation in, and monitor the activities of, the national TRANSCAER® initiative, which promotes dialogue and emergency preparedness along chemical transportation routes.

By investing time and money in security efforts, managers can reduce the likelihood of adverse effects on employees, the public, and the environment, as well as help their companies avoid costly losses. In effect, security is a tool for maintaining operations integrity. Even a small incident, such as threatening graffiti by an intruder, can leave employees too distracted to work well and can cost a significant sum to rectify. A large incident, such as a deliberate release of a site's hazardous materials, can injure people, harm the environment, and seriously damage a company by disrupting operations, inviting multi-million-dollar lawsuits, requiring costly remediation, upsetting employees, and injuring the company's reputation. If a risk assessment determines that an access control system and closed-circuit television surveillance are warranted, the cost of those systems is minimal compared to the potential costs from a serious security breach.

Implementation of the 13-part Security Code is mandatory for all members of the American Chemistry Council. This guide is written to help plant managers, operations managers, and other managers in implementing that code. The American Chemistry Council wishes to thank the Synthetic Organic Chemical Manufacturers Association for its participation in developing this implementation guide.

Due to the rapidly evolving nature of security issues and related expertise, the American Chemistry Council will reassess the Responsible Care® Security Code, its management practices, and its implementation timetable no later than two years after Code adoption. Security Code implementation guidance will be updated as necessary in the interim.

Scope of This Guidance

This guidance has been prepared to assist ACC member companies and others within the industry in applying the new code elements to site security activities. For the purpose of this guidance, "site" means *domestic* (U.S.) facilities at which operations occur that *involve chemicals*, e.g., manufacturing, storage, processing, and handling, including laboratories or pilot plants. This guidance does *not* apply to non-chemical activity sites, such as administrative or sales offices, nor does it apply to transportation sites outside operating facilities. However, depending on specific situations, companies may want to consider evaluating security at sites other than chemical operations (such as corporate headquarters) that because of location or other factors may be a direct target or else an object of collateral damage. Subsequent guidance is under development regarding security of the distribution and chemical value chain as well as cyber security. Additional guidance is expected to be available beginning late summer and through fall 2002.

II. ACC Security Code of Management Practices

Each company must implement a risk-based security management system for people, property, products, processes, information, and information systems throughout the chemical industry value chain. The chemical industry value chain encompasses company activities associated with the design, procurement, manufacturing, marketing, distribution, transportation, customer support, use, recycle, and disposal of our products. The corresponding security management system must include the following 13 management practices:

1. **Leadership Commitment.** Senior leadership commitment to continuous improvement through published policies, provision of sufficient and qualified resources, and established accountability.

   The chemical industry's commitment to security starts at the top. This element calls for each company's leadership to demonstrate through their words and actions a clear commitment to security within their company, from corporate headquarters to our facilities.

2. **Analysis of Threats, Vulnerabilities, and Consequences.** Prioritization and periodic analysis of potential security threats, vulnerabilities, and consequences using accepted methodologies.

   Using generally accepted tools and methods, companies will conduct analyses to identify how to further enhance security. This process will be applied at chemical operating facilities using methods developed by Sandia National Laboratories, the Center for Chemical Process Safety, or other equivalent methods. Companies also will be using tools to analyze the security of product sales, distribution, and cyber security. These initial analyses will be conducted on an aggressive schedule, then conducted periodically thereafter.

3. **Implementation of Security Measures.** Development and implementation of security measures commensurate with risks, and taking into account inherently safer approaches to process design, engineering and administrative controls, and prevention and mitigation measures.

   Companies will take action when they identify and assess potential security risks. Actions can include putting additional or different security measures into place to provide greater protections for people, property, products, processes, information, and information systems. At facilities, actions can include measures such as installation of new physical barriers, modified production processes, or materials substitution. In product sales and distribution, actions can include measures such as new procedures to protect Internet commerce or additional screening of transportation providers.

4. **Information and Cyber Security.** Recognition that protecting information and information systems is a critical component of a sound security management system.

   Companies will apply the security practices identified in this Code to their cyber assets as well as their physical assets. Information networks and systems are as critical to a

company's success as its manufacturing and distribution systems. Special consideration should be given to systems that support e-commerce, business management, telecommunications, and process controls. Actions can include additional intrusion detection and access controls for voice and data networks, verification of information security practices applied by digitally-connected business partners, and new controls on access to digital process control systems at our facilities.

5. **Documentation.** Documentation of security management programs, processes, and procedures.

   To sustain a consistent and reliable security program over time, companies will document the key elements of their program. Consistency and reliability will translate into a more secure workplace and community.

6. **Training, Drills, and Guidance.** Training, drills, and guidance for employees, contractors, service providers, value chain partners, and others, as appropriate, to enhance awareness and capability.

   As effective security practices evolve, companies will keep pace by enhancing security awareness and capabilities through training, drills, and guidance. This commitment extends beyond employees and contractors to include others, when appropriate, such as product distributors or emergency response agencies. Working together in this fashion improves our ability to deter and detect incidents while strengthening our overall security capability.

7. **Communications, Dialogue, and Information Exchange.** Communications, dialogue, and information exchange on appropriate security issues with stakeholders such as employees, contractors, communities, customers, suppliers, service providers, and government officials and agencies balanced with safeguards for sensitive information.

   Communication is a key element to improving security. Maintaining open and effective lines of communication includes steps such as sharing effective security practices with others throughout industry and maintaining interaction with law enforcement officials. At the same time, companies understand that their role is to protect employees and communities where they operate, while safeguarding information that would pose a threat in the wrong hands.

8. **Response to Security Threats.** Evaluation, response, reporting, and communication of security threats as appropriate.

   Companies take physical and cyber security threats very seriously. In the event of such threats, companies promptly will evaluate the situation and respond. Real and credible threats will be reported and communicated to company and law enforcement personnel as appropriate.

9. **Response to Security Incidents.** Evaluation, response, investigation, reporting, communication, and corrective action for security incidents.

Companies will be vigilant in efforts to deter and detect any security incident. If an incident should occur, however, the company promptly will respond and involve government agencies as appropriate. After investigating the incident, the company will incorporate key learnings and will, as appropriate, share those learnings with others in industry and government agencies, and implement corrective actions.

10. **Audits.** Audits to assess security programs and processes and implementation of corrective actions.

    Companies periodically will assess their security programs and processes to affirm those programs and processes are in place and working and will take corrective action as necessary. In appropriate circumstances, assessments also will apply to the programs and processes of other companies with whom the company conducts business, such as chemical suppliers, logistics service providers, or customers.

11. **Third-Party Verification.** Third-party verification that, at chemical operating facilities with potential off-site impacts, companies have implemented the physical site security measures to which they have committed.

    Chemical industry security starts at our facilities. Companies will analyze their site security, identify any necessary security measures, implement those measures, and audit themselves against those measures. To help assure the public that our facilities are secure, the companies will invite credible third parties—such as firefighters, law enforcement officials, insurance auditors, and/or federal or state government officials—to confirm that the companies have implemented the enhanced physical security measures that they have committed to implement. In addition, companies should consult with these same parties as enhanced physical security measures are being considered and implemented.

12. **Management of Change.** Evaluation and management of security issues associated with changes involving people, property, products, processes, information, or information systems.

    Our employees and our processes contribute to, and rely upon, changes and innovations in products and technologies. As any changes are considered, our companies will evaluate and address related security issues that may arise. This can include changes such as new personnel assignments or installation of new process equipment or computer software or hardware.

13. **Continuous Improvement.** Continuous performance improvement processes entailing planning, establishment of goals and objectives, monitoring of progress and performance, analysis of trends, and development and implementation of corrective actions.

    Our industry commitment to security calls for companies to seek continuous improvement in all of our security processes. Since practices for addressing security will evolve, it is anticipated that company security programs and measures will evolve, reflecting new knowledge and technology. Companies continually will be tracking, measuring, and improving security efforts to keep people, property, products, processes, information, and information systems more secure.

III. Implementing the Code in Your Company

Each company shall implement a risk-based security management system for people, property, products, processes, information, and information systems throughout the chemical industry value chain. *This* guidance has been prepared to assist ACC member companies in applying the new code elements to *site security* activities. Subsequent guidance is under development regarding security of the distribution and chemical value chain as well as cyber security.

For each of the 13 management practices, this document presents the following:

- Formal statement of the practice
- Anticipated benefits
- Sample strategies
- Implementation resources

The implementation resources are typically segments taken from chemical company policies, procedures, plans, or memos, or from other sources, such as industry research documents. Company names have been removed, and in some cases sections within a resource have been removed and replaced with an ellipsis (…). Users of this implementation guide may wish to adopt the resources into their own security plans, changing the language to fit the particular characteristics of their companies. Note: it is advisable to examine all the resources and examples given in this implementation guide. Because of the interconnectedness of the 13 management practices, a resource offered for one management practice may be useful in implementing other management practices as well.

Due to the rapidly evolving nature of security issues and related expertise, additional materials and resources will be made available as they become available. Companies are encouraged to send materials they develop and are willing to share with others in the industry to Dorothy Kellogg at Dorothy_Kellogg@americanchemistry.com.

To help companies implement the Security Code, ACC has also created a new website, www.responsiblecaretoolkit.com. The site features information on security, performance metrics, certification, and other topics.

The Security Code complements, and should be implemented in conjunction with, other ACC Codes of Management Practices.

In implementing this Security Code to satisfy a company's Responsible Care® commitment, managers may wish to consider the following approach:

1. Develop a thorough understanding of the Security Code and its relationship to other Responsible Care® Codes. This implementation guide briefly explains each practice.

2. Identify company activities that currently involve security. Most companies already have security measures in place. Surveying current measures will reveal what has already been instituted and what remains to be done.

3. Develop a priority list of activities to be implemented. Some activities are easier, or more important, to implement than others. In setting priorities, take into account such factors as urgency, the need for outside resources, potential exposure, and risk.

4. Design a security management program that will implement the Security Code of Management Practices.

5. Develop a detailed plan that establishes a schedule, company responsibilities, and resources needed for each activity to be completed. When developing a plan, involve personnel representing various job functions. The plan should be updated on a regular schedule or whenever changes, such as the introduction of a new process, necessitate a review.

6. Implement the security improvements. Changes to existing practices are often hard to make. Begin implementing the program in small steps. Build employee trust and involvement by encouraging employee participation during each program step.

Implementation of these management practices will vary from company to company, or even in various plants of the same company. Some companies rely mainly on corporate security staff, while others, more decentralized, may depend primarily on site managers who do not specialize in security but have security responsibility.

Additionally, implementation of this Code will vary according to the regulatory climate. Companies, particularly those with several locations, must become aware of specific state requirements that may preempt or go beyond federal requirements. Adherence to the Security Code of Management Practices does not ensure regulatory compliance; therefore, companies should remain aware of new regulations or changes in existing regulations that deal with security.

Measurement and Reporting

In past Responsible Care codes, companies have annually tracked and reported on Practice-in-Place. The Practice-in-Place system is *not* part of the Security Code for several reasons. First, the schedule for implementing the Security Code is more aggressive than for past codes, suggesting the need for streamlined measurement and reporting. Second, Responsible Care® as a whole is moving from Practice-in-Place measurement and reporting to certification of company Responsible Care® management systems. While the new Responsible Care® certification system does not apply to the Security Code at this time, the change suggests that a different reporting and measurement system be used in the Security Code.

A streamlined system is being developed for periodic company reporting to ACC of progress in meeting the schedule of deadlines for assessment of plant sites, implementation of site security enhancements, and verification. Reports will need to be signed by both the company Responsible Care® Coordinator and Executive Contact. Statements will also need to be signed half way through the Code process attesting to the company's progress in meeting all of the Code practices as well as at the end of process (June 30, 2005). Materials will be included both in an updated version of this guidance and online at www.responsiblecaretoolkit.com.

Companies, of course, may continue to use their own Practice-in-Place measurement tools for purposes of internally tracking progress. However, they will not be asked to report these measurements to ACC, as they would have in the past.

Implementation Timing

All practices of this code must be in place as soon as practicable, but not later than June 30, 2005. Site security vulnerability assessments, implementation of security enhancements and third-party verification must be conducted according to the following schedule:

Facility Prioritization	**Complete Site Vulnerability Assessment[1]**	**Implement Security Enhancements**	**Conduct 3rd-Party Verification[2]**
Tier 1 Facilities	No later than December 31, 2002.	No later than December 31, 2003.	No later than March 31, 2003.
Tier 2 Facilities	No later than June 30, 2003.	No later than June 30, 2004.	No later than September 30, 2004.
Tier 3 Facilities	No later than December 31, 2003.	No later than December 31, 2004.	No later than March 31, 2005.
Tier 4 Facilities	No later than December 31, 2003.	No later than December 31, 2004.	

[1] Facilities in Tiers 1-3 will conduct full site vulnerability assessments; Tier 4 facilities will conduct a modified assessment.

[2] Tier 4 facilities have no off-site consequences expected to result from uncontrolled release, theft, or product contamination. Facilities with no expected off-site consequences do not require independent third-party verification of security enhancements.

IV. Management Practices

The following sections discuss the 13 management practices. Each section restates the practice and names anticipated benefits and sample strategies. It then provides a brief description of several implementation resources, the full text of which is provided separately in Section VI.

1. Leadership Commitment

Management Practice 1

Senior leadership commitment to continuous improvement through published policies, provision of sufficient and qualified resources, and established accountability.

The chemical industry's commitment to security starts at the top. This element calls for each company's leadership to demonstrate through words and actions a clear commitment to security within their company, from corporate headquarters to our facilities.

When a security program has visible, top-level support, it is more likely that program implementation and compliance will function more smoothly. Senior leadership commitment helps security staff gain cooperation from fellow employees and obtain the funding and materials necessary to implement security programs. Senior leadership commitment, expressed in the form of written security policies, also leads to a clearer company-wide understanding of security expectations. A company can use those expectations as baselines for continuous performance improvement.

Anticipated Benefits

Senior leadership commitment may provide the following benefits, among others:

- Employees embrace and cooperate with company security policies.
- Sufficient resources are made available to the security program.
- Employees are held accountable for their security-related duties.
- The public, employees, and other stakeholders are reassured as to the seriousness of the company's commitment to security.

Sample Strategies

The following are various strategies that senior leadership can consider adopting in their efforts to support their companies' security programs:

- Provide leadership, active involvement, and support.
- Approve, oversee, or participate in the company's security risk assessment.
- Include security as one of the company's core values.
- Set, approve, or promulgate company security policies.
- Set and communicate expectations.

- Track and monitor progress.
- Ensure appropriate priority.
- Monitor progress and intervene as appropriate.
- Provide and allocate resources necessary to meet established goals.
- Incorporate security into facility strategic and annual plans.

Implementation Resources

Section VI of this Guide provides policies and other documents that show how companies state the importance of senior leadership commitment to security efforts. The sample resources are intended to stimulate thinking and offer helpful ideas on code implementation. Other approaches not described here may be just as effective or even more effective for a particular company. If a company so chooses, it may adopt any of these sample strategies or may modify them to fit the company's unique situation. The sample resources are described in brief below:

Resource 1-1: Management Approval

This resource emphasizes the importance of management approval in support of security risk assessments.

Resource 1-2: Management Participation in Risk Assessment

This chemical company resource refers to companies with corporate security directors.

Resource 1-3: Security as a Core Company Value

This segment of *Site Security Guidelines for the U.S. Chemical Industry*, published in October 2001 by the American Chemical Council, the Synthetic Organic Chemical Manufacturers Association, and the Chlorine Institute, encourages managers to support security by treating security as a core company value and establishing clear security policies.

2. Analysis of Threats, Vulnerabilities, and Consequences

Management Practice 2

Prioritization and periodic analysis of potential security threats, vulnerabilities, and consequences using accepted methodologies.

Using generally accepted tools and methods, companies will conduct analyses to identify how to further enhance security. This process will be applied at chemical operating facilities using methods developed by Sandia National Laboratories, the Center for Chemical Process Safety, or other equivalent methods. Companies also will be using tools to analyze the security of product sales, distribution, and cyber security. Analysis of the distribution systems, the value chain, and information (cyber) systems will be addressed in other guidance. These initial analyses will be conducted on an aggressive schedule, then conducted periodically thereafter.

The business of chemistry has moved quickly to respond to new challenges since the September 2001 assaults. The ACC Board of Directors expects that all ACC member companies will complete a two-step process consisting of an initial prioritization of facilities and a full vulnerability assessment.

Recognizing the impracticality of conducting full vulnerability assessments at all facilities simultaneously, the Board provided a mechanism for ACC members to prioritize their facilities. A prioritization guidance tool developed by member company experts is presented as Resource 2-1, presented in Section VI of this document.

Once the prioritization is completed, companies should conduct a full vulnerability assessment on facilities in Tiers 1-3 and a modified assessment on facilities in Tier 4, according to the following schedule:

- **Tier 1 Facilities:** No later than December 31, 2002.
- **Tier 2 Facilities:** No later than June 30, 2003.
- **Tier 3 Facilities**: No later than December 31, 2003.
- **Tier 4 Facilities:** No later than December 31, 2003.

To fulfill expectations under the new Security Code, ACC members must conduct a vulnerability assessment using the Sandia methodology, CCPS methodology, or an equivalent methodology determined by CCPS to exhibit their SVA criteria. To date, three company methodologies have been determined to be equivalent and are available under Security Guidance Documents at http://www.responsiblecaretoolkit.com.

Anticipated Benefits

Prioritizing facilities enables companies to proceed in their security planning in the most efficient and effective manner by helping managers determine which facilities to focus their efforts on first. The benefit is that, by prioritizing facilities, a company can be confident that it is devoting extra attention to the right sites first, thereby maximizing security for employees, the community, the environment, plant operations, and company information and product.

Vulnerability assessment is the vital tool that helps managers decide what specific resources at a site need protection, what threats may be directed at those resources, and how to protect those resources. Vulnerability assessment is the necessary foundation of all security efforts.

Sample Strategies

The following are various strategies for analyzing the threats, vulnerabilities, and consequences at a given chemical site, as well as for prioritizing a company's various sites by level of risk:

Prioritize Sites

- Evaluate RMP facilities with program 2 or 3 processes based on (1) relative difficulty of attack, (2) relative severity of attack, and (3) relative attractiveness of target.
- Rate the security "worst case" scenario for each Risk Management Program (RMP) process on a scale of 1-4 for difficulty, severity, and attractiveness. Add the three factors together to determine the Security Risk Index (SRI) for the process. The overall facility SRI is the highest of the SRIs calculated for each RMP process.
- Evaluate all other facilities using a similar methodology based on factors such as (1) the materials present at the site, (2) potential impact on off-site receptors, and (3) potential for simultaneous attacks against adjacent equipment.
- Include, among materials of concern, those with a potential for misuse in terrorism or the production of weapons of mass destruction or illegal drugs. Also, pay special attention to manufactured products use as or in production of human or animal food or the provision of human or animal health care.

Establish Vulnerability Assessment Team

- Obtain senior management approval and sufficient resources.
- Establish multidisciplinary vulnerability assessment team.

Conduct Vulnerability Assessment

- Conduct a vulnerability assessment using the Sandia methodology, CCPS methodology, or an equivalent methodology determined by CCPS to exhibit their SVA criteria.
- Select an appropriate methodology considering factors such as local security needs, nature of the assets, complexity of the asset infrastructure, available information, available personnel and resources, company interest, community concerns, and national interests.

- Take into account vulnerabilities that could arise because of inadequate security measures of nearby sites. For example, an intruder might enter through an unsecured gate or inadequate fence maintained by a neighboring company.
- Consider vulnerabilities that could arise because of the site's proximity to attractive targets, such as government buildings, military installations, or national monuments. An attack on one of those targets could cause collateral damage to the chemical site.
- Undertake preparation and planning commensurate with the methodology selected, including problem definition, scoping, data collection, and compilation of asset/hazard/threat information.
- Consider internal and external threats potentially resulting in (1) chemical theft/misuse, (2) loss of containment, (3) contamination or spoilage of plant materials, and (4) degradation of assets, business function, or value of the facility.
- Consider and select appropriate means to analyze the likelihood of successful attack based on analysis scope, local needs, and quality of available information.
- Identify relevant layers of protection and the consequences of failure of layers of protection.
- Consider potential consequences of security events on the workers, the community, the environment, and critical infrastructure. Base any consequence analyses on reasonable worst-case conditions.
- Use a systematic approach to identify options for security enhancements. Consider methods that will deter, detect, delay, diminish, prevent, mitigate, or contain an attack. Consult lists of potential security countermeasures. (For example, see Sample Strategies in Section IV.3, Implementation of Security Measures.)
- Document results and technical basis.

Establish Process and Schedule for Reviewing Vulnerability Assessment

- Identify events or actions involving people, property, products, processes, information, or information systems that could trigger a change in security status or needs (see Management Practice 12, Management of Change)
- Establish a schedule for reviewing the site's security status, based on the potential security risks presented by the facility, in the absence of a review triggering event.

Implementation Resources

Section VI of this document provides policies and other documents that show how companies prioritize and analyze potential security threats, vulnerabilities, and consequences. The samples are intended to stimulate thinking and offer helpful ideas on code implementation. Other approaches not described here may be just as effective or even more effective for a particular company. If a company so chooses, it may adopt any of these sample strategies or may modify them to fit the company's unique situation. The sample resources are described in brief below:

Resource 2-1: ACC Facility Security Prioritization Process

The ACC Facility Security Prioritization Process outlines a method for prioritizing both RMP and other facilities. The process includes links for more information on the Chemical Weapons Convention, FBI materials, and Australia Group activities.

Resource 2-2: CCPS Facility Vulnerability Screening Tool

The Center for Chemical Process Safety (CCPS) Facility Vulnerability Screening Tool tracks the ACC process for RMP facilities, but provides additional assistance for non-RMP facilities. The tool is available from CCPS at www.aiche.org/ccps/.

Resource 2-3: Sandia Vulnerability Assessment Methodology

The Sandia workbook is an Official Use Only (OUO) document and is being distributed to selected organizations and others that have a need-to-know and agree to the terms of the Distribution Agreement. Individuals requesting a copy of the workbook should send an email to cdjaege@sandia.gov and also fax a signed copy of the Distribution Agreement to 505-844-0011. A copy of the agreement is available at http://www.responsiblecaretoolkit.com.

Resource 2-4: CCPS Assessment of Fixed Chemical Sites

The Security Vulnerability Methodology (SVM), "Assessing the Vulnerability of Fixed Chemical Sites," developed by the Center for Chemical Process Safety (CCPS) is available from Scott Berger of CCPS at scotb@aiche.org.

Resource 2-5: CCPS Security Vulnerability Assessment

"Security Vulnerability Assessment Essential Features/Criteria," a publication of the Center for Chemical Process Safety (CCPS), describes the attributes of a layered risk analysis approach to site security vulnerability assessment methodologies.

CCPS will evaluate other security vulnerability assessments against its Security Vulnerability Criteria www.responsiblecaretoolkit.com. Companies wishing to submit their vulnerability assessments to CCPS for evaluation are encouraged to first conduct a self-audit against the CCPS design criteria. Submissions should be made to Scott Berger of CCPS at scotb@aiche.org. CCPS will charge a nominal fee based on the time required to complete the evaluation and to resolve any gaps. The response time will depend on the number of methodologies submitted for evaluation.

Resource 2-6: Security Program Elements and Practices

This segment of *Site Security Guidelines for the U.S. Chemical Industry*, published in October 2001 by the American Chemical Council, the Synthetic Organic Chemical Manufacturers Association, and the Chlorine Institute, outlines typical elements of a good security program and suggests security practices that managers can consider and tailor to their facilities' particular circumstances.

Resource 2-7: Risk Assessment/Risk Management Process

This policy describes one chemical company's risk assessment and risk management process. This methodology meets the requirements of the Center for Chemical Safety (CCPS) and the American Chemistry Council (ACC).

Resource 2-8: Concise Vulnerability Analysis

This chemical company document describes a straightforward, three-step process for analyzing site vulnerability. This methodology meets the requirements of the Center for Chemical Safety (CCPS) and the American Chemistry Council (ACC).

Resource 2-9: Security Vulnerability Assessment

The objective of this Security Vulnerability Assessment (SVA) is to conduct an analysis to identify security hazards, threats, and vulnerabilities facing a fixed facility handling hazardous materials from malicious acts, and to evaluate the countermeasures to ensure the protection of the public, workers, national interests, the environment, and the company. This methodology meets the requirements of the Center for Chemical Safety (CCPS) and the American Chemistry Council (ACC).

3. Implementation of Security Measures

Management Practice 3

Development and implementation of security measures commensurate with risks, and taking into account process design, material substitution, engineering, administrative and process controls, prevention, and mitigation measures.

Companies will take action when they identify and assess potential security risks. This may mean putting additional or different security measures into place to provide greater protections for people, property, products, processes, information, and information systems. At facilities, this can entail measures such as installation of new physical barriers or modified production processes (often referred to as inherently safer approaches). In product sales and distribution, this can entail measures such as new procedures to protect Internet commerce or additional screening of transportation companies.

Anticipated Benefits

Implementing new security measures to address identified vulnerabilities protects people, property, product, and proprietary information. Beneficiaries include employees, the community, suppliers, contractors, shareholders, and many others. Security measures that keep criminals from obtaining hazardous materials benefit even members of the public who live far from a given chemical plant. The benefits of effective implementation of security measures are indeed widespread.

More specifically, developing and implementing security measures helps a company protect employees, the community, and the environment; maintain the integrity of operations; reduce litigation risk, insurance costs, and theft; decrease the risk of vandalism and sabotage by employees and non-employees; safeguard trade secrets; and improve relationships with local authorities and surrounding communities.

Sample Strategies

The following are strategies to consider in developing and implementing security measures:

- Assign responsibility for site security coordination and establish lines of responsibility.
- Perform a site security survey to determine the status of current security measures and the particular physical and procedural conditions in which protection must be provided, including vulnerability created by "natural" perimeters such as rivers or other waterways.
- Develop a comprehensive plan for site security, based on a thorough vulnerability assessment. In the plan, address all relevant categories, among which are perimeter protection (fencing, clear zones), access control (doors, gates, keys, locks), cyber security for process controls, training, drills, surveillance, lighting, signage, alarms, badging,

vehicle and property control, security communications, law enforcement or other emergency response, intrusion detection, security officers and post orders, visitor control, package and mail inspection, investigations, employment termination procedures, and bomb threat procedures.

- Assign responsibility to implement the measures decided upon.
- Establish an implementation schedule and allocate appropriate resources.
- Confirm that measures have been put in place and are working as desired.

Implementation Resources

Section VI of this document provides samples from corporate policies and research publications that illustrate specific ways in which companies have developed and implemented security measures commensurate with risk. The samples are intended to stimulate thinking and offer helpful ideas on code implementation. Other approaches not described here may be just as effective or even more effective for a particular company. If a company so chooses, it may adopt any of these sample strategies or may modify them to fit the company's unique situation. The sample resources are described in brief below:

Resource 3-1: Identification of Security Measures

This chemical company policy names general site security measures and countermeasures.

Resource 3-2: Key Security Plan Elements

This chemical company policy identifies and explains key elements of a security plan, such as a site security coordinator, access control, employee and contractor security, and other elements.

Resource 3-3: Security Handbook

This chemical company handbook defines, in detail, security measures for a site where the level of threat is greater than it was before the terrorist attacks of September 11, 2001.

Resource 3-4: Technical Security Measures

This document from a chemical member company details principles for selecting and implementing security technologies.

Resource 3-5: Principles, Elements, and Best Practices

This chemical company document describes both general principles and specific practices of site security.

Resource 3-6: Requirement for Background Screening

This document clarifies a company's expectation that, to the extent possible, all personnel (including contractors and visitors) will be subject to background screening before being allowed on-site.

4. Information and Cyber Security

Note: This section is still under development. More information will be forthcoming soon through materials being developed in a joint effort with the Chemical Industry Data Information Exchange (CIDX).

Management Practice 4

Recognition that protecting information and information systems is a critical component of a sound security management system.

Companies will apply the security practices identified in this Code to their cyber assets as well as their physical assets. Information networks and systems are as critical to a company's success as its manufacturing and distribution systems. Special consideration should be given to systems that support e-commerce, business management, telecommunications, and process controls. Actions can include additional intrusion detection and access controls for voice and data networks, verification of information security practices applied by digitally connected business partners, and new controls on access to digital process control systems at our facilities.

Anticipated Benefits

Proper security for information and information systems helps protect a site's electronic systems, digital process controls, telecommunications, and management and commerce functions. Information security also helps deprive adversaries of information that might facilitate their actions against the company.

The objective of cyber-security practices is to protect the confidentiality, integrity and availability of information and the safety and operational effectiveness of process controls, as well as to prevent information from being used that could compromise the physical security practices of companies. To be most effective, these controls should address not only technology, but also processes and people.

Sample Strategies

Cyber-security risk assessment, particularly regarding process control system security, should be coordinated with physical security assessment (see Management Practice 2, above). The following are various examples of considerations in evaluating a site's information and process control systems:

- Exercise caution when creating connections between internal networks and the Internet or other company networks; check for potential vulnerability at the "gaps" and "interface points" within and among companies, such as connections between old and newer systems or between different off-the-shelf technologies.

- Strict adherence to access control policies and procedures including usernames and passwords; reset security "keys" provided by vendors with unique keys or passwords for the system.
- Consider whether and, if warranted, how to isolate or compartmentalize higher-risk systems from the rest of the facility or company network.
- Evaluate vulnerability that may be associated with use of open systems, identity authentication, remote access, network management, wireless communications, enterprise systems, and access to process control systems.
- Consider implementing authentication technology commensurate with the risk of information or system exposure, including screening (i.e., background checks) for users with privileged access to critical resources.
- Provide appropriate levels of cyber-security awareness, training and education for those who are authorized to use and maintain information and process control systems.
- Establish an incident reporting and response plan that describes actions to be taken if and when a suspected or actual intrusion takes place.
- Upgrade anti-virus programs regularly.

Implementation Resources

Section VI of this document provides samples from corporate policies and research publications that illustrate specific ways in which companies protect their sites' information and information systems. The samples are intended to stimulate thinking and offer helpful ideas on code implementation. Other approaches not described here may be just as effective or even more effective for a particular company. If a company so chooses, it may adopt any of these sample strategies or may modify them to fit the company's unique situation. The sample resources are described in brief below:

Resource 4-1: U.S. Chemicals Sector Cyber-Security Strategy

Prepared by the Chemicals Sector Cyber-Security Information Sharing Forum and focusing on cyber-security risk management and reduction for information and process control systems. A copy of the draft report (June 2002) is available at http://www.responsiblecaretoolkit.com.

Resource 4-2: Security of Process Control Computer Systems

This chemical company document defines the management systems that must be in place to provide an appropriate level of security, ensure accurate information flow, and establish expectations and accountability for computers and computer networks used for control of manufacturing processes.

5. Documentation

Management Practice 5

Documentation of security management programs, processes, and procedures.

To sustain a consistent and reliable security program over time, companies will document the key elements of their program. Consistency and reliability will translate into a more secure workplace and community.

Documentation may take the form of written expressions of corporate expectations, philosophies, policies, practices, or guidelines.

Anticipated Benefits

Accurate documentation of a company's security programs, processes, and procedures, as well as documentation of compliance with them, provides three key benefits. First, documentation leads to institutionalization of security activities so that security will not falter as security employees leave the company. Documentation helps the program outlast the person who developed the program. Second, documentation of compliance with security measures tends to increase that compliance. Rules are generally followed more closely when someone is looking and keeping records. Third, documentation of security performance, violations, successes, and failures helps security staff determine where various security measures may need to be strengthened.

In addition, complete, accurate documentation of a company security program will position that company for a smooth transition to third-party certification of the company's security program down the road. On June 5, 2002, the ACC Board of Directors approved transition of Responsible Care® as a whole from a system of codes of management practices to a new modern management system (in which the key elements of the codes will be retained). Under this new approach, company Responsible Care® management systems will be certified by approved independent auditors. Documentation is a key aspect of management systems and certification.

At this time, the Security Code is being implemented separately and will not be initially incorporated into the new Responsible Care® management system and certification process. However, under the terms of the Security Code itself, the Code is to be reviewed no later than two years after it was adopted on June 5, 2002. As part of the review, it is expected that the question of whether to integrate Security Code practices within the new Responsible Care® management system and certification process will be evaluated. Documentation of a company's security program should ease any transition of this kind.

Sample Strategies

The following are various strategies that a company can use to document its security management programs, processes, and procedures:

- Issue a directive stating that the company or site will have written security guidelines and clearly assign roles and responsibilities to implement them.
- Develop *general* security guidelines, naming the types of assets that require protection and the general types of protective measures that are deemed appropriate.
- Develop *specific* security guidelines, naming the actual material and procedural requirements, such as fence height, employee badging procedures, visitor accompaniment requirements, lighting specifications, etc.
- Develop guidelines for sites that face varying degrees of threat. For example, write criteria for sites that face a high level of threat, a medium level of threat, and a low level of threat.
- Set a guideline that security incidents must be documented.
- Keep documentation up-to-date so that staff who are not intimately familiar with security operations at the site can keep the program going when more experienced staff leave.
- Assure adequate and appropriate transition and training for new personnel.

Implementation Resources

Section VI of this document provides samples from corporate policies and research publications that illustrate specific ways in which companies have approached the issue of documentation of security programs, processes, and procedures. The samples are intended to stimulate thinking and offer helpful ideas on code implementation. Other approaches not described here may be just as effective or even more effective for a particular company. If a company so chooses, it may adopt any of these sample strategies or may modify them to fit the company's unique situation. The sample resources are described in brief below:

Resource 5-1: Application of Standards

This document expresses a chemical company's commitment to the implementation of security standards.

Resource 5-2: Compact, Unified Security Policy (1)

In one brief document, a chemical company clarifies its policies on access control, pre-employment screening, workplace violence, drug and alcohol abuse, protection of information, weapons on company property, and incident reporting.

Resource 5-3: Compact, Unified Security Policy (2)

This concise policy from a chemical company describes the purposes of security measures, the harms to be prevented, the desirability of designating a site security coordinator, and a number of

specific security measures, such as access control, perimeter protection, after-hours security, backup power systems, and others.

Resource 5-4: Documentation of Specific Security Practice (1)

This policy from a chemical company stresses the importance of documenting security penetration exercises.

Resource 5-5: Documentation of Specific Security Practice (2)

This policy from a chemical company states particular procedures that are to be performed and documented during nightly security checks.

Resource 5-6: Documentation of Security Practices for Low, Medium, and High Threat Sites

This chemical company policy documents expected security practices at sites facing differing threat levels.

6. Training, Drills, and Guidance

Management Practice 6

Training, drills, and guidance for employees, contractors, service providers, value chain partners, and others, as appropriate, to enhance awareness and capability.

As effective security programs evolve, companies will keep pace by enhancing security awareness and capabilities through training, drills, and guidance. This commitment extends beyond employees and contractors to include others, when appropriate, such as product distributors or emergency response agencies. Working together in this fashion improves our ability to deter and detect incidents while strengthening our overall security capability.

Anticipated Benefits

Training, drills, and guidance provide numerous benefits to a security program. Employees and others who receive training may serve as extra eyes and ears for the security program and report or respond to security violations. Joint training may create better working relationships with local emergency responders and law enforcement, and provide responders and law enforcement with the knowledge of your plant site that they may require to serve you in the event of a threat or emergency.

Sample Strategies

The following are various strategies for providing security training, drills, and guidance:

- Ensure that everyone who is assigned specific security responsibilities receives appropriate training, including appropriate responses at a potential crime scene.
- Establish training as a routine, expected practice.
- Consider using both internal and external personnel as trainers to ensure that employees receive the best training and to promote contact with others in the security field.
- In appropriate cases, provide security and emergency response training to community members and employees of other companies.
- Consider joint training with local emergency responders and law enforcement.
- Reinforce training in security practices through e-mailed security reminders, security tips posted on a corporate intranet, advice and contact numbers in local and company-wide internal publications, and the distribution of security-related videos, pamphlets, tent-cards for lunch tables, posters, memos, brochures, and public address announcements.
- Keep records of training provided.
- Develop evaluation criteria to measure the effectiveness of each element of the training program. Review evaluation results to provide feedback to trainers.

- Conduct drills to test effectiveness of preventive measures and response. Use critiques to improve system as appropriate.

Implementation Resources

Section VI of this document provides samples from corporate policies and research publications that illustrate company plans regarding training and drills for employees, contractors, and other on-site visitors for the purpose of enhancing their security awareness and capability. The samples are intended to stimulate thinking and offer helpful ideas on code implementation. Other approaches not described here may be just as effective or even more effective for a particular company. If a company so chooses, it may adopt any of these sample strategies or may modify them to fit the company's unique situation. The sample resources are described in brief below:

Resource 6-1: Emergency Response Training Program

This example from the ACC Community Awareness and Emergency Response Code describes characteristics of training programs to ensure that response plans can be well executed in an emergency.

Resource 6-2: Memo as Security Training Tool

This document from a chemical company shows how a simple memo can serve as a direct training tool.

Resource 6-3: Statement of Training Requirement

This document from a chemical company spells out the company's requirement for annual training, as well as the need for evaluation and documentation.

Resource 6-4: Statement of Drill Requirement

This section of *Security Guidance for the Petroleum Industry* (American Petroleum Institute, 2002) calls for simple but robust drills to practice for security-related events.

Resource 6-5: Developing Security Awareness

This sample from *Site Security Guidelines for the U.S. Chemical Industry*, published in 2001 by the American Chemistry Council, Synthetic Organic Chemical Manufacturers Association, and The Chlorine Institute, Inc., discusses benefits and methods of developing security awareness among employees.

Resource 6-6: Collaborative Training Policy

This chemical company document urges that company security training include instructors from both the company and the law enforcement community.

Resource 6-7: Penetration Exercises

This chemical company document describes various types of penetration exercises to test a site's security, and it offers some guidelines for conducting those exercises safely and effectively.

7. Communications, Dialogue, and Information Exchange

Management Practice 7

Communications, dialogue, and information exchange on appropriate security issues with stakeholders such as employees, contractors, communities, customers, suppliers, service providers, and government agencies balanced with safeguards for sensitive information.

Communication is a key element to improving security. Maintaining open and effective lines of communication includes steps such as sharing effective security practices with others throughout industry and maintaining interaction with law enforcement officials. At the same time, companies understand that their role is to protect employees and communities where they operate, while safeguarding information that would pose a threat in the wrong hands.

Through meetings with representatives of prominent external stakeholder groups, including the executive and legislative branches, nongovernmental organizations, private citizens, academics and think tanks, and representatives of customer organizations, ACC has learned that transparency is the key to our credibility. This was the single most powerful message from all stakeholders.

Anticipated Benefits

Effective security-related communication can provide numerous benefits. For example, employees, contractors, vendors, and others who enter the site will better understand security requirements and therefore may adhere to them more strictly. By becoming better attuned to security concerns, they may also be more likely to recognize and report anomalies.

Building liaison with law enforcement officials and other responders can increase the effectiveness of support when needed. Moreover, once liaisons are established, outside sources are more likely to provide advance notice of threats and security-relevant developments. Further, good communication between chemical plant mangers and emergency responders makes it easier to coordinate incident response in a way that does not cause conflicts between on-site and off-site sources of assistance.

Providing information to the community—including elected officials and neighbors—can foster understanding that will benefit everyone. Voluntary information-sharing reduces tension between communities and companies, opens the door to constructive dialogue, and may lead to improved site security. Communicating openly about a plant's security efforts and concerns and soliciting public involvement can result in more informed decision-making on the part of the plant and the community as a whole.

Sample Strategies

Security-related communication can lead to understanding, compliance, cooperation, and collaboration. It is also a key technique in the prevention and control of security incidents.

The following are various strategies that companies can consider:

- Maximize employee awareness of security issues and procedures to increase employees' role in company security efforts. Employ brochures, posters, the company intranet, meal room tabletop tent cards, briefings, and other measures to convey information to personnel. Establish a variety of means by which employees can report concerns, such as anonymous tip lines, suggestions boxes, a widely promulgated security e-mail address, etc.
- When appropriate, pass threat information to employees so they can increase their personal safety.
- Develop formal and informal liaisons with local, state, and federal law enforcement agencies to improve information-sharing, clarify emergency response, track threat conditions, and support investigations.
- Develop guidelines for communicating with community groups, including elected officials, balancing information needs with security concerns. The public wants to know that facilities are aware of the possible risks, that they are making every reasonable effort to reduce those risks, that they have instituted new safeguards since September 11, and that they have response measures in place in case of attack. Facilities should especially consider communicating the following points:
  - Employees have up-to-date security guidelines and training.
  - Crisis management teams work with local first responders.
  - The company has up-to-date crisis management, response, and evacuation plans.
  - The company employs security personnel.
  - Company-wide security policies or procedures are in place.
  - Criminal background checks are conducted on new hires.
  - Access control mechanisms, perimeter barriers, visitor entry/exit control systems, intrusion alarm systems, and closed-circuit television are in place. (However, do not share the details of the systems.)
  - Packages are searched.

  Site staff should also reinforce the value that the facility and the industry provide to the country and the fight against terrorism, emphasizing these points:
  - The business of chemistry is front and center in our nation's war on terrorism.
  - Our objective is to detect, deter, and respond to terrorism so we can continue to provide essential, life-saving products.
  - The industry is working to ensure an enhanced quality of life for people and their families.

The Security Code recognizes that communications strategies like these must be balanced with the need for safeguards for sensitive information. In many cases, information may be sensitive for security reasons. Sometimes information may also be confidential for business reasons. Such information needs to be protected from improper disclosure in order to protect communities, employees, and the public, as well as the company. Each company on a case-by-case basis must ultimately make decisions on what information is sensitive and whom information should be released to. The need to secure sensitive information should not, however, obscure the simultaneous need for an on-going company communications and dialogue program concerning appropriate information.

Implementation Resources

Section VI of this document provides samples from corporate policies and research publications that illustrate how companies have described the importance of security-related communication, as well as the particular steps they have taken to communicate security information. The samples are intended to stimulate thinking and offer helpful ideas on code implementation. Other approaches not described here may be just as effective or even more effective for a particular company. If a company so chooses, it may adopt any of these sample strategies or may modify them to fit the company's unique situation. The sample resources are described in brief below:

Resource 7-1: Employee Security Awareness (1)

This policy from a chemical company spells out the company's commitment to maintaining employees' security awareness and specifies measures for doing so.

Resource 7-2: Employee Security Awareness (2)

This section of *Site Security Guidelines for the U.S. Chemical Industry*, published by the American Chemistry Council, Synthetic Organic Chemical Manufacturers Association, and The Chlorine Institute, Inc., in October 2001, articulates the importance, benefits, and methods of maintaining employees' security awareness.

Resource 7-3: Law Enforcement Liaison

This chemical company policy identifies expectations for communicating security issues with peers in other companies and with law enforcement and emergency response officials.

Resource 7-4: Public-Private Cooperation (1)

This sample from a chemical company describes a formal program for security liaison with law enforcement officials so that security personnel will be kept up-to-date on developments that affect company security.

Resource 7-5: Public-Private Cooperation (2)

This section of *Site Security Guidelines for the U.S. Chemical Industry*, published by the American Chemistry Council, Synthetic Organic Chemical Manufacturers Association, and The Chlo-

rine Institute, Inc., in October 2001, describes the benefits of establishing partnerships or enhancing relationships with local, state, and federal law enforcement and other public safety agencies.

Resource 7-6: Public-Private Cooperation (3)

This sample from *Operation Cooperation: Guidelines for Partnerships Between Law Enforcement and Private Security Organizations* (Bureau of Justice Assistance, U.S. Department of Justice, 2000) names benefits of public-private cooperation and lists many specific techniques for fostering such cooperation.

Resource 7-7: Public-Private Information Exchange

This standard operating procedure from the Chemical Sector Information Sharing & Analysis Center (Chemical Sector ISAC) and the National Infrastructure Protection Center (NIPC) Information Sharing Program establishes voluntary procedures for implementing the information reporting, analysis, and warning provisions of NIPC's national-level program for the chemical sector.

8. Response to Security Threats

Management Practice 8

Evaluation, response, reporting, and communication of security threats as appropriate.

Companies take physical and cyber security threats very seriously. In the event of such threats, companies will promptly evaluate the situation and respond. Real and credible threats will be reported and communicated to company and law enforcement personnel as appropriate.

ACC, in cooperation with the FBI's National Infrastructure Protection Center (NIPC), has established the Chemical Sector Information Sharing and Analysis Center (ISAC). A primary goal of the Chemical Sector ISAC is to enable NIPC to disseminate timely and actionable assessments, advisories, and alerts to appropriate government and private sector entities when such incidents are deemed to have possible serious national security, economic, or social consequences.

The Chemical Sector ISAC is intended for companies involved in the manufacture, storage, transportation, distribution, or handling of chemical products. Participation by the chemical industry is intended to be inclusive to maximize the value and utility of the ISAC. To learn how to become registered as an ISAC participant, visit http://chemicalisac.chemtrec.com/ChemISACReg2.nsf/RegIE3?openform.

The Chemical Sector ISAC utilizes CHEMTREC, the chemical industry's 24-hour emergency communication center, as the communication link between the NIPC and ISAC participants. When CHEMTREC receives information from the NIPC, that information is immediately transmitted, on an around-the-clock basis, to Chemical Sector ISAC participants via electronic mail and a secure website.

Anticipated Benefits

By collecting threat information, staff may be able to detect and prevent impending security incidents. In addition, analyzing threat information may make it possible to discern trends that can be supported or combated, as appropriate. If staff report and communicate security threats to company employees and other interested parties, more people can be involved in supporting the security effort. Ultimately, a threat could become an incident if not evaluated and acted on immediately. So threat response is critical to a secure company.

Sample Strategies

The following are various strategies for evaluating, responding to, reporting, and communicating security threats:

- Regularly evaluate the number and severity of reported security incidents. Communicate any significant increases or decreases in threat levels to upper and line management.
- Make the security operation a clearinghouse for inquiries on real or rumored reports of security threats.
- Upgrade security measures incrementally as the threat level escalates. Review threat escalation with management and obtain their endorsement to boost security procedures.
- Disseminate pertinent threat information affecting the safety of employees, the operations of the company, and the protection of sensitive information.
- Develop a procedure for reporting suspicious purchases of or inquiries about chemicals or equipment that could be precursors for weapons of mass destruction or that could be used for chemical or biological terrorism.
- Devise and disseminate procedures for responding to bomb threat telephone calls. Establish a decision-making tree regarding whether to search or evacuate the building.
- Devise and disseminate procedures to examine, analyze, and handle suspicious mail and packages.
- To improve response to threats, develop liaison with emergency responders and other appropriate contacts.

Implementation Resources

Section VI of this document provides samples from corporate policies and research publications that illustrate specific ways in which companies respond to security threats. The samples are intended to stimulate thinking and offer helpful ideas on code implementation. Other approaches not described here may be just as effective or even more effective for a particular company. If a company so chooses, it may adopt any of these sample strategies or may modify them to fit the company's unique situation. The sample resources are described in brief below:

Resource 8-1: Incremental Threat Response (1)

This chemical company policy names levels of escalating threat conditions and identifies security responses appropriate for each level.

Resource 8-2: Incremental Threat Response (2)

This chemical company policy provides a different threat level system and identifies security responses appropriate for each level.

Resource 8-3: Response to Bomb Threat

This section of *Site Security Guidelines for the U.S. Chemical Industry*, published by the American Chemistry Council, Synthetic Organic Chemical Manufacturers Association, and The Chlorine Institute, Inc., in October 2001, describes specific measures that companies may wish to take in response to bomb threats received by telephone and mail.

Resource 8-4: Response to Suspicious Mail

This section of *Site Security Guidelines for the U.S. Chemical Industry*, published by the American Chemistry Council, Synthetic Organic Chemical Manufacturers Association, and The Chlorine Institute, Inc., in October 2001, offers considerations for dealing with letters and packages that might contain bombs or hazardous chemical or biological materials.

Resource 8-5: Reporting of Suspicious Purchases and Inquiries

This document from the FBI Community Outreach Program for Manufacturers and Suppliers of Chemical and Biological Agents, Materials, and Equipment is designed to help companies identify and report suspicious purchases of or inquiries about chemical, biological, nuclear, or radiological materials and equipment.

Resource 8-6: Threat Collection, Analysis, and Dissemination (1)

This chemical company document describes measures and responsibilities for responding to security threats.

Resource 8-7: Threat Collection, Analysis, and Dissemination (2)

This chemical company document emphasizes techniques for disseminating threat information to employees.

9. Response to Security Incidents

Management Practice 9

Evaluation, response, investigation, reporting, communication, and corrective action for security incidents.

Companies will be vigilant in efforts to deter and detect any security incident. If an incident should occur, however, companies will respond promptly and involve government agencies as appropriate. After investigating the incident, the company will incorporate key findings and will, as appropriate, share those findings with others in industry and government agencies and implement corrective actions.

ACC, in cooperation with the FBI's National Infrastructure Protection Center (NIPC), has established the Chemical Sector Information Sharing and Analysis Center (ISAC). A primary goal of the Chemical Sector ISAC is to enable NIPC to disseminate timely and actionable assessments, advisories, and alerts to appropriate government and private sector entities when such incidents are deemed to have possible serious national security, economic, or social consequences.

The Chemical Sector ISAC is intended for companies involved in the manufacture, storage, transportation, distribution, or handling of chemical products. Participation by the chemical industry is intended to be inclusive to maximize the value and utility of the ISAC. To learn how to become registered as an ISAC participant, visit http://chemicalisac.chemtrec.com/ChemISACReg2.nsf/RegIE3?openform.

The Chemical Sector ISAC utilizes CHEMTREC, the chemical industry's 24-hour emergency communication center, as the communication link between the NIPC and ISAC participants. When CHEMTREC receives information from the NIPC, that information is immediately transmitted, on an around-the-clock basis, to Chemical Sector ISAC participants via electronic mail and a secure website.

Anticipated Benefits

The way a company responds to a security incident can reduce the incident's impact on the company, as well as the likelihood of future, similar incidents. The right response (especially in terms of investigation and corrective action) can minimize losses and prevent future incidents. The way a company responds to an incident can reduce the incident's impact on the company and it's employees and neighbors.

Sample Strategies

The following are various strategies for evaluating, responding to, investigating, reporting, and communicating security incidents:

- Develop a process for immediate reporting of security incidents. Provide employees with examples of reportable incidents so they can better comply with reporting requirements.
- Study security incident records to look for patterns of loss and to identify issues of security concern. Some companies may wish to use incident management software as a tool in that process.
- Develop a process for investigating incidents. Consider using a multidisciplinary team to conduct the investigation. Determine a threshold of seriousness below which incidents are not investigated but simply recorded for trend analysis. Refer incidents to counsel or security management for investigation authorization. Ensure that trained professionals conduct investigations. Report any suspected illegal activity to law enforcement, if appropriate.
- Keep in mind that it may be necessary to respond differently to a security incident than to an accident. At the scene of a security incident, it is important to respond in a way that preserves evidence of a possible crime. These are some possible evidence-preserving steps: avoid cleaning the scene of the crime; keep all witnesses and victims on-site, and separate them all so they cannot talk to each other about the incident; ask medical responders not to contaminate or spoil possible evidence (for example, by cutting through bullet holes when cutting victims' clothes away, or by throwing those clothes away); and make note of all vehicles, people, objects, smells, sounds, etc. It may be helpful to contact the local law enforcement agency or nearest FBI office for guidance in advance.
- Consider classifying incidents based on the potential outcome instead of the actual outcome. The level of investigation may need to be upgraded depending on the potential seriousness of the incident.
- Review final incident investigation reports with all personnel whose job tasks are relevant to the incident findings, including contract employees where applicable.
- Keep final incident investigation reports on file for at least five years.
- Develop a crisis management plan that addresses, at a minimum, response to the crisis, coordination with the corporate crisis management team, and public relations, political, and security considerations. Establish a crisis operations center for managing security incidents that rise to the level of crises.
- Keep in mind that smaller sites, especially those without security officers, should not respond in person to potentially dangerous situations but instead should immediately contact law enforcement.
- Develop a mechanism to ensure that corrective measures are taken after a security incident.

Implementation Resources

Section VI of this document provides samples from corporate policies and research publications that illustrate ways in which companies respond to security incidents. The samples are intended to stimulate thinking and offer helpful ideas on code implementation. Other approaches not described here may be just as effective or even more effective for a particular company. If a com-

pany so chooses, it may adopt any of these sample strategies or may modify them to fit the company's unique situation. The sample resources are described in brief below:

Resource 9-1: Examples of Reportable Irregularities

This chemical company document names types of irregularities and incidents that must be reported.

Resource 9-2: Security Incident Reporting and Response Policy

This chemical company policy defines the management systems that must be in place to ensure that, following an incident, appropriate notification, classification, investigation, reporting, and recommendations are completed.

Resource 9-3: Security Incident Reporting and Analysis

This section of *Site Security Guidelines for the U.S. Chemical Industry*, published by the American Chemistry Council, Synthetic Organic Chemical Manufacturers Association, and The Chlorine Institute, Inc., in October 2001, discusses techniques for and advantages of collecting and analyzing data on security incidents.

Resource 9-4: Irregularity Response Table

This chemical company document names categories of irregularities or security incidents and specifies the sequence of response actions that should follow.

Resource 9-5: Investigation Guidelines (1)

This section of *Site Security Guidelines for the U.S. Chemical Industry*, published by the American Chemistry Council, Synthetic Organic Chemical Manufacturers Association, and The Chlorine Institute, Inc., in October 2001, names types of security incidents that might warrant formal investigation and possible referral to law enforcement.

Resource 9-6: Investigation Guidelines (2)

This chemical company guideline names procedures for initiating and conducting investigations of security incidents.

Resource 9-7: Crisis Management Guidelines

This chemical company document states corporate expectations regarding the development of a crisis management team, crisis operation center, and crisis management plan. It also specifies some of the responsibilities of participants.

10. Audits

Management Practice 10

Audits to assess security programs and processes and implementation of corrective actions.

Companies will periodically assess their security programs and processes to ensure that those programs and processes are in place and working. If the assessments identify opportunities for improvement, the company will promptly take corrective action. Based on risk, it may also be appropriate to assess the programs and processes of other companies with which the company conducts business, such as chemical suppliers, transportation service providers, or customers.

Anticipated Benefits

Security policies, procedures, and technologies must be operational in order to succeed. An audit provides managers who have security responsibilities with a tool for assessing, in detail, whether those measures are implemented and functioning. Identifying measures that need corrective action—and then following through to ensure that the corrections are completed—makes it possible for a security program to meet its full potential.

Sample Strategies

The following are various strategies for auditing security programs, processes, and corrective actions:

- Establish a policy of conducting regular security audits to ensure proper deployment, identify weaknesses, incorporate lessons learned, and develop corrective actions.
- Develop a detailed, holistic audit checklist or protocol that covers all key aspects of security, including physical security measures, procedures, documentation (such as security policies and threat or incident reports), cyber security, product stewardship considerations, and management/supervision practices.
- Consult with legal team in the development of audit program.
- Review the previous security audit to identify prior issues of concern. Also, determine whether corrective actions named in the last report or identified through third-party input or inspections have been completed.
- Conduct personal interviews, make observations at the site, test the functioning of security equipment, and examine documentation.
- Record the specific steps taken in the audit, such as persons interviewed (name and position), equipment tested, and documents reviewed.
- Review the audit's preliminary conclusions with the appropriate facility contacts to ensure accuracy.

- Produce a final audit report that clearly specifies issues that require corrective action.

Implementation Resources

Section VI of this document provides samples from corporate policies and research publications that illustrate specific ways in which companies have approached the issue of auditing security programs and processes. The samples are intended to stimulate thinking and offer helpful ideas on code implementation. Other approaches not described here may be just as effective or even more effective for a particular company. If a company so chooses, it may adopt any of these sample strategies or may modify them to fit the company's unique situation. The sample resources are described in brief below:

Resource 10-1: General Policy on Security Self-Assessments

This chemical company policy states the expectation that security self-assessments will be conducted to ensure that security systems and programs meet company expectations.

Resource 10-2: Specific Policy on Security Program Reviews

This chemical company policy names nine security topics that should be reviewed to ensure proper functioning. The topics are as follows: guard force, access procedures, search procedures, badge management, restricted access, perimeter, emergency procedures, information security, and personnel protection.

Resource 10-3: Security Management Benchmark/Audit Protocol

This extensive chemical company protocol shows a detailed method of auditing company security procedures.

Resource 10-4: Baseline Audit Questions

This section of *Security Guidance for the Petroleum Industry* (American Petroleum Institute, 2002) provides a list of basic questions that could be used as a starting point in developing a company-specific audit program.

Resource 10-5: Asset-Based Vulnerability Checklist

This checklist identifies key components of a site that should be examined in an audit. For example, it names the perimeter, entry-access control, surveillance, vehicles and materials delivery management, and hazardous material control.

Resource 10-6: Audit Checklist

This section of *Site Security Guidelines for the U.S. Chemical Industry*, published by the American Chemistry Council, Synthetic Organic Chemical Manufacturers Association, and The Chlorine Institute, Inc., in October 2001, provides an example of a detailed audit checklist covering risk assessment and prevention strategies; management issues; physical security; employee and contractor security; and information, computer, and network security.

Resource 10-7: Criteria for Stages Leading to Excellence

This chemical company document outlines a six-step process of continuous improvement, leading to a comprehensive, effective security program.

11. Third-Party Verification

Management Practice 11

Third-party verification that, at chemical operating facilities with potential off-site impacts, companies have implemented the physical site security measures to which they have committed.

Chemical industry security starts at our facilities. Companies will analyze their site security, identify any necessary security measures, implement those measures, and audit themselves against those measures. To help assure the public that our facilities are secure, the companies will invite credible third parties—such as firefighters, law enforcement officials, insurance auditors, and/or federal or state government officials—to confirm that the companies have implemented the enhanced physical security measures that they have committed to implement. In addition, companies should consult with these same parties as enhanced physical security measures are being considered and implemented.

Anticipated Benefits

Independent third-party verification that a company has implemented physical site security enhancements that it committed to implement as an outgrowth of its security vulnerability assessment provides a number of anticipated benefits, including:

- Both plant employees and the plant community will be further reassured that the company has taken important precautionary steps to appropriately secure the site.
- The partnership between plants and local first responders or other government security agencies, where they are used as verifiers, will be strengthened. For example, plants will better understand the capabilities of the local responders they are relying on and may receive valuable advice as well. Similarly, the local responders will better understand the needs of the plant and demands that may be placed on them in the event of a threat or incident.
- If an incident occurs, partnerships with local responders or other law enforcement and/or security agencies may be helpful in follow-up communications with government and the public.
- Independent third-party verification enhances stakeholder confidence in the integrity of the facility's security program and builds industry credibility relating to security. In industry meetings with stakeholders during the development of the Security Code, stakeholders consistently indicated that third-party verification would be an important element to the credibility of any security management system.

Sample Strategies

Given that independent third-party verification is a tool being used for the first time in a Responsible Care® Code, it is important to understand what the Code does and does *not* require of companies and how verification may be accomplished.

- Identify verifiers that will be seen as independent and credible to employees, neighbors and other facility stakeholders.
- Determine key points at which to engage verifiers in the facility's security assessment process. Facilities are encouraged to bring verifiers into the process as early a practicable.
- Solicit recommendations from verifiers for improving the facility's security assessment process.
- Assure verifiers view physical security enhancements implemented as a result of the facility's security vulnerability assessment.
- Document that verification has occurred using format appropriate to site/company.

What is to be Verified?

Under the Security Code, verification must be conducted on a one-time basis at company chemical operating facilities with potential off-site impacts. This includes sites that have been prioritized as being in either Tier 1, 2 or 3 due to the potential for uncontrolled releases, theft of material, or product contamination. Sales and administrative offices will typically not fall within this scope, though administrative offices would fall into the scope if the company is using a distributed control system.

In the verification process, verifiers are to confirm that the *physical* site security enhancements (e.g., fences, cameras, gates) a company determined were advisable during the vulnerability assessment stage have in fact been implemented. Facilities may also request verification of *physical* security process changes, such as badge display or visitor escort provisions, locks/master key control or vehicle control systems, or package search processes.

Verification of such physical site security enhancements will allow for credible, visible verifications, avoid jeopardizing confidential process information, and allow a broader range of verifiers to constructively participate. The Code does not contemplate verifiers independently assessing which site security measures or enhancements could or should be implemented, but rather, that those physical security enhancements selected through the facility's security assessment and evaluation are in place.

In addition, under the Security Code, *non*-physical site security enhancements, such as manufacturing process modifications, are *not* subject to verification, given the complexity of these types of changes, the expertise required to verify them, the difficulty of doing so, and the potential strategic business sensitivity of the information. For these reasons, in industry stakeholder meetings during the Security Code development process, there was generally agreement that the verification process could be confined to physical enhancements. For similar reasons, *non-site* secu-

rity enhancements, such as value chain and cyber security measures, also do *not* have to be verified. Under Security Code Practice 10, companies will conduct internal self-audits of these and other security systems.

Who Can Verify?

Companies may use any independent third party they believe will be *credible* in the eyes of their plant community and other important company stakeholders. Determination of who will be considered "credible" at a given facility is a company decision. Based on corporate and facility-specific factors companies may select verifiers on a company-wide or plant-by-plant basis. Factors to consider when determining credibility of a potential verifier can include:

- Expertise (e.g., security, law enforcement, emergency response)
- Affiliation (e.g., local government, well regarded security consulting firm)
- Experience, education and accreditation (especially important in the case of private verifiers such as security consultants)
- Reputation (e.g., does the plant community consider the person reputable and reliable)
- Independence (companies should be *very cautious* about using as a verifier someone who is being reimbursed for other non-verification services, such as consulting services; the financial aspect of the other relationship may create a question about the independence of the verification no matter how diligent the process)
- Ability to maintain the confidentiality of sensitive security and business information.

Persons companies may want to consider as verifiers include:

- Local first responders (e.g., fire fighters, law enforcement)
- State emergency planners
- Other security-related government agency personnel
- Security consultants
- Insurance company auditors

Based on meetings with industry stakeholder during development of the Security Code, each of these categories of verifiers was viewed as potentially credible depending on specific circumstances. Companies could also consider bringing in a group of verifiers made up of persons from more than one of these groups. Members of the public may further bolster the credibility of the verification process. If considering public participation, community advisory panels may be a resource to draw upon. However, in each case, companies must consider both the credibility of the potential verifier and the ability of the potential verifier to maintain confidentiality of any sensitive security or corporate business information made available in the course of the verification process.

When Does Verification Happen and How is it Reported?

Companies are encouraged to have the verification of physical site security enhancements completed as soon as possible and *must* have the verification completed no later than *three months* after the enhancements are to be in place for each tier. *See* schedule for site security assess-

ments, enhancement implementation, and verification found in Section III of this guidance, Implementing the Code in Your Company. Thus, companies will need to arrange for verification early enough in the process to meet this schedule.

In addition, under the Code, companies are *strongly* encouraged to consult with the verifiers as enhanced physical site security measures are being considered and implemented, rather than for the first time when the verification is actually conducted. "Consultation" could include, for example, information exchange with the verifiers when a company reviews the steps it will take leading up to verification and provides the verifier an opportunity to dialogue with the company. Consultation does *not* envision verifiers independently assessing site security or enhancement options, or decision-making authority or review. It does envision active regular dialogue, which should help the quality of the entire process, help assure the availability of a verifier at the end of the process, and respond to industry stakeholders.

The Code envisions verification on a *one-time* basis for each of the tiers of sites with potential off-site impacts such as uncontrolled releases, theft of materials or product contamination (Tiers 1, 2 and 3). Future site security enhancements are not subject to verification under the Code.[*]

Finally, the Code does *not* require that verifiers sign any documents or complete any special forms attesting to the fact of the verification. Rather, the Code requires, under Code Practice 5 ("Documentation"), that companies themselves document the fact of verification with enough detail to satisfy the company that it can attest to who conducted the verification, when it was conducted, and the general conclusions reached. Of course, companies may, if they deem it appropriate in their unique circumstances, choose for verifiers to attest to verification in writing or to complete more extensive written company documentation. However, the Code does not require this.

Implementation Resources

Given that independent third-party verification is a new concept for a Responsible Care® code, there are currently no company or industry implementation resources that have emerged. They will be added to this material as they become available.

[*] Longer term company security systems may become subject to the third-party *certification* process that will apply to company Responsible Care® management systems beginning in 2005. Extension of third-party certification to the Security Code process will be assessed in the review of the Security Code required by the Code itself within two years of its adoption (June 5, 2002).

12. Management of Change

Management Practice 12

Evaluation and management of security issues associated with changes involving people, property, products, processes, information, or information systems.

Our employees and our processes contribute to, and rely upon, changes and innovations in products and technologies. As any changes are considered, our companies will evaluate and address related security issues which may arise. This can include changes ranging from new personnel assignments to installation of new process equipment or computer software or hardware.

Managing security is not a one-time process. A security management program involves a continuous cycle of monitoring conditions, identifying and assessing risks, and taking action to minimize the most significant risks.

The conditions surrounding a security effort change constantly. Employees come and go, a facility's contents and layout may change, various threats wax and wane, and plant operations may vary. Even such mundane changes as significant growth of bushes or trees around a facility's exterior may affect the security plan (for example, by providing cover for intruders).

In addition, to be effective in a security leadership role, a manager must be proactive and be able to plan for and manage risk. Knowledge of whether and when the risks may change is critical.

This management practice overlaps somewhat with Management Practice 8, Response to Security Threats. The distinction between the two is that this management practice focuses more on internal changes that could lead to revision of a site's vulnerability assessment, while the other management practice emphasizes external changes that require an immediate response.

Anticipated Benefits

Awareness of impending changes to plant conditions provides managers who are responsible for security with the opportunity to predict security implications and adjust security measures before problems arise. Security's greatest success comes in preventing, not reacting to, undesirable acts and conditions. Forwarding-looking management of change is a powerful tool in the prevention of security incidents.

Sample Strategies

The following are various strategies that companies can consider adopting in their efforts to keep security measures up-to-date with changing conditions:

1. Continuously determine the level of threat as conditions change, and adjust security measures accordingly.

- Establish a process to ensure that security staff is informed at the earliest opportunity of changes to operations and processes. Make security staff responsible for seeking out such information, and make other company managers responsible for providing it.
- Look for existing change-management systems at the site, and modify them to take account of security.

2. Learn of, and respond to, changes that may affect a plant's security requirements.

Changes in Operations

- Planning or execution of a new project
- Any significant change in a facility or operation (such as a change in production quantities or methods, product type, shipping method, supplier, etc.)
- Contractor or vendor changes that might have security implications (such as theft of equipment or tools)
- New computer software or hardware
- Technological changes
- Contemplated purchase, lease, or rental of a manufacturing site or office space
- Contemplated corporate acquisition
- Upcoming purchase of valuable, hazardous, or unfamiliar equipment
- Security-relevant personnel issues, such as hirings, transfers, suspensions, terminations, labor unrest, or employees exhibiting unusual behavior
- Strikes
- Restarting equipment or systems that have been out of service for an extended time or that have not been maintained
- Changes to existing procedures or addition of new procedures

Changes in the Criminal Threat

- Any serious security incident
- Identification of new threat scenarios not originally identified by risk assessment teams
- Gradual increase or decrease in the general threat level from a variety of causes
- Incidents of terrorism or other criminal activity
- Industrial and state-sponsored espionage
- Conflict of interest or misappropriation of funds
- Threat of kidnapping

Changes in the External Environment

- Changes in the threat condition for the site's geographic area, as determined by the Office of Homeland Security.
- Changes in the environment of the plant (for example, foliage growth, population growth, building development)
- New standards, regulatory mandates, or laws
- Political or community changes
- Upcoming protest demonstrations or other events that would potentially results in crowds around the facility (e.g., parades, races)
- Possibility of civil unrest
- Changes in the competency, efficiency, and responsiveness of local police, fire, and medical facilities
- Changes in land use near the plant

Implementation Resources

Section VI of this document provides samples from corporate policies and research publications that illustrate specific ways in which companies anticipate and manage the effects of change on site security. The samples are intended to stimulate thinking and offer helpful ideas on code implementation. Other approaches not described here may be just as effective or even more effective for a particular company. If a company so chooses, it may adopt any of these sample strategies or may modify them to fit the company's unique situation. The sample resources are described in brief below:

Resource 12-1: Notification of Change

This chemical company document calls for a process to ensure that staff is notified of changes that may have security implications. It assigns responsibility for notification, management, verification, measurement, and feedback.

Resource 12-2: Updating Risk Assessments

This chemical company document names events that should trigger the updating of the company risk assessment and provides a "risk assessment short form" for conducting those updates.

Resource 12-3: Assessing New Sites

This chemical company document states that a security assessment should be conducted before the purchase, lease, or rental of a manufacturing site or office space.

Resource 12-4: Change Management Cycle

This section of *Security Guidance for the Petroleum Industry* (American Petroleum Institute, 2002) calls for a systematic process to ensure that changes to a facility or its operations are

evaluated for their potential risk impacts prior to implementation, and to ensure that changes in the environment in which the facility operates are evaluated.

Resource 12-5: Tracking Change (1)

This chemical company document describes the monitoring and evaluation of external changes (in terms of potential security impact) as a stage that leads to excellence.

Resource 12-6: Tracking Change (2)

This section of *Site Security Guidelines for the U.S. Chemical Industry*, published by the American Chemistry Council, Synthetic Organic Chemical Manufacturers Association, and The Chlorine Institute, Inc., in October 2001, identifies several types of events that could lead to the need for security changes. It also states several potentially useful responses to change.

13. Continuous Improvement

Management Practice 13

Continuous performance improvement processes entailing planning, establishment of goals and objectives, monitoring of progress and performance, analysis of trends, and development and implementation of corrective actions.

Our industry commitment to security calls for companies to seek continuous improvement in all of our security processes. That means companies continually will be tracking, measuring, and improving security efforts to keep people, property, products, processes, information, and information systems more secure.

Anticipated Benefits

A formal process of continuous improvement can help a company maintain its security effort at the highest level. By constantly tracking, measuring, and testing security measures, a company can identify gaps and make improvements before incidents occur.

Sample Strategies

The following are various strategies for ensuring continuous performance improvement:

- Employ a continuous improvement process that follows the sequence "Plan, Do, Check, Act."
- Monitor internal and external security-relevant conditions and trends.
- Develop a sense of employee ownership of site security. Employee security training and drills can help create such ownership.
- Provide a confidential system for employees to report security issues.
- Train security personnel and other site personnel to identify and control potential threats and breaches of security.
- Encourage employees to help visitors and contractors comply with identification requirements.
- Review prevention measures and countermeasures needed to address the identified threats:
  - Identify existing systems and determine whether discrepancies or gaps exist.
  - Develop and implement an improvement plan.
  - Periodically review the security plan.
- Periodically conduct penetration exercises.

- Gather, update, and review security data and revise the site security plan accordingly.
- Use the security program evaluation to answer the following questions:
  - Did you do what you said you were going to do?
  - Was what you did effective in addressing security issues?
- Conduct internal comparisons (current performance versus past performance) in order to analyze trends.
- Conduct external comparisons through benchmarking against other similar sites.
- Ensure that all requirements of the Responsible Care® Security Code have been met.

Implementation Resources

Section VI of this document provides samples from corporate policies and research publications that illustrate specific ways in which companies have worked toward continuous improvement. The samples are intended to stimulate thinking and offer helpful ideas on code implementation. Other approaches not described here may be just as effective or even more effective for a particular company. If a company so chooses, it may adopt any of these sample strategies or may modify them to fit the company's unique situation. The sample resources are described in brief below:

Resource 13-1: Continuous Improvement Cycle

This chemical company document illustrates a four-part continuous improvement cycle that calls on employees to plan, do, check, and act.

Resource 13-2: Gap Analysis and Improvement Plan

This chemical company document describes a four-step process for ongoing identification of gaps in site security measures.

Resource 13-3: Security Program Reviews

This chemical company document describes the benefits of penetration exercises and offers advice for safe, effective testing of a site's security measures.

Resource 13-4: Prioritizing Audit Findings for Continuous Improvement

This chemical company document presents a table for prioritizing the findings of a security audit as part of a continuous improvement process.

Resource 13-5: Program Evaluation

This section of *Security Guidance for the Petroleum Industry* (American Petroleum Institute, 2002) describes a system of ongoing security program evaluation.

V. References

Publications

Asset-Based Vulnerability Checklist for Wastewater Utilities. Washington: Association of Metropolitan Sewerage Agencies, 2002.

Counterterrorism and Contingency Planning Guide. Special publication from *Security Management* magazine and American Society for Industrial Security, 2001.

Dalton, Dennis. *Security Management: Business Strategies for Success.* Newton, MA: Butterworth-Heinemann Publishing, 1995.

Fennelly, Lawrence. *Handbook of Loss Prevention and Crime Prevention (3d)*. Newton, MA: Butterworth-Heinemann Publishing, 1996.

Fischer, R., and G. Green. *Introduction to Security (5th).* Stoneham, MA: Butterworth-Heinemann Publishing, 1992.

Guidance for Protecting Building Environments from Airborne Chemical, Biological, or Radiological Attacks. Washington: Department of Health and Human Services and National Institute for Occupational Safety and Health, 2002. Publication 2002-139. Also available at www.cdc.gov/niosh.

Gundry, Craig S. *Chemical Plant Bomb Threat Planning Handbook.* Clearwater, FL: Critical Intervention Services, Inc., 2002.

Jones, Radford W. *Critical Incident Protocol: A Public and Private Partnership*. Michigan State University: 2000.

Moritz, Milton E., ed. *CPP Study Guide, Revised 10th Edition*. Alexandria, VA: American Society for Industrial Security. As preparation for Certified Protection Professional exam, this book covers emergency planning, investigations, legal aspects, personal and physical security, protection of sensitive information, management, substance abuse, loss prevention, and liaison with law enforcement.

Operation Cooperation: Guidelines for Partnerships Between Law Enforcement and Private Security Organizations. Operation Cooperation is a national initiative to encourage partnerships between law enforcement and private security professionals. Its details are explained in a booklet and video, produced in 2000, available from the Bureau of Justice Assistance of the U.S. Department of Justice (www.ojp.usdoj.gov/bja). The booklet is available on-line at www.asisonline.org/opcoop.pdf.

Security Guidance for the Petroleum Industry. Washington: American Petroleum Institute, 2002.

Security Vulnerability Methodology. New York: Council for Chemical Process Safety, 2002.

Site Security Guidelines for the U.S. Chemical Industry. Arlington, VA: American Chemistry Council, Synthetic Organic Chemical Manufacturers Association, and The Chlorine Institute, Inc., 2001.

U.S. Chemicals Sector Cyber-Security Strategy: Reducing the Risks to Our Society and Economy by Leveraging Technology, Processes and people to Protect Chemicals Sector Cyber-Security (June 2002 Draft). Chemicals Sector Cyber-Security Information Sharing Forum.

Vulnerability Assessment Methodology. Albuquerque, NM: Sandia National Laboratories, 2002.

Vulnerability Assessment Methodology. Washington: Synthetic Organic Chemical Manufacturers Association, 2002.

Walsh, Timothy J., and Richard J. Healy, eds. *Protection of Assets Manual.* Santa Monica, CA: Merritt Co. Four-volume loose-leaf reference manual, updated monthly.

Organizations

American Chemistry Council, 1300 Wilson Blvd., Arlington, VA 22209. Telephone: (703) 741-5000. Fax: (703) 741-6000. www.americanchemistry.com.

American Society for Industrial Security, 1625 Prince Street, Alexandria, VA 22314-2818. Telephone: (703) 519-6200. Fax: (703) 519-6299. www.asisonline.org.

Center for Chemical Process Safety, 3 Park Avenue, New York, NY 10016-5991. Telephone: (212) 591-7319. Fax: (212) 591-8895. www.aiche.org/ccps.

International Security Management Association, P.O. Box 623, Buffalo, IA 52728. Telephone: (800) 368-1894. Fax: (800) 568-1894. www.ismanet.com.

Sandia National Laboratories, New Mexico, PO Box 5800, Albuquerque, NM 87185. Telephone: (505) 284-5200. www.sandia.gov.

Synthetic Organic Chemical Manufacturers Association, 1850 M St., N.W., Suite 700, Washington, DC 20036. Telephone: (202) 721-4100. Fax: (202) 296-8120. www.socma.com.

VI. Implementation Resources

The resources that follow are samples from chemical company policies, procedures, and other documents, as well as from research papers and other sources. The chemical companies that provided written matter are not named herein. However, other sources are identified.

1. Leadership Commitment

Management Practice 1

Senior leadership commitment to continuous improvement through published policies, provision of sufficient and qualified resources, and established accountability.

The chemical industry's commitment to security starts at the top. This element calls for each company's leadership to demonstrate through words and actions a clear commitment to security within their company, from corporate headquarters to our facilities.

The following samples are intended to stimulate thinking and offer helpful ideas on code implementation. Other approaches not described here may be just as effective or even more effective for a particular company. If a company so chooses, it may adopt any of these sample strategies or may modify them to fit the company's unique situation.

Resource 1-1: Management Approval

Senior management must approve the conduct and scope of the risk assessment. This will ensure cooperation at management levels and enhance the quality of information received by the assessment teams.

Resource 1-2: Management Participation in Risk Assessment

The director of corporate security, in consultation with corporate officers and outside sources, will conduct a threat assessment of risk factors (such as political climate, possibility of civil unrest, terrorism, strikes, criminal activity, extortion, industrial or state-sponsored espionage, or kidnapping) at the proposed site. The data will be included as the basis for the physical and operational requirements of the plant.

Resource 1-3: Security as a Core Company Value

Source: *Site Security Guidelines for the U.S. Chemical Industry* (Arlington, VA: American Chemistry Council, Synthetic Organic Chemical Manufacturers Association, and The Chlorine Institute, Inc., 2001).

A security effort works best when employees see it as an important part of the company's mission. Employees are more likely to see security as a company priority if the company's top management visibly supports security efforts. Among the best ways to demonstrate that support are to include security as one of the company's core values and to promulgate official company policies regarding security. Security policies can be established on the site level or a company-wide level, and they can address a wide range of topics.

2. Analysis of Threats, Vulnerabilities, and Consequences

Management Practice 2

Prioritization and periodic analysis of potential security threats, vulnerabilities, and consequences using accepted methodologies.

Using generally accepted tools and methods, companies will conduct analyses to identify how to further enhance security. This process will be applied at chemical operating facilities using methods developed by Sandia National Laboratories, the Center for Chemical Process Safety, or other equivalent methods. Companies also will be using tools to analyze the security of product sales, distribution, and cyber security. These initial analyses will be conducted on an aggressive schedule, then conducted periodically thereafter.

Implementation Resources

The following samples show methods for prioritizing facilities and analyzing threats, vulnerabilities, and consequences. They are intended to stimulate thinking and offer helpful ideas on code implementation. Other approaches not described here may be just as effective or even more effective for a particular company. If a company so chooses, it may adopt any of these sample strategies or may modify them to fit the company's unique situation.

Resource 2-1: ACC Facility Security Prioritization Process

Source: American Chemistry Council.

Prioritization consists of three steps: (1) prioritize RMP facilities with program 2 or 3 processes into three tiers; (2) report back to ACC that initial prioritization is completed; and (3) evaluate Tier 4 (non-RMP) facilities for possible elevation to a higher tier.

Scope—Definition of "Facility"

For the purpose of this prioritization, "facility" means domestic, U.S. sites at which operations occur that involve chemicals, e.g., manufacturing, storage, processing, handling, laboratories, or pilot plants.

This prioritization does not apply to non-chemical activity sites such as administrative or sales offices, nor does it apply to transportation sites outside operating facilities. Depending on specific situations, companies may also want to consider evaluating security at sites other than chemical operations, e.g., corporate headquarters.

Step 1—Conduct Security Prioritization on RMP Facilities with Program 2 or 3 Processes

Evaluate RMP facilities with program 2 or 3 processes based on (1) relative difficulty of attack, (2) relative severity of attack, and (3) attractiveness of target. The information needed to perform such an evaluation should be available in the facility's risk management plan (RMP).

The security "worst case" scenario for each RMP process will be rated on a scale of 1-4 for each of the three factors: difficulty (D), severity (S), and attractiveness (A). The three factors are added together to determine the Security Risk Index (SRI) for the process. The overall facility SRI is the highest of the SRIs calculated for each RMP process. Facilities will be assigned to Tiers 1-3 based on the facility's overall SRI.

Since this prioritization process is used primarily for determining the order for performing site vulnerability assessments, it would be acceptable to calculate the SRI for only the single hypothetical "worst case" from a successful terrorist attack for each site. However, since an analysis of each RMP scenario is likely to be needed during the subsequent assessment, it is recommended that sites consider each case during the prioritization process.

Instructions for estimating difficulty, severity, and attractiveness follow.

1. Relative Difficulty of Attack (D)

	Description and factors which influence the likelihood of attack	**Examples**
1	The scenario could be caused by a successful attack, which would require a well-planned and coordinated series of events involving several individuals with special knowledge/training and breaching several independent security levels of protection.	Hijacking a commercial aircraft; organized paramilitary attack within a facility, etc.
2	The scenario could be caused by a successful attack, which could be accomplished by a small group of individuals with equipment or materials available to organized terrorist organizations (or an insider with special knowledge of the facility), and **does** require access to restricted access areas.	Use of explosive materials within the plant boundaries; breach of facility perimeter barrier; use of control system to override protective layers via access to process control system.
3	The scenario could be caused by a successful attack, which could be accomplished by a small group of individuals with equipment or materials available to organized terrorist organizations, but **does not** require access to restricted access areas.	Use of explosives materials from outside the plant boundaries; disgruntled employee with access to small-sized explosives.
4	The scenario could be caused by a successful attack accomplished by a single individual with readily available equipment or materials	The creation of a reactive chemicals incident via connection of a water hose; rifle shot from outside of fence line.

2. Relative Severity of Attack (S)

Severity of attack will be estimated by the population density within the radius of the attack utilizing methods required by EPA for RMP "worst case" or "alternative case" scenario submittal requirements.

	Toxic Scenarios	**Flammable Scenarios**
1	Up to 1,000	Up to 100
2	1,000 to 10,000	100 to 1,000
3	10,000 to 100,000	1,000 to 10,000
4	100,000 or greater	10,000 or greater

3. Attractiveness of Target (A)

	Description and factors which influence the attractiveness of target to terrorists
1	A successful attack is unlikely to cause disruption to local economy or local infrastructure. Therefore, an attack is unlikely to create more than limited localized concern or attention.
2	A successful attack could cause local evacuations, disruption to local economy, or disruption of local infrastructure. Such an attack would create primarily local concern and attention.
3	A successful attack could impact regional economy, disruption of regional infrastructure, or cause extensive property damage. Such an attack would be likely to generate some national concern and attention.
4	Facility located adjacent to a major recognizable landmark (e.g., Washington, DC, or NYC). A successful attack could impact national economy, disrupt a major supply of a critical material or national infrastructure. Such an attack would create significant national/international concern and attention.

4. Security Risk Index (SRI) Calculation

A qualitative score from 3 through 12 can be produced for each RMP scenario.

Difficulty of Attack (D)	Severity of Attack (S)	Attractiveness of Target (A)	Security Risk Index (SRI)
1	1	1	3 + 2 + 4 = 9
2	2	2	
3	3	3	
4	4	4	

The highest of the SRI for each RMP process will determine the prioritization tier for the facility.

Security Risk Index									
Tier 4	Tier 3			Tier 2			Tier 1		
3	4	5	6	7	8	9	10	11	12

Example—Facility with Multiple RMP Processes

RMP Process	Description	Difficulty of Attack (D)	Severity (S)	Attractive-ness (A)	D + S + A = SRI
1	*Total rupture of tank containing flammable chemical "A" (located in a non-secure area)*	3	2	2	7
2	*Total rupture of sphere containing chemical "B", a non-flammable toxic chemical (located in a highly secured area)*	1	4	2	7
3	*Total loss of contents of tank of chemical "C", a highly toxic chemical*	2	4	2	8
4	*Total loss of contents of a highly toxic chemical "D" via reactive chemicals incident caused by introduction of water*	4	4	3	11

The maximum SRI for the RMP processes at the facility is for RMP process #4, which generates an SRI of 11. Therefore, the facility would be placed in Tier 1.

Step 2—Report Back to ACC

The ACC Board expects a report that ACC members have prioritized their domestic facilities. At the conclusion of the prioritization, members should provide the attached response form to ACC.

Step 3—Evaluate Other Facilities

By September 2002, Tier 4 facilities (facilities with no RMP program 2 or 3 processes) will be further evaluated to determine whether they should be elevated to a higher tier. Any reprioritization will be based on good engineering judgment and consideration of factors such as: (1) the materials present at the site, (2) potential impact on off-site receptors, and (3) potential for simultaneous attacks against adjacent equipment. These factors are described further below.

The purpose of this step is to determine if potential risks exist that are not identified by the RMP-based prioritization methodology. A facility would not be expected to conduct air dispersion modeling or use similar tools for this evaluation. Using good engineering judgment, the facility will determine whether it should act more quickly than indicated by a Tier 4 status to assess the vulnerability of the facility.

If elevated in priority, a full vulnerability assessment would be performed within the time frame specified in the Responsible Care® Security Code. Facilities remaining in Tier 4 will be subject to a modified vulnerability assessment. The following factors may be considered when assessing Tier 4 facilities to determine whether they should be elevated to a higher tier.

1. Materials Present at the Site

Materials of concern should include those with a potential for misuse in terrorism or the production of weapons of mass destruction or illegal drugs. Some of these materials have been identified under the Chemical Weapons Convention (CWC) and in guidance to industry developed by the Federal Bureau of Investigation (FBI). In addition, the Australia Group has developed lists of chemical weapons precursors, dual-use chemical manufacturing facilities and related technology, dual-use biological equipment, biological agents, and plant and animal pathogens that could be used in the proliferation of chemical and biological weapons. (See Attachment C for FBI-list chemicals and Attachment D for chemicals identified under the CWC. Information on the Australia Group lists is available at www.australiagroup.net/).

A facility should also consider non-RMP materials or RMP substances below the regulatory threshold amount likely to cause an offsite "injury" as defined in the RMP regulations (40 CFR 68.3): "any effect on a human that results either from direct exposure to toxic concentrations; radiant heat; or overpressures from releases or from the direct consequences of a vapor cloud explosion (such as flying glass, debris, and other projectiles) from a release and that requires medical treatment or hospitalization."

2. Potential Offsite Receptors

A facility would not be expected to conduct air dispersion modeling or use similar tools for this evaluation since the purpose is to determine whether a vulnerability assessment should be conducted at the facility more quickly. Using good engineering judgment, the facility should determine whether a significant potential exists to adversely impact (e.g., cause irreversible health effects) one or more potential offsite receptors, and possible change the facility rating to a higher tier.

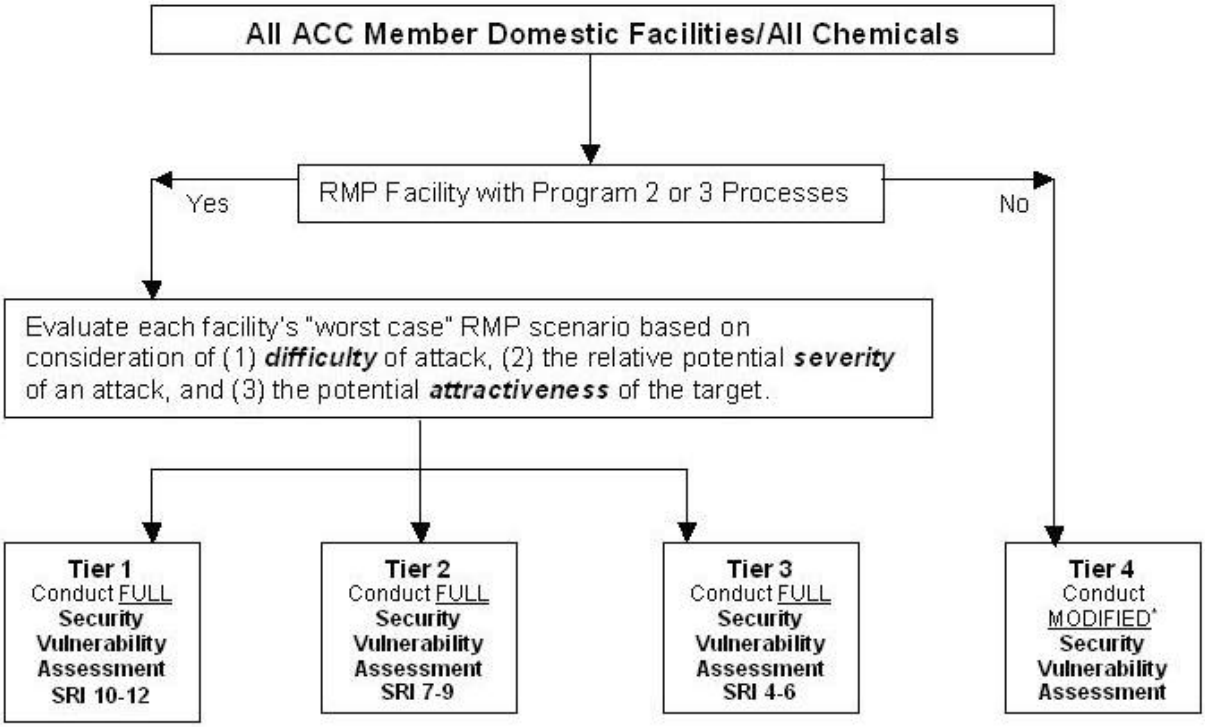
For the purpose of this activity, "potential offsite receptor" would have the same meaning as "public receptor" under the RMP regulations (40 CFR 68.3): "offsite residences, institutions (e.g., schools, hospitals), industrial, commercial, and office buildings, parks, or recreational areas inhabited or occupied by the public at any time without restriction by the stationary source where members of the public could be exposed to toxic concentrations, radiant heat, or overpressure, as a result of an accidental release."

3. Potential for Simultaneous Attacks Against Adjacent Equipment

Potential for simultaneous attacks against adjacent equipment acknowledges that an adversary might attack adjacent equipment located remote enough from each other to preclude a simultaneous release due to an accidental release. In this case, the adversary attack scenario potentially could impact more off-site public receptors than the accidental release scenario. Using good engineering judgment, the facility should determine whether a simultaneous release from unconnected, adjacent inventories would increase the relative severity of attack (S) or attractiveness of the target (A) factor, and possibly change the facility rating to a higher tier.

Attachment A

ACC Facility Security Prioritization Tool



ACC members will have prioritized all U.S. facilities by June 2002.

…

Attachment C

Chemicals with Potential for Misuse in Weapons of Mass Destruction Terrorism

The Federal Bureau of Investigation (FBI) issued industry guidance that includes a list of chemicals with potential for misuse in weapons of mass destruction (WMD) terrorism. The following list of chemicals is based on FBI experience, investigations, and intelligence. It is designed to increase industry's awareness of chemicals that could potentially be sought, stolen, diverted, or purchased to further WMD terrorism.

*Ammonia	Arsenic	Arsine
Boron trichloride	Boron trifluoride	Butyric acid
Carbon disulfide	*Chlorine	Chloroacetone
*Cyanides	Diborane	Dimethyl sulfate
Dimethyl Sulfoxide (DMSO)	Ethylene oxide	Fluorine
Formaldehyde	Hydrogen bromide	Hydrogen chloride
Hydrogen fluoride	Hydrogen sulfide	Mercury
Methyl phospho-nothioic dichloride	Methyl phosphonous di-chloride	Methyl phosphonyl dichloride
Methyl phosphonyl difluoride	N,N'-Dicyclohexylcarbo-diimide (DCCDI)	N,N'-Diisopropylcarbo-diimide (DICDI)
N,N'-Dimethylamino phosphoryl dichlo-ride	Nitric acid	Phosphine
Phosphorus trichlo-ride	Sodium azide	Sodium Fluoroace-tate
Sulfur dioxide	Sulfuric acid	Thallium
Thiodiglycol	Thionyl chloride	Tributylamine
Tungsten hexafluoride	2-(Diisopropylamino) ethane thiol	2-(Diisopropylamino) ethanol

* Chemical agents that may be more likely to be used in furtherance of WMD terrorism or criminal activity

Attachment D

Chemicals Covered by the Chemical Weapons Convention

The Chemical Weapons Convention (CWC) is a global arms control treaty that bans the production, storage, transfer, and use of chemical weapons. The CWC's impact on chemical companies results primarily from industry's production, processing, consumption, export, or import of chemicals covered by the convention that possess both civilian and military utility—so-called dual-use chemicals. The CWC covers some

dual-use chemicals as well as chemical weapons agents and their direct precursors as well as a broader category of Discrete Organic Chemicals (DOCs) with potential for misuse in producing chemical weapons. While industry is already obligated to report on, and to host inspections of specific activities involving, CWC chemicals, their presence should also be a factor in planning for facility security.

Schedule 1 Chemicals (CW agents, key final stage precursors)

Lewisites, sulfur and nitrogen mustards, chlorosoman and chlorosarin, among others.

Schedule 2 Chemicals (Potential CW agents and key precursors, low volume/high value commercial chemicals)

Amiton, Perfluoroisobutylene, and 3-Quinuclidinyl benzilate (BZ)

Chemicals (except those listed in Schedule 1) containing a phosphorus atom to which is bonded one methyl, ethyl or propyl group (organo-phosphorus chemicals)

Arsenic Trichloride, Quinuclidine, Thiodiglycol, Pinacolyl Alcohol

Dialkyl (Me, Et, n-Pr or I-Pr)

N, N-Dialkyl (Me, Et, n-Pr or I-Pr)

N, N-Dialkyl (Me, Et, n-Pr o I-Pr)-phosphoramidic dihalides

N, N-Dialkyl (Me, Et, n-Pr or I-Pr) aminoethyl-2-chlorides and corresponding protonated salts

N, N-Dialkyl (Me, Et, n-Pr or I-Pr) aminoethane-2-ols and corresponding protonated salts

N, N-Dialkyl (Me, Et, n-Pr or I-Pr) aminoethane-2-thiols and corresponding protonated salts

N, N-Dialkyl (Me, Et, n-Pr or I-Pr) phosphoramidates

2,2-Diphenyl-2-hydroxyacetic acid

Schedule 3 Chemicals (Old CW agents, other high volume, commodity precursors)

Phosgene
Cyanogen chloride
Phosphorus oxychloride
Phosphorus trichloride
Phosphorus pentachloride
Triethyl phosphite
Dimethyl phosphite
Diethyl phosphite
Ethyldiethanolamine
Sulfur monochloride
Sulfur dichloride
Chloropicrin (trichloronitromethane)
Hydrogen cyanide
Triethanolamine
Thionyl chloride
Trimethyl phosphite
Methyldiethanolamine

Discrete Organic Chemicals (DOCs)

All compounds of carbon except for its oxides, sulfides, and metal carbonates, produced by chemical synthesis. (Refer to Part 715 of 15 CFR Parts 710-722 of the Chemical Weapons Convention Regulations (CWCR) for the definition and exemptions.)

Resource 2-2: CCPS Facility Vulnerability Screening Tool

The Center for Chemical Process Safety (CCPS) Facility Vulnerability Screening Tool tracks the ACC process for RMP facilities, but provides additional assistance for non-RMP facilities. The tool is available from CCPS at www.aiche.org/ccps/.

Resource 2-3: Sandia Vulnerability Assessment Methodology

The Sandia workbook is an Official Use Only (OUO) document and is being distributed to selected organizations and others that have a need-to-know and agree to the terms of the Distribution Agreement. Individuals requesting a copy of the workbook should send an email to cdjaege@sandia.gov and also fax a signed copy of the Distribution Agreement to 505-844-0011. Either in the email or the fax, sufficient information to identify the requester and the requester's organization should be provided. An electronic copy of the VAM-CF[SM] workbook will then be sent to the requester. Only one copy of the workbook will be provided to a given organization and under the terms of the Distribution Agreement the requester can distribute copies within that organization. A copy of the distribution agreement is available at http://www.responsiblecaretoolkit.com.

Resource 2-4: CCPS Assessment of Fixed Chemical Sites

The Security Vulnerability Methodology (SVM) developed by the Center for Chemical Process Safety (CCPS) is available from Scott Berger of CCPS at scotb@aiche.org.

Resource 2-5: CCPS Vulnerability Assessment

"Security Vulnerability Assessment Essential Features/Criteria," a publication of the Center for Chemical Process Safety (CCPS), describes the attributes of a layered risk analysis approach to site security vulnerability assessment methodologies.

CCPS will evaluate other security vulnerability assessments against its Security Vulnerability Criteria www.responsiblecaretoolkit.com. Companies wishing to submit their vulnerability assessments to CCPS for evaluation are encouraged to first conduct a self-audit against the CCPS design criteria. Submissions should be made to Scott Berger of CCPS at scotb@aiche.org. CCPS will charge a nominal fee based on the time required to complete the evaluation and to resolve any gaps. The response time will depend on the number of methodologies submitted for evaluation.

Resource 2-6: Security Program Elements and Practices

Source: *Site Security Guidelines for the U.S. Chemical Industry* (Arlington, VA: American Chemistry Council, Synthetic Organic Chemical Manufacturers Association, and The Chlorine Institute, Inc., 2001).

B. Threats, Vulnerabilities, and Consequences

Once assets have been evaluated, a security manager may want to consider which assets may be vulnerable. This procedure helps identify and prioritize likely targets and save companies from expending resources where the likelihood of attack is remote. For example, companies involved in certain polymer markets may produce a suspension in which a powdered polymer is suspended in solution. Even if this product is made in significant quantities, it is an unlikely candidate for a terrorist target. Therefore, expending resources to counter a terrorist threat against that target would not be wise. How, then, do companies assess the likelihood that an asset would be a desirable target?

Since chemical companies routinely perform many different evaluations and assessments, this guidance attempts to build on those existing practices to provide a tiered approach to risk-based assessment. A tiered, risk-based approach is the most effective and efficient way to evaluate, identify, and prioritize potential targets. A tiered approach is nothing more than starting with simple evaluation techniques, usually qualitative in nature, and identifying areas in which more information would be useful to reach a risk-based conclusion.

A common type of assessment in the chemical industry is a chemical hazards evaluation, in which the hazards of a chemical are compared with the potential for exposure or potentially dangerous conditions. This comparison helps answer whether a given chemical is likely to cause harm. The comparison can begin with a simple, qualitative description of how and under what circumstances a chemical is manufactured and used. The assessor can then analyze the physical and chemical properties of the substance and quickly weed out less hazardous scenarios before prioritizing on the likelihood of the scenarios.

In addition to a chemical hazards evaluation, companies routinely perform a process hazard analysis (PHA). A PHA analyzes the potential causes and consequences of fires, explosions, releases, and major spills of chemicals. The PHA focuses on equipment, instrumentation, human actions, and external factors. These considerations help managers determine the hazards and potential failure points or failure modes in a process. This type of analysis could easily be adapted to a vulnerability assessment.

Another type of assessment used in the chemical industry is a security risk assessment. Security risk assessment focuses specifically on whether a company's security

management program is adequate for protecting its assets. Physical and geographical factors, too, should be evaluated in the context of vulnerability.

One approach is described below that could be used by companies that want to perform a vulnerability assessment. Many practices performed by companies on a regular basis could easily be incorporated into this approach. This is not a prescriptive approach; instead, it is a suggested flow of thought and information. It is entirely conceivable that one or more steps would not apply to certain chemicals. It is up to the assessor to use professional judgment and determine the appropriate areas to be addressed.

Step 1: Chemical Hazards Evaluation

Chemical hazards evaluations are routinely performed in the chemical industry. They are often done in the context of the Responsible Care® Product Stewardship Code. Although they can and do differ in methodology, chemical hazards evaluations are designed to answer this two-part question: How likely is a chemical release, and how harmful would it be? These evaluations can easily be incorporated into a vulnerability assessment. Doing so augments the assessment of a given facility and helps in evaluating whether it might be considered an attractive target.

Step 2: Process Hazard Analysis (PHA)

PHAs are often done in the context of the Responsible Care® Process Safety Code and are considered good practice in the chemical industry. PHAs may be a good place to begin a vulnerability assessment for chemicals and processes of security concern. A PHA is designed to highlight areas of potential vulnerability, which, upon further study, may also be a potential target of an adversary.

Step 3: Consequence Assessment

Although it may be convenient to use worst-case scenarios and err on the side of safety, that approach is not practical for assessing all threats and appropriate countermeasures. Economics and common sense dictate that potential threats and consequences (as well as the actions to counter them) be prioritized.

Step 4: Physical Factors Assessment

After assessing the hazards and the likelihood that something could cause harm, it may be useful to address the physical factors that could affect the attractiveness of a potential target. These factors can potentially be used to reduce the likelihood that an object or location might be chosen as a target.

Some questions that can be asked include these:

- What size and type of container is it?
- Where is it located?

- Are the containers side-by-side, stacked, and isolated?
- What surrounds the plant site, and at what distance?

Step 5: Mitigation Assessment

The information in risk management and emergency response plans can help managers assess factors that could mitigate the effects of a chemical release. The presence of effective risk management and emergency response plans may affect the likelihood that a facility is chosen as a potential terrorist target. For example, anhydrous ammonia is readily absorbed and controlled by a water fog. This reduces the likelihood that anhydrous ammonia will spread in its gaseous state to large areas, and thus could reduce its attractiveness as a target for terrorism.

Step 6: Security Assessment/Gap Analysis

After identifying potential vulnerabilities, threats, and countermeasures, the manager could then turn to a security assessment. This assessment helps identify whether the security policies and measures in place are appropriate for meeting the potential threat. Security audits are often performed to help determine whether protective measures are adequate. The person responsible for security at a company, if he or she is not primarily a security professional, may want to consider consulting with security professionals for this part of the vulnerability assessment. Professional judgment is an integral part of the security assessment.

The following list identifies some of the potential threats that a chemical facility may wish to address:

- Loss of containment
- Sabotage
- Cyber attack
- Workplace violence
- Theft
- Fraud
- Product contamination
- Infiltration by adversaries
- Attack on a chemical plant as part of chemical and biological terrorism
- Assault
- Bomb threats
- Workplace drug crime
- Theft of confidential information
- Hacking into information systems to disrupt computer-controlled equipment, causing an unplanned release of chemicals
- Product tampering
- "Hands-off" threats, such as cutting off electricity, telephone, or computer network, or else contaminating or cutting off water

- Trespassers committing vandalism or setting fires for fun
- Thieves looking for precursor chemicals to use in illegal drug manufacture; break-in can also result in valves being left open, causing a chemical release
- Protesters disrupting plant operations through trespassing, vigils, assemblies, rallies, intimidation of employees, chaining selves to plant, or blocking traffic
- Vandalism of control rooms and equipment, and destruction of system documentation to make repair more difficult
- Disruption of cooling systems for electronic equipment rooms
- Creation of destructive or hazardous conditions through modification of fail-safe mechanisms or tampering with valves (done in person or electronically from a distance)

There is no one-size-fits-all approach to a vulnerability assessment, nor is there a one-size-fits-all approach to security. A multidisciplinary approach may benefit companies performing an overall vulnerability assessment. The professional judgment of security personnel, combined with environmental health and safety employees, process safety engineers, and process operators, can yield a comprehensive approach without draining scarce resources.

Resource 2-7: Risk Assessment/Risk Management Process

1.0 Introduction

Risk Management is the technical procedure for identifying and evaluating vulnerabilities and for balancing risks against cost of countermeasures. This document addresses the security risk management framework. The process is technical and deliberate. As such, risk management efforts evolve into an objective system to classify risk that can be statistically valid and reliable. This document further constructs a framework for risk management planning, assignment of roles and responsibilities, team development/training, monitoring, and follow-up tracking.

Safeguards and Security Qualitative Risk Assessment (RA) - Risk Assessment is the key component of Risk Management programs. The RA methodology is the approach that has been adopted by Security for conducting these assessments. The methodology can be applied at project stages from conceptual through detailed design, post-construction, and operations, and can be adapted to varying levels of available information and depths of evaluation.

In the methodology, a team of five to eight with expertise in engineering, operations, security, and risk assessment techniques uses its knowledge and experience to identify potential vulnerabilities associated with the system of interest. The team then uses a structured brainstorming approach to identify credible scenarios that could result in threats exploiting vulnerabilities. Each scenario is analyzed to identify assumed or existing safeguards, potential causes, and effects. Using a risk matrix, scenarios are assigned a qualitative risk rating based on the team's judgment of its severity or consequence and likelihood of occurrence or probability.

Risk Assessment Process

1. *Senior management approval*. Senior management must approve the conduct and scope of the assessment. This will ensure cooperation at management levels and enhance the quality of information received by assessment teams.

2. *Asset valuation and judgment about consequences of loss*. This step determines what is to be protected and its value. Value can be tangible (e.g., dollars) or intangible (e.g., reputation). Part of asset valuation is understanding that assets may have a value to an adversary that is different from their value to the company. People, operations, information, facilities, and equipment should be considered.

3. *Identification and characterization of the threats to specific assets.* This step identifies specific threats to identified assets. An analysis of threat is critical to the RA process.

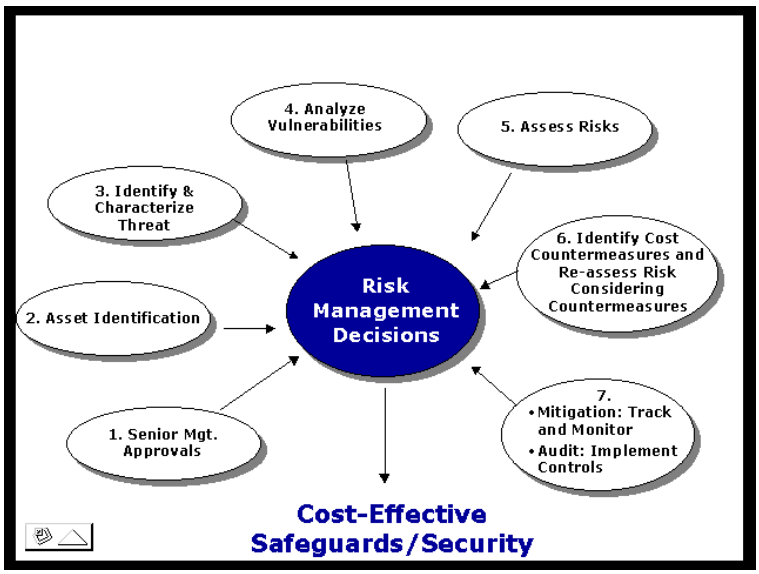
4. *Identification and characterization of the vulnerability of specific assets.* Vulnerability assessments help identify weaknesses that could be exploited to gain access to an asset.

5. *Assess risk.* In this step a risk calculation using cause-effect analysis is made. Risk is a product of probability and severity. In this step countermeasures to mitigate risk are considered.

6. *Identification of countermeasures, costs, and tradeoffs.* There may be a number of different countermeasures available to protect an asset, each with varying costs and effectiveness. In many cases, there is a point beyond which adding countermeasures will raise costs without appreciably enhancing the protection afforded. **Risk is recalculated after the application of countermeasures.**

7. *Countermeasure evaluation* is an evaluation, at a prescribed time interval, of the effectiveness of implemented countermeasures and a review of those countermeasures to ensure they have not created new, unforeseen vulnerabilities. A tracking and monitoring system will be in place to ensure implementation of agreed-upon countermeasures.

This process is depicted below:

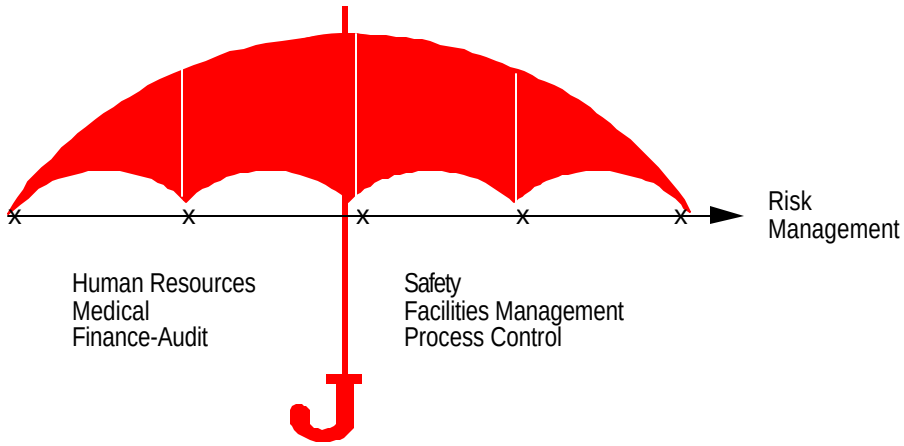


When any of these steps are left out, the result can either be inadequate or unnecessary and overly expensive protection. Frequently, the missing element is incorporation of specific, up-to-date threat assessments. With no documented threat information, countermeasures are often based on worst-case scenarios.

It must be stressed that managers must make tradeoffs during the decision phase between cost and risk, balancing the cost in dollars and manpower against possible asset compromise or loss. Policy decisions resulting from this process can then guide security planning. These decisions should form the backbone of, and provide the standards for, the safeguards and security system. The resulting standards promote consistency, coherence, and reciprocity across programs.

The umbrella image below is a further illustration of the safeguards and security risk management concept. The vertical lines represent typical organization boundaries (such as a department within the organization context, or a unit within the department context). The curved lines at the umbrella base represent the risk management/assessment process—a process that examines relationships that exist *between boundaries.* This interrelational concept is what separates risk management from traditional inspection or audit programs (which tend to examine programs vertically for "efficiency" rather than horizontally for "effectiveness").

Risks are assessed and evaluated using the SSQRA software and the Risk Scenario Worksheet. The information provided in the worksheet is derived from the SSQRA dialog box which captures the risk assessment and risk evaluation work of risk assessment teams. Use of the SSQRA is mandatory.



Risk Management Umbrella Concept

Definitions - To better explain this process, the following definitions are presented:

- ***Risk*** is the potential of loss to an organization or entity.
- ***Risk Management*** is analysis of an organization's existing resources and its vulnerabilities. It determines loss potential for each resource or combination of resources to establish potential loss levels. Both tangible (dollar losses, or

to an undetected intrusion) and intangible (loss of sensitive information, damage to reputation) resources must be considered.

- ***Threat*** is an entity—individuals, programs, policies, hazards, and events—that is capable of exploiting a vulnerability.
- ***Vulnerability*** is a condition that can be exploited by a threat, thus causing deviation from intended outcomes or unauthorized access to an asset.
- ***Countermeasure*** is an action used to reduce or eliminate one or more vulnerabilities.

To summarize, the risk assessment process provides a mechanism that

- Reviews potential threats to security interests;
- Determines appropriate levels of protection for assets;
- Emphasizes backup systems and in-depth protection;
- Addresses cost-risk benefit-analysis tradeoffs;
- Promotes action to reduce risks that are not acceptable;
- Promotes decisions that accept certain levels of risk; and
- Provides a means to judge whether the resultant risks meet acceptability criteria.

2.0 Management of Risk

The following describes the RA methodology. This methodology consists of distinct phases: a qualitative *risk assessment* phase of threat and vulnerability identification, characterization, and ranking (in terms of adverse consequences and their probability of occurrence) and a *risk evaluation* phase entailing risk mitigation and re-estimation of the occurrence probabilities and the consequences of weaknesses or hazardous events. Following the capture of risk, appropriate risk management options can be devised and considered. Risk-benefit or cost-benefit analysis may be undertaken and risk management (or countermeasure) policies and/or procedures may be formulated and implemented. The main goals of risk management are to prevent actions of threat agents by reducing the probability of their occurrence (e.g., practice "surprise" avoidance), to reduce impacts of undesirable events (e.g., prepare and adopt emergency responses), and to transfer risk (e.g., via insurance coverage).

RA is a structured brainstorming technique in which a team uses its knowledge and experience to identify potential vulnerabilities and qualitatively assess the risks associated with those vulnerabilities. Vulnerabilities are identified using one or more methodologies such as brainstorming and a "what-if" checklist.

Risk Scenario Analysis (RSA) refers to the process of converting identified vulnerabilities into risk scenarios, and the systematic analysis of these scenarios to determine the risk level they represent. It is intended to supplement and extend vulnerability evaluation by explicitly considering the two components of risk, consequence and probability. In risk scenario analysis, identified vulnerabilities are used to postulate undesired events and their possible causes, effects, and safeguards; credible scenarios are developed to describe how each event may occur; and qualitative estimates are made of the consequence and probability of each scenario.

Uses—Because of flexibility in approach, especially in choice of vulnerability identification tools (such as questionnaires, surveys, interviews) and subsystem analysis, RA using RSA can be applied to almost any activity involving risk (an entire facility, a division/department within a facility, or an operation). It is useful over a broad range of projects and work scopes, from early stages of a project (pre-conceptual design) through life cycle gates. The basic approach is further applicable to risks associated with use of technology in operations.

Benefits—Like some traditional vulnerability evaluation methods, benefits of RA center on the team concept. By involving personnel responsible for both engineering and operations of a facility under study, security and operations personnel gain a better understanding of the facility and its vulnerabilities. The experience base of the team brings historical operational perspective to the process.

Limitations—A potential limitation of RA is that it may not capture the total risk picture for a given operation. Furthermore, its success depends heavily on the knowledge, experience, and creativity of the team. The nature of the process and risk rating system make direct comparisons between studies difficult. Apparent risk differences between operations may be greater or less then indicated in the results of separate studies conducted by different teams. These differences are primarily in the risk ratings, which are only one part of the risk assessment results. Differences in follow-up considerations depend on team makeup, the quality of available information, and depth of analysis. Also, as the system under study becomes more complex, it may be necessary to supplement RA with other tools, such as software-based quantitative methods.

Keys to Success—The limitations of RA are reduced by

- Careful planning and team selection (including the security and engineering and operations personnel);
- Providing all relevant information to the team prior to and during the QRA, by using a systematic approach to vulnerability (scenario) identification; and,
- Choosing the depth of analysis appropriate to the magnitude of vulnerabilities and degree of system definition. Further benefit is gained by encouraging open discussion during team meetings, and by prompt reporting of results.

The remainder of this report describes QRA in more detail. Section 3 describes planning, assignment of roles and responsibilities, team development, and training. Section 4 describes the risk assessment process.

3.0 Risk Management Planning, Roles and Responsibilities, Team Composition, and Training

…

Special Risk Studies *(Limited Scope Risk Assessments)*—Special risk studies are generally aimed at developing an understanding of findings from other risk assessments. Their goal should be to provide a better understanding of exposure from the assessment findings. Methods used in special risk studies should be coordinated with the RMCs and tailored to fit the specific objectives being examined (e.g., personnel suitability investigations). The scope of each RA must be identified, and any previous RAs and other similar evaluations should be reviewed prior to beginning a new RA. However, the base plan developed by RMCs may account for special risk studies that have been or will be conducted.

…

3.1 Planning

The basic steps in organizing a RA include

- Identifying an owner and a qualified team leader,
- Identifying participants representing other disciplines,
- Developing a detailed schedule (duration), including requirements of support facilities,
- Identifying data and individuals who must be interviewed,
- Defining deliverables,
- Providing an adequate budget,
- Agreeing on scope (refinery security) and assumptions (such as threat levels),
- Agreeing on report review procedures, and
- Agreeing that the owner develops the follow-up plan.

3.2 Roles and Responsibilities

As part of the process, team members work together to determine the risk index for each of the scenarios developed. Developing this index is an independent process, and intervention from the RA owner should not occur at this stage. To further ensure accuracy of their findings, the team should conduct an "error of fact" review with the owner at the conclusion of the assessment (this may be an element of the exit brief-

ing). The team should explain what led to risk calculations as they will appear in the draft report. See RA Team Composition (3.3) for further discussion.

***Owners*—O**wners should be responsible for post RA follow-up actions. In this context, the owner is defined as a manager in whose operation the risk assessment is being conducted and who has overall responsibility for the follow-up and close-out process, including

- Evaluating possible mitigating alternatives and related impacts) upon risk levels,
- Assisting in final draft review (after which, modifications should be limited),
- Assigning corrective action responsibilities (to assignees), and
- Communicating results to affected personnel.

The owner is responsible for communicating risk levels associated with operations and activities to senior management. The owner documents risk to management by preparing and submitting the Risk Management Summary Report (RMSR). The RMSR should include copies of risk scenario worksheets. Management approval of the RMSR acknowledges the existence of the risks and the related mitigation countermeasures. **Where significant risks have been accepted by management, it is important to include contingency planning as part of the risk management process.** Owners are responsible for providing the RMCs with follow-up documentation, including identification of assignees and their respective responsibilities. See Step 7 for further discussion of the owner's role in tracking and monitoring activities.

Assignee—An assignee is a person whom the owner appoints to implement specific follow-up actions. The owner should identify assignees and their responsibilities in the risk assessment documentation. The owner must clearly communicate information and expectations relating to follow-up actions.

Security Risk Management Coordinator—Senior security advisor (risk management) who has overall responsibility to ensure program integrity.

Risk Management Coordinator (RMC)—RMC is a person in a security business center who has responsibility to ensure that risk management execution is in accordance with the risk management program.

3.3 RA Team Composition and Training

RA quality depends on team composition, experience, and qualifications. RMCs should provide guidance to owners in assembling high quality teams. Generally, security staff should represent no more than one-third of a team and those security team members, most importantly the team leader, should be from outside the element being assessed. Other suggested team members include: safety, process control, logistics, transportation, facility operations, audit (so long as the assessment is not perceived as

being audit oriented), human resources, maintenance, or other risk assessment experts. Members should come from mid-level management with knowledge of senior management strategic and tactical planning and day-to-day operations. Use of knowledgeable, non-organizational third parties as members (such as consultants or senior university staff), is strongly encouraged. A team leader and an assistant with the requisite experience should be designated.

The team leader is responsible for managing activities, completing the RA study and the RA Report, and complying with all aspects of SSQRA software and the risk management system. The assistant team leader is responsible for capturing and documenting all assessment activities, findings, and recommendations in the SSQRA software. This person may serve as the scribe or guide the activities of a third-party scribe.

All team members (including third parties) should be approved by the owner and documented in the RA Execution Plan.

Training Security Team Members—Training should maintain capabilities of team members and qualify potential candidates. There are several levels of training:

- **Level 1**—RA orientation briefing that gives examples of security risks and related mitigation measures; discusses risk identification techniques; and provides an overview of the RMS, addressing team composition, individual responsibilities, and general risk assessment reporting requirements.
- **Level 2—**Formal training composed of a brief history of vulnerability analysis and risk assessment; experiences from specific security risk assessments; and in-depth knowledge of the risk matrix concept, the SSQRA software, related analysis techniques (such as HAZOPS, fault tree analysis, consequence analysis, and probabilistic risk analysis), the operational integrity processes, and emergency management. Level 2 must have participated in at least one major, complex, full-scope risk assessment and contributed to development of an execution plan and the review of the draft report.
- **Level 3—**All Level 2 requirements plus direct participation as a team member on at least two major, complex, full-scope risk assessments and co-authorship of at least one full-scope RA report.

Refresher training should be provided every three years at all levels. For Level 2 and Level 3, additional specialty training should take place every five years. Refresher training for Level 3 staff should also focus on progressive courses that teach new techniques (e.g., university courses, training seminars, and professional industry/government risk assessment conferences). The RMCs are responsible for identifying and endorsing this training.

To identify potential team members, the RMCs should maintain a database of security staff training and experience. The RMCs should approve all candidates for Level 2/3

designation. Qualifying criteria should emphasize relevant substantive experience in previous assessments. Security management should ensure that appropriate numbers of security personnel with the requisite depth and mix of skill levels are maintained within their group or are available through third-party sources.

3.4 RA Reporting and the SSQRA Software

The security department and the University of Pennsylvania developed the SSQRA software. The tracking features of SSQRA allow for easy transfer of findings (causes, effects, and recommendations) into a central Risk Management Summary Report (RMSR). Use of this tool is required by Security.

After conducting a risk assessment, the RA Team Leader should complete the first draft report within four weeks. This draft report should only be sent for review to the owner and the specific team members, with a two-week turnaround requirement. During this timeframe, the team leader should conduct an "error of fact" review with the owner. This is a critical step that could later serve to maximize risk mitigation/prevention alternatives. The team leader should then complete the final draft report within two weeks of the review phase. The final draft report should be sent to the owner and to all team members. Distribution decisions beyond that rest with the owner.

4.0 Qualitative Risk Assessment Process

The following seven steps comprise the Security RA process and are formatted in the SSQRA software.

Step 1—Management Approval, Planning, and Preparation

RAs are normally commissioned by management responsible for operations being assessed, in coordination with the Security Business Centers and RMCs. Subject, scope, team composition, and organizational concerns and constraints should be addressed. Management approval should be granted with an emphasis that risk assessment is a **"fact" finding, not a "fault" finding** analysis. This approval will generally improve quality and speed by ensuring cooperation of mid-level management.

This phase begins with preparation of the Risk Assessment Execution Plan. The plan consists of objectives and scope, identification of team leader, scribe and team member designations, methodology discussion, questionnaire, time duration, logistics, and costs.

Objectives and scope are communicated to the team by the execution plan. As previously stated, the risk assessment methodology requires five to eight full-time members. The team leader should then subdivide the risk assessment into components and determine which members will conduct what activities. Generally, these assignments include who will interview key staff, review what data, analyze processes and opera-

tions, etc. Logistics (travel, hotel, work areas, computer support, costs, etc.) must also be addressed at this time. Effectiveness is enhanced if members have a visual display of analysis results via computer screen projection (which allows for copying, printing), flip charts, etc., during team discussions.

Quantifiable data should also be reviewed. Local team members should prepare a detailed interview matrix showing interviewees with associated dates and times. Generally, interviews take the first three to four days of an assessment (with scenario discussion daily) and the risk calculation phase another three to four days. Cost calculations, prioritization of recommendations, and exit briefing preparation take another day to day and a half. The management exit briefing usually takes two hours and finishes the in-facility phase.

Team activities should initially begin with a presentation by senior staff and familiarization with the facility/operation being assessed. The team leader should then review the RA process with the team. It is particularly important that the team reach a common understanding as to the use of the SSQRA risk scenario classifications and the risk matrix, which provide a framework for classification by vulnerability type, consequence, and probability. The team leader should also encourage team members to express any concerns.

Keys to Success—Step 1

- Multi-disciplined team with scope and assumptions defined
- Team understanding of RA process and SSQRA software

Step 2—Identification of Critical Assets: System Definition

Identification of assets is a crucial step in the process because it provides the basis for subsequent steps.

CA/EECA means Identification of Critical Assets (CA) and Identification of Essential Elements of Critical Assets (EECA). In this approach, CA are those assets that are most important to safeguard and EECA are elements that lead or support those assets. Critical assets are typically people, activities/operations, information, facilities, and equipment. Identification of EECA refers to the policy, programs, processes, audit controls, and procedures that threats might exploit to cause CA vulnerability. For example, from an adversarial perspective one might ask, "If my task were to disrupt operations of a process control center, what would disrupt it, and where are the elements that support it operationally?" The "what" is the CA, and the "where" is the EECA.

The concern with critical assets and their loss impact is what distinguishes a security program based on risk assessment from a security program that primarily focuses on

generic protection (such as only securing a plant perimeter). This broader approach requires an understanding of the totality of an activity, knowledge of threats, and an imperative to cross organizational boundaries in activities which involve more than one entity.

To gain an understanding of CA and totality of activity, the team should identify key individuals for interviews. A wide array of individuals should be slated for interviews (ranging from senior managers to protective force members) and both inside staff and outside staff should be considered (e.g., support contractors, military, law enforcement, other agencies, and similar industries).

Questions that are generally derived from the risk assessment questionnaire should be formatted according to the person's responsibilities (a doctor would be asked different questions than an auditor). Use of standard interview questions should be encouraged to guide these interviews. Structured questionnaires should also be considered. These are generally distributed randomly to a large cross-section of the operation before the assessment. These are intended to generate a snapshot of security program effectiveness, identify assets, and solicit suggestions for improvement from a broad base. Results tend to enhance the quality of structured interviews.

Asset "owners" or program managers are generally the most knowledgeable about the assets in need of protection.

Focus on "Totality of an Activity"—Through this analysis, the team will learn where and how critical assets reside, how they operate, and how they relate and impact from one location or organization to another. As the team collects data, the focus should be on those few "golden nuggets" called critical assets. This and a solid knowledge of the threat-agent potential will keep the system analysis from bogging down in an endless accumulation of data.

One basic approach that a team may use in its systems analysis is to construct a chronological description of the actual or predicted unfolding of the activity or operation. This will determine who does what, when, where, why, and how, not only in the organization that has primary responsibility for the conduct of the activity, but also all supporting or related organizations. This is what is implied in examining the "totality of an activity."

During this phase of analysis the team will also identify undesirable events and the potential impacts to assets if those events were to occur. Some of the key questions in assessing loss impact of an asset are "what would we lose," "what would an adversary gain," and/or "what is the impact on safety, health and the environment." Once the consequences have been determined for each potential undesirable event, the criticality of each asset can be rated or ranked relative to the other assets. The question is how the need for protection of this asset compares with the other valued assets. Knowledgeable individuals should rank the criticality of each asset in order of importance using one of the following categories:

- Catastrophic
- Critical
- Marginal
- Negligible

The results should be validated by the asset owner.

Keys to Success—Step 2

- The major elements (CA/EECA) that define a system should be identified by the team.
- Ranking of CA—These system elements are typically people, activities/operations, information, facilities and equipment.
- Team analysis or data, surveys, assessments.
- Team use of checklists and questionnaires.

Step 3—Analysis of Threats

Knowledge of the threat aids in identification of vulnerabilities that could be exploited by threat agents. The term *threat* refers to range of events or hazards that can exploit a vulnerability. Threat agents consist of two elements: *static* (or relatively constant) threats and *dynamic* (or changing) threats. Threat analysis measures identifiable threat against safeguards (controls and mechanisms that protect assets from threats).

The Design Basis Threat Statement should serve as the base. Local threat data (e.g., data from the Security Incident Reporting System) and local inputs should be added to generate an overall threat statement. Threat should be evaluated in terms of insider (our most significant threat), outsider, and system induced (organizational or operational flaws).

By examining threat totality and assuming "threat agent perspective," a team can construct a threat strategy—that is, the probable sequence of steps that threat would go through to achieve an objective. These steps will identify how an asset can be exploited. This is important in devising countermeasures to control identified vulnerabilities.

Once complete, the team should pair threats (adversaries) with assets and begin developing scenarios to gain an understanding of potential causes of vulnerabilities. These scenarios are intended to briefly outline potential situations that could impact on security and safeguards functions. Knowledge of threat and scenario development

enables a team to identify vulnerabilities and indicators in programs and activities that might otherwise remain undetected through reliance standard program reviews.[6,7]

Keys to Success—Step 3

- At the conclusion of this step the team should understand the system and have a preliminary understanding (through threat/asset pairing and scenario development) of potential vulnerabilities and potential causes of vulnerabilities.

Step 4—Analysis Of Vulnerability (Scenario Development)

This is the core step and involves an examination of the totality of an activity to identify vulnerabilities. Vulnerability analysis identifies weaknesses that result in deviation from intended operations. Sources of information used to assess vulnerabilities include

- Evaluation of data developed during direct surveys;
- Evaluation of historic data from related incidents and/or system operating experience;
- Threat information, scenario development, and judgment by knowledgeable individuals;
- Use of generic checklists, structured interviews and questionnaires; and,
- Formal vulnerability analysis techniques, such as fault/event tree analysis, etc.

Team Review of Data from Evaluations of the Current Security Program—Existing security, safeguards, and, to some extent, safety procedures should be evaluated in terms of day-to-day operations. Previous evaluations (including audits) should be reviewed and facilities and assets toured. Security programs should be evaluated against certain standards, such as those associated with fire codes, laws, regulations and directives.

Team Review Data from Previous Security Incidents—Examination of previous security incidents can provide insight into what may happen in the future. Previous "insider," "outsider," and "system induced" threats should be evaluated. It is the joint responsibility of the sponsor's representative and the team leader to assemble useful summary information and provide it to other team members prior to assessments. The data should be assembled and catalogued for quick reference.

Expert Opinion and Risk Scenario Development—The judgments of knowledgeable team members—a multi-disciplined group of recognized experts—should be used as a starting point for final refinement of types of security vulnerabilities that could realistically occur from developed scenarios ("what-if" brainstorming). These scenarios should be used to assist in understanding the mechanism by which security incidents

occur—the causes and effects. **The scenarios should correspond, to the maximum extent possible, with asset priorities/threats determined in previous steps.**

Scenario Development—Scenarios are categorized based on current security program elements:

- Management Leadership
- Intelligence/Threat Assessment
- Risk Management
- Personnel Protection
- Incident/Investigation Analysis
- Information Protection
- Technical Security
- Operations Protection
- Emergency Procedures
- Management of Change

Examples of Scenarios Derived from Findings

The following are examples of findings derived from results of interviews, expert opinion, data reviews, etc. They represent categories of security system anomalies, which may impact on scenario development.

Findings include these:

- Failure of the sensor system to detect or respond to an intrusion
- Inadequate capability or performance failure of a video system
- Inadequate response by security staff in the command and control centers
- Operational failure of the command and control center
- Inconsistent security response to emergencies
- Inadequate access control procedures
- Inadequate security reporting by affiliates;
- Lack of security interface into project management teams
- Lack of procedures for tracking and control of sensitive information
- Personnel security assurance concerns

Scenarios that may be derived from the above findings include these:

- Security not a full partner in project management, which results in expensive security retrofits
- Abduction of a senior executive
- Shutdown of off-site supply/utility valves by environmental activist, resulting in shutdown of some key processes in a refinery
- Theft of replacement parts from a warehouse, resulting in suspension of operations
- Copying of sensitive data from research area by unknown intruder
- Failure of security systems due to damage to the primary power feed at a command center
- Disabling of telecommunications node due to a break-and-entry
- Access to company facilities gained by a fired, irate, former employee through a lobby
- Chaotic bomb response after improvised explosive device is delivered to a mailroom
- Armed hostage situation when former contractor, with a history of mental illness and arrests (unknown to the company), holds an employee at gunpoint
- Burglary of an office by a contractor fired from one site and still granted access to another site
- Media publication of sensitive litigation findings copied by "trusted" employee
- Attempts by a competitor to influence litigation after receiving sensitive findings via the media
- Discovery of the removal of sensitive information from a computer but no reporting of incident
- Theft of sensitive litigation information valued at $25M by a computer hacker
- Management office bugged by cleaning force member working for a foreign competitor
- Acquisition of sensitive information by a foreign business partner from a Company foreign national scientist
- Promotion into a key financial management position of an employee with a history of personal financial mismanagement and an arrest record

Keys to Success—Step 4

- Team pairing of threats and assets to develop scenarios

- A determination of the existing security and safeguard systems in light of the threat/asset pairs
- A thorough understanding of the system; a final list of refined scenarios; an understanding of causal factors

Step 5—Risk Calculation

Assessment of Scenarios (Undesired Events or Vulnerabilities)—It may not be possible to assess in detail each of the vulnerabilities and cause/effect factors identified by analysis. RA values or calculations should be based on expert opinion (the process values what people think) and assessment results. The following sections address assessment of undesired events. Assessment results provide guidance on future security needs of the security program.

Cause-Effect Analysis—The team must next consider the causes and effects of the undesired event. The findings serve as the basis for calculating risk. In determining causes, the team must consider the data, including data sources, and must factor in whether the cause is direct or indirect (i.e., a direct cause for a warehouse intrusion would be failure of a sensor system, an indirect cause could be allowing contractors unrestricted access inside a perimeter). The team should be aware that there is generally a one-to-one relationship between causes and recommendations, so, for quality recommendations, teams should vigorously brainstorm causes.

Effects must be realistically evaluated and not "worst case." Effects must be analyzed in terms of whether they are tangible (i.e., dollar based) or intangible (i.e., loss of reputation). The SSQRA software requires selection of one of these variables.

Undesired Event Severity and Probability Estimates—To establish an understanding of vulnerabilities and related countermeasures, the undesired events are assessed for their severity and probability of occurrence. This assessment is subjective—again, it relies on what experts think. It can provide an indication of which undesired events pose the greatest threat. This understanding will determine which available countermeasures address those threats.

Severity of Undesired Events—Severity or magnitude of consequences of an undesired event will depend on the following factors: (1) type of threat, (2) type of asset being protected, and (3) whether threat can be deterred through application of countermeasures. It is recognized that severity of an individual event may vary considerably. It should be noted that the potential severity of a compromise cannot be reduced unless the vulnerability is completely eliminated through a major redesign (i.e., the application of encryption to a "unauthorized interception of a video teleconference" scenario). However, the probability, and therefore the associated risk, can be reduced by incorporation of security controls.

Probability of Occurrence of Undesired Events—A calculation based on previous experience is needed to establish the probability that an event will occur. This calculation should consider that the event may have occurred or been reported to occur a certain number of times. Only some security data may be available. With limited quantitative data, such as that contained in a survey questionnaire, the evaluation may have to be based primarily on historical information and judgment of knowledgeable individuals.

Teams must also decide on a definable end date in order to estimate probability. This date can be the lifecycle of a technical security system (generally 10 years), be tied to key project/program milestones, etc. Once established, the timeline must apply to all scenarios.

RA Estimates and RA Matrix—Risk associated with an undesired event is the product of event severity and probability of its occurrence. The RA Matrix is used to calculate the SSRC in a weighted fashion. The Risk Index, or SSRI, is a standardized ranking which characterizes a risk-ranking system that mandates certain management actions.

Although in many cases the probability of occurrence will not be estimated as frequent, the potential severity of certain undesired events requires that some type of action be taken to minimize the risk. Estimates can be useful in determining whether individual vulnerabilities should be eliminated or controlled to reduce the occurrence of the particular undesired event, or whether associated risk should be accepted. Contingency planning is a critical part of the risk management process where significant risk is accepted.

As an example, the undesired event "executive abduction" was assigned a Safeguards and Security Risk Category (SSRC) of IC (highest severity, occasional probability) and a Safeguards and Security Risk Index (SSRI) of 1, which requires management action to reduce risk to the next lower level. Therefore, assuming correct evaluation, action must be taken to eliminate or control the risk associated with this event.

The Risk Scenario Worksheet generated by the SSQRA software presents vulnerability analysis data in a format that assists the decision maker in determining whether the vulnerabilities should be eliminated, controlled, or accepted. The SSRI also provides a basis for decisions to apply available resources to higher risks.

Keys to Success—Step 5

- Assessed scenarios (including cause-effect analysis) in terms of severity and probability
- Assigned SSRI ranking number using risk matrix

Step 6—Risk Evaluation and Countermeasures/Risk Recalculation

Risk Reduction Countermeasure Identification—Actions taken to minimize security risks are termed countermeasures. A countermeasure is defined as any action or series of actions that may be taken to reduce the risk of an undesired event and/or the frequency of its occurrence. The emphasis is on preventing occurrence of the event.

The recommendations for corrective actions describe the method selected to eliminate the causes or minimize the effects of each vulnerability. One or more recommendations should be provided for each identified vulnerability or cause, and the team must recalculate risks based on the effect of a recommendation on the scenario. A new risk rating is then given by the team. For some very complex/special recommendations, it may be useful for the team to incorporate a new subject matter expert at this stage to assist in the evaluation of risk reduction efforts. Also, it may not be possible to recalculate risks until certain system redesign, re-engineering, etc., is complete. The team may have to recalculate risks at a future time, on a case-by-case basis.

Evaluation of Potential Countermeasures—Countermeasures should also be categorized in terms of program elements. Within each of these areas, the team should identify specific countermeasures that may be applied. In some instances, more than one countermeasure may be identified for a particular program element.

It is important that all possible elements and component vulnerabilities and causal effects be examined to identify countermeasures that will prevent occurrence of the undesired event or mitigate its consequences. After identification, the most appropriate countermeasure should be selected based on:

- Effectiveness
  - Does it reduce the probability of occurrence?
  - Does it reduce the severity?
- Cost of implementation
  - Is it incorporated into the design prior to production or operation?
  - Can occurrence be controlled with operational procedures?
  - Does the countermeasure require retrofits?
- Enforcement and audit requirements

The following discussion provides guidance on how these factors may be evaluated and assessed.

Effectiveness of Countermeasures—Effectiveness requires a judgment on how implementation will influence probability of occurrence and, to some extent, severity (noting again that severity can only be reduced through a major redesign). With regard to probability of occurrence, the countermeasure may result in no change, reduce

the probability of occurrence of the event, or totally eliminate the possibility of event occurrence (no event). With regard to event severity, the countermeasure may result in no change, slightly reduce the severity of the event, or minimize the effect of the event.

***Cost of Implementation*—**The cost incurred will depend on when and how the countermeasure is adopted. In general, it is more cost-effective to incorporate the countermeasure into the design of the system or subsystem prior to its production or operation. A procedural change (such as enhancing security program interfaces) will generally cost less to implement than changes that involve the acquisition of new or modified equipment. Technical retrofitting is usually 10 times more costly than incorporation at the design stage. Cost methodology guidelines should address the following:

- Design
- Fabrication
- Testing
- Operation
- Maintenance;
- Retrofit
- Change of operations and procedures

Within each of the above phases, the cost will depend on consideration of the following:

- Materials
- Labor
- Training
- Operation
- Downtime
- Procedural modifications

The cost of implementation must be considered relative to the effectiveness of that countermeasure. For example, the cost associated with a design change early in the design phase may be worthwhile if that countermeasure will eliminate a security vulnerability.

Costs for labor and materials should be expended (if possible) in the design and testing phases (as opposed to the construction or operations phase) to eliminate vulnerabilities in the subsystem or component. Labor, training, and downtime costs associated with implementing a countermeasure during operation and maintenance are more

likely directed at controlling known vulnerabilities. This approach is not as desirable or as safe as eliminating the vulnerability prior to operation.

Enforcement and Audit Requirements—A secondary cost associated with the implementation of a countermeasure is ensuring that the countermeasure has actually been implemented, is operating properly, and has not created any new vulnerabilities. Enforcement will require the dedication and expenditure of resources. Enforcement is a function of day-to-day performance and is not discussed in detail here. However, the cost should be evaluated prior to selecting and implementing countermeasures.

Keys to Success—Step 6

- The team should resolved vulnerabilities and made corrective recommendations to eliminate or control risk.

Step 7—Mitigation Tracking and Monitoring and Audit of Implemented Countermeasures

This final assessment step involves monitoring implementation of recommendations and quality control and audit reviews of implemented countermeasures to assure they provide the desired effect and have proven system efficiency. This analysis should examine whether additional vulnerabilities have been generated from implementation of countermeasures and controls. This should be completed at specific range gates (e.g., one year) after action item closeout.

Post Risk Assessment Follow-up Tracking and Monitoring

The owner should do the following:

- Review team recommendations and prioritization. If necessary, revise prioritization in consultation with the RA team leader.
- Recommend alternatives in addition to those proposed by the team. If higher risk scenarios are identified, notify the RA team leader.
- Prepare a Risk Management Summary Report that includes an action plan addressing team recommendations, assigns people to implement specific follow-up actions, and has management approval. The team leader and both the Senior Security Advisor (Risk Management) and Regional Security Business Center RMCs should be provided a copy.
- Report critical safety, health, and environmental concerns identified by the team to affected personnel.
- Steward the implementation plan and provide the team leader and RMCs with status reports.

- Communicate changes in the follow-up plan to the RA team leader and the RMCs.

Risk Assessment Draft Review—The owner should review the draft RA report with a view toward "error of fact" analysis and reevaluate risk priorities. During the review process, risk calculations may be modified. However, when the final draft report is issued, no further risk calculation should be allowed.

Final Draft RA Report and Action Plan—Within two months of receiving the final draft, owners should develop an action plan that addresses team recommendations. If a recommendation is rejected, owners should document the justification and develop alternatives to all risk index (SSRI) ratings 1 or 2. The action plan for addressing recommendations—and/or new alternatives—should consist of actions to be completed, resource requirements, responsible personnel (assignees) for each action, and a schedule for anticipated completion dates. The plan should also document use of any outside resources.

The owner should identify assignees and their respective responsibilities in RMSR documentation. The owner must clearly communicate information and expectations of performance relating to follow-up actions to each assignee. The RMCs have region-wide responsibility. Owners are responsible for providing the RMCs with follow-up documentation, including identification of assignees and their respective responsibilities.

Once approved by RMCs and management, the follow-up plan should be implemented in accordance with specific change-management procedures. It may become apparent through these evaluation cycles that risk severity and probability have changed and those action plans may have to be reevaluated.

A communications plan is a required element of each risk assessment and should be included as an "action-list item" in the RMSR. The owner is responsible for developing and implementing this plan, as well as determining its form and content. The purpose of the communications plan is to increase risk awareness and commitment to improve security and safeguards, as well as to inform relevant management, contractors, and security staff of the status of risk assessment elements. In support of the communications plan, owners should closely monitor integrity-critical items with appropriate personnel throughout the development of the RMSR. Scenarios that have an impact on specific operations (e.g., emergency response) should be communicated to staff in charge of those units.

Changes—Organizational procedures specifically address change management. In accordance with published change management procedures, modifications in operations may require a recycle of previous RAs or an entirely new assessment when a change results in a situation (e.g., creates new vulnerabilities) that has not been addressed by earlier assessments. The change procedure should document risk aspects of change. If change is considered significant, constitution of a formal RA team may

be required. Examples of "significant change" include major modifications; new standards, regulatory mandates, and laws; political/community changes; and new technology. A revision process should also be initiated when new information alters planned follow-up activities. The process for revising the original assessment and the owner's follow-up plan should do the following:

- Charter, in concert with line management and the owner, a new RA to verify changes to the original risk index.
- Verify risk index ratings with the original team leader(s).
- Develop a response plan that notifies appropriate management.
- Incorporate the response into the follow-up and tracking process that clearly identifies revisions to original recommendations.
- Provide copies of the plan to the RMCs.

Transition Management—An important element is transition of risk findings from one operational or activity phase to another. This transaction ensures that responsible individuals continue to be assigned to follow-up and closeout risk mitigation activities, throughout the entire life cycle of the project. The owner should prepare a memorandum documenting or referring to all necessary follow-up and closeout activities and forward it to the new owner, assignee, security management, and the RMCs.

Addressing Higher Risk (Levels 1 and 2)—The owner should report all higher risk scenarios' action items to security management and the RMC within a reasonable time of the assessment. This can be a formal request to continue operations despite the identified high risk or a memorandum notifying management of the higher risk levels inherent in continued operations. As previously indicated, it is important that contingency planning be part of the risk management process where significant risk is accepted.

The SSQRA software produces a weighted sum calculation that prioritizes risk assessment recommendations. In some cases, the owner may have to adjust these prioritizations in light of data that may not have been available to the team (such as budget resources). However, owners must remain cognizant of risk reduction objectives when altering priorities developed by the risk assessment team. Any changes owners make to prioritized risk ratings must be communicated to the team leader and the RMC.

The Business Center Security Manager in consultation with RMCs should approve reductions in risk evaluations to lower levels attributable to proposed prevention or mitigation measures. Approval of risk reduction by management should be documented in writing and sent to the RMC for inclusion into a risk management summary report containing risk-related libraries, management response and follow-up plans, and current status of follow-up plans being implemented.

The RMC should include all higher risk scenarios in quarterly and annual status reports along with documented management responses.

Monitoring and Tracking Follow-on Process—A system should be in place to ensure that mitigation recommendations receive proper attention so that risks are adequately addressed. The RMSR serves as the tracking system. The status of each action item should be monitored until formal closeout or circumstances have changed where any remaining action item no longer relates to unacceptable risk exposure (such as completion of a project phase or cessation of facility activity). In addition, the status of risk assessments that have been undertaken and risk assessments still planned should also be monitored and reported quarterly. All of these action-item and status reporting activities constitute the tracking and closeout system. The system depends heavily upon both owner and action item assignee input. Security owns the tracking system and the Senior Security Advisor (Risk Management) is the administrator.

Responsible and Accountable Resources—RMCs, working with the owners, are responsible for establishing, monitoring, communicating, and maintaining the follow-up plan. RMCs should ensure that procedures are in place and that periodic updates and verification of those procedures occur. Both the risk assessment owners and the RMCs must approve any changes to the risk management procedures.

Verification and Measurement—RMCs are responsible for evaluating follow-up plan effectiveness at least yearly. Checks should be made to determine if assessments and follow-up activities have occurred as planned and can be easily measured using automated tracking tools (such as SSQRA). Annual verification to assure that the follow-up action plan is providing high-quality results should be performed through formal interface with owners and end users. Other elements that help contribute to the effectiveness of evaluations include these:

- Reviewing risk assessment logs held by RMCs with special emphasis placed on examination of unacceptable risks.
- Involving non-security staff in risk assessment reviews.
- Conducting field compliance reviews by both security and non-security staff.
- Monitoring the total number of identified risks.

Reports—An electronic copy of all assessments should be made available to the RMCs for input to the tracking system. The RA reports are the starting point for the tracking system. The RMC should inform involved security of due dates, format, and the collection mechanism used for periodic status reports. The formats of the RA and the RMSR are incorporated into the SSQRA software and used to document RA results and follow-up plans. The SSQRA software will also reflect action-item closeout.

RMCs should prepare updated quarterly and annual RMSRs for distribution to Security Business Centers and the Senior Security Advisor (Risk Management). The quar-

terly reports should contain updated RMSRs from all open risk assessments in the Security Business Centers with a cover memorandum that identifies the total number of open recommendations, closed recommendations, and the number closed during the quarter. Distribution of these reports should also include outside elements, such as safety programs.

The content of the annual status report should be the annual equivalent to the quarterly status report. The Senior Security Advisor (Risk Management) should make a presentation to senior management periodically (at least annually) providing an overview of major assessments held, major action items, and the status of those items.

Closeout—Once mitigation countermeasures have been implemented, the owner should close out the follow-up plan. This report should describe the major action items that resulted from the assessment, any major changes experienced in implementation, and any experience that may be worthwhile for future assessments.

A copy of all closeout reports should be sent to the Senior Security Advisor (Risk Management) and Regional RMC. They should log closeout reports into the database and inform management as to the status, especially those actions mitigating high risks.

Keys to Success—Step 7:

- Monitoring should be in place to assess corrective action effectiveness and to detect unexpected new vulnerabilities.
- Risk should be recalculated after countermeasures are evaluated. (See table that follows.)

Severity Levels

SEVERITY	CHARACTERISTICS
I	Loss of life, loss of critical proprietary information, loss of critical assets, significant impairment of mission, loss of system.
II	Severe injury to employee or other individual, loss of proprietary information and physical equipment resulting from undetected or unauthorized access, unacceptable mission delays, unacceptable system and operations disruption.
III	Minor injury not requiring hospitalization, undetected or delay in the detection of unauthorized entry resulting in limited access to assets or sensitive materials, minor mission impairment, minor system and operations disruption.
IV	Less than minor injury, undetected or delay in the detection of unauthorized entry with no asset loss or access to sensitive materials, less than minor system or operations disruption.

Undesired Event Probability Categories

PROBABILITY CATEGORY	LEVEL	SPECIFIC EVENT
A	Frequent	Possibility of repeated incidents
B	Probable	Possibility of isolated incidents
C	Occasional	Possibility of occurring sometime
D	Remote	Not likely to occur
E	Improbable	Practically impossible

Risk Assessment Matrix

SEVERITY CATEGO-RIES	PROBABILITY OF OCCURRENCE				
	(A) Frequent	(B) Probable	(C) Occasional	(D) Remote	(E) Improbable
I	IA	1B	IC	ID	IE
II	IIA	IIB	IIC	IID	IIE
III	IIIA	IIIB	IIIC	IIID	IIIE
IV	IVA	IVB	IVC	IVD	IVE

Safeguards & Security Risk Category (SSRC)		Safeguards & Security Risk Index (SSRI)	SSRI Number
IA, IB, IC, IIA, IIB, & IIIA		Implement countermea-sures that reduce risk to an SSRI of a level 2, at a minimum	1
ID,IIC,IID,IIIB,& IIIC		Not acceptable without management reevaluation	2
IE,IIE,IIID,IIIE,IVA, & IVB		Acceptable with review by management	3
IVC,IVD, & IVE		Acceptable without re-view	4

Resource 2-8: Concise Vulnerability Analysis

Step 1: Identify critical assets/vulnerabilities

- Critical assets: if unavailable, continued business operation not possible or seriously interrupted
- Critical assets may include
  - People
  - Buildings, facilities, and property
  - Process equipment, machinery, tools, office equipment
  - Material storage and warehousing facilities
  - Information: products, supplies, financial, process, HR
- Vulnerabilities may include:
  - Vehicle access to tank/container storage
  - Access to water supplies and discharges
  - Access to electrical & communication lines, public way, etc.
  - Access to business records
  - Access to people; directly, through mail
  - Access to finished products and raw materials

Step 2: Conduct a threat analysis

Identify threats for each critical asset and vulnerability

- Theft of equipment (e.g., computers)
- Loss of containment (hazardous material)
- Mail/postal threats
- Bomb threats
- Workplace violence or assault
- Theft of confidential information
- Trespassers vandalizing, setting fires, impacting equipment
- Theft or destruction of system documentation
- Product contamination and tampering
- Hands-off threats, such as cutting off electricity, telephone, or computer network, or contaminating water or HVAC

- Activists disrupting plant operations
- Attacks as part of chemical or biological terrorism

Consider individuals and groups with special interest in stopping, disrupting, or destroying business activities.

Step 3: Assessing Security Risks

- Compare assets/vulnerabilities to threats
- Evaluate the likelihood and severity of threats against assets and vulnerabilities
  - Use criteria as a baseline
  - Consider other factors pertinent to business or operation
- Identify scenarios for evaluation when multiple levels or redundant levels of security are suggested
- For chemical operations, consider process hazard analyses findings

Likelihood considerations:

- High
  - Operations readily visible to the public
  - Industry or business with history of negative publicity
  - Operations known to handle hazardous materials;
  - Operations are physically accessible
  - Operations lack visible sophisticated security systems
- Medium
  - Operations known in the community, but not prominent
  - Industry or business has received some recent publicity
  - Operations handle moderate volumes of hazardous materials
  - Operations have limited accessibility
  - Operations have some level of visible security systems
- Low
  - Operations generally physically isolated from the public
  - Industry or business has not received publicity
  - Small amounts of hazardous materials handled
  - Operations are inaccessible or shielded from public view
  - Visible evidence of security activity all times

Severity consideration

- High—A security incident that may result in
  - Threat to life or health of people
  - Property loss, cleanup costs, information or technology loss, or other business disruptions in excess of $250k
  - Direct loss in market share
- Medium—A security incident that may result in
  - Property loss, cleanup costs, information or technology loss, or other disruptions between $50k and $250k
  - Loss of sales that will be recovered within two months
- Low—A security incident that may result in
  - Property loss, cleanup costs, information or technology loss, or other business disruptions below $50k
  - No loss in sales or market share

Resource 2-9: Security Vulnerability Assessment

What questions will this Security Vulnerability Assessment Address:

- **What do we want to protect?**
- **Why do we want to protect it?**
- **What is the consequence of an attack?**
- **Is it likely to be attacked?**
- **Who are we protecting it from?**
- **How do we protect it?**

Security Vulnerability Assessment Objectives

The objective of this Security Vulnerability Assessment (SVA) is to conduct an analysis to identify security hazards, threats, and vulnerabilities facing a fixed facility handling hazardous materials from malicious acts, and to evaluate the countermeasures to ensure the protection of the public, workers, national interests, the environment, and the company. This SVA meets the requirements of the Center for Chemical Safety (CCPS) and the American Chemistry Council (ACC).

Security Vulnerability Assessment Scope

1. The analysis of the following security events involving malicious acts with hazardous materials at a minimum:
    a) Theft/Diversion of material for subsequent use as a weapon or a component of a weapon
    b) Causing the deliberate loss of containment of a chemical present at the facility
    c) Contamination of a chemical, tampering with a product, or sabotage of a system
    d) An act causing severe degradation of assets, infrastructure, business and/or value of a company or an industry.
2. All site operations that may involve the four malicious acts mentioned in 1 above.
3. The SVA includes the analysis of both internal and external attacks.

SVA Team Composition

The SVA team has to include skilled individuals to provide sufficient knowledge, experience, and perspective to adequately analyze the security related hazards. The team leader should have knowledge and/or prior experience of SVAs and be impartial.
At a minimum, the SVA team needs to have people on it that possess the following knowledge and/or skills:

- Security vulnerability analysis procedures and methods
- Security procedures, methods, and systems
- Process safety
- Knowledge of the site under study including:
  - Potential hazards associated with the process chemistry, raw materials, finished goods, and the physical location of each
  - Process and equipment design basis.

Other skills, which the SVA team should consider as appropriate, are:

- Military doctrine, especially in terrorism, weapons, targeting and insurgency/guerilla warfare and knowledge of weapons of mass destruction (WMD)
- Adversary characteristics and capabilities knowledge, especially of trans-national terrorist groups
- Safety and industrial hygiene
- Environmental engineering.

Security Vulnerability Assessment

Facility: **Date:**

Initial Security Screening Result:

Facility Type (per Standard 01.21.06):

Team Composition		
	Name	**Function** **Security, Process Safety, Site Managers, Engineering/Operations, etc.**
1		
2		
3		
4		
5		
6		

Facility

Documentation

	Check if used
Plot Plan*	
Available Crime Data	
Regulatory Submission (RMP – US, SEVESO – EUROPE, etc.)*	
P&ID	
Process Flowsheet	
Emergency Procedures*	
Security Procedures*	
Computer/Control/Communications (Cyber attack issues)	
Utility Issues (e.g. – critical CW supply)	
Existing Security Profile/Incidents*	
Any Previous Security Review	

* Minimum Requirements.

Documentation Requirements

The SVA program documentation should ensure that all information required for the SVA team to properly assess the security vulnerabilities of the site is identified and made available as required for the SVA. Examples of standard information/data includes lists of hazardous materials and their locations and uses, material characteristics, facility plot plan, description of existing security program and protections, etc.

Facility Staffing

Total number of employees and contractors:

Total number of employees and contractors per shift:

Number of employees and contractors per shift by location (e.g. – Plant 1, tank farm)

Location	Number of Employees

Existing Security Systems

Using the checklist below, assess the existing security at the facility.

- **Site Perimeter** - What is the construction and condition of your facilities perimeter? (e.g. chain link fence, razor wire, poor condition in many locations, etc.)

- **Access Control -** How do you permit vehicles and persons to enter and exit through your facility? (e.g. automated vehicle gate controlled through a phone or intercom, photo ID Cards, electronic card access, manual gate controlled through security officers, visual inspection, etc.)

- **Lighting -** How would you rate the effectiveness of your facilities lighting? (e.g. good at gates, poor along perimeter, good around production areas, poor near product storage areas, etc.)

- **Alarm/Intrusion Detection Monitoring -** Does your facility have any alarm/intrusion detection system in operation? If so, what type of system is it, and where is it in use? (e.g. product storage, perimeter, buildings, etc.)

- **Uniformed Security Officers -** Does your facility have uniformed security officers on site to manage security? If so, what is the name of the company, how many officers, and what is their work schedule? (e.g. 2 officers, 24hours a day, etc.)

- **Closed-circuit Television Systems** - Does your facility have any security cameras in operation. If so, how many cameras, where are they deployed, and who monitors them? (e.g. 2 cameras, 1 at main gate, 1 at loading dock, monitored at control room, etc.)

- **Product Storage and Security -** How does your facility store the majority of its hazardous, toxic or flammable products? Are there any additional security precautions taken to better protect these products? (e.g. open dock, enclosed buildings, trailers, increased lighting, locked cages, etc.)

- **Previous Security Concerns or Activities -** Has your facility experienced any security concerns or incidents such as theft, vandalism, unauthorized entry, threats of violence from external persons, etc.? If so, what type of incidents and how many times have these incidents occurred?

Hazard Identification and Consequence Evaluation

1. General

The next few pages cover the identification of hazards and an evaluation of the potential consequences of terrorist attack. The SVA should ensure that all four CCPS key security events are considered for each target to the worst -case basis. Consideration should also be given to consequences resulting from cyber terrorism. For the event of 'loss of containment', for example, this means that the SVA assessment of consequences should possibly go beyond the worst-case scenarios, events, and assumptions that govern accidental release scenario definition in process safety activities. For example, it is generally assumed that accidental release worst-case scenarios involve the release of the contents of only the largest volume of hazardous substances at the site. In a SVA, engineering judgment should be used to consider if it is credible to assume multiple items of equipment should be assumed to be included in the scenario, e.g., several storage tanks damaged and releasing material instead of only the largest one. For theft, this might mean a sufficient amount of hazardous materials is stolen that would pose a significant risk to the public from the subsequent manufacture of chemical weapons.

2. Critical Asset Identification

- **The SVA program documentation should ensure that the determination of critical assets includes people, facilities, information, operations, and activities.**
- **Specific chemical assets, such as those on regulated chemicals lists (e.g. EPA RMP covered chemicals list, or SEVESO chemicals list) as well as possible terrorist threat chemicals identified by the FBI or other law enforcement agencies, and lists of chemicals that may be used for Weapons of Mass Destruction (WMD), should be considered. Those chemicals covered by other accidental release prevention programs, such as OSHA's Process Safety Management (PSM), and country or state process safety programs, should be considered.**
- **Other toxic, combustible, flammable, or reactive materials onsite should be included, particularly when the inventories of the materials are large enough that they would cause severe offsite harm if released or be used as weapons of mass destruction if stolen or diverted or if they otherwise may pose an attractive target.**

3. Internal and External Threat Identification

- **The SVA requires a qualitative, analytical method for threat identification that is rigorous, systematic, and objective. This may include a list of possible adversaries and their capabilities.**
- **The SVA should qualitatively judge the level of threat against the site.**
- **Absent specific threat information, the SVA can still be applied based on assuming general capabilities and characteristics of a typical adversary from the ones mentioned above. This would include armed intrusion, criminal activity stealing our**

materials, and other threats to the workforce. Internal threats from, for example, disgruntled employees should be considered.

Facility Hazard Identification

Yes **No**

EPA RMP submitted

Yes **No**

SEVESO

Other Regulation: _____

Yes **No**

APCI Chemical of Concern Present at site?

Chemicals of Concern

Chemical	Quantity (pounds, Kgms)	Hazard	Impact*

Impact: Off-site, theft, product contamination, business interruption

Consequence Evaluation

Off-site impact

		Worst Case Scenario		*More Realistic Scenario*		
Chemical	**Hazard**	**Distance in miles**	**Population impacted**	**Distance in miles**	**Population impacted**	**Evaluation Source (e.g. – EPA Submittal, Engineering Judgment)**

Consequence Evaluation

Theft, Product Contamination, Business Interruption

Chemical	Hazard	Consequence

Plot Plan

Identify areas containing Chemicals of Concern and critical control/utility areas on the plot plan. Number these "Areas of Concern" for use later. (Note: Identify location relative to fence line, loading docks, manned operations, roads, etc.)

Potential Attack Scenarios for Plot Plan Areas of Concern and Existing Security Counter Measures

For each "Area of Concern", describe the area, describe potential methods that terrorists (insiders or outsiders) might cause problems and also describe what existing security countermeasures would prevent that scenario.

Plot Plan Area of Concern	Description	Potential Attack Scenario	Existing Security Counter Measures

Assessment of Attractiveness of Areas of Concern

This should take into account the attractiveness definitions in Table 1, Appendix I, and the attractiveness of neighboring facilities, waterways, etc. using the checklist in Table 2, Appendix I and Assessment of Attractiveness Factors for product contamination, theft, etc. from Table 3 and 4, Appendix I. This table will help us to ascertain if the "Area of Concern" is an attractive target that could attract a terrorist act (e.g. – potential for large off-site impact, close to major waterway, close to major tourist event).

Plot Plan Area of Concern	Attractiveness from Table 1	Assessment of Attrac-tiveness Factors and Severity from Table 2	Assessment of Attrac-tiveness Factors for Product Contamina-tion, Theft, etc.

Gap Analysis

After assessing what security measures are in place to counteract the scenarios developed earlier, and after assessing the attractiveness of attack for the "Areas of Concern," describe what additional security measures would help to reduce the risk of terrorist attack. Also, describe what engineering or operational measures could be employed.

Plot Plan Area of Concern	Potential Additional Security Measures	Potential Engineering and Operational Measures

Security Program Recommendations

SVA Communications to Management.

SVA recommendations shall be documented and be reported to the Director of Process Safety Integrity in a timely fashion by the Project Manager responsible for the SVA. The Director of Process Safety Integrity shall then be accountable for reporting the recommendations to upper management and for developing a funding plan covering the implementation of the recommendations.

For future projects the SVA shall be performed at the project stage and funding for implementation of the recommendations shall be incorporated into the project scope. Engineering and Operations standards contain details on facility counter- terrorism security requirements and guidelines.

SVA Recommendation Prioritization.

The SVA recommendations shall be prioritized by the SVA team and the Project Manager for the SVA taking into account the risks and difficulty of implementing the recommendations.

SVA Documentation Requirements

SVA documentation containing information for "outside team" review suitable for future revalidation, shall be maintained for the life of the asset. This shall be a highly confidential document with limited distribution to the Corporate Security and EH&S Departments.

Recommendations	Priority	Responsible Person	Completion Date

Appendix I

Table 1

Attractiveness of Target

Description and factors which influence the attractiveness of target to terrorists

1	**A successful attack is unlikely to cause disruption to local economy or local infrastructure. Therefore, an attack is unlikely to create more than limited localized concern or attention.**
2	**A successful attack could cause local evacuations, disruption to local economy, or disruption of local infrastructure. Such an attack would create primarily local concern and attention.**
3	**A successful attack could impact regional economy, disruption of regional infrastructure, or cause extensive property damage. Such an attack would be likely to generate some national concern and attention.**
4	**Facility located adjacent to a major recognizable landmark (e.g., Washington DC, Petronas Towers, Panama Canal, UK Houses of Parliament). A successful attack could impact national economy, disrupt a major supply of a critical material or national infrastructure. Such an attack would create significant national/international concern and attention.**

Table 2

Attractiveness Factors Severity of Attack

Severity of Attack will be estimated by the population density within the radius of the attack utilizing methods required by regulatory requirements. (E.g. - by EPA for RMP "worst case" or "alternative case" scenario submittal requirements.)
Population Impact Greater than*:

	Toxic Scenarios	Flammable Scenarios
1	**Up to 1,000**	**Up to 100**
2	**1,000 to 10,000**	**100 to 1,000**
3	**10,000 to 100,000**	**1,000 to 10,000**
4	**100,000 or greater**	**10,000 or greater**

*Based on US RMP

National or Company Critical Node	**Will loss of the site cause severe economic disruption to:** **Global Economy** **US National Economy** **Region/Major Customers** **Corporation** **Business Unit**
Proximity to Major Transportation Routes and Public Water Supplies	**Will loss of containment threaten closure/contamination of:** **A nationally-critical route/supply** **A regionally-critical route/supply** **A locally-critical route/supply** **Partial impact on any above** **No impact**
Process Chemistry	**Can a single act of Sabotage create a loss of containment:** **Site and beyond – severe** **Site and beyond – limited** **Plant-Process – severe** **Plant-Process – limited** **Other damage – severe** **Other damage – manageable**
Publicly Known	**Is the site well-known and visible to:** **International population** **National population and Press** **Regional Population and Press** **Local Population and Press** **Interested Parties Only** **Publicly Obscure**
Other Factors	**Are there other factors impacting site vulnerability** **E.g. – Media attention, local public concern, public authority concern**

Table 3

Product Contamination Attractiveness

	Relative Severity of Product Contamination
1	The contamination of a product results in serious injury and/or has a local impact.
2	The contamination of a product results in loss of life and/or serious injury and/or has a local impact.
3	The contamination of a product results in loss of life and/or serious injury and/or has a regional impact.
4	The contamination of a product results in major loss of life and/or serious injury and/or has a national impact.

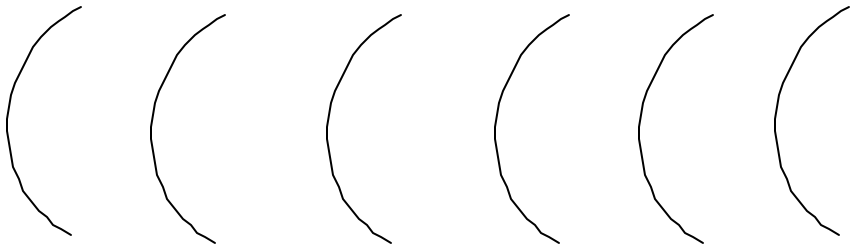
Table 4

Stolen/Misused as WMD or Precursor to WMD

	Relative Consequences for Stolen/Misused Products Used as WMD or Precursors to WMD
1	Product/products in easily transportable containers that can be used directly as WMD or as a precursor to WMD. Ability to directly impact up to 10 people by worst-case scenario.
2	Product/products in easily transportable containers that can be used directly as WMD or as a precursor to WMD. Ability to directly impact from 10 – 100 people by worst-case scenario.
3	Product/products in easily transportable containers that can be used directly as WMD or as precursors to WMD. Ability to directly impact from 100 – 1000 people by worst-case scenario.
4	Products/products in easily transportable containers that can be used directly as WMD or as precursors to WMD. Ability to directly impact >1000 people by the worst-case scenario.

Appendix II

Levels of Security



Background Checks
- Employees
- Contractors

External Intelligence
- FBI
- State Police
- Local Police

Perimeter Barriers
- Fencing
- Gates

Surveillance
- Electronic
- People

Operating Safeguards
- Locks
- Minimizing inventories

Engineering Design Integrity
- Location of sensitive equipment

AIR PRODUCTS

7

Appendix III

Appendix III contains a list of Chemicals of Concern (this is derived from EPA RMP FBI WMD and chemicals of special concern for the Corporation).

3. Implementation of Security Measures

Management Practice 3

Development and implementation of security measures commensurate with risks, and taking into account process design, material substitution, engineering, administrative and process controls, prevention, and mitigation measures.

Companies will take action when they identify and assess potential security risks. This may mean putting additional or different security measures into place to provide greater protections for people, property, products, processes, information and information systems. At facilities, this can entail measures such as installation of new physical barriers or modified production processes (often referred to as inherently safer approaches). In product sales and distribution, this can entail measures such as new procedures to protect Internet commerce or additional screening of transportation companies.

The following samples are intended to stimulate thinking and offer helpful ideas on code implementation. Other approaches not described here may be just as effective or even more effective for a particular company. If a company so chooses, it may adopt any of these sample strategies or may modify them to fit the company's unique situation.

Resource 3-1: Identification of Security Measures

Identify Protective Measures

- Security measures focus on prevention and deterrence
  - Physical security measures
  - Policies and procedures
  - Management systems
- Physical security measures
  - Perimeter protection; physical barriers (fences); intrusion deterrence (lighting, open visible spaces around facilities)
  - Access control; identify all entrants (access cards, guards); sign-in/out and escorting; vehicle controlled access points
  - Identifying and securing all sensitive information
  - Signage to direct visitors and contractors
  - Off-hours intrusion alarm
  - Security guards
  - Special barriers and monitors for sensitive areas
  - Means to protect computer systems from intrusions
- Policies and Procedures
  - Annual security information to employees
  - Pre-screening of employees and contractors
  - HR policies: weapons, violence, employee termination
  - Emergency response plans and crisis management plans
- Management systems
  - Current plans identifying key activities & responsibilities
  - Clear accountability for security at all levels in the organization
  - Periodic (e.g., annual) audits of security systems and policies
  - Dialogue with law enforcement and referral policy
  - Systems to report and investigate security breaches

Identify Countermeasures

- Countermeasures: minimizing loss from an incident
- May require coordination with emergency and crisis communications plans
  - Prompt implementation of remedial actions

  - Notification of consequences and contingencies
- Countermeasure consideration
  - For chemical operations, refer to process hazard analysis findings on countermeasures considered
  - Review emergency plans for specific pre-planning activities
  - Review disaster recovery/crisis management plan for critical business functions; data recovery systems; alternate suppliers; facilities to maintain basic business operations identified; succession planning; public relations plan

Resource 3-2: Key Security Plan Elements

Site Security Coordinator

- Coordinates plan development
- Oversees plan implementation
  - Works with affected departments
  - Works with site management to set accountability
- Establishes rapport with law enforcement
- Coordinates security activities with site emergency plan to assure protection of people, property, and information in the event of an emergency
- Conducts periodic (annual) audit of site security

Access Control

- Site defines controlled areas: production areas (tanks, equipment), warehouses (raw materials, products), offices (business information), utilities (water, power)
- Access control into controlled areas includes:
  - Clearly visible signs directing all visitors and vehicles
  - Check that vehicles/entrants are expected and authorized
  - Safety and security briefing provided to all entrants
  - Mandatory visitor sign-in, sign-out, and escort (no escort may be needed with successful background screen)
  - All visitors provided with/wear an identification badge
  - Employees follow ID badge requirements
  - Controlled areas have physical barriers
  - Barriers that do not impede emergency egress from facilities
- Access points should provide clear and remote viewing

Employee/Contractor Security

- Employee background screening
- Contractor employee screening (non-escorted)
  - Includes temps, cleaning services, drivers, etc.
  - Procedures must be at least equivalent to site procedures
  - May be conducted by contractor, must show evidence

- Existing HR policies that must be in effect:
  - Employee termination
  - Access to EAP
  - Workplace violence
  - Prohibiting weapons on all company facilities
  - Protecting confidential business information
  - Internal incident reporting systems
  - Disciplinary procedures
- Incidents with illegal/criminal activities referred to law enforcement promptly; Legal and HR notified

Other Plan Elements

- Annual evacuation/emergency drills consider security
  - Securing information and equipment
  - Visitor sign-in book to account for non-employees
- Annual employee information on site security
- Backup power systems for intrusion alarms and safety systems
- Reporting and investigating security systems (use existing incident near-miss reporting systems)
- Perimeter protection and deterrence: lighting, fences, exterior walls, gates to block vehicles
- Off-hours protection to include at least one of the following:
  - Supervised intrusion alarms
  - Contract security guard, frequent random tours
  - Frequent random security tours by supervisors

Resource 3-3: Security Handbook

Security Measures Handbook for Site Managers

Level B (defined below)

Introduction and Purpose

ABC Corporation has always been committed to providing reasonable and effective security for the protection of our people, information, and property. In light of the change in security conditions taking place since the events of September 11, 2001, the company has determined to revise, where necessary, the estimate of "reasonable and effective security" measures. The company will apply those new or modified measures necessary and appropriate in order to provide for the security of facilities, and to provide for the security of those who may be affected by a terrorist attack on a company site. The company will undertake revisions/upgrades to security at those locations, which, by their nature and/or location, now require a higher level of protection.

The company will apply the security principles outlined in this document and in other sources appropriate to the level of risk associated with each given location. Site management, working in conjunction with the corporate security department and supported by other corporate staff as necessary, has developed site-specific security measures based on this guiding concept of security:

> *To DETER an attack if possible, to DETECT an attack if it occurs, and to DELAY the attacker until the appropriate authorities can intervene.*

This handbook has been developed to address the myriad issues inherent in providing a secure environment for our personnel and our communities. In order to ensure security at all company locations, and particularly our production sites, it is imperative that each site address security in a logical and systematic process.

No two sites are the same in terms of personnel, location, products, materials, or security structure. Therefore, the vulnerability of and threat to each site is different. It is with these basic understandings that this handbook was developed.

Threat Assessment and Vulnerability Analysis

Following the September 11 attacks, the company conducted a thorough "Threat Assessment" of our facilities. It was based on

- Ecology & Safety Audit—Hazard Potential Assessment
- Corporate Security—Security Vulnerability Assessment

The Hazard Potential Assessment consists of three components:

- Hazardous Substances

- Reaction Chemistry and Process Parameters
- Hazards of Location (population, waterways, etc.)

The Security Vulnerability Assessment was comprised of the following:

- Target Value Assessment
- Attack Consequences Assessment

The tools employed in completing these assessments are available through both corporate security and corporate ecology.

Site Classifications

Based on the results of the threat assessment and vulnerability analysis, each company facility in the United States has been placed into one of three categories:

- Level A—Sites where the highest level of threat is present, so these are the sites requiring the greatest level of security. There are very few such facilities.
- Level B—Sites where the level of threat is clearly greater today than before 9/11, so these sites may require a significant increase in the level of security. There are a about a dozen such facilities.
- Level C—Sites where the level of threat is probably greater today than before 9/11, but not substantially so. These sites may require some increase in the level of security. Most sites are in this category.

This handbook describes the specific security measures which may typically be applied at a Level B facility.

Material Classifications

In addition to sites, the corporate staff has evaluated the risk associated with certain materials used in, produced, or otherwise handled by our facilities. A small number of chemicals, especially those generally associated with the production of chemical weapons, are being placed under significantly greater security control. Several others are being controlled more carefully than in the past, but not to the same degree. All other chemicals are handled in accordance with the principles of Responsible Care®, albeit with an even greater care than before 9/11.

Like the sites, chemicals have been categorized as

- Level A—Requiring the greatest degree of control and security
- Level B—Requiring increased control and security
- Level C—Requiring increased dedication to Responsible Care®

Those sites holding Level A and/or B chemicals will be contacted directly and should anticipate increased security requirements surrounding those chemicals.

The company employs a basic security principle—deter, detect, delay—to establish the minimum reasonable level of security for each site, based on that site's evaluated risk level. It is the responsibility of each site to apply these principles and, in so doing, to achieve security standards in a way that best assures the reasonable security of the site, the surrounding community, and the company.

General headings are:

I. Physical Security & Access Control

II. Personnel, Property & Vehicle Control

III. Loss Prevention & Control

IV. Control Rooms & System Security

V. Crisis Management & Emergency Response

VI. Policies & Procedures

Implementation—Level B Facilities

Site management should review this guide in order to gain insight into both the objectives of a security program, and the techniques used to implement a program. It is not necessary or appropriate to become an "expert" on securing your facility; the corporate staff is responsible for providing that expertise to you. It is, however, appropriate to initiate procedural changes where they would clearly yield beneficial results and to prepare for a detailed discussion (with the corporate staff) on changes that may be required due to the changed threat to our facilities.

A key element in that preparation is to review the site operations and layout in order to identify the following:

- Potential target areas within the facility, such as key storage vessels, process equipment, and utility systems
- Chemicals that are of concern due to volatility, toxicity, or usefulness in the preparation of weapons
- Safety and emergency response systems and equipment that would be crucial in containing/mitigating the consequences of an attack

This guide provides a list of potential measures aimed at achieving the stated objectives. While most Level B facilities will require security upgrades, it is anticipated that extensive projects will not be required in many cases. In order to achieve the stated security principle, the typical Level B facility will have to increase the following:

- procedural measures (such as the inspection of inbound vehicles, restricting parking to non-operating areas, etc)

- security (such as patrolling or electronic surveillance of the perimeter, increased lighting, etc.) so as to raise the apparent level of security for the facility

The typical Level B facility should have a security program with a high deterrent value.

I. Physical Security & Access Control

Objective

The objective of physical security and access control is to

- Gain and maintain knowledge and control of all personnel and material entering or leaving the site and
- Deter, detect, and delay an intrusion

Discussion

In order ensure that the physical space in which you are operating remains under your control, you must know who and what is in it. Attaining this objective is greatly simplified or greatly complicated by the physical layout of the facility, and by the size, structure, and use of the facility. The typical measures employed to achieve this objective are as follows:

- Perimeter protection, including fencing, walls, landscaping, natural barriers, etc.
- Access control systems, such as card readers, key and lock systems, etc.
- Intrusion detection, including alarm and/or video systems, guard forces, etc.
- Procedures, such as package control, employee screening, visitor escorts, etc.

Perimeter Fencing (Deter/Detect/Delay)

- Fence the site or the developed portion of the site.
- Fence key areas and critical assets .
- Fencing used as a perimeter barrier must be at least six feet in height, plus a one foot top guard of barbed wire, with the angle arm facing out. It must meet the technical specifications for chain link fencing established by Corporate Engineering. (Generally, 11 gauge chain-link fence, 6' high with tube steel galvanized members, set in concrete, to include a 1' barbed wire top guard, and top and bottom wire for stability.)
- In the case where a building façade is part of the perimeter, provide appropriate locking devices for all windows and doors.
- Consider placing the perimeter under supervision using intrusion detection technology, video surveillance, or both.

Clear Zones/Perimeter Inspections (Detect)

- Maintain clear zones at least five feet wide on each side of the fence line.
- Maintain the zones (no weeds, no saplings growing through the links of the fence, no tree/branch overhangs, etc.).
- Make at least two inspections daily.
- Log the first daylight daily inspection, noting date and any findings.
- Log the first nighttime daily inspection, noting any problems with lighting.

Signs (Deter)

- "No Trespassing" signs posted along the fence line per local ordinance or every 200 feet, whichever is less.
- Signs advising that the premises are under (electronic, security patrol) surveillance as per local ordinance or every 200 feet, whichever is less.
- Visitor directional signs and "Employee Only" signs posted at all possible venues.
- Signs denoting the prohibition of drugs, alcohol, and weapons posted at all visitor, commercial vehicle, contractor, and employee entrances.
- Signs advising that all vehicles entering the facility are subject to inspection.

Buildings as Part of the Perimeter (Deter/Detect/Delay)

- Where buildings, less than two stories, form part of the site perimeter, all doors and windows should be properly secured.
- Where such a building is itself a possible point target (storage of a CW chemical, critical infrastructure, etc.), doors and windows should be alarmed.

Gates and Doors (Deter/Delay)

- All perimeter gates/doors should be properly controlled and maintained.
- Active gates should be kept to the minimum number consistent with safe operations.
- Perimeter doors that do not require entry should be devoid of exterior hardware.
- Double and overhead doors along the perimeter should be secured by an appropriate locking device.
- Where perimeter gates/doors provide immediate access to point targets, they should be alarmed.
- All active perimeter gates/doors should be effectively monitored.

Security Lighting (Deter/Detect)

Level B Sites should provide appropriate security lighting in the following areas:

- Vehicle gates
- Personnel entrance(s)
- Shipping/receiving docks
- Parking lots (employee and contractor)
- Interior point targets
- Outside storage areas
- Security patrol routes
- Rail sidings
- Avenues of approach to the perimeter
- All potential target areas

In addition, the following should be done regarding lighting:

- Perimeter illumination should be sufficient to discourage unauthorized entry and make detection probable should the perimeter barrier be breached.
- Lighting should be sufficient for security officer patrol routes while avoiding easy observation from outside the property.
- Lighting should be sufficient to permit security officers to view the interior of vehicles at all gates.
- All buildings that form the perimeter should have rooftop and/or lighting on poles to illuminate all windows and door areas.
- Light fixtures susceptible to vandalism must be protected by a polycarbonate or similar shield and be sufficient distance/height from the perimeter exterior.
- All lighting fixtures should be on timing or photoelectric devices to ensure they are operational during periods of reduced visibility.
- Critical structures/utilities such as power, water, heat, communications, etc. should be adequately lighted.
- An effective plan must be in place to address maintenance and testing of lighting.
- Where appropriate, consumable components (bulbs, etc.) should be replaced at 95% of rated service life.
- An auxiliary power source for security lighting must be in place and tested quarterly.

Key & Lock Control (Deter/Delay)

- A key control administrator should be appointed in writing
- For issuance/accounting of keys, these procedures should be in place:
  - Key holder list
  - Recovery at termination
  - Accountability
  - Number of masters
  - Issued on basis of need
  - Control of blanks and devices
  - Investigation of loss
  - Replacement of device
- Wherever possible, sites should have a guarded keyway system. The keyway should be exclusive for a radius of at least 120 miles (except cooperating company facilities).
- If a grandmaster, master, submaster system is used, grandmasters must be controlled and limited to only those with an absolute need.
- Key inventories should be performed on an annual basis by the key control administrator.
- Keys must be kept in a secured cabinet or safe.
- Locks must be changed/rotated in critical locations at least annually, more frequently in potential target areas.
- Combinations to safes and vaults should be restricted to personnel with a clear "need to know" and changed when such personnel leave the company or no longer require the combination.

Intrusion Detection Systems (Deter/Detect)

- For buildings that are outside the fence or that form part of the perimeter, protect all exterior doors and windows with an intrusion detection system (IDS).
- The IDS must be monitored by a contracted central station, site security, another company's site security, or local police.
- An IDS is recommended for sensitive proprietary information storage, critical assets, and/or potential target areas.
- The IDS should have at least a 24 hour battery backup.
- Where the IDS is employed in securing Level A chemicals, there must be multiple signal transmission methods and line monitoring.

- The IDS should be maintained, monitored, and tested by the vendor as needed.
- Opening and closing reports should be provided and reviewed as needed.
- Master codes should be kept to a minimum and safeguarded as "confidential."
- Codes for non-company personnel should be monitored and reviewed as needed.
- A procedure is suggested for unscheduled openings/closings.
- A local alarm (such as a horn or klaxon) is suggested.
- False alarms should be investigated, logged, and corrected as soon as possible.
- Systematic false alarms should be reported to Corporate Security.

Video Surveillance Systems (Deter/Detect)

- A video surveillance system (VSS) should be employed for personnel and vehicle entrances, target areas within the site, Level A chemical storage, and access points. Some level B sites should consider extending the VSS to the general perimeter.
- If the system is not actively monitored, a recording system is required.
- Recorded video should be reviewed as needed by Site Security.
- The system should be routinely maintained and kept fully operational.
- In some cases, parts of the system (especially those providing safety-related views) may be monitored by operations/engineering personnel.
- Any system installed at the site must be reviewed/approved by Corporate Security.

Electronic Access Control System (Deter/Detect/Delay)

- An electronic access control system (EACS) should be installed at key locations such as main entrances to administrative, operations, and material areas. Where EACS is employed,
  - The site security representative will be responsible for the management of the EACS, with support from Operations and/or Human Resources as needed, and
  - The control computer must be appropriately protected, both physically and electronically.
- Where intrusion detection and video surveillance systems are used, the EACS should be integrated with those systems.
- Systems must be approved by Corporate Security.
- The number of card readers should be appropriate.

- The EACS should be divided, where appropriate, into different access levels (variations of time, locations, zones, etc.) as designed and approved by site management.
- A procedure should be in place to ensure the timely deletion of terminated employees from the system.
- The EACS should provide records of use (who, which door, when, time, etc.).
- These records should be reviewed periodically by the Site Security representative or other management personnel to detect actual or potential breaches of security.
- The EACS should have an alert feature to warn of unauthorized entry attempts or a "3X refusal" shutdown or other alarm feature.
- The EACS should be capable of expansion to accommodate potential growth.
- The EACS should have anti-passback capability. The site may use or disable this feature according to need.
- Alternatives to an EACS include: use of receptionist or security officer, or locked door and buzzer/intercom/telephone system.

Security Officers (Deter/Detect)

- Security officers should be deployed in a visible manner. At least one officer must be on duty at all times.
- Where possible, security officers should patrol using a tour management system.
- Patrol routes and times should be variable, but the perimeter and point targets should be inspected at least every other hour during darkness.
- Where security officers are contracted through an outside provider, the site must use a standard contract (available through ACC).
- Post orders should be complete, clear, current, and accessible for each post or responsibility covered by the security officer.
- Post orders should cover the following:
  - Visitor control procedures
  - Employee access rules/restrictions
  - Package pass instructions
  - Access to the site during emergencies
  - Use of video surveillance
  - Electronic access control and intrusion detection systems
  - Inspection of the perimeter
  - Inspection of point targets

  - Lighting
  - Locks and other site control features
  - Emergency response procedures
- The site security representative (SSR) should meet with all prospective officers prior to their assignment.
- The SSR must ensure that all aspects of the standard contract, especially qualifications and training, are met by the vendor company.
- Contract security officers should not be used for critical condition monitoring.
- Where company-employee security officers are expected to perform any critical function monitoring, they must receive adequate training from site operations.
- Security officers must receive all necessary and appropriate on-site training for such activities as gate control, access control, inspections, etc.
- Routes and times of security patrols should vary to avoid predictability.
- Security officers should be equipped with appropriate communications devices (two-way radio, cell phone, etc.) in order to ensure their safety.
- These communication systems should be able to be monitored by plant operations if necessary.
- Security officers should be furnished, through the security service provider and/or the company, with the proper equipment to perform their duties.
- Security officers are not to carry or store lethal weapons on company property.

Barriers & Barricades

- Certain point targets, either within the perimeter or outside the operating areas of the plant, may require protection through the use of barriers and/or barricades.
  - A barrier is intended to delay an individual or group of individuals, regardless of how they are traveling. A fence is a barrier.
  - A barricade is intended to stop the approach to a target, and is generally effective only against certain types of travel. A cinderblock building is an effective barricade against someone on foot but is not a barricade against a truck. A "J channel" will stop a truck but not a person on foot.
- Examples of point targets that may require a barrier or barricade include these:
  - Piping, vessels, production equipment, etc. carrying inhalation poisons, explosives, or large volumes of flammables that are accessible to vehicles
  - Pigging stations, etc. outside the perimeter

II. Personnel, Property and Vehicle Control

Objective

To establish positive control over who and what is permitted entry to the site by any means.

Discussion

Control over personnel, property and vehicles passing through the site's perimeter is an essential feature of access control. Control, for the purpose of this guide, will include equipment, building and grounds design, and security practices. Effective control will deter unauthorized personnel or vehicles from entering the facility contrary to the interests of the company. It will deter introduction or removal of any item without the knowledge of or against the interests of the company. Elements of control include those physical security measures discussed above and other measures.

The following measures may be implemented to complement exterior security controls where and when possible. Each site shall have a means of properly identifying non-employees, of determining their need to enter onto the site, and of controlling their movement on site and their exit. The site may restrict access only to those with a legitimate need to enter.

Access for non-employees, including visitors, contractors, and vendors, will be restricted within the site. All non-employee visitors and vendors will be escorted as appropriate.

Employee Controls (Deter/Detect)

- All employees are to be provided with a company-issued photo ID. All personnel at sites of 50 or more employees are required to wear the ID. At smaller sites, the ID must be carried on the person while on company property.
- A management representative will be assigned to issue, control, and recover IDs.
- In operating areas where safety is a factor, other means of identification, such as company supplied work overalls with the company logo and the employee's name may be used.
- Each site should establish an ID card accountability procedure.
- ID Badges should bear a visible code or color indicating which, if any, restricted areas the employee may have unsupervised access to.
- Access should be limited to the minimum required to perform job responsibilities.
- Lost or missing ID cards must be reported by the employee to the site security representative immediately.

- Employee access for off-hours should be limited and controlled through the use of an electronic access control system, security officers, or lock and key.
- All special access/restricted areas should be controlled through the use of electronic access control systems, push-button combination locks, or conventional lock/key.

Visitor Controls (Deter/Detect)

- Visitors should be admitted to the site only where there is a reasonable business need to do so. The site should issue a site policy to that effect.
- All visitor badges must be distinct from the employee, contractor, and temporary worker ID badges.
- Visitor badges must be numbered and controlled.
- Visitors (any non-employees) are required to wear their assigned ID badges at all times while on company property.
- Prior to receiving a badge, visitors must complete the visitor log.
- The visitor log must have the required statement addressing access to company information.
- Visitors are to be escorted at all times.
- Visitors are not permitted in restricted/sensitive areas without the approval of site management.
- Group visits should be approved by the site manager, and the site security representative must be made aware of the visits.
- A roster of all visitors should be submitted one day prior to the visit and include full names of visitors, group represented, and reason for visit.
- Group visitors will not be permitted into areas containing Level A or B chemicals.
- All group visitors should be escorted and remain with the group for the entire visit.

Contractor and Temporary Personnel Controls (Deter/Detect)

- Individuals assigned to the company from companies that provide temporary personnel should be assigned a distinct picture ID card if their assignment is one month or more.
- All contractor and temporary personnel must have been screened in accordance with company policy.
- The temporary employee should be made aware of all relevant company policies and procedures on the first day of his assignment.
- Temporary employees do not require an escort.

- Contractors working within the perimeter for one month or more should be issued and should wear a distinctive picture ID.
- If, due to safety concerns, the badge cannot be worn, the contractor should wear a uniform shirt or other identifier and carry the ID badge with him while on company property.
- Contractors on extended assignment do not need to be escorted.
- If possible, sites should avoid granting unsupervised access to sensitive areas to non-company employees. Where such access must be granted, the site security representative must be advised of the access and the reason it is granted.

Property and Vehicle Controls

Property Pass Systems

- If the site allows for the borrowing and use of company tools and equipment, a property pass system should be implemented.
- A management representative should be responsible for the system and its controls.
- The number of persons authorized to sign property passes should be identified in writing and kept to a minimum.
- Signatures of those supervisory personnel authorized to approve the property pass should be kept on file with the site manager, site security representative, and the authorized personnel themselves.
- A suspense system should be developed that provides for the tracking of borrowed items not yet returned, their condition, etc.
- Items being returned should be carefully inspected before being accepted.

Inspection Programs (Deter/Detect)

- Inspection programs should be initiated after reasonable notification to staff.
- Corporate Security must review inspection programs prior to implementation.
- The following areas should be incorporated into an inspection program: incoming packages, rail cars, visitor vehicles, and commercial vehicles.
- The following areas may also be incorporated into an inspection program: lockers, mail rooms, employee vehicles, and company-owned vehicles

Packages/Briefcases/Lunch Pails

- Sites should inspect incoming packages and containers once notice has been given (signs are sufficient for visitors).

- A random program of package inspections generally requires security officers for implementation.
- Inspections may be full (all packages/containers) or random.
- Random inspections must be truly random—that is, the persons selected for inspection must be selected based upon a verifiable random system.

Rail Cars

- All rail cars (full or empty) should be inspected upon arrival.
- Ensure the seal is intact and matches the paperwork.
- Conduct a walk around looking for unusual items attached or missing.
- Careful attention should be given to the dome, valves, connectors, etc. for vandalism, tampering and/or sabotage.
- Rail cars containing potential target materials (explosives, inhalation poisons) should not be spotted in areas near the perimeter or in easily accessible areas.
- Rail cars containing potential target materials that are spotted in an area visible to the public should be secured (guards or video and security lighting).
- Rail cars with broken/missing seals will be isolated and investigated, and ER should be notified.
- Be aware that the Department of Transportation and certain other regulatory/law enforcement agencies may open seals. In those cases, the agency will replace the seal with its own departmental seal and annotate the paperwork accordingly.
- Report unusual findings to Corporate Security or ER immediately.

Visitor Vehicles

- A random program of visitor vehicle inspections requires security officers for implementation.
- Security officers must be trained on the proper conduct of a vehicle inspection.
- Inspections should include the passenger compartment, trunk, engine compartment, wheel wells, and engine compartment.
- Appropriate equipment (rubber gloves, trolley or stick-mounted mirror, etc.) must be provided.
- If there is no inspection program, vehicles should be parked at least 100 meters from the operating areas of the site and pipelines and vessels containing sensitive chemicals.

Commercial Vehicles

- The site should determine and document which types of vehicles/loads will be granted access, through which gates, during which hours, and under what circumstances.
- All commercial vehicles (bulk, tanker, box trailers, delivery trucks, etc.) should be inspected prior to entering the operations area of the site.
- The driver's ID and/or license and other documentation should be verified before allowing entry to the site.
- Unannounced deliveries should not be accepted without first contacting the shipper or the carrier or using some other reasonable method to ensure the validity of the delivery.
- Vehicle inspections should be performed by security officers where available and by shipping/receiving personnel where necessary.
- A truck inspection should cover the exterior of the tractor and trailer, looking for extra or missing items; the load itself, to the extent possible; places where persons could hide; and any place where weapons or other contraband could be kept.
- If a weapon is found, the shipment should be turned away.
- The carrier should be notified of the incident immediately.
- Corporate security should be notified as soon as possible.
- A vehicle log should be completed for each shipment to the gate. The log should include this information:
  - Vehicle ID numbers (tractor and trailer)
  - Time and date of arrival
  - Time and date departed
  - License plate on the tractor and trailer
  - Driver's name
  - Driver's license
  - Company
  - Bill of lading number
  - Purpose of visit and comment section
- Vehicle directional signs should be clear.
- The signs should include a "weapons prohibited" notice.
- Once cleared into the site, the driver must stay with his/her vehicle or be escorted to a segregated rest facility.

Lockers

- Sites may institute regular or spot check inspection program for lockers.
- Locker inspection program should be conducted by the site security representative and at least one other management or HR representative.
- Where employees are represented by as collective bargaining unit (CBU), a representative of that CBU should be present for locker inspections.
- The locks for the employee lockers should be provided by the company.
- Signs should be posted notifying all employees of this procedure.
- A for-cause search must be approved in advance by Corporate Legal Services or Corporate Security.
- In the case of a for-cause search, a still or video camera should be used during the search process.
- A report should be written noting which lockers were searched, who conducted the search, to whom the locker was assigned, and the contraband items (if any) recovered.
- If the contraband items are criminal in nature (drugs, weapons, etc.), the items should be left as they are and Corporate Security should be notified immediately.
- The police should be notified only after consultation with Corporate Security and Corporate Legal.

Mail Rooms

- Site mail handling procedures should be written to reduce/eliminate the possibility of losing the use of a critical building due to receipt of a suspect substance.
- Sites should reduce personal mail received at the site to the degree possible.
- All outside mail (non-company internal) arriving at the site should be opened at a central facility.
- The central facility should be established so as to allow the air handling for the area to be isolated from the remainder of the facility.
- Mail room and shipping/receiving personnel and/or employees that handle mail and other parcels (FedEx, UPS, etc.) should be briefed in the recognition of suspicious packages and trained in the handling of potentially dangerous items.
- The training program should cover letters and parcel containing bombs, biochemicals, and threatening and/or harassing communications.
- Supplies/equipment should be available to all employees who handle these goods.

Employee Vehicles

- A random program of employee vehicle inspections requires security officers for implementation.
- If there is no inspection program, employee vehicles should be parked outside the operating areas of the site.

Company Owned Vehicles

- A weekly inspection program of company vehicles should be conducted to ensure the vehicles have not been tampered with.
- This inspection should be conducted by the vehicle operators.
- A log should be kept showing the inspection date and time, person conducting the inspection, and comments.
- Company vehicles should parked inside the perimeter and secured during off hours.
- If any unusual items are found, they should be reported to the site security representative or the immediate supervisor as soon as possible. Corporate Security should then be notified by the site security representative.

III. Loss Prevention & Controls

Objective

Establish physical security and procedural control measures to ensure the integrity and the environment in which products, equipment, goods, and information are maintained.

Discussion

Traditionally, "loss prevention and control" refers to proper adherence to company rules and practices governing the conduct of business. The primary focus of controls has been on financial matters, although, within this company, there has been a strong emphasis on safety as well. In the wake of the 9/11 attack, a new emphasis on material control is required. There are, at virtually every site, chemicals and other materials that can be employed as weapons. In some cases, these materials can be used "as is" and are capable of producing mass casualties. It is therefore critical that every company site impose the controls necessary to ensure these materials are not stolen or diverted and used as a weapon.

Building Security (Deter/Delay)

- Operations buildings with valuable equipment, goods, and/or information should be secured during non-business hours.

- Administrative office areas should be secured during non-business hours through, at least, lock and key. Critical areas should be secured through an intrusion detection system.
- Individual desks and offices should be secured during non-business hours.
- Proprietary information should be stored in a lockable container (desk, safe, cabinet, etc.) during non-business hours.
- Keys to all offices should be controlled as noted above.
- Information that could encourage or facilitate an attack on the facility or point targets within the facility should be properly secured.

Restricted Areas (Deter/Delay)

- Site management should identify and restrict access to sensitive areas as appropriate.
- Areas containing Level A and B chemicals should be restricted.
- Control rooms must be designated as "restricted."
- Special access areas such as computer rooms, telephone closets, etc., should be designated as "restricted" and be secured at all times when an employee is not present.
- Computer rooms should be secured in accordance with corporate procedure 018.006, "LAN Room Security."
- The offices housing the Human Resources and Medical departments shall be secured during non-business hours.
- Unsupervised access should be granted only to employees who work in those areas.
- Others, such as cleaning crew and maintenance, should be allowed entry only when escorted.
- A designated employee should check restricted areas at the end of the workday.
- Level A and B chemicals in transportable packaging should be stored in a secure area and monitored through electronic measures, or security officers, or both.

Research and Development Areas (Deter/Delay)

- Research and development areas should be secured during non-business hours.
- Access restrictions to these areas should be in place and enforced.
- Proprietary and/or trade secret information should be secured in lockable containers, such as desks, filing cabinets, or other storage containers.

- Valuable, sensitive, or critical equipment should be accounted for and an inventory conducted yearly.
- Keys should be strictly controlled.
- Sensitive waste should be discarded in a manner that would not disclose crucial research and development work.
- Document trash should be shredded (minimal standard is the strip shredder).
- Computer CDs and diskettes that are considered trash should be destroyed.
- Lab books should be properly accounted for from issuance to completion to storage.
- Notebooks should be numbered and recorded against an employee name upon issuance. Notebooks should be signed, dated, and witnessed.
- Notebooks should be properly secured when not in use.
- Notebooks, when no longer active, should be turned in for documentation and properly placed in secured storage/archives.
- Termination procedures should ensure the timely collection of active notebooks.
- All PCs should be password-protected.
- Research area PCs should be secured against the theft of the PC itself.
- All related CDs, diskettes, and tape backups should be properly secured.

Maintenance Area (Deter)

- Access to the maintenance area should be controlled, at a minimum, by lock and key during operational hours to prevent unauthorized removal of tools and equipment.
- If the area cannot be secured, tools and expensive equipment should be secured in lockable cabinets, cages, or carts assigned to maintenance personnel.
- The equipment/tool loss/replacement history should be monitored by site accounting/management and reported to the site security representative bi-annually.
- Expensive tools and equipment should be received by an employee assigned to the receiving function prior to being delivered to maintenance.
- Where feasible, maintenance should not be able to initiate an order, approve payment, and directly receive materials.
- All maintenance purchase orders should include a plain language description of the item being ordered.

- Maintenance POs should be approved by someone other than the person placing the order.

Receiving (Deter/Detect)

- All raw materials, intermediates, supplies, and equipment ordered by the site should be received by receiving personnel and documented on approved forms.
- All incoming loads should be checked for obvious signs of tampering or having been tainted, such as broken seals, missing components, unexpected powders, etc.
- All "will call" items should be verified by receiving personnel after pickup by other employees.
- Only authorized persons and employees on official company business should be allowed in the receiving area.
- The receiving area, where feasible, should be physically separated from other areas and activities.
- Receiving personnel should be prohibited, if feasible, from involvement in shipping and warehouse activities.
- The receiving area should be occupied at all times by authorized personnel or properly secured.
- Drivers should remain in their trucks or be restricted to a driver's lounge.
- Valuable items susceptible to theft should be delivered promptly, or provisions should be made to secure them awaiting delivery.
- Trucks should be required to leave immediately upon unloading or should be sealed to prevent goods from being stolen, tampered with, or sabotaged.
- An employee should be designated to secure the area at the end of the work day.
- Where sensitive and high value items subject to theft are received on a regular basis, a physical security system should be employed to monitor the area.
- There should be a secure area (cage) in the shipping/receiving area for the temporary secure storage of sensitive or high value items.

Shipping (Deter)

- Shipping and receiving areas should be physically separated where possible.
- A supervisor should be present during hours of operation.
- Drivers should not be allowed to load their own trucks.
- A procedure should be in effect to ensure that employees are assigned to load/unload vehicles to prevent collusion with drivers.

- Shipping areas should be controlled and only authorized personnel allowed in the area.
- Drivers should remain in their trucks or be restricted to a driver's lounge.
- Provisions should be made for emergency shipping (after normal working hours).
- Outbound shipments of sensitive cargoes should be secured with seals adequate to prevent tampering without detection.
- Outbound shipments should be inspected to ensure there are no unexpected powders, etc. which will cause undue alarm when received.
- Seal numbers should be recorded on all shipping and receiving documentation.
- Outbound loads that are awaiting shipment should be secured.
- Security officers, where available, should be informed of the status of the shipment.
- Unloaded vehicles should be pulled away from the dock immediately, sealed to prevent tampering, or required to leave immediately.
- Unloaded railcars should be pulled from docks/terminals and either placed in a holding area or taken off-site immediately.

Pipelines & Valves (Deter/Delay)

- Pipelines and valves outside the site perimeter should be routinely inspected for tampering and/or damage. Pipelines and valves that are company responsibility should be checked as part of the perimeter inspection program.
- Any signs of tampering and/or damage should be reported to plant operations and/or the site security representative as soon as possible.
- Pipelines carrying inhalation poisons through populated areas should be underground or under frequent surveillance.
- Pigging stations for such pipelines should be secured using fences and electronic measures.
- Where possible, pipelines carrying inhalation poisons should be electronically monitored for loss of pressure, and such loss of pressure should cause automatic closure of all isolation valves in the reduced pressure area.

Storage Tanks/Large Vessels (Deter/Delay)

- Where possible, storage tanks and large vessels containing flammable, explosive, or toxic material should have no readily visible identifier to persons outside the perimeter.

- Tanks/vessels containing flammable, explosive, or toxic material and located adjacent to the perimeter, public access road, or residential area may require shielding so as to prevent loss of containment by a person using a rifle, etc.
- Tanks containing flammable/explosive materials that are within the danger area of other such non-company controlled tanks should be insulated and/or have cooling water available so as to reduce the possibility of sympathetic detonation.

IV. Control Rooms and Systems Security

Objective

To establish physical security and procedural control measures to ensure the integrity of control rooms, distributed control systems (DCSs), and process logic controllers (PLCs).

Discussion

System integrity is a critical factor in the security of our facilities. The key feature in our overall system security program is to rigidly restrict access to the system itself. To accomplish this, we rely heavily on control of physical space and physical connections. We assume that any logical security feature can be defeated in time, so adherence to our security practices is essential.

Control Rooms (Deter/Detect/Delay)

Building Security

- Control rooms must be designated as "restricted."
- Control room access should be via an electronic card access system or push-button combination locks.
- A control room sign-in log should be maintained and reviewed monthly by the site security representative.
- Where possible, intrusion detection and video surveillance should be used.
- Badges or other company identifier (uniform shirt, etc.) should be worn at all times.
- Control room should be inspected frequently for unauthorized items by the operations manager or the site security representative.
- Mail that has not been screened and opened must not be allowed into a control room.
- Unscreened personal effects (radios, TVs, etc.) and lunch boxes should not be allowed into control rooms.

Authorized Personnel

- An authorized persons access list should be developed and maintained by the control room supervisors and the site security representative.
- All visitors to control rooms must be cleared by the operations director and the site security representative.

Distributed Control Systems (DCS) and Process Logic Controllers (PLC)

Site Access

- Site access to DCS/PLC should be limited to authorized personnel only.
- An authorized persons access list should be developed and maintained by the administrator/supervisor of each DCS/PLC system.
- Access to the DCS/PLC should be password-protected.
- Override keys should be maintained in a secured location.

Remote Access

- Remote access to the DCS/PLC should be limited to the extent possible.
- Remote access can be granted to only those individuals with a need to know/access.
- This access can be granted only by the site manager or designee.
- All remote access users should use an encryption system for access.
- PCs used for access should be company-provided and should have, as a minimum, firewalls, virus protection, and password protection
- No outside software or standing Internet connections should be allowed.

V. Crisis Management & Emergency Response

Objective

The purpose of the crisis management plan (CMP) is to provide planned response to a wide range of potential crises, define organizational structure with clear roles and responsibilities, establish relationships among various response teams, and facilitate efficient and proactive management of a corporate crisis.

Discussion

The CMP applies to all company entities in the NAFTA Region. It provides a guideline for the corporate-level management of a large-scale, fast-moving crisis. The basic principles and concepts are applicable to the management of any crisis.

Planning

- Each site is required to maintain and update, as required, a list of contacts and telephone numbers.
- The site security representative is to provide to Corporate Security an update of the crisis management security database yearly, and as changes occur.
- Each site is expected to develop and maintain liaisons with local and state emergency services organizations and with local and state law enforcement, especially with those agencies that would respond to a site emergency.
- Each site is required to have a plan for implementation of a site administrative center should a crisis be declared.
- All required elements are required to be contained in the site emergency plan (SEP) and the SEP must be up-to-date and on file with Corporate Emergency Response.
- SEPs are valid for two years from date of publication.

Site Security Representative

- The site security representative (SSR) must be appointed in writing.
- The SSR must ensure that local law enforcement personnel are prepared to respond to an incident at the site, that they have the necessary information about the site, and, where feasible, that they have been trained/familiarized with the site.
- The SSR, in conjunction with the site safety manager, should ensure that a mutually-supportive approach to response issues has been developed for the area, including neighboring facilities and the regional/state chemical manufacturers' association, if any, and information sharing with local/regional law enforcement.
- The SSR should be involved with the development of the SEP and be completely familiar with it.

VI. Policies and Procedures

Objective

All sites must adhere fully to those company policies and procedures relevant to the conduct of security and its related functions.

Discussion

Site policies and procedures should reflect corporate policies and procedures and provide guidance specific to each site.

Policy Implementation

- All sites are required to implement all policies/procedures applicable to the site.
- Where appropriate, waivers to specific clauses or entire policies/procedures may be sought from the policy owner.
- Sites should consider issuing local policies/procedures addressing the following:
  - Security awareness training
  - Termination procedures
  - Suspicious parcel/package procedure
  - Mail handling procedure
  - Inspection procedures
  - Bomb threat procedure
  - Local incident reporting procedure
- Security policies and procedures appropriate for issuance at the corporate level include security policies and procedures regarding physical security and access control, incident reporting, LAN/server room and other data facility security, pre-employment background checks, termination procedures, logical security and data protection (virus, etc.).

Resource 3-4: Technical Security Measures

Scope and Objectives

Cost-effective technical security measures should be based on vulnerabilities identified by applying risk assessment methodology. Technical security systems include CCTV, automated access control, intrusion detection, and explosive detection. Whenever possible, security systems should be integrated with related systems—such as fire and process control—and report to and be managed by a central control center.

Key Procedures

Application of risk management principles will be used prior to implementing security technology.

Wherever feasible, technical security systems should be used to optimize/reduce the use of guards.

Technologies should be commercially available ("off the shelf"), proven, and compatible with the IS technical set in order to ensure a flawless operation.

Performance indicators should be built into procedures developed for all security systems in order that effectiveness can be tested and measured.

Security will do the following:

- Maintain an updated working knowledge of new and emerging security systems and technologies and assist with the development of technical specifications, including the provision of maintenance agreements.
- Support the procurement process.
- Assist with the commissioning process.
- Assist with the development of operating procedures.
- Periodically review technical security systems to ensure continued effectiveness against existing and new and emerging threats.

Responsible and Accountable Resources

Security will be responsible for researching, designing, and deploying technical security best practices.

Major technical security systems will be designed and deployed by the senior security advisor responsible for technical security, in conjunction with the security business center, and delivered by line management.

Security business centers will conduct periodic external reviews to ensure that technical security systems function as intended and are supported by operational procedures.

Verification and Measurement

Procedures should be established in the design phase to enable line management to conduct an annual self assessment of total system performance.

Feedback

Lessons learned should be communicated to line management and actions taken to improve system suitability and effectiveness.

Resource 3-5: Principles, Elements, and Best Practices

The design of a physical protection system requires a methodical evaluation of threat and target identification. Intelligence and community relations programs are an integral component of a security protection program. An effective physical protection system accomplishes its objective by either deterrence or a combination of detection, delay, and response. Deterrence occurs when security measures are perceived by an adversary to be difficult to breech, causing the choice of another target. Deterrence is not effective against a determined adversary and is therefore secondary to systems designed to ensure detection, delay, and response. Security countermeasures should be applied in accordance with the following principles:

- The threat conditions should be defined and documented.
- Physical protection systems should be designed to ensure detection, delay, and response to adversaries.
- All security sensor data and security-related communications should be monitored in a central control center—either at the actual facility or remotely by personnel trained in system monitoring and response.
- There should be a continuous line of security—physical or technical—around the areas to be protected. (Security sensors tend to reduce reliance on staffed checkpoints and may reduce security guard costs.)
- Multiple lines of security should be used to achieve protection-in-depth at critical assets. The system should provide a high probability that intruders into critical asset/entry control areas would be detected.
- Complementary devices using different means of detection (such as a video camera used in conjunction with an alarm) decrease the probability of defeat.
- A maintenance program should be in place to ensure operational reliability of security systems.
- Security systems should perform normally under degraded circumstances through redundancy and non-interruptible power supplies.
- The functional capabilities of security systems should be monitored and improved by operational experience at other facilities.
- Management should periodically review access records of personnel entering or leaving a facility and specific sensitive areas (such as IS assets). In "guardless" buildings or during off-hours, installation of egress card readers should be considered in combination with entry/exit control-point video coverage.
- Emergency preparedness plans should be kept updated to address all aspects of change management, emergency planning, and emergency response. Plans should be tested regularly.
- Staff should interface with security business center advisors.

- Liaison should be made with local law enforcement and other relevant public and private sector entities.

Minimum Protection Requirements

General security system design should include the following:

- Identification of assets requiring protection (facility characterization)
- Identification of specific threats to identified assets (threat definition and target identification)

Detection

- Entry control for both vehicles and personnel (could be automated card access, turnstiles, security guards)
- Intrusion detection—procedural (guards) or technical (external/internal sensors, CCTV)
- Alarms with monitoring/response capability
- Security lighting
- Inspection procedures (packages, mail, vehicles)
- Senior management security (zoned area controls, duress alarms, designated parking)

Delay

- Barriers (such as perimeter security doors, locks, and fences)
- Use of security guards

Response

- Guards, roving/motorized patrol
- Law enforcement
- Security emergency management procedures

Security Best Practices

After review of a variety of sites, the Corporate Security Department has recommended the following best practices for physical security of our facilities:

External Perimeter Fence

Permanent or long-term facility perimeter barriers are either fences or buildings that serve as physical demarcation of protected areas and limit access. The protective force controls the entry control points. This can be complemented by technical security measures.

Fence requirements include the following:

- Fencing must be a minimum of 11-gauge galvanized steel fabric with mesh openings not larger than 2 inches square.
- The barbed tape obstacle outriggers are angled out, away from the secured area, and topped by a minimum of three strands of barbed wire or two or more coils of concertina.
- Fence height is 2.5 meters (8 feet), excluding barbed wire outriggers.
- Ground clearance is maintained at 4 inches or less.

A minimum clear zone of 15 meters is maintained outward from the perimeter barrier, and a corresponding 3-meter clear zone will be maintained inward from the perimeter barrier.

Lighting

Illumination used as a part of the physical protection shall be provided to permit detection and assessment of adversaries, reveal unauthorized persons, and permit examination of credentials and vehicles at pedestrian and vehicle entrances. Isolation zones and all exterior areas within the protected area shall be continuously illuminated to allow for sufficient monitoring and observation. Security and safeguard lighting systems used for this illumination shall have a backup electrical power system.

Gates

The primary vehicle gate should have remote communication/intercom outside gate, monitored at the control room to authorize access. It should be an automated gate or combination of manned and automated gate with proximity access cards, imbedded egress sensor, and timed delay for closure and positive lockdown in closed position.

Secondary vehicle gates should be locked with hardened, uniquely keyed security padlocks and secured with heavy-gauge welded-link steel chain.

Seldom-used vehicle gates should remain locked and barricaded with "Jersey bouncer" concrete barriers.

CCTV at Main Gate

CCTV cameras should be fixed or pan-tilt-zoom in protected housing, monitored at the control room and also at the guardhouse (if applicable).

Signage

Property signs should be posted at all entry control points. The signs should state that vehicles and items are subject to inspection upon entry, while on company sites, and

upon departure. The signs must list articles prohibited from entering the site. Locate fence signs at each entrance to the facility.

Signs should be posted displaying "No Trespassing" at entrances and around company facility property boundaries. At locations where the property boundary and the security perimeter coincide, the "No Trespassing" signs should be posted at the security perimeter barrier.

At perimeter gates not identified as primary entrance points, signs should be posted stating that the gate must be kept locked.

Signage considerations vary by site and facility type. The above may not be applicable in some environments. Corporate Security should be contacted for advice.

ID Badges

All company and contractor employees should be issued regular site access company photo ID badges, which should be displayed while personnel are on facility property. All visitors (including non-regular employees) should be required to sign in and present positive picture identification before being granted access to the facility.

Other Recommended Security Enhancements

These recommended enhancements should be reviewed by the area manager and evaluated for implementation.

Protective Force

Security guards should provide access control at the main gate during periods of high volume traffic, and they should conduct roving perimeter patrols after hours during escalated alert levels.

Anti-Vehicle Barriers

Permanent metal pipe or concrete barriers should be placed around critical above-ground structures, robust enough to stop or deflect assault by vehicle.

Access Control System

The following are design considerations:

- Application to perimeter doors/entry points, buildings, and/or critical areas/assets
- Use of proximity (preferred) or swipe identification card systems with readers control entry to the facility and critical areas, offering a strong combination of functionality and user convenience
- Photo ID badge-making system to create identification badges for use at all access points. Badge design, including selection of technology for tamper

protection, pictorial badge layout, numbers, and types of badges (employee, contractor, visitor, restricted access, etc.) is critical to maximize operational integrity and usefulness.

- Electromagnetic door locks are preferred for most safety/security applications, especially where emergency egress is required in the event electric power is lost. Electronic strike locks are another option, but more prone to maintenance problems.
- Electronic log of entries that allows for audits of all personnel entering or leaving an entire facility, or even specific areas
- Alarms on controlled-entry areas to detect unauthorized breach or doors being propped open
- Alarmed crash bars on emergency exits allow emergency use without reduction in access control effectiveness

Access control systems should be implemented with expansion potential to include other facilities. With a small initial system investment, this may avoid or minimize upgrade costs.

Resource 3-6: Requirement for Background Screening

No personnel (including contractors and visitors) should be allowed on our sites without vetting of identification. This can be initially instituted with simple measures, but we should promptly ramp up to more in-depth/formal vetting processes. Businesses should ensure that current and future contract language requires third parties to conduct and show proof of appropriate background screening of their employees prior to entering our facilities. Until appropriate vetting is complete, access should be limited and/or additional supervisory/security oversight should be employed.

4. Information and Cyber Security

Management Practice 4

Recognition that protecting information and information systems is a critical component of a sound security management system.

Companies will apply the security practices identified in this Code to their cyber assets as well as their physical assets. Information networks and systems are as critical to a company's success as its manufacturing and distribution systems. Special consideration should be given to systems that support e-commerce, business management, telecommunications, and process controls. Actions can include additional intrusion detection and access controls for voice and data networks, verification of information security practices applied by digitally connected business partners, and new controls on access to digital process control systems at our facilities.

The following samples are intended to stimulate thinking and offer helpful ideas on code implementation. Other approaches not described here may be just as effective or even more effective for a particular company. If a company so chooses, it may adopt any of these sample strategies or may modify them to fit the company's unique situation.

Resource 4-1: U.S. Chemicals Sector Cyber-Security Strategy

Prepared by the Chemicals Sector Cyber-Security Information Sharing Forum. The forum, consisting of global chemicals sector trade associations representing key industry segments, has developed a chemical sector cyber-security strategy to guide the industry's efforts in enhancing cyber-security risk management and reduction for information and process control systems. A copy of the draft report (June 2002) is available at http://www.responsiblecaretoolkit.com.

Resource 4-2: Security of Process Control Computer Systems

1.1 SCOPE

This standard defines the management systems that must be in place to provide an appropriate level of security, assure accurate information flow, and establish expectations and accountability for computers and computer networks used for control of enterprise manufacturing processes.

…

5.3.1 Software installed on computers connected to the process control network (PCN) shall be used exclusively for tasks that directly relate to control and monitoring of the manufacturing process.

5.3.2 Only software applications from the approved process control software list may be purchased and loaded onto process control computer system (PCCS) computers.

5.3.3 Every piece of PCCS equipment shall have a designated primary and backup manager/owner. The site shall keep a record of these assignments.

5.5 NETWORK INFRASTRUCTURE

5.5.1 The PCCS and PCN shall be segregated from IT networks by a network firewall. This segregation shall limit access to only those personnel and applications that have been authorized by the site organization.

5.5.2 All non-local (not within the PCN) access to the PCN shall be through the IT-PCN firewall or through remote access methods authorized in the "Remote Access" section of this document.

5.5.3 Process control applications shall not be installed utilizing the IT infrastructure (fiber, telephone lines, etc.) in such a way that the IT infrastructure becomes critical to unit operation.

5.5.4 The plant PCN may use IT infrastructure fiber for non-critical applications, if the fiber pairs are dedicated, labeled, and documented.

5.5.5 A list of allocated IP address blocks for each site shall be maintained centrally. The site shall use only addresses from the allocated blocks and shall maintain a list of assigned IP addresses within the address blocks.

5.5.6 PCN procedures and documentation shall be maintained to support ongoing modification and troubleshooting activities.

5.5.7 Network access to on-line safety systems or their programming stations is not allowed except for certain types of protocol-limited, pre-specified process data transfers.

5.6 SECURITY

5.6.1 Each user shall have an individual account and password for access to the PCCS, with access limited and controlled to that necessary to perform their job. In the case of PCCS equipment with only key lock access control, a list of key assignments shall be maintained by the site. Common or shared accounts may be used for non-privileged users (read-only access) and for control room operators where the account must remain continuously logged in. Operator accounts will be secured by geographic area (i.e., the account is only accessible from a specific workstation) and the system administrator must be able to determine the individual user from the shift log.

5.6.2 Where supported by the PCCS system, individual accounts shall be set up for all maintenance and system administration tasks; common or shared accounts shall not be used. Privileged accounts such as Administrator (Windows), System (OpenVMS), and root (Unix) shall be retained but shall not be used for routine administration and maintenance. Use of these accounts shall be controlled only by the system administrator for the plant/unit, so that use and changes can be tracked.

5.6.3 System administration personnel for each plant/unit shall review account access at least annually to ensure proper authorization for current users. Passwords shall be changed at least annually.

5.6.4 Individual accounts shall be immediately disabled by the system administrator for the plant/unit upon termination or reassignment of the user.

5.6.5 Highly privileged accounts shall not be left logged on, unprotected and unattended.

5.7 REMOTE ACCESS

5.7.1 Enterprise employees requiring remote phone access shall access the PCN using dial-back modems or technology providing equivalent security. Subsequent user authentication shall be required. No unsecured dial-in access shall be allowed into the PCN.

5.7.2 Third-party access to the PCN shall be controlled by procedure TEC-04-P1.

5.7.3 PCCS changes made via remote access shall use the same control procedures (e.g., work permitting) as if the change were done locally, with additional levels of communication to ensure that local PCCS users are aware of, understand, and approve any actions taken remotely.

5.7.4 No changes shall be made via remote access to a controller or console's configuration or control application that could adversely affect process operation. Examples of such changes include the following: a controller setpoint or mode change, a change of the status of an interlock, or a change to a value or the derivation of a signal value used for control.

5.8 CHANGE/PROBLEM MANAGEMENT

5.8.1 PCCS changes that affect process control shall use the corporate "management of change" procedure.

5.8.2 A risk assessment shall be conducted before the introduction of new operating system and application software versions and major applications. A written test and commissioning procedure shall be prepared and approved (by stakeholders) for each new application or major upgrade.

5.8.3 A log shall be kept of significant problems with each PCCS.

5.9 SUPPORT

5.9.1 An approved plan shall be in place to address hardware failures and software problems and ensure that equipment is adequately maintained and available.

5.9.2 Disaster recovery plans shall exist for PCCS elements at each site. These plans shall be reviewed annually.

5.9.3 Site disaster recovery plans shall include reference to control system disaster recovery plans and control system backup and recovery.

5.9.4 Backups of the on-line PCCS equipment shall be done on a frequency commensurate with the amount of changes, but not less frequently than annually.

5.9.5 Data from on-line historians (where history recording is not deemed transient, such as short-term trending) shall be backed up no less frequently than monthly.

5.9.6 Backups of PCCS critical information shall periodically be made and stored remote from the operating unit (a minimum distance of 1,000 feet) for disaster recovery purposes, and shall include some duplication in case of media failure.

5.9.7 Procedures shall be maintained for each PCCS describing how backup and recovery is done, what is backed up, the frequency of backups, labeling and logging of backups, and backup media and copy requirements. These procedures shall be reviewed annually.

5.9.8 A procedure to verify the integrity of backups for each system shall exist and be used at a predetermined frequency.

5. Documentation

Management Practice 5

Documentation of security management programs, processes, and procedures.

To sustain a consistent and reliable security program over time, companies will document the key elements of their program. Consistency and reliability will translate into a more secure workplace and community.

The following samples are intended to stimulate thinking and offer helpful ideas on code implementation. Other approaches not described here may be just as effective or even more effective for a particular company. If a company so chooses, it may adopt any of these sample strategies or may modify them to fit the company's unique situation.

Resource 5-1: Application of Standards

The site manager at each site will be responsible for implementing corporate security standards.

Expectations

The company is committed to basic security standards and will employ them in new construction standards for manufacturing sites and for offices.

Standards will be flexible to the site security situation and will be based on an analysis of the current and projected threat levels.

Existing facilities will be upgraded to current minimum standards, as appropriate, based on cost-benefit analyses and approved schedule.

Resource 5-2: Compact, Unified Security Policy (1)

It is important that management state the security behavior expected while persons are on company property or performing duties directly related to work requirements. This may best be done by the issuance of a written policy, which articulates expectations and compliance criteria. Procedures to comply with the policy should also be provided.

Access Control

Policy: It is the policy of ABC Corporation that access to the facility be limited to those who have been granted authorization for access.

Procedures: The property boundary will be clearly defined. Signage will be used to direct entrants to the appropriate entry point for processing onto the facility. Management will define the process for granting authorization for access to an individual. This may include verification of safety briefings and utilization of personal protection equipment. Employees, visitors, and contractors will log into and out of the facility, when entering or exiting the facility after being granted access authorization.

Pre-employment Screening

Policy: It is the policy of ABC Corporation that pre-employment screening will be conducted on candidates for employment.

Procedures: Human Resources will contract with a third-party provider approved by Corporate Human Resources to conduct such screens.

Workplace Violence

Policy: ABC Corporation has "zero tolerance" for any incident of violence in the workplace, whether it be physical violence, verbal abuse, willful destruction of company property, or any form of intimidation that affects the morale of the workforce. Such acts may be cause for counseling, reprimand, or even termination of employment. Alleged incidents will be investigated and sanctions exercised when warranted.

Procedures: Incidents of violence shall be reported to management immediately. Management will take appropriate action to defuse an ongoing confrontation and to gather evidence for investigation. Those involved in the incident shall be suspended from work, pending conclusion of the investigation. After consideration of the facts, management will adjudicate the incident.

Employees victimized by violence, who obtain court-issued restraining orders, shall notify management immediately and provide copies of documentation. Management will notify law enforcement of any violations.

Drug and Alcohol Abuse

Policy: ABC Corporation has a corporate policy on this subject.

Procedures: Local management should publicize the policy to all employees and, as necessary, supplement the policy to reflect local conditions and requirements. NOTE: Local management can only increase the severity of the policy, not reduce any conditions of the corporate policy.

Protection of Information

Policy: It is the policy of ABC Corporation that all company information—classified confidential, internal, or external—be secured from unauthorized disclosure or misuse.

Procedures: Management will define information to be safeguarded. Information will be disclosed on a limited basis and will be stored in a locked desk, file cabinet, or safe when not in use. Employees, visitors, vendors, and contractors will be required to sign statements of confidentiality before being granted access to the facility.

Weapons on Company Property

Policy: ABC Corporation has a corporate policy on this subject.

Procedures: Management should ensure that anyone entering an ABC Corporation facility is made aware of the restriction of weapons on company property. Exceptions to the policy are available based on specific needs. The policy and procedures should be supplemented at the local level to ensure compliance and enforcement.

Incident Reporting

Policy: It is the policy of ABC Corporation that security incidents be reported immediately to Corporate Security.

Procedures: Security incidents should be reported to Corporate Security by calling [phone number]. This will be followed by the submission of an incident reporting form. If security guards are employed, the security post orders should include a requirement that the officer call [phone number] about all emergency incidents.

Resource 5-3: Compact, Unified Security Policy (2)

1.0 APPLICABILITY: This policy shall apply to all company facilities.

2.0 PURPOSE: To require that minimum site security provisions be implemented to prevent harm to individuals, to avoid business interruption, and to prevent loss of property and information, due to theft, vandalism, violence, illegal and disruptive activities by extremist groups, and other criminal acts against the company.

3.0 POLICY: Each company location shall implement a site security program. The program will be developed considering the following potential sources of loss or disruption:

3.1 Theft, vandalism, and break-ins, considering both internal and external threats

3.2 Theft of confidential business information

3.3 Sabotage of equipment, utilities, and records; product contamination and tampering

3.4 Bomb threats

3.5 Demonstrators disrupting plant access and operations

3.6 Workplace violence and assaults

4.0 POLICY: Each company location shall designate an employee as the site security coordinator. This person shall be responsible for performing the following security management functions:

4.1 Preparing and implementing a site security plan consistent with the requirements contained herein

4.2 Establishing relationships with law enforcement agencies

4.3 Developing and managing incident reporting systems and conducting investigations of breaches of company security policy

4.4 Developing methods to increase employees' security awareness

4.5 Working with the site emergency coordinator to address security issues in emergency and crisis management planning and execution

4.6 Periodically reassessing the site's security program

5.0 POLICY: The security measures at each site shall include the following provisions:

5.1 Access control for people and vehicles into production areas, warehouses, utility facilities, and offices that contain business information that needs to be protected ("controlled areas")

5.1.1 Signs to direct all visitors and vehicles to the appropriate entry points

5.1.2 A system to verify visitors (any non-employee) and vehicles prior to entering company premises, along with safety and security briefing for all visitors

5.1.3 For non-employees, mandatory sign-in for access to controlled areas for at least the first visit (policy on escorting visitors during subsequent visits to be developed by the location)

5.1.4 Identifying badge for all visitors, along with requirement to wear the badge so it is visible

5.1.5 Controlled areas to be provided with physical barriers capable of keeping unauthorized people and vehicles out, except through designated entrance points (barriers shall not impede emergency egress from facilities)

5.1.6 Access points to controlled areas placed so that receptionist has a clear and remote view of visitors and vehicles approaching the facility

5.2 Perimeter protection (such as fences, solid exterior walls, gates to block vehicle traffic, and perimeter lighting) around controlled areas

5.3 Off-hours protection for controlled areas, such as remotely supervised intrusion alarms or a contract security guard service touring the facility regularly

5.4 Back-up power systems for controlled areas where operations are critical and for intrusion alarm and safety systems

6.0 POLICY: For employee security issues, refer to existing HR policies on the following subjects:

- Pre-employment screening
- Employee termination
- HR services
- "Zero tolerance" for violence
- Prohibition of weapons on company facilities, including parking lots
- Confidential business information
- Internal incident reporting systems
- Referring illegal or criminal activities to law enforcement

Resource 5-4: Documentation of Specific Security Practice (1)

Penetration exercises and security program reviews should be documented (facility name, location, date) and include a summary of what the exercise consisted of and the subsequent findings, lessons learned, and corrective actions, as needed/required. Summary results should be included in the monthly security program status report.

A penetration exercise will be considered "SUCCESSFUL/PASS" when the person/vehicle attempting to enter is successfully detected. An exercise will be considered "UNSUCCESSFUL/FAIL" when the person/vehicle is able to gain access.

The results of penetration exercises and security program reviews should be analyzed regularly by facility management to ensure that appropriate security measures are in place.

If penetration exercises continue to indicate that the security measures in place at a particular facility are not effective, local line management is required to request a corporate security review and report the subsequent actions taken to appropriate functional management.

Resource 5-5: Documentation of Specific Security Practice (2)

Nightly Security Check SOP

The following security measures are to be followed whenever personnel are on-site outside of normal, workweek, business hours. This will not affect weekend/holiday security measures (including gate/door locking and security system engagement). Unless otherwise specified, normal business hours will be defined as 8:00 a.m. until 5:00 p.m., Monday to Friday. It will be the responsibility of all on-site personnel to assure that these measures are maintained.

1.0	**Evening Shift Start Assignments**	**Check**
1.1	Front office personnel (receptionist unless otherwise assigned), will check/lock the front office doors on both sides (north and south) of the main entrance hallway. They will also engage the coded lock on the interior, main plant entrance door.	
1.2	Shipping/receiving department personnel will engage the easy exit slip-on security chains to secure the two south truck gates and the shipping department gate. They will also check/lock the equipment yard (bone yard) gate. Note: The walkthrough gate will remain latched (not locked) with its slip-on chain, throughout the week.	
2.0	**Morning Assignments**	
2.1	When front office personnel arrive and are prepared to answer the phone and sign in visitors, they will disengage the front door lock.	
2.2	Maintenance operators will unlock the two south gate slip-on chains referred to in step 1.2. Shipping/receiving personnel will unlatch the gate by their area.	
3.0	**General Evening Security**	
3.1	It is critical that security measures be maintained and not shared with anyone outside the company. Specifically, sharing the front door code with non-company employees is not permitted. The front door buzzer will be on at all times. This will allow on-site personnel to know the identity and arrival time of any visitor. Unless authorized by supervisory personnel, no after-hours visitors (truck drivers, etc.) are allowed unescorted access to the building.	

Resource 5-6: Documentation of Security Practices for Low, Medium, and High Threat Sites

Concept

During the site selection or acquisition phase, the director of corporate security or his representative should be integrated into appropriate planning teams to ensure early input of security criteria and features. Standards and operational plans will be based on perceived threat levels.

Threat Assessment

The director of corporate security, in consultation with corporate officers, outside sources, and government political analysts, will conduct a threat assessment of risk factors (such as political climate, possibility of civil unrest, terrorism, strikes, criminal activity, extortion, industrial or state sponsored espionage, kidnapping, etc.) at the proposed site. This information will be included as the basis for the physical and operational requirements of the plant. For planning purposes, sites or facilities will be assigned a low, medium or high threat rating and a rationale will be given as to specific threats perceived or projected.

Security Survey

As a basis for the security programs, a plant or site will be inspected and security review or survey made of the existing or planned assets, including the following:

- Personnel to be protected (number, type, national or expatriate, etc.)
- Physical assets to be protected (plant, material, equipment, etc.)
- Business, technical, financial, and human resource information (quantity and level of sensitivity of data, etc.) on hard copy, diskettes, videotapes, overheads, or books
- Internal restrictions at site of business, technical, financial, and human resource information on hard copy, diskettes, videotapes, overheads or books
- Local infrastructure to respond to routine and emergency situations (police, fire, medical, bomb threat, strikes, etc.)

An approved security survey form will be used to compile appropriate data for evaluation.

Application of Security Standards

After the threat level for a site is established, the standards for that level should be applied as a minimum.

Exceptions to Standards

The application of security standards should generally be firm; however, each site must be evaluated individually. If the project team leader or regional president feels that more or less than the minimum standards should be included in plant construction, a formal request for an exception should be prepared with accompanying rationale. Exception requests should be presented to the corporate security director. The matter will then be resolved after consultation with interested parties.

Security Standards: Low Threat Manufacturing Site

Physical Plant

Setbacks—Plant operations and buildings should be established not less than 75 feet from the perimeter fencing. The most sensitive operations should be located greater distances from uncontrolled areas.

Control Booth—A central control booth should be established and manned on a continuous basis. Facility should be at least 12' by 12' and be adjacent to and just inside the main personnel entry point. Facility should be heated and air-conditioned and contain racks to install alarm and closed-circuit television monitoring units, telephone, radio links, etc.

Perimeter Control—Perimeter fencing should be heavy-duty galvanized steel mesh (l.5" squares). Fencing should be at least 9' in height, topped by triple-strand barbed wire. All buildings, including the main administration building, should have perimeter fencing. In some cases, it is acceptable to substitute secure decorative fencing.

Retaining Wall—Perimeter chain link fencing should be mounted on a 3 ft. concrete wall, 9" wide, 1.5 ft. above and 1 ft. below ground.

Lighting—Adequate lighting should be installed within the plant and especially along the perimeters to permit remote monitoring by closed-circuit television (CCTV).

Closed-Circuit Television (CCTV)—CCTV should be installed on poles along the perimeter. Cameras should be pan-tilt-zoom, with monitoring in the guard booth. Also, CCTV and a panic alarm should be installed in the reception area in the main administration building with monitoring in the guard booth.

Intercom Systems and CCTV—These should be installed at all entry points to facilitate personnel screening.

Access Controls—Perimeter fencing should enclose all plant and office facilities. All facilities should be protected by perimeter fencing in an emergency even if access to the administration building is left open on a routine, non-emergency basis.

Cleared Areas—There should be cleared areas at least 12 feet wide on either side of perimeter fencing. Vegetation should be removed and controlled via ground mesh and aggregate topping to retard regrowth.

Operational Standards

Unit Security Officer—This person should be appointed by the site manager to handle and be responsible for all security activities.

Security Orientation—All employees should be briefed regularly on the local security situation to cover emergency plans for crises, personal safety, internal security procedures, protection of proprietary information, computer security, etc.

Access of Vehicles—All delivery trucks should be logged in and out. Rail cars should be similarly entered in a permanent log and their entry and departure times noted, as well as any irregularities.

Parking Guidance—Except for senior management personnel, parking for employees should be in areas outside plant operations.

Access Controls—Employees' presence at the plant should be recorded either by signing in or via electronic means. There should be a way to ascertain the identity of all persons present at a plant quickly.

Guard Force

- Guards should be unarmed and can be either contract or employee. If cross-training is desired in fire control, emergency medical treatment, and chemical emergencies, an employee guard force should be used.
- All actions should follow written guidance given to the guard force on their mission responsibilities, scope of authority, and requirement to follow procedures. The force should be exercised regularly. Management should emphasize that good relations should be maintained with other employees.
- Monitoring of guard activities should be constant by review of their log books, review of their patrols by reviewing patrol recorders, etc.
- Guards should be uniformed and their activities fully coordinated with external security organizations (e.g., police, fire, medical services) that will respond to requests for assistance and emergencies at the plant.

Internal Security

- All visitors should be screened by the external guard or by a receptionist at the entry door of the administration building. Visitors should be announced to the appropriate office and then be accompanied by a company employee.
- Contractors should have no access to sensitive company information without specific authorization from a competent company officer. Their access to

company computer systems must be authorized by the systems security coordinator.

- All sensitive information must be stored in lockable security cabinets, and keys or combinations must be controlled.
- The administration building should be alarmed and monitored by the security guard when not occupied.
- All sensitive documents should be destroyed by an approved cross-cut shredder or by burning. Videotapes and other types of media containing sensitive information should be returned to headquarters for appropriate disposal if no local facilities are available.
- Offices of senior management officers (managing directors, site managers, etc.) should be locked after hours.
- There should be a "clean desk" policy on sensitive information for all persons working on sensitive projects or handling sensitive documents. The unit security officer should inspect to ensure compliance.
- All operating units must report all significant security incidents to the director of corporate security. Guidelines on incidents that must be reported are contained in the guideline titled "Significant Security Incident Requirements."
- Facilities should be equipped with a scramble phone, scramble e-mail, and scramble fax. These units should be installed in a locked, secured, alarmed area of the site.

Residential Security

- A survey should be made of the residences of all expatriate employees. Measures should be taken to reduce their exposure to burglary, harassment, etc. These protection measures should also ensure that business, technical, financial, and human resource information located at the residence is protected.
- If appropriate, alarm systems and protective measures (grill work, locks) should be installed at the residence. In some cases, guards should be assigned to the residence to protect the employee and his or her family.

Security Standards: Medium Threat Manufacturing Site

At medium threat level, all factors at low level threat should be implemented as well as those that follow.

Security Survey

Purpose is to obtain expanded explanation of threat situation from whatever source. Description of negative experience or projected risk and specific reasons for upgrad-

ing risk assessment should be developed and should be supported by statistics, if possible.

Physical Plant

Consider (based on circumstances) the following:

- Alarm systems for perimeter fence to guard booth
- Augmented perimeter barriers (walls, double fencing, additional guard patrols)
- Continual police or private guard presence on exterior of facility
- Metal screening
- Search of vehicles
- Security patrols at homes of exempt employees
- Security fencing and grill work at homes of exempt employees
- Retaining wall 3 ft. high, 9 in. wide, and 1.5 ft. above and l.5 ft. below ground

Internal Security

- Increased compartmentalization in plant interior
- Creation of safe haven areas (locked areas inside the plant used for the safety of staff)
- Addition of armed guards
- Regular drills of emergency procedures, ideally involving host government support

Security Standards: High Threat Manufacturing Site

High threat sites will normally follow all guidance for low and medium levels as well as the following additional steps.

Security Survey

- Complete security survey to determine how best to maximize plant security
- Construction of turnstiles, searches of employees
- 100% vehicle searches
- All vehicles except exempt employees parked outside of plant

Physical Plant

- Construction of interior apron fence

- Presence of armed guards
- Permanent presence of local police and/or military
- Regular drills of emergency plans with host government
- Preparation of travel documents (passports, tickets) for quick evacuation, shipment of personal effects, etc.
- Preparation of plant shutdown and/or custodial care during evacuation phase
- Drawdown of personnel
- Evacuation of dependents

6. Training, Drills, and Guidance

Management Practice 6

Training, drills, and guidance for employees, contractors, service providers, value chain partners and others, as appropriate, to enhance awareness and capability.

As effective security programs evolve, companies will keep pace by enhancing security awareness and capabilities through training, drills, and guidance. This commitment extends beyond employees and contractors to include others, when appropriate, such as product distributors or emergency response agencies. Working together in this fashion improves our ability to deter and detect incidents while strengthening our overall security capability.

The following samples are intended to stimulate thinking and offer helpful ideas on code implementation. Other approaches not described here may be just as effective or even more effective for a particular company. If a company so chooses, it may adopt any of these sample strategies or may modify them to fit the company's unique situation.

Resource 6-1: Emergency Response Training Program

Source: American Chemistry Council, Community Awareness and Emergency Response Code

Responsible Care® Management Practice #3

An ongoing training program for those employees who have response or communications responsibilities in the event of an emergency.

Plant employees who have emergency response or communication responsibilities as well as other facility employees need to have up-to-date skills to respond effectively in the event of an emergency. Everyone who occupies a position that is identified in the plan must have appropriate training. Together with Emergency Response Management Practice #4, this management practice establishes a support mechanism to ensure that well-developed plans can be well executed in an actual emergency.

Suggested Activities

Set aside a period each year to provide corporate-wide training to selected employees. Establishing a set time each year for training helps to ensure that the training program will continue. Similarly, encourage corporate-wide training within your company. This will ensure that all facilities are aware of overall corporate training policies and standards for personnel. Provide HAZMAT training to plant response personnel. Typically, unit operators or specialist employees will be the first on the scene of an emergency, before the plant response personnel are notified. Therefore, it is important that these employees receive training in wearing proper personal protective equipment and using the "buddy system" when in the midst of an incident. Plant response personnel must receive HAZMAT training to enable them to respond properly to the incident and at the same time protect themselves and other workers from known hazards.

> *ABC Corporation's plant provided 48 hours of training to seven members of its hazardous materials team to qualify them. Four others were trained to qualify as HAZMAT technicians. Members of the team were also given incident command training. The site's rescue team was trained in high-rise and confined space techniques. Each team receives an additional eight hours of training per month.*

> *XYZ Company has an eight-member off-site emergency response team that receives formal annual training and in addition has formally trained all site personnel who would possibly be involved in an emergency to the HazMat Technician level. All training is supplemented by annual refresher courses*

Pitfalls and Considerations

Do not limit your facility to training by internal personnel only. Training by both internal and external personnel will result in the sharpening of response personnel skills, the presentation of up-to-date methods, and promoting contact and coordination with others involved in emergency planning. Plant managers are not always the most appropriate incident commanders. Incident commanders should be thoroughly trained emergency response personnel who will operate from the scene of the incident. Plant managers retain their overall management but the actual emergency response is better directed by an incident commander who regularly trains with the emergency response team.

Suggested Activities

Provide periodic training to all response personnel on site emergency response. Everyone with a role referenced in the emergency response plan must be trained to fulfill that role effectively. If the emergency plan changes, whether due to scheduled updates or as the result of lessons learned in exercises, the personnel involved must be made aware of the changes. Periodic training focusing on the facility emergency response plan will ensure that those involved are prepared to implement the plan.

Provide training to plant managers on the use of the incident command system for managing emergencies. The incident command system will be the primary means of communication during an emergency. This includes communication between responders as well as communication with workers in areas away from the incident. It is critical that you as a plant manager be trained and able to use the incident command system at your facility.

> *ABC Corporation conducted a role-playing exercise for its Manufacturing Group plant managers. The exercise simulated a tornado striking a fictitious plant. In the exercise, the incident command system was activated before the tornado struck and was continued after it passed. Participants followed scripts to keep the exercise moving. Using the incident command system allowed participants to address several problems such as plant damage, fires, and unaccounted for persons, simultaneously through a unified command structure.*

Invite local responders to observe training and demonstrations by first responders to build confidence in the plant's level of preparedness. By observing first-hand the level of training and preparedness maintained by facility response personnel, local responders will have higher confidence in the ability of your personnel to respond to an incident at the facility.

To boost the local fire department's confidence in facility responders, plant management at XYZ Company enhanced training for its own fire brigade and invited the local fire department to demonstrations on fighting chemical fires.

Suggested Activities

Provide emergency response training to personnel from the community and other companies. If your responders have not yet faced, or have not yet received specialized training for, a chemical emergency, they may be wary of their ability to respond to such an incident. Providing emergency response training to personnel from the community and other companies will encourage shared knowledge and experience and result in greater and more effective coordination and cooperation among all involved.

> *ABC Corporation provided a 16-hour, two-day chlorine seminar for local hazardous materials emergency responders. The program was conducted at the city's fire department academy and consisted of four hours of classroom and 12 hours of practical hands-on training. The facility arranged for an empty chlorine truck to be used for demonstration purposes.*
>
> *XYZ Company offered a three-day technician level emergency response course at its facility. Approximately 80 people from the company, local fire and police departments, emergency medical services, government agencies, and various agencies attended. The course is offered twice a year.*

Identify training needs for facility emergency responders. Identifying the training needs of your facility emergency responders will ensure that time and resources are not used on training that either is not needed or is not applicable to the facility. Similarly, responders may need process-specific or chemical-specific training depending on the types of incidents likely to occur.

Develop internal training capabilities or identify outside sources. Once the training needs have been identified, it is time to build the resource of internal facility personnel capable of providing the needed training for other employees. If this resource does not exist or cannot be developed internally, external sources should be examined.

Resource 6-2: Memo as Security Training Tool

Security Memo

Date: 11/05/01

To:

From: Site Safety Coordinator

RE: People Approaching the Site

Priority: Urgent

Under NO circumstances are any passersby to be allowed access to the site or allowed to cross over the property line en route to some other location or destination. If you are faced with this situation from anyone, as occurred this past weekend with horseback riders, they are to be flatly denied and turned away. We are living in a time of heightened security and awareness. What may seem like an innocent request could be something more, and these types of requests WILL NOT be honored at this site. Further, security aside, when we allow anyone on the property, for any reason, ABC Corporation assumes liability. We do not want this liability, especially with persons not associated with the company or conducting company business. The site supervisor on duty cannot and will not authorize permission for anything like this to occur. If there are any questions whatsoever, or if any passerby is adamant or confrontational about his/her request, contact me personally 24 hours a day. If a decision is to be made regarding access to the site or right-of-way, I'll make it. The only other person who can give you permission to vary from these guidelines is [name]. DO NOT LET ANYONE ON THIS SITE WHO IS NOT SUPPOSED TO BE HERE. IT WILL NOT BE TOLERATED!!

STAY ALERT! STAY FOCUSED! BE WARY OF REQUESTS NO MATTER HOW INNOCENT THEY MAY SEEM! USE GOOD JUDGMENT! USE LOTS OF COMMON SENSE!

Resource 6-3: Statement of Training Requirement

A security training program is in place to develop and maintain the necessary skills to perform jobs safely and effectively and comply with all governmental regulations.

5.2 ANNUAL SECURITY TRAINING PLAN

A training program is developed and implemented to satisfy all training requirements.

5.2.1 Required training to satisfy all government regulations and company policies is identified.

5.2.2 Training objectives are established for each element of the training plan.

5.2.3 Employee training is scheduled and training resources are allocated to successfully complete the plan.

5.2.4 An employee database is maintained so that training status of each employee is available and up-to-date. This includes any directly supervised contract personnel.

5.2.5 Employee training records are maintained and contain, at a minimum, the following:

5.2.5.1 Title of Course

5.2.5.2 Dates and times of training

5.2.5.3 Instructor (by signature in the U.S.)

5.2.5.4 A copy of the lesson plans and course description.

5.2.5.5 Copy of all test results

…

5.4 PERSONNEL DEVELOPMENT

Management works with the appropriate Human Resource Groups to identify developmental needs and implements training to address those needs.

5.5 MEASURING TRAINING PROGRAM EFFECTIVENESS

A program is in place to measure the effectiveness of each element of the training program.

5.5.1 Evaluation criteria are developed for each element.

5.5.2 Evaluation results are reviewed and feedback is provided to trainers.

5.5.3 Modifications to the training program are documented.

5.5.4 Certification results are available for assessment of the training program.

6.0 REPORTS AND RECORDKEEPING

6.1 RECORDS

6.1.1 The facility is responsible for maintaining training records for each employee. These records are to be kept up-to-date.

6.1.2 Employee training documents will be retained in accordance with the Corporate Records Retention Policy or any overriding legal requirement.

Resource 6-4: Statement of Drill Requirement

Source: *Security Guidance for the American Petroleum Industry*, American Petroleum Institute, 2002.

8.13.6 Drills

Drills allow for a prepared and organized response to a variety of security-related events. Their essential purpose is to demonstrate knowledge and understanding of the security management plan as well as a readiness to respond to security-related events. They should be simple, flexible, and robust and should provide for:

- a scripted event indicative of a security related event
- emergency management and reporting procedures
- availability of essential resources and response actions
- review of lessons learned, i.e., critique of drill
- modifications to plan

A security drill could also be included as a part of other drills. For example, the cause of a product release could be a security incident with consideration given for the legal implications and personnel hazards associated with the incident.

Resource 6-5: Developing Security Awareness

Source: *Site Security Guidelines for the U.S. Chemical Industry*, American Chemistry Council, Synthetic Organic Chemical Manufacturers Association, and The Chlorine Institute, Inc., 2001.

It is axiomatic in security that employees and contractors can serve as the eyes and ears of a company-wide security effort. Employees and contractors see much that occurs in and around a chemical facility and are in a good position to notice when something or someone does not seem quite right. Training and awareness measures can transform employees and contractors into a natural surveillance system.

Developing security awareness can also reinforce existing security practices, such as the following:

- Locking doors
- Looking for and reporting suspicious packages
- Challenging people who are not wearing ID badges
- Not writing computer pass-words on computers
- Not taping exterior doors open to facilitate outdoor smoking breaks

Managers may reinforce personnel training in security practices through e-mailed security reminders, security tips posted on a corporate intranet, advice and contact numbers in local and company-wide internal publications, and the distribution of security-related videos, pamphlets, tent-cards for lunch tables, posters, etc.

Resource 6-6: Collaborative Training Policy

Teams of Company security personnel and law enforcement agencies and/or qualified individuals conduct information and training sessions. Employees are able to identify and respond to warning signs of potentially violent situations. All employees share responsibility for site security and contribute to improvements. Drills are conducted in cooperation with local law enforcement and emergency response agencies.

Resource 6-7: Penetration Exercises

Penetration exercises are a key component of security program reviews. Such exercises should generally be coordinated and arranged by the line manager responsible for the facility or by a security business center advisor. Reviews of this type should be unannounced and should take place during both regular and off-hours. Discretion and good judgment should be applied when deciding on methods to be employed. Individuals undertaking the activity should not be generally known at the facility. This could include visiting employees, contractors, or local counterparts. Exercises should include the following:

- Attempted entry through established entrances/exits, e.g., pedestrian doors/turnstiles, drive-in gates, etc., without proper identification badges. Persons conducting this exercise should not be generally known at the facility.
- Attempted entry to a restricted area by an unauthorized person.
- Review of discarded material for sensitive information or information which would allow unauthorized entry or access.

The following are sample exercises that could be conducted:

- **Office Building**—Persons attempt to gain access to the building or facility. Probably one of the best times to attempt access is when employees are entering or leaving the building. Depending on the entrance configuration, the "violator" could attempt to 'piggyback' in with employees or tell them or a guard he forgot his ID (if challenged). Ruse telephone calls can be used in an attempt to arrange an appointment. If the violator does gain access, then (depending on the circumstances) he may want to wander around the building until further challenged.
- **Terminals**—Persons attempt to enter the terminal by driving through an open gate or talking their way past a guard. A "violator" could present tell a guard or receptionist that he has a meeting (and name an employee or manager) and see if he is permitted entry without authorization from the person being visited.

There are many potential ways to penetrate a facility. However, under no circumstances should such attempts endanger the safety of any person or disrupt business operations. Structured clandestine penetration testing should be coordinated with the corporate security department.

Do's and Don'ts

- Do not endanger the safety of individuals.
- Do not disrupt business or operations.
- Do document the scope and objectives of the exercise and inform senior management at the location prior to the start of the exercise.

- Do ensure there is an effective communication link with senior location management at all times.
- Do consider informing local police that penetration exercises are taking place, especially if an exercise is carried out at night.
- Do not attempt a clandestine penetration exercise at locations such as terminals and refineries where armed guards are used.
- Do not undertake any illegal activity.

7. Communications, Dialogue, and Information Exchange

Management Practice 7

Communications, dialogue, and information exchange on appropriate security issues with stakeholders such as employees, contractors, communities, customers, suppliers, service providers, and government agencies balanced with safeguards for sensitive information.

Communication is a key element in improving security. Maintaining open and effective lines of communication includes steps such as sharing effective security practices with others throughout industry and maintaining interaction with law enforcement officials. At the same time, companies understand that their role is to protect employees and communities where they operate, while safeguarding information that would pose a threat in the wrong hands.

The following samples are intended to stimulate thinking and offer helpful ideas on code implementation. Other approaches not described here may be just as effective or even more effective for a particular company. If a company so chooses, it may adopt any of these sample strategies or may modify them to fit the company's unique situation.

Resource 7-1: Employee Security Awareness (1)

Essential Element

7.1 ABC Corporation management is committed to a security program designed to protect its employees, operations, and proprietary information and communicates to its employees an awareness of security vulnerabilities and measures to reduce these risks.

Expectations

7.1.1 ABC Corporation will develop a security awareness program to communicate specific risks and appropriate countermeasures. Formal briefing sessions will be held for all new employees, and periodic refresher courses will be provided for existing employees to cover changes in the security situation.

> *Guideline:*
> *The security awareness program will include viewing of the "Security Awareness" video developed by Corporate Security and a review of SOP 100-7-1, "Information Resource Protection Program," by all new employees where appropriate translations are available. Evidence of briefing will be maintained via log or other appropriate means.*

7.1.2 The director of corporate security will coordinate the development of security awareness programs and develop resource material for this activity.

7.1.3 A security orientation program will be developed for employees and their families who are relocating outside the U.S. and will include area and site briefings prior to departure and, as appropriate, at their residential sites abroad.

7.1.4 Each site will develop local security guidelines and instruct its employees in appropriate security practices and responsibilities, including site policies concerning employee, visitor, and contractor pass display, vehicle entry control, and property removal.

…

Essential Element

7.10 A process to disseminate pertinent threat information affecting the safety of employees, the operations of the company, and the protection of sensitive information will be maintained.

Expectations

7.10.1 Special briefings on the incidence of crime, civil unrest, war, etc., will be made to employees who travel or reside in high threat areas.

7.10.2 Corporate Security will serve as a clearinghouse for corporate inquiries on real or rumored reports of security threats affecting operations and personnel.

7.10.3 Special briefing programs will be made to employees and their dependents who are scheduled to reside abroad. The briefing programs will include the existent threat in the country of assignment and countermeasures that should be taken to reduce or eliminate these factors.

Resource 7-2: Employee Security Awareness (2)

Source: *Site Security Guidelines for the U.S. Chemical Industry*, American Chemistry Council, Synthetic Organic Chemical Manufacturers Association, and The Chlorine Institute, Inc., 2001.

It is axiomatic in security that employees and contractors can serve as the eyes and ears of a company-wide security effort. Employees and contractors see much that occurs in and around a chemical facility and are in a good position to notice when something or someone does not seem quite right. Training and awareness measures can transform employees and contractors into a natural surveillance system.

Developing security awareness can also reinforce existing security practices, such as the following:

- Locking doors
- Looking for and reporting suspicious packages
- Challenging people who are not wearing ID badges
- Not writing computer passwords on computers
- Not taping exterior doors open to facilitate outdoor smoking breaks

Managers may reinforce personnel training in security practices through e-mailed security reminders, security tips posted on a corporate intranet, advice and contact numbers in local and company-wide internal publications, and the distribution of security-related videos, pamphlets, tent-cards for lunch tables, posters, etc.

Resource 7-3: Law Enforcement Liaison

Security Expectations	**Guidelines**
1. Regional and local managers should ensure that communications with other industrial firms in the country are in place to provide early information regarding possible evacuation or other threat response actions.	• Advise personnel of escalating threat. • Review and consider enhanced security measures for high profile management. • Reinforce personal security awareness. • Review liaison with local industrial firms.
2. Strong linkages with Public Affairs should be ensured to enable prompt communications with the public, officials, and employees if disruptions or serious threats occur around key productions assets or facilities.	• Evaluate under what circumstances we could expect agency assistance in supplementing protection or employees, contractors, or assets, if required. • Understand, confirm, and document agencies and names of individuals we should contact if threat conditions escalate significantly (police, fire, Coast Guard, etc.). • Understand and confirm appropriate sequence of notification to request assistance. • Understand and confirm type and mode of protection likely to be provided.

Resource 7-4: Public-Private Cooperation (1)

The Security Liaison Program involves local and regional law enforcement at multiple levels to ensure support during normal and emergency situations and, in concert with the security business centers, keeps security personnel abreast of the latest developments in chemical industry security. The program is implemented through meetings, coordination of emergency planning, and joint activities. This program also includes establishing liaison with other necessary security emergency response organizations.

Resource 7-5: Public-Private Cooperation (2)

Source: *Site Security Guidelines for the U.S. Chemical Industry*, American Chemistry Council, Synthetic Organic Chemical Manufacturers Association, and The Chlorine Institute, Inc., 2001.

Managers may wish to consider establishing partnerships or enhancing relationships with local, state, and federal law enforcement and other public safety agencies. Through such a network, managers may learn more easily of looming threats, dangerous trends, and successful and unsuccessful security measures. It may also be possible to obtain threat and other information from Local Emergency Planning Committees, community advisory panels, mutual aid groups, and state chemical associations.

Resource 7-6: Public-Private Cooperation (3)

Source: *Operation Cooperation: Guidelines for Partnerships Between Law Enforcement and Private Security Organizations*, U.S. Department of Justice, Bureau of Justice Assistance, 2000.

What are the actual benefits of law enforcement–private security cooperation? Here are just a few:

- Networking and the personal touch
- Collaboration on specific projects (urban quality-of-life issues, high-tech crime)
- Increased crime prevention and public safety
- Cross-fertilization (on "crime prevention through environmental design," community policing, or the use of technology)
- Information sharing (police can share some, but not all, crime data; private security can supply business information to help with investigations and can share research on such topics as false alarm reduction, non-sworn alarm responders, model legislation on high-tech crime, mobile security devices, closed-circuit television for public safety, and standards for security officers)
- Leveraging of resources (through cooperation, a law enforcement agency may be able to teach or help the private sector to do some work that law enforcement now handles—including, perhaps, contracting out various non-crime, non-emergency tasks that do not require sworn, highly trained law enforcement personnel; likewise, security organizations may be able to get police to help them more effectively in reducing a variety of crimes against businesses)

Constantly arising are new crimes and concerns with so many dimensions that only a joint effort between the public and private sectors can lead to a solution. To name just one example, on the Internet, children are now both victims and offenders. Public–private collaboration may be just the right approach for such a problem.

[The following are various techniques of cooperation that some companies and law enforcement agencies have practiced:]

Networking Breakfast and lunch meetings (to discuss common problems and help each side understand the pressures, motivations, and constraints on the other) Lectures by private security professionals at police recruit training Speeches by one field at conferences of the other field Sponsorship of law enforcement appreciation functions and scholarships by security organizations Directories of local law enforcement and private security contacts Honors and awards (from private security to law enforcement and vice versa) Information Sharing Information (provided by law enforcement to the private sector) on criminal convictions (if authorized by law), local crime trends, modus operandi, and incidents, shared via e-mail trees, web pages, mailed newsletters, fax alerts, or telephone calls Information (provided by the private sector to law enforcement) on business crime and employees Crime Prevention Joint participation in security and safety for business improvement districts (BIDs) Consultation on crime prevention through environmental design and community policing Special joint efforts on local concerns, such as check fraud, video piracy, graffiti, or false alarms Joint public–private support of neighborhood watch programs Joint participation in National Night Out Research and guidelines Review of, distribution of, and action on research papers and protocols regarding false alarms, workplace drug crimes, workplace violence, product tampering, mobile security devices, non-sworn alarm responders, closed-circuit television, security personnel standards, etc.	Resource Sharing Lending of expertise (technical, language, etc.) Lending of "buy" money or goods Lending of computer equipment needed for specific investigations Donation of computer equipment, cellular telephones, etc. Donation of security devices to protect public spaces Creation of a booklet that makes it easier for law enforcement to borrow equipment and resources from private security, listing specific contact information for using auditoriums, classrooms, conference rooms, firing ranges, four-wheel drive vehicles, helicopter landing areas, indoor swimming pools, lecturers on security, open areas for personnel deployment, printing services, and vans or trucks Training Hosting speakers on topics of joint interest (terrorism, school violence, crime trends, etc.) Exchange of training and expertise (corporations offer management training to police; private security trains law enforcement in security measures; law enforcement teaches security officers how to be good witnesses or gather evidence in accordance with prosecutorial standards) Police training of corporate employees on such topics as sexual assault, burglary prevention, family Internet safety, drug and alcohol abuse, traffic safety, and vacation safety Legislation Drafting and supporting laws and ordinances on such topics as security officer standards and licensing, alarms, and computer crime Tracking of legislation of importance to law enforcement and security operations Operations Investigations (of complex financial frauds or computer crimes) Critical incident planning (for natural disasters, school shootings, and workplace violence) Joint sting operations (cargo theft)

Resource 7-7: Public-Private Information Exchange

Source: Chemical Sector Information Sharing & Analysis Center (Chemical Sector ISAC) and the National Infrastructure Protection Center (NIPC) Information Sharing Program

Standard Operating Procedure (SOP)

April 24, 2002

1. PURPOSE

This SOP establishes voluntary procedures for implementing the information reporting, analysis, and warning provisions of the National Infrastructure Protection Center (NIPC) national-level program for the chemical sector. The chemical sector is comprised of entities engaged in the production, storage, transportation, sales, and delivery of chemical materials and supplies, and for purposes of this SOP is represented by the Chemical Sector Information Sharing and Analysis Center (Chemical Sector ISAC). This program has been established to enable the NIPC to receive incident reports from Chemical Sector ISAC participants and to provide timely, accurate, and actionable warning for physical, operational, and cyber threats or attacks on the national chemical infrastructure. No procedure established by this Standard supersedes existing mechanisms and channels for reporting incident data to the FBI or any other agencies.

2. Background and Overview

Presidential Decision Directive (PDD)-63, signed on May 22, 1998, authorized the creation of a full-scale National Infrastructure Protection Center. The PDD tasked the NIPC to serve as the national critical infrastructure assessment, warning, vulnerability, and law enforcement entity. Further, it directed all executive departments to share information with the NIPC about threats, warnings, and actual attacks on critical government and private sector infrastructures to the extent permitted by law. In addition, it authorized the NIPC to establish its own relations directly with others in the private sector and with any information sharing and analysis entity that the private sector may create.

To fulfill one portion of its assessment and warning mission as assigned by the PDD, and with the assistance of government officials and industry representatives from the chemical sector, the NIPC has developed general guidelines for voluntarily reporting operational and cyber incidents adversely affecting the nation's chemical infrastructure. Reporting entities are expected on a voluntary basis to provide the NIPC with information on serious threats to corporate information systems, operations, and plants, provided they meet established reporting criteria and thresholds.

Following receipt of standardized incident reports from the chemical and other sectors, the NIPC will process and evaluate the information and will disseminate timely and actionable assessments, advisories, and alerts to appropriate government and pri-

vate sector entities when such incidents are deemed to have possible serious national security, economic, or social consequences. Among the entities the NIPC routinely will coordinate with in furtherance of the SOP is the FBI's Weapons of Mass Destruction Operations Unit (WMDOU). WMDOU's specialized mission is to combat the use or threatened use of weapons of mass destruction, whether by chemical, biological, nuclear, or radiological means. Although the WMDOU does not produce a warning product, it conducts assessments of threats and of actual incidents that could subsequently provide the basis for a NIPC warning product. MWDOU also serves as a program manager and coordinating response entity for incidents involving weapons of mass destruction.

3. Applicability

This SOP is intended to apply, on a voluntary basis, to all entities engaged in activities in the chemical sector. The SOP is not entered into as a legally binding agreement, nor is it a formal expression of a legally binding agreement, but it is an expression of the purpose and intent of the organizations concerned. Similarly, this SOP does not confer, grant, or authorize any rights, privileges, or obligations as to any third parties.

4. Responsibilities

A. The NIPC is responsible for:

1. Ensuring that incident reports received by the NIPC pursuant to this SOP are processed in near real-time, and that timely and actionable warning notices are disseminated to appropriate government and industry Information Sharing and Analysis Center (ISAC) participants with appropriate protections applied to the proprietary and/or sensitive nature of such information.

2. Maintenance of this SOP.

B. The Chemical Sector ISAC is responsible for establishing the voluntary basis for:

1. Reporting to the NIPC by members of the Chemical Sector ISAC incidents from malicious or unknown causes that meet established criteria.
2. Assistance by cleared Chemical Sector ISAC staff and other designated industry personnel to work with the NIPC to declassify and sanitize threat and warning messages to permit broader dissemination.

3. Having experts available to consult directly with the NIPC on selected incident reports when appropriate for specific assessments.

4. Assuring that an up-to-date version of the SOP is available on the Chemical Sector ISAC Website when available.

C. All companies participating in the information sharing program are expected to report, on a voluntary basis, to the NIPC information pertinent to incidents or threats affecting the chemical sector in accordance with reporting criteria and thresholds.

5. Incident Reporting

Events reports should be submitted when the cause is known or suspected to be of malicious origin. Reporting of events where the cause is uncertain or unknown is strongly encouraged. NO report should be submitted when it is considered highly probable that the cause is NOT of malicious origin.

A. Reporting Incident Data

An incident report will be submitted by entities participating in the Chemical Sector ISAC, or by the Chemical Sector ISAC itself, for events meeting specific criteria and thresholds. Report filings may be sent non-securely, by email, to the NIPC at NIPC.Watch@fbi.gov, or securely, by sending sensitive information to the NIPC via encrypted email procedures established by the NIPC and the Chemical Sector ISAC (e.g., Pretty Good Privacy encryption software). Additionally, incident reports can be sent by fax to the NIPC Watch and Warning Unit (202-323-2079 or -2082). If the submitting entity is an InfraGard member, information also can be sent securely via the FBI secure InfraGard web server (https://www.infragard.org).

Three timeframes or stages for reporting are envisioned by this SOP. These stages represent an ideal. While it is desirable for reporting entities to follow these stages where possible, entities should not delay a report, or decide not to report, because they may have missed one of the time frames set out below. Participants are encouraged to report in any case at the earliest opportunity.

- Stage 1 Report: The first report is intended to provide notice that an incident meeting one or more of the criteria and thresholds described in Attachment A has occurred. Stage 1 reports are requested immediately following the first 60 minutes after detection of an incident.
- Stage 2 Report: These reports are requested within 4-6 hours after submittal of the initial (Stage 1) report when more complete information generally is available.
- Stage 3 Report: This third and last report will be filed only for malicious events and will represent the final entry for the incident report. It should contain all the relevant facts that can be determined within a 60-day period following filing of a Stage 1 report, or on a closeout schedule established by the originator and filed with the NIPC.

This SOP does not supersede existing mechanisms and channels for reporting incident data to law enforcement and other emergency first responders, which should also be utilized, especially when there is likelihood of imminent physical harm. Local FBI offices, for example, are listed in the phone book as well as online at www.fbi.gov/contact/fo/fo.htm.

B. Receipt and Processing by the NIPC

Each report will be received at the NIPC Watch &Warning Unit (7x24), immediately logged, assigned a unique identification number, and acknowledged to the originator. It then will be integrated into an incident database and made available to appropriate NIPC analyst servers and/or databases while observing established protocols to protect sensitive information. Incident reports designated by their originators as "Public" are releasable without further restrictions. Those designated as "Proprietary" or "Sensitive" are releasable to authorized personnel at the Chemical Sector ISAC if the originator also designates it "For Limited Release to Chemical Sector ISAC." Those designated "Proprietary" or "Sensitive" will be maintained by the NIPC as exempt from disclosure under the Freedom of Information and Trade Secrets Acts.

1. CONFIRMATION OF RECEIPT OF INFORMATION AND REVIEW. NIPC Watch Unit personnel will send a reply to the originator assigning a unique identification number and indicating receipt of the report. The NIPC then will examine the incoming data report to verify that the incident being reported does, in fact, meet the established reporting threshold.

2. RESOLVING QUESTIONS ABOUT INCIDENT REPORTS. The NIPC sincerely intends to minimize reporting burdens on participant entity personnel who are likely to have their hands full attempting to restore operations and recover from consequences produced by reported incidents. To accomplish this objective and yet render effective and timely assessment, and consistent with the originator's document marking, assigned NIPC analysts may contact the originator and/or appropriate Chemical Sector ISAC staff or members to resolve questions concerning any of the associated facts, handling restrictions, and/or possible relationships to other contemporaneously reported incidents.

3. ANALYSIS OF INFORMATION AND DETERMINATION OF WHETHER TO SEND OUT WARNING NOTIFICATION. The NIPC will evaluate information filed by members of the chemical sector, compare it with similar information submitted by entities from other critical infrastructures and federal/state agencies, and attempt to determine whether a coordinated attack is underway against U.S. national interests. This information, when it appears to pertain to the commission of a crime, could also be used by law enforcement to identify, apprehend, and prosecute perpetrators. If the government determines that an investigation against the perpetrators is warranted, the NIPC will affirmatively consider the Chemical Sector ISAC's and/or reporting company's equities in such an investigation, to include seeking the Chemical Sector ISAC's and/or reporting company's cooperation as appropriate.

C. DISTRIBUTION OF WARNING NOTIFICATION:

Some of the information available to the NIPC may be classified or law enforcement sensitive and, thus, unavailable to many in the industry. A select group of Chemical Sector ISAC officials and other designated industry personnel is being sponsored for clearances by, and at the expense of, the NIPC and will be provided with the means to

receive classified material. The NIPC may seek information from, and provide information to, members of this group for the purpose of declassifying and sanitizing warning material so that it may be disseminated to all appropriate personnel industry-wide. Once the NIPC has determined that a warning should be issued all, or a sufficient subset, of these individuals should be available as needed to assist the NIPC in sanitizing and finalizing warning notices so as to provide non-proprietary, timely, and actionable information to the maximum extent possible.

The table below describes the plan envisioned by this SOP for disseminating warning products.

Class of Information:	**Distribution Media:**	**Recipients:**
Classified (e.g., Confidential, Secret)	STU-3	Participating industry and government personnel with appropriate clearances and need-to-know for each particular incident.
Limited Distribution (e.g., Proprietary, Secure Access, Law Enforcement Sensitive)	Email (encrypted or non secure) or fax via Chemical Sector ISAC If InfraGard member, secure InfraGard web server and email	Chemical Sector ISAC participants InfraGard Members with signed Agreement
Public	NIPC public web server NIPC email to Chemical Sector ISAC	All Chemical Sector ISAC participants and other sector entities

The NIPC and information recipients recognize that each organization receiving warning notifications may incur expenses or possibly suffer some degraded operations temporarily by raising security levels. Consequently, and to assure that such periods of heightened security are kept to the minimum commensurate with the situation, the NIPC will endeavor to establish and include a time horizon in each warning message.

In addition to the warning products noted above, the NIPC periodically will make available analytic products (e. g., Cyber Notes, NIPC Highlights) to Chemical Sector ISAC members using various means of communications, including the NIPC's public web site. The NIPC and information providers and recipients recognize that all information shared is submitted, received, and disseminated in good faith, but otherwise is without warranty.

Full Extent of Understanding

This SOP is not an obligation or commitment of funds nor a basis for a transfer of funds, but rather a statement of the understandings among the parties. Unless otherwise agreed in writing, each party is to bear its own costs in relation to this SOP. Expenditures by each party are subject to its budgetary processes and to the availability of funds and resources pursuant to applicable laws, regulations, and policies.

This SOP can be amended at any time by mutual, written consent of the signatory parties through their authorized representatives. This SOP becomes effective upon signature by the parties noted below and can be terminated by delivery of written notice by either party.

Frederick L. Webber President and CEO American Chemistry Council	Ronald L. Dick Deputy Assistant Director, FBI Director, National Infrastructure Protection Center

Specification:

Indications, Analysis & Warning Criteria & Thresholds for Reporting Incidents Affecting the Chemical Sector

Entities involved in the production, storage, transportation, sales, and delivery of chemical materials and supplies are requested to report voluntarily to the NIPC data on incidents that meet the criteria specified on the following pages. The data to be reported is specific to each event criterion, as identified under the major categories of "Physical Events" and "Threat Events." "Physical" means "produces observable consequences" (e.g., a release), as well as cyber attacks. In either case, events are requested to be reported when they are known to be, or are potentially, of malicious origin. Reporting should be made in accordance with the guidelines of the SOP to which this specification is attached. The data requested to be reported is either readily available operational data or data that is available through an entity's physical or information security operations.

The procedures established by this specification are in addition to, and do not supersede, any existing requirements or mechanisms for reporting incident data to the FBI, EPA, DOT, or any other governmental entity.

Physical Events

The purpose of the Indications, Analysis, and Warning (IAW) process in this category is to provide data that enables NIPC to warn others, if appropriate, of attacks that are imminent or underway. Reporting of events meeting the guidelines in this attachment is strongly encouraged when the cause is **known** or **suspected** to be of malicious ori-

gin. Where the cause of an event is uncertain or unknown, reporting is also strongly encouraged. Reporting is not necessary if it is considered highly probable that the cause is NOT of malicious origin, or until such time as a reportable cause is established.

Following are the events, and corresponding thresholds, for determining whether to report physical events:

1. Event Criterion: **Explosion, fire or other damage to a production facility**

1.a. Event Threshold: Explosion, fire or other damage to a production facility that results in a loss of 50% of domestic productive capacity for one or more of the products being produced. Consider only capacity that is actually being utilized (versus idle) at the time of the event.

1.b. Event Threshold: Explosion, fire or other damage to a production facility that is a single supplier, or one of very limited number of suppliers, of a product deemed by the reporting organization to be critical to the manufacture of a crucial product or supply to critical infrastructures (such as critical pharmaceuticals, public water supplies, electronics, or national defense).

1.c. Event Threshold: Explosion, fire or other damage to a production facility that releases a chemical product that could cause death or serious injury to humans, or a massive, long-term impact on the environment, external to the facility.

2. Event Criterion: **Damage to, or intentional opening of, a stationary storage tank**

Event Threshold: Damage to, or intentional opening of, a stationary storage tank that releases a chemical product that could cause death or serious injury to humans, or a massive, long-term impact on the environment, external to the facility.

3. Event Criterion: **Damage to, or intentional opening of, a tank truck, rail tank car, barge, bulk transportation container, or pipeline**

Event Threshold: Damage to, or intentional opening of, a tank truck, rail tank car, barge, bulk transportation container, or pipeline that releases a chemical product that could cause death or serious injury to humans, or a massive, long-term impact on the environment, in the vicinity of the release.

4. Event Criterion: **Contamination of a finished consumer product**

Event Threshold: Contamination of a finished consumer product that has the potential to result in death or illness to, or other severe reaction by, consumers.

5. Event Criterion: **Known or suspected theft or unlawful removal (including lost or missing bulk containers) of a chemical product**

Event Threshold: Known or suspected theft or unlawful removal (including lost or missing bulk containers) of a chemical product with the potential to cause death or serious injury to humans or a massive, long-term impact on the environment.

6. Event Criterion: **Loss of or damage to computer information or control systems or telecommunications**

Event Threshold: Significant loss of computer information or control systems, or telecommunications, for functions essential to system operation (including radio, wireline, and wireless—both voice and data) (e.g., SCADA) or other critical operational or maintenance functions.

7. Event Criterion: **Lost or degraded market functionality**

Event Threshold: Lost or degraded market functionality, or of information systems or telecommunications systems (e.g., chemical e-commerce websites) critical to that functionality, including national or regional chemical markets, and having a financial impact greater than $1 million.

8. Event Criterion: **Cyber surveillance, intrusions & attacks**

Event Threshold: Any unauthorized, highly focused and concerted cyber attempts against, or intrusions into, critical operational systems that, in the judgment of the reporting organization, potentially could affect the ability of the organization to conduct business or fulfill its mission. (Reports should identify the target systems, impact on those systems, and external network addresses or other identifiers of the apparent source of the attempts or intrusions.)

Threat Events

The purpose of the IAW process in this category is to provide data that enables NIPC to disseminate advance warnings ("strategic warning").

9. Event Criterion: **Announced and credible threats**

Event Threshold: Any credible explicit threat conveyed by any means that, in the judgment of the reporting organization, if accomplished potentially could affect the ability of the organization to conduct business or fulfill its mission.

10. Event Criterion: **Intelligence gathering**

10.a. Event Threshold: **Physical surveillance**—any unauthorized or suspicious physical, photographic or electronic surveillance (e.g., passive microwave control signal imaging, infrared imaging) being conducted on a facility, distribution modality or distribution route that, in the judgment of the reporting organization, potentially could affect the ability of the organization to conduct business or fulfill its mission.

10.b. Event Threshold: **Social engineering**—any outside or unauthorized inside attempts to extract sensitive or proprietary information from employees that, in the

judgment of the reporting organization, potentially could affect the ability of the organization to conduct business or fulfill its mission.

11. Event Criterion**: Security breaches affecting computer systems, networks, communications, or data storage systems**

Event Threshold: Detection of breach in security in any one or combination of the following security components that, in the judgment of the reporting organization, potentially could affect the ability of the organization to conduct business or fulfill its mission: information availability (through denial-of-service), corporate network boundary, access control, authentication, confidentiality, data integrity, and non-repudiation.

12. Event Criterion: **Planting or pre-positioning of malicious code/exploit tools**

Event Threshold: Activities such as unauthorized downloading, transferring, planting or pre-positioning malicious code (including viruses) or computer/network exploit tools that, in the judgment of the reporting organization, potentially could affect the ability of the organization to conduct business or fulfill its mission.

8. Response to Security Threats

Management Practice 8

Evaluation, response, reporting, and communication of security threats as appropriate.

Companies take physical and cyber security threats very seriously. In the event of such threats, companies will promptly evaluate the situation and respond. Real and credible threats will be reported and communicated to company and law enforcement personnel as appropriate.

The following samples are intended to stimulate thinking and offer helpful ideas on code implementation. Other approaches not described here may be just as effective or even more effective for a particular company. If a company so chooses, it may adopt any of these sample strategies or may modify them to fit the company's unique situation.

Resource 8-1: Incremental Threat Response (1)

Note: This threat-level color scheme preceded and is different from the color scheme developed by the Office of Homeland Security.

Operations Protection: Threat Response

Purpose: To provide incremental procedural security upgrades that can be taken as a threat escalates. These measures are generally progressive in nature and may be fully or selectively applied to establish the appropriate defensive posture required to counter the facility's assessed threat condition. Security should review threat escalation with management and obtain their endorsement to implement incremental security upgrades.

Four levels of escalating threat conditions have been defined:

Blue Applies when there is a general possibility of threat activity above the baseline threat statement. Security should monitor intelligence and consider application of some measures from higher threat levels. This level should be capable of being maintained indefinitely

Yellow Applies when there is an increased and more defined/validated level of threat. The elements of this level must be capable of being maintained for weeks without causing undue hardship, affecting operations, or aggravating relations with authorities.

Orange Applies when an actual threat incident occurs or when intelligence indicates threat activity is imminent. Activation of this level for more than a short period will probably affect operations.

Red Applies in the immediate area where a threat action has occurred or when intelligence indicates a specific threat against a specific company target or person is imminent. This level can only be kept for a short period of time.

Threat response measures appropriate to each of the four levels are depicted in the following matrix:

	Blue	Yellow	Orange	Red
Intelligence/ Threat Assessment	Consider enhancing intel monitoring Reinforce info. sec. procedures Review liaison w/local authorities and other local companies As appropriate, consult local authorities on the threat and security countermeasures	Provide "real time" collection of threat data Consult w/authorities and neighboring facilities on mutual threat measures	Carefully monitor "real time" threat data Share and compare with neighboring facilities and other companies	Carefully monitor "real time" threat data Share and compare with neighboring facilities and other companies
Personnel Protection	Advise personnel on rising threat Consider enhanced security measures for high profile management Reinforce personal security awareness	Update personnel on rising threat Implement additional security measures for high profile mgmt. Remind drivers to lock vehicles and travel in pairs	Update personnel on escalating threat Minimize business activity outside the facility	Update personnel on escalating threat
Physical Security	Secure buildings, rooms, and storage areas not in normal use Review security hardware on doors, locks & windows Check fences & lighting, CCTV, and communication systems Ensure alarm systems work Consider "panic alarm" for employees in critical position	At beginning and end of each workday inspect interior/exterior of buildings & storage areas in regular use Raise awareness regarding delivery of suspect mail and packages Enhance mail inspection procedures Consider removing/covering company logos Increase building spot checks	Secure and regularly inspect all buildings, rooms and storage areas in regular use Consult local authorities on closing of roads/facilities that contribute to vulnerabilities Check/screen all deliveries Extend protection to additional vulnerable points (include outside the immediate area of base facility)	Make frequent checks of all facility exterior areas, including parking Search all items coming into the facility Coordinate with local authorities closing of public roads and facilities Move objects that could become projectiles 25 meter away from buildings
Access Control	Ensure adequate access control, enhance as needed Limit points of access for vehicles and personnel, considering operational activities Reassess barrier delay time at critical facilities. Enhance as needed	Limit access to facility to an absolute minimum	Strictly enforce access control Restrict access to facility to that essential for operational purposes only	No visitors
Pedestrian Access	Conduct security spot checks of personnel entering facility Reinforce ID badges displayed at all times	Randomly inspect visitors' briefcases Increase frequency of personnel spot checks	Increase frequency of random briefcase inspection	Search all persons prior to entering the facility
Vehicle Access	Conduct security spot checks of vehicles entering facility Limit vehicle access to protected area to essential vehicles only	Increase vehicle spot checks Prevent visitor vehicles from parking within 25 meters of buildings Consider centralized parking Positively identify all vehicles allowed entry to the site	Enforce centralized parking away from facilities & arrange security for those vehicles Erect barriers and obstacles to control vehicle flow Search all vehicles and contents prior to entering the facility	Search all vehicles and contents prior to entering the facility
Guard Force	Review existing countermeasures and operational procedures to ensure adequate guard allocation, access control procedures, and enhanced outer perimeter security	Consider guard reinforcement and ensure guards are adequately trained in company procedures Expand roving/motorized patrols to outer perimeter	Consider deployment of law enforcement personnel and instruct guards on procedural implications Increase numbers of security guards and patrol activities	Augment security guards with law enforcement/military personnel where feasible Consider armed guards
Emergency Response Plans	Key personnel on call, can implement sec. plans and seal off areas Ensure that radio/phone contact w/local law enforcement works Review contingency, evac/reloc plans & emerg response manuals Check plans for implementation to next threat level	Ensure all personnel responsible for countermeasures are on call Enhance interface w/safety and related emergency groups Review facility "shutdown" plans Check plans for implementation to next threat level	Ensure all personnel responsible for implementing countermeasures are immediately available Check plans for implementation to next threat level	Check all available emergency equipment; test communications and notification procedures Advise site mgmt of potential implementation of evacuation/relocation plan

Resource 8-2: Incremental Threat Response (2)

Note: This threat-level color scheme preceded and is different from the color scheme developed by the Office of Homeland Security.

Security Levels and Required Response

Green (Low)

- Photo ID badges worn by employees and resident contractors.
- Security badges worn and visible by non-resident contractors and visitors.
- Visitors and short-term contractors comply with access control procedures.
- Vehicular passes for entry into facility.
- Trucks have appropriate documentation (i.e., Bill of Lading, Material Shipping Order, delivery ticket, etc.).
- Post "no trespassing", "no weapons", and "authorized access only" signs along with signs stating that vehicles and visitors are subject to search.
- Daily perimeter patrols of facility.
- Instruct employees to notify Security of suspicious vehicles or personnel in and around the facility.
- Instruct mail and package handlers to be on the alert for any questionable mail or packages.

Blue (Guarded)

- Comply with green level requirements.
- Secure all access gates including rail entry and exit gates not staffed by a security officer (closed and locked or card entry access only).
- Conduct perimeter patrols of property on each shift.

Yellow (Elevated)

- Comply with green and blue levels.
- Security guards visually inspect the interior and exterior of all vehicles entering the main gate (a brief visual inspection by walking around the vehicle and looking inside cab and cargo hold, no undercarriage inspections).
- More frequent perimeter inspections are conducted.
- The host must be contacted to authorize visitor entry.
- Close and lock all non-essential gates for entry.

- Implement special mail handling procedures as warranted.

Orange (High)

- Comply with yellow, blue and green levels.
- Perimeter patrols are conducted as frequently as sustainable.
- Law enforcement officers are used during daylight hours as available.
- Definition of "daylight" (i.e., dawn to dusk or 8 to 5, Monday to Friday.
- Visitors must be escorted at all times in the process area.
- Security guards conduct thorough internal and external inspections of all vehicles entering the process area including undercarriage inspections. Two classes of vehicles: trusted and other. For trusted vehicles (defined as employee and company owned), a brief visual inspection by walking around the vehicle and looking inside cab and cargo hold, no undercarriage inspections. For all other vehicles, conduct thorough internal and external inspections of all vehicles entering the process area including undercarriage inspections.
- Visual external inspection of railcars focusing on undercarriage and tops of cars. Inspections may be done as the cars arrive at the loading/unloading point.

Red (Severe)

- Comply with orange, yellow, blue and green levels.
- No visitors (non-company) allowed in the plant.
- Mail is processed off-site.
- Perimeter patrols are done continually.
- Law enforcement officers are on the site 24 hours as available.
- No non-essential vehicles allowed into process areas. Essential vehicles are thoroughly searched—undercarriage, cargo holds are entered as able, cabs are thoroughly inspected.
- Railcar entry and exit points are continually manned while open. All cars entering are stopped and thoroughly inspected at the entry point—under-carriage, inside cargo holds (if safe to do so), tops of cars.

Resource 8-3: Response to Bomb Threat

Source: *Site Security Guidelines for the U.S. Chemical Industry*, American Chemistry Council, Synthetic Organic Chemical Manufacturers Association, and The Chlorine Institute, Inc., 2001.

The most popular method of making bomb threats is by telephone. It is important that as much information as possible be received from the caller. All bomb threats should be taken seriously. However, experience has shown that most anonymous threat calls are a hoax, intended to create an atmosphere of anxiety and panic in order to interrupt normal activities. Therefore, absent positive target identification (PTI) indicators or other credible information, an evacuation may not be considered appropriate.

Threats by Phone

All persons who could receive a telephone bomb threat should be taught how to handle the situation effectively. In the event a call is received, the following procedure should be followed:

- Stay calm, be courteous, and do not display fear.
- Activate telephone recording unit, if available.
- Listen carefully. During or immediately after the conversation, take notes of the exact time the call was received, the exact words of the caller, and all details such as sex of caller, accent, attitude, background noises, and motive. Use a bomb threat checklist to record the details of the call.
- Advise the caller that the building, plant, or facility may be occupied and the explosion could result in death or serious injury to many innocent people.
- Keep the caller talking; the more he or she says, the more helpful the information. If the caller does not indicate the location of the bomb or the time of detonation, ask him or her what time it is to go off and where it is located.
- After the phone call, notify the appropriate facility staff.
- Do not discuss the call with anyone else unless authorized to do so or required by law.

Threats by Mail

Following are the instructions on how to handle bomb threats received by mail. The most likely recipients are mail room personnel and secretaries.

- Place all papers and envelopes associated with the threat in a bag or large envelope (clear plastic bag if possible). Pick up any bomb threat note ONLY by the edge.

- Do not handle the written threat any more than absolutely necessary.
- Do not allow anyone else to touch the note unless specifically authorized by a security representative or senior management.

Manager's Responsibility

In all cases of bomb threat, the facilities or security manager should assess the seriousness of the threat using the following bomb threat assessment and bomb threat response guidelines. He or she should also, if appropriate, notify law enforcement authorities.

Bomb Threat Assessment

Is the threat credible?

Consider:

- Time of day and day of week
- Mode—telephone or mail
- Identity of caller—child, female/male, young/old, drunk, foul language
- Specificity of the threat—time, location, type of explosive device
- Possibility of access to allow placing of the device

Does the threat contain Positive Target Identifications (PTIs)?

Did caller identify:

- Time the bomb is to detonate?
- Target to be destroyed?
- Bomb's construction, shape, or description?
- Bomb's location?

Bomb Threat Response

What is the proper response?

Do not evacuate?	This may be an appropriate response if there have been a number of recent, publicized hoax bomb threats in the area; if the caller seemed to be drunk; if the caller was a young child, or if it is a beautiful Friday afternoon about an hour or so before quitting time. This is especially true when no PTIs were provided in the bomb threat call.
Conduct a limited or general search of the facility?	Searches are usually the most appropriate choice and should generally be the chosen response, especially if no PTIs or only one PTI was given in the threat.
Order limited evacuation, general evacuation, or move to a safe haven?	Evacuations are usually ordered only when the call is judged to be serious, the threat credible, there is insufficient time to conduct a thorough search, and the judgment is made that employees will be at less risk evacuating or moving to a safe haven than remaining in place and seeking cover. **If two or more PTIs are given in the bomb threat call, an evacuation may be in order.**

How should the chosen response be executed?

- Use a PA announcement, telephone cascade, messenger, or other local notification plan.
- Determine who is to search and in what area. In general, employees should search their own area to determine if there are any suspicious objects. Common areas should be searched by those most familiar with the areas.
- Notify public law enforcement and emergency services as appropriate; notify immediately if a suspicious object is found.
- If appropriate, determine who is to be evacuated and to what location.
- If evacuation is ordered before a search is done, determine for how long. Consider options if weather is inclement. Consider possible effect on operations if evacuation occurs at or near shift change.
- Ensure that procedures are in place to account for all persons ordered to evacuate and determine that they have in fact evacuated and there is an orderly shutdown of operations, if required.

- Coordinate with local authorities to determine if the area needs to be searched and who will determine that operations can resume and people can return to their work stations.

Search Plans

A predetermined search should be organized. It is not effective to delegate the search to the police alone because they are unfamiliar with the area and do not know which objects in the facility would look unusual or out of place. The most effective search is possible when all employees are calmly told about the bomb threat and the reason for the search and are then asked to check their familiar areas for suspicious objects. Teams should be organized to search common areas. A search team leader should be designated and a notification protocol developed to report search results to the facilities manager. A plan should be developed to designate who is responsible for searching a specific area—for example, security will search restrooms and outside areas, while facilities staff will search LAN and electrical rooms.

The objective of the search activity is to search for and report suspicious objects. There are several points to be stressed within search plans:

- The search should be systematic (divide the facility into search areas), it should be thorough, and it should be done calmly. It should be done by company personnel. Identify the areas that are most accessible to outsiders and the areas that are most vulnerable; search them first.
- When searching a room, the room should first be searched from floor to waist height, then from waist height to eye level, and finally from eye level to ceiling. If the room has a false ceiling, the false ceiling should also be inspected and searched.
- Nobody should move, touch, or jar any suspicious object or anything attached to it. The removal or disarming of a bomb must be left to law enforcement professionals.

No Bomb Found

If no bomb (or suspicious object) is found, the facilities manager should advise employees, the police, and local management and return the operation to normal activity.

Suspicious Object Found

If a suspicious object is found, the search team coordinator and the facilities manager should do the following:

- Stress again to personnel not to touch or move the object.
- Evacuate personnel from the surrounding area.
- Prevent re-entering of the evacuated area.

- Inform the police who will take charge of getting the object deactivated and removed.
- After the object has been removed, finish searching to ensure that no other bombs have been placed.

Bomb Explosion

If there is a bomb explosion, the facilities or security manager should take these steps:

- Determine if there are any injuries and attend to them immediately.
- Evacuate the surrounding area.
- Ensure no one goes near the scene of the explosion except to remove the injured.
- Control access to the area as other bombs may have been set to detonate at intervals.
- Advise police who will take charge of the situation.
- Initiate the on-site emergency plan if fire fighting or other medical response becomes necessary.

After-Action Plan

An after-action report, including incorporation of lessons learned, should be prepared immediately after resolution of the event.

Sample Bomb Threat Telephone Card

A card like this can be printed on narrow paper and placed under telephones to help employees who receive bomb threats.

Time Call Received:

Date:

Exact wording of bomb threat:

Listen—do not interrupt! After caller stops volunteering information, ask these questions, trying to keep the caller on the line:

1. When is the bomb going to explode?
2. Where is the bomb right now?
3. What does the bomb look like?
4. What kind of bomb is it?
5. What will cause the bomb to explode?
6. Did you place the bomb?
7. Why?
8. What is your address?
9. What is your name?

Record the following information:
Sex of caller:
Age:
Length of call:

Telephone number at which call was received:

Caller's voice (check the appropriate descriptors):

Calm	Disguised
Angry	Soft
Excited	Loud
Slow	Laughter
Rapid	Crying
Distinct	Normal
Ragged	Whispered
Cracking	Deep Breathing
Nasal	Accent
Stutter	Clearing Throat
Lisp	Slurred
Rasp	Deep

Familiar—If familiar, who does it sound like?

Background sounds (check the appropriate descriptors):

Street Noises	Factory Machine	Voices
Crockery	Animal Noises	Clear
PA System	Static	Music
House Noises	Long Distance	Local
Motor	Office Machinery	Booth

Other: _____

Bomb threat language (check the appropriate descriptors):

Well-spoken (educated)	Incoherent	Foul
Irrational	Taped	Threat
Read		

Your Remarks:

Your name:
Your position:

Report the call immediately to:

Resource 8-4: Response to Suspicious Mail

Source: *Site Security Guidelines for the U.S. Chemical Industry*, American Chemistry Council, Synthetic Organic Chemical Manufacturers Association, and The Chlorine Institute, Inc., 2001.

The considerations below apply to letters and packages that might contain bombs or hazardous chemical or biological materials.

Workplaces tend to receive a great number of letters and packages every day. However, not even one piece in a million contains a bomb or chemical or biological material designed to harm the recipient, and closely analyzing each piece would drastically slow down delivery. Furthermore, there is no way to prevent dangerous letters and packages from being sent. Detection and interception are the only responses possible.

A prudent, risk-based approach to detecting dangerous letters and packages is likely to involve general, initial screening by the mail clerk. Possible indicators of suspicious mail include the following:

- Lumps, bulges, protrusions, or lopsidedness
- Unusual rigidity or bulk (in an envelope)
- Handwritten or poorly typed addresses or labels
- Use of string to bind a package
- Excess postage (suggests the object was not weighed by the Post Office or a company mailroom)
- Lack of postage or uncanceled postage
- Mismatching postmark and return address
- Any foreign writing, address, or postage
- Handwritten notes, such as: "To Be Opened in the Privacy of...," "PERSONAL," "CONFIDENTIAL," or "Prize Enclosed"
- Incorrect spelling of common names, places, or titles
- Generic or incorrect titles
- Leaks, stains, strange odor, or protruding wires, string, or tape
- No return address or nonsensical return address
- Arrival before or after a phone call from an unknown person asking if the item was received

Mail that does not pass the simple, initial test should be subjected to interception (removal from the mail flow) and follow-up screening. To conduct follow-up screening,

the screener could ask the recipient whether he or she was expecting the package, call the apparent sender, or use screening technology. If the screener is still concerned after taking those steps, he or she should report those concerns as directed by the company. The screener also should not open, shake, sniff, or taste the package or its contents.

Resource 8-5: Reporting of Suspicious Purchases and Inquiries

Source: FBI Community Outreach Program for Manufacturers and Suppliers of Chemical and Biological Agents, Materials, and Equipment

In an effort to prevent Weapons of Mass Destruction (WMD) terrorism in the United States, especially those incidents that may involve large scale explosive devices or the use of chemical, biological, nuclear, or radiological (CBRN) agents, the FBI is reaching out to the community to ask for its voluntary assistance. The following information is provided to manufacturers and suppliers of CBRN materials and equipment, to better assist them in identifying suspicious purchases or inquiries.

Mission/Objective

The FBI, in an effort to thwart terrorism in the United States, is asking suppliers and manufacturers nationwide to review this publication and to voluntarily report any suspicious purchases or inquiries. This publication contains information relevant to identifying suspicious purchases, the materials or precursors that may be used in furtherance of WMD terrorist activity, and contact information that will be needed to report the activity.

What Is a Suspicious Inquiry or Purchase?

The FBI recognizes that there are literally hundreds of legitimate commercial, industrial, and agricultural applications that may require the purchase of materials or products mentioned in this publication. It is only the purchase of materials or supplies in furtherance of criminal or terrorist activity that are of concern to the FBI. This booklet contains some questions and identifiers that may assist the retail clerk, store owner, manufacturer, or supplier in distinguishing determination between a legitimate customer and one that may have illicit motives.

Guidelines

The following guidelines are provided to assist manufacturers and suppliers to more readily identify suspicious purchases of materials for the production of biological agents/toxins and chemicals or chemical precursors that could be used in an act of terrorism or for purely criminal activity.

Identifiers/Questions:

- Approach from a previously unknown customer (including those who require technical assistance) whose identity is not clear.
- Transaction involving an intermediary agent and/or third party/consignee that is unusual in light of their usual business.
- Customer's reluctance to give sufficient explanation of the chemicals to be produced with the equipment and/or the purpose or use of those chemicals.

- Customer's use of evasive responses.
- Customer's reluctance to provide information on the locations of the plant/place where the equipment is to be installed.
- Customer's reluctance to explain sufficiently what raw materials are to be used with the equipment.
- Customer's reluctance to provide clear answers to routine commercial or technical questions.
- Customer is associated or employed with a military-related business, such as a foreign defense ministry or foreign armed forces.
- Customer's reason for purchasing the equipment does not match the customer's usual business or technological level.
- Equipment to be installed in an area under strict security control, such as an area close to military-related facilities or an area to which access is severely restricted.
- Equipment to be installed in an area that is unusual and out of character with the proper use of the equipment.
- Unusual customer request concerning the shipment or labeling of goods.
- Unusually favorable payment terms, such as a higher price or better interest rate than the prevailing market or a higher lump-sum cash payment.
- Unusual customer request for excessive confidentiality regarding the final destination or details of the product to be delivered.
- Customer does not request a performance guarantee, warranty, or service contract.
- Order for excessive safety, protective, or security devices.
- Requests for normally unnecessary devices (for example, an excessive quantity of spare parts) or a lack of orders for parts that are typically associated with the product being ordered, coupled with an unconvincing explanation for the omission of such an order or request.
- Customer does not request, declines or refuses the assistance of a technical expert/training assistance when the assistance is generally standard for the installation or operation of the equipment.
- Customer unable to complete an undertaking (due to inadequate equipment or technological know-how) and requests completion of a partly finished project.
- Contractor is denied access to parts of the plant other than those directly involved with the contract.
- Contract for the construction or revamping of a plant is provided by the customer, but does not indicate the complete scope of the work and/or final site of the plant under construction.

- Packaging and/or packaging components are inconsistent with the shipping mode or stated destination.
- Modification of a plant, equipment, or item in an existing or planned facility that changes production capability significantly and could make the facility more suitable for the manufacture of chemical weapons or chemical weapon precursors. (This also applies to biological agents and weapons).
- Customer states or documents that the plant, equipment, or item is for a use inconsistent with its design or normal intended use, and the customer continues these misstatements even after being corrected by the company/distributor.
- Customer cancels sale, but then requests to purchase the exact same product with the same specifications and use, under a different name.
- Customer cancels sale, but then the exact same product is stolen or "lost" shortly after the customer's inquiry.

Chemical/Biological Materials Likely to Be Used in Furtherance of WMD Terrorist Activities

The FBI is working with other Federal agencies to assess the chemical and biological materials that may be more likely to be used in furtherance of WMD terrorism. Based upon available public source materials, FBI investigations, product availability, and the complexity of manufacture and development, the ensuing lists of chemicals, chemical precursors, and biological agents have been constructed. These lists are not absolute and are made available to provide guidance to suppliers and manufacturers.

Industrial Chemical Materials/Agents

*Ammonia
Arsenic
Arsine
Boron trichloride
Boron trifluoride
Butyric acid
Carbon disulfide
*Chlorine
Chloroacetone
*Cyanides
Diborane
Dimethyl sulfate
Dimethyl sulfoxide (DMSO)
Ethylene oxide
Fluorine
Formaldehyde
Hydrogen bromide
Hydrogen chloride
Hydrogen fluoride
Hydrogen sulfide
Mercury
Methyl phosphonothioic dichloride
Methyl phosphonous dichloride
Methyl phosphonyl dichloride
Methyl phosphonyl difluoride
N,N'-Dicyclohexylcarbodiimide (DCCDI)
N,N'-Diisopropylcarbodiimide (DICDI)
N,N'-Dimethylamino phosphoryl dichloride
Nitric acid
Phosphine
Phosphorus trichloride
Sodium azide
Sodium fluoroacetate
Sulfur dioxide
Sulfuric acid
Thallium
Thiodiglycol
Thionyl chloride
Tributylamine
Tungsten hexafluoride
2-(Diisopropylamino) ethane thiol
2-(Diisopropylamino) ethanol

*Chemical agents that may be more likely to be used in furtherance of WMD terrorism or criminal activity.

Biological Pathogens & Toxins/Others

There are many biological pathogens and toxins, such as ricin and anthrax, that are of concern to law enforcement because of their use or threatened use. These agents, if improperly handled or misused, have the potential to harm targeted individuals or several hundred persons depending on the circumstance and delivery method. Because of the implications should these agents be purchased for criminal or terrorist use, the FBI requests that careful attention be paid to individuals or entities seeking to purchase the following list of agents for non-commercial or for "independent research." The list of biological agents that appear in this booklet is based upon available public source materials, FBI investigations, product availability, and the complexity of manufacture and development. As previously mentioned, this list is not all inclusive and is made available to provide guidance to suppliers and manufacturers.

Industrial Biological Agents/Other

Abrin
Aflatoxin
Anthrax
Botulinum toxin
E. coli
Nicotine
Ricin
Salmonella
Shigella
Sodium fluoroacetate
Staphylococcus enterotoxin B (SEB)

Equipment

Equipment exists that may assist would-be WMD terrorists in the development of a functional chemical or biological device; however, at this time, the commercial applications for these products are too great and the range of choices are practically limitless. Due to these and other considerations, the FBI believes that a "short list" of equipment that could be used in furtherance of WMD terrorism would not be comprehensive nor concise; therefore this booklet will not attempt to address this aspect at this time.

Reporting Sheets

After meeting with your local WMD Coordinator and reading this publication, if you become aware of a purchase or inquiry that contains some of the above mentioned criteria, the FBI kindly requests that you voluntarily report this information to your local FBI field office. Please complete the following sheet, as completely as possible, to better assist our investigative agents.

Suspicious Inquiries or Purchases

1. Your name, organization, phone number, and mailing address

2. Your business

3. Name, business or military affiliation, telephone number, and address of the person making the inquiry or purchase (if known)

4. Product(s) or equipment being inquired about or purchased

5. Criteria being met (Match to any of the indicators mentioned in this booklet) (if applicable)

6. Date of Purchase/Inquiry or visit (list all dates if multiple contacts)

7. Other

Please contact your local FBI WMD Coordinator to report any suspicious inquiries or purchases. The FBI appreciates your cooperation and participation in this very critical outreach initiative.

Resource 8-6: Threat Collection, Analysis, and Dissemination (1)

Liaison and working relationships will be developed and maintained with appropriate national and local authorities and industry sources. This will facilitate the obtaining of intelligence in order to advise line management of actual and potential threats.

Threats will be assessed by establishing a process to collect, analyze, and disseminate information. The Security Incident Reporting System (SIRS) and other outside sources will be used for this purpose.

Travel advisories will be disseminated to line management.

Security will work with Public Affairs, where required, to develop and deliver a community relations program to obtain local information to assist in threat assessment.

Threat assessment will be a continuous process.

Responsible and Accountable Resources

Security will identify threat assessment best practices and communicate them to security business centers.

Security will be responsible for the development and update of the Design Basis Threat Statement and for strategic threat assessment. Security business centers will be responsible for local, tactical threat assessments.

Security will administer SIRS and use it to collect, analyze and assess insider, outsider, and system-induced threats and other relevant information.

Security will ensure appropriate liaison contacts are developed and maintained.

Security will disseminate travel advisories to security business centers and Travel Services.

Security business centers will ensure travel advisories are disseminated to company personnel and local affiliate travel services.

Line management, in coordination with Security, will ensure measures are in place to limit travel consistent with advisories.

Where appropriate, Public Affairs will normally be responsible for the design of community support programs. Security will be consulted as necessary.

Verification and Measurement

The number and severity of reported incidents over any given period will be evaluated by Security business centers and compared with threat assessments to establish their degree of accuracy.

Feedback

Significant increases or decreases to threat levels should be communicated to line management and a risk assessment or reassessment conducted.

Resource 8-7: Threat Collection, Analysis, and Dissemination (2)

Essential Element

7.10 A process to disseminate pertinent threat information affecting the safety of employees, the operations of the company, and the protection of sensitive information will be maintained.

Expectations

7.10.1 Special briefings on the incidence of crime, civil unrest, war, etc., will be made to employees who travel or reside in high threat areas .

7.10.2 Corporate Security will serve as a clearinghouse for corporate inquiries on real or rumored reports of security threats affecting operations and personnel.

7.10.3 Special briefing programs will be made to employees and their dependents who are scheduled to reside abroad. The briefing programs will include the existent threat in the country of assignment and countermeasures which should be taken to reduce or eliminate these factors.

9. Response to Security Incidents

Management Practice 9

Evaluation, response, investigation, reporting, communication, and corrective action for security incidents.

Companies will be vigilant in efforts to deter and detect any security incident. If an incident should occur, however, companies will respond promptly and involve government agencies as appropriate. After investigating the incident, the company will incorporate key findings and will, as appropriate, share those findings with others in industry and government agencies and implement corrective actions.

The following samples are intended to stimulate thinking and offer helpful ideas on code implementation. Other approaches not described here may be just as effective or even more effective for a particular company. If a company so chooses, it may adopt any of these sample strategies or may modify them to fit the company's unique situation.

Resource 9-1: Examples of Reportable Irregularities

Reportable Incidents	Example/Explanation
1. Any condition or event where there has been a probable violation of the company's policy on ethics	Intentional or negligent violation of laws Improper payments to government officials or others Deceit or concealment of information from higher management or internal or external auditors Falsification of books or records and other deliberate inaccuracies in recording transactions or for any other purpose
2. Conflicts of interest (COI) and other significant or unusual irregularities which may not necessarily involve the loss of company assets (see policy on conflict of interest)	Employee activities related to, but not limited to: - Ownership of related business interest - Spouses in substantially identical employment - An employee, employee's spouse, or any dependent member of the employee's family to participate in any transaction in stock, options or other securities of the corporation, any of its affiliates, or any other company on the basis of material information not yet made public - An employee, employee's spouse, or any dependent member of the employee's family purchasing or selling puts, calls, or other options on the corporation's stock - Ownership of equipment/facilities, rented/leased to the company or company contractors - Receipt of gifts, entertainment, or loans. - Misuse of company information - Outside employment to the detriment of job performance - Outside directorships
3. Losses suffered by those with whom the company does business due to dishonest acts by company employees or agents	Losses caused by dishonest acts of company employees and agents to customers, suppliers, contractors, joint venture partners, etc.

4. Misuse of assets, defalcations, or embezzlement by company employees or agents	Misappropriation or theft of cash, inventories, plant and equipment or other company property by employees/agents. Misuse of corporate credit card.
5. Losses suffered as a result of dishonest acts by suppliers, contractors, or others	Losses to the company (>$5k) resulting from activities such as: - Intentional short deliveries of materials - Falsification of records such as billings for labor or materials - Intentional misrepresentation of quality of materials used/delivered
6. Thefts, burglaries, robberies, and holdups involving company property by outside parties	Losses to the company (>$5k) resulting from activities of outside parties
7. Losses or suspected losses of company proprietary or private information	Information significant in content, scope, and nature, even though a precise value cannot be readily established
8. Unauthorized access to computer systems or computer programs	Intentional access (by employees, contractors or outside parties) to computer information, which is either unauthorized or circumvents intended controls
9. Disappearance or unexplained loss of company assets	Excludes operational losses attributable to processing, handling, storing, and delivery of bulk products or normal operating losses of packaged products and materials, supplies, equipment and cash resulting from clerical errors or omission (however, losses above departmental tolerance levels that cannot be explained should be reported)

Note: irregularity reports should be prepared even if the full amount (loss) involved has been or will be recovered.

Resource 9-2: Security Incident Reporting and Response Policy

1.1 SCOPE

This standard defines the management systems that must be in place to ensure that, following an incident, the appropriate notification, classification, investigation, reporting, and recommendations closeout are completed expeditiously in order to prevent recurrence.

1.2 FIELD OF APPLICATION

This standard applies to all manufacturing, laboratory, storage terminal, pipeline, and R&D facilities operated by ABC Corporation.

2.0 REFERENCES

2.1 LAWS AND REGULATIONS

2.1.1 All applicable laws and regulations.

2.2 COMPANY STANDARDS AND REFERENCES

2.2.1 Company Crisis Management Plan

2.2.2 Emergency Preparedness and Response

2.2.3 Safety Critical Variable Monitoring

3.0 RESPONSIBILITIES

3.1 PROCESS OWNER

The owner of the process described in this standard is the General Manager, Manufacturing.

4.0 DEFINITIONS

4.1 INCIDENT: An occurrence or condition which resulted in or could have reasonably resulted in an undesired outcome such as, but not limited to, an injury, illness, fire, explosion, spill, property damage, a significant production interruption, or release of hazardous chemicals into the environment.

4.2 INVESTIGATION REPORT: A written document organized in a standard reporting format that contains the investigating team's findings, conclusions, and recommendations.

4.3 INCIDENT INVESTIGATION: The process of identifying the root cause of incidents and recommending steps to prevent similar events from recurring.

4.4 MAJOR COMPLIANCE ISSUES: Those issues that could potentially subject the company to substantial liability, result in a significant enforcement action, or impose a significant monetary impact on the enterprise.

4.5 SAFETY CRITICAL VARIABLE: A process variable (or set of variables) established by a team of experts knowledgeable in the technology where operation outside of the safety critical limits would compromise a safety system design and present a Category IV or V hazard as defined in the corporate procedure for risk assessment and risk classification.

4.6 SAFETY CRITICAL LIMIT: The predetermined level or value of a safety critical variable at which troubleshooting ends and immediate, pre-established action is taken. The safety critical limit is the level at which the process will no longer be intentionally operated.

4.7 CORPORATE EMERGENCY RESOURCE TEAM: A management team charged with strategic decision making, internal direction, and rapid commitment of the company's resources to effectively mitigate the adverse consequences of events that pose a significant threat to the well-being of the company, its employees, or the community.

4.8 LEVEL ONE INCIDENT: Any incident that does not meet the threshold of a Level Two, Three, or Four incident. Incidents in this category include abnormal conditions that, if left uncorrected, could develop into more substantial consequences.

4.9 LEVEL TWO INCIDENTS: Level Two Incidents involve the following:

4.9.1 OSHA recordable injuries or illnesses.

4.9.2 An incident that results in an unplanned release in excess of permitted or otherwise authorized levels to the environment.

4.9.3 A release of a chemical into the environment in an amount that equals or exceeds reportable quantities. This includes release from emergency flares.

4.9.4 Fire requiring response from the site Emergency Response Team.

4.9.5 Exceeding a safety critical limit.

4.9.6 Release of materials that pose a threat to the health and safety of workers within the facility.

4.10 LEVEL THREE INCIDENTS: Level Three Incidents involve the following:

4.10.1 Admission of employee(s) or contractor(s) to a hospital for an overnight stay for more than observation purposes.

4.10.2 Fire or explosion that requires actual fire fighting or other assistance from organizations outside the facility (mutual aid) or results in major damage or downtime to the unit involved.

4.10.3 Release of materials that pose a potential threat to the health and safety of members of the public or results in a shutdown or evacuation outside the release area.

4.10.4 Major compliance issues.

4.10.5 Community impact or significant media interest.

4.11 LEVEL FOUR INCIDENTS: Level Four Incidents involve the following:

4.11.1 Single fatality or permanent disabling injury to any person, or hospitalization for more than observation purposes of three or more employees, contractors, or members of the public.

4.11.2 An incident that results in significant business interruption.

4.11.3 An incident that has the potential to focus extensive adverse news media and public attention on the company;

4.11.4 Release of materials which results in the evacuation of off-site facilities; restricts the navigational or recreational use of a water way; or affects a source of drinking water.

4.12 ENVIRONMENT: Includes rivers, streams, lakes and other water bodies; the ground, groundwater, and ambient air.

4.13 REPORTABLE QUANTITIES (RQ): A quantity of material which, when released, requires internal reporting and investigation.

5.0 REQUIREMENTS

5.1 INCIDENT REPORTING AND INVESTIGATIONS

5.1.1 Each site shall have a process for immediate reporting of incidents to supervision and/or management and a procedure to investigate incidents.

5.1.2 Site Management or their representative(s) shall determine the level or classification of the incident.

5.1.3 Incident investigation reports shall contain the following sections:

5.1.3.1 Title of the incident,

5.1.3.2 Date of the incident,

5.1.3.3 Names of individuals serving on the investigation team including the chairperson or team leader,

5.1.3.4 Date the investigation began,

5.1.3.5 Summary of the incident,

5.1.3.6 Chronology of events or findings,

5.1.3.7 Incident cause(s),

5.1.3.8 Recommendations,

5.1.3.9 Attachments and/or supporting documents, and a

5.1.3.10 Signature page for appropriate approval and sign-off.

5.1.4 Incident investigation reports are considered to be in "draft" form and confidential (i.e. circulation restricted) until the investigation team signs and issues the final incident report.

5.2 LEVEL ONE INCIDENTS

5.2.1 All incidents must be reported and recorded. Site management must decide if Level One incidents should be investigated or simply recorded for trend analysis.

5.2.2 All incidents shall be classified on the basis of what the incident could have become instead of what it actually was. The level of investigation may be upgraded depending on the potential seriousness of the incident.

5.3 LEVEL TWO INCIDENTS

5.3.1 Include requirements for Level One incident investigations.

5.3.2 Team members should be selected from the site and have expertise relevant to the process being investigated. A contract representative must serve on the investigation team if the incident involved a contract employee or work of the contractor.

5.3.3 Preset site procedure defines minimum requirements.

5.3.4 Investigations shall begin within 48 hours.

5.3.5 Investigation reports shall contain corrective actions that include, identification of the person(s) assigned specific responsibility for follow-up on the recommendations and the timing to close.

5.4 LEVEL THREE INCIDENTS

5.4.1 Include requirements for Level One and Two incident investigations.

5.4.2 Investigation team must be multi-disciplined with expertise relevant to the process being investigated and must consider having at least one team member from outside the facility.

5.4.3 Requires Legal Department notification by site management. Site management and Legal will determine the extent of the Legal Department's involvement.

5.4.4 Requires notification of the Corporate Emergency Resource Team as soon as possible.

5.4.5 Incident investigations must utilize an industry-recognized formal investigation process.

5.4.6 Requires preservation and control of the incident scene as soon as practical following the incident.

5.4.7 A preliminary report will be issued to local management within 10 working days in the local language.

5.5 LEVEL FOUR INCIDENTS

5.5.1 Include requirements for Level One, Two and Three incident investigations.

5.5.2 Investigation team must be multi-disciplined with expertise relevant to the process being investigated and must consider having at least one member of the team from outside the company.

5.6 CORRECTIVE ACTION

5.6.1 Each site shall have a mechanism within their incident investigation process to promptly address and resolve incident report findings and recommendations. This system shall address the following minimum requirements:

5.6.1.1 Clear identification of corrective action measures for each recommendation.

5.6.1.2 Assigned responsibility for follow-up of each recommendation.

5.6.1.3 Periodic up-dates to site management concerning the progress being made toward completion of recommendations.

5.6.1.4 A process by which recommendations and reports receive final closure.

5.7 SITE INFORMATION SHARING

5.7.1 Final incident investigation reports shall be reviewed with all affected personnel whose job tasks are relevant to the incident findings including contract employees where applicable.

5.7.2 Historical incident data, analysis, and trends should also be shared with employees to heighten awareness of potential problem areas.

5.8 COMPANY INFORMATION SHARING

5.8.1 Final Level Three and Four incident investigation reports shall be in English and receive Company wide distribution. The sites will forward final Level Three and Four incident reports to the Manager, of Corporate Safety for distribution within the company.

6.0 REPORTS AND RECORDKEEPING

6.1 INCIDENT REPORTS

6.1.1 Reporting, filing, and maintaining incident investigation reports shall be the responsibility of the site where the incident occurred.

6.1.2 Final incident investigation reports shall be retained on file at the incident site or other designated location for a period of current year plus five years.

Resource 9-3: Security Incident Reporting and Analysis

Source: *Site Security Guidelines for the U.S. Chemical Industry*, American Chemistry Council, Synthetic Organic Chemical Manufacturers Association, and The Chlorine Institute, Inc., 2001.

By keeping detailed records of security incidents, managers may be able to spot trends and piece together facts that lead to successful investigations. Some security managers use incident management software, which has graphing, charting, and search functions that can help bring an offense or loss pattern to light and identify issues of security concern.

Incident data will only be available for analysis if incidents are reported and recorded. Managers may wish to establish several channels for incident reporting. For example, they may decide to promulgate the phone number and e-mail address of the person in charge of security. Some companies have set up anonymous employee hot lines to encourage employees to report suspicions. It may also be useful to make it obligatory for employees to report security incidents.

Resource 9-4: Irregularity Response Table

Responsibility for assuring that an adequate and thorough investigation is initiated into an alleged irregularity rests with local functional management. Audit, Controllers, Law, and Security play key roles in the investigation and reporting process. An agreed investigative process flowchart has been developed by Audit to ensure that consistent responsibility assignment and coordination is applied to all investigations.

Security violations have the same notification requirement as any reportable irregularity. See following table for examples of reportable irregularities.

Nature of Potential Irregularity Identified	Immediate Action: Parties Notified or Involved	Preliminary Communication	Investigation: Facts Established or Confirmed	Interim Reporting	Decision Re Reportable Violation / Further Reporting Requirement	Advice to Senior Management	Discipline Determined	Final Reporting
Ethics Violation: Conflict of Interest	Audit, Law, HR, Controllers, Security, and appropriate local management are notified immediately. Each function is responsible for ensuring that the others are informed. Audit advises on nature of potential irregularity to facilitate future reporting.	Known facts documented; Audit mgmt. kept advised; formal reporting not yet required.	Audit, Security, and local functional management determine investigation strategy and approach. Joint participation is appropriate on front end; Audit or Security may opt out of further involvement depending on nature of incident.	Report prepared by local functional mgmt. with input from investigating team; submission to general auditor.	General auditor (in consultation with law where legal compliance is in question).	Local sr. mgmt. is informed and, in turn, communicates with HQ functional mgt. General auditor provides input to HQ mgmt. as requested.	Audit advises both local sr. mgmt. and functional headquarters mgmt. re discipline in comparable cases. Local sr. mgmt. confers w/ functional headquarters mgmt. on discipline. Law/HR consulted/involved as appropriate. Audit endorses final discipline recommendation.	Communication from local sr. mgmt. to functional HQ mgmt. required for ethics violations and for significant conflict of interest cases.
Other Major Irregularities with Employee Involvement		Preliminary information communicated to Audit, Security, and Controllers. General auditor notified of any incident >$25k.		Report may be prepared/ submitted to Audit, Security, and Controllers.	General auditor.			[Report name] generally serves as final reporting.
Other Irregularities					Determined by local functional mgmt. with advice from Audit as appropriate.	Local functional mgmt. informed in line with local guidelines. Functional headquarters mgmt. and HQ advised by Audit for incidents >$50k.	Audit endorses final discipline recommendation re: employees. Actions re third parties determined locally at appropriate level of mgmt. Audit involved in advisory capacity.	Report prepared by local functional mgmt. submitted to general auditor for irregularities: -->$5k --unusual in nature --involving [certain category of] employees.

Resource 9-5: Investigation Guidelines (1)

Source: *Site Security Guidelines for the U.S. Chemical Industry*, American Chemistry Council, Synthetic Organic Chemical Manufacturers Association, and The Chlorine Institute, Inc., 2001.

Suspicious incidents and security breaches (of company policies) should be investigated by trained professionals. Site management should refer such incidents to corporate counsel or corporate security management. Any suspected illegal activity should be reported for referral to law enforcement, if appropriate.

The following are some types of security incidents that might warrant investigation:

- Doors not secured, holes in fence lines, indication of illegal entry
- Unauthorized egress by personnel in restricted areas of the facility
- Signs of vehicles in restricted areas along pipelines, fence lines, electrical substations, or remote plant security gates
- Individual asking for technical information about the facility that could be used by an adversary to cause harm
- Major unexplained process upsets
- Unexplained loss of containment of hazardous material
- Unexplained loss of raw material or product
- Major cyber attack against internal process control systems

Resource 9-6: Investigation Guidelines (2)

Essential Element

7.8 Standards will be developed to ensure that all security investigations are within legal guidelines, are well-planned, and are factually reported and conveyed to proper authorities.

Expectations

7.8.1 Security investigations must be authorized in writing by corporate or site management, as appropriate, to ensure that the purpose and limits of the investigation are clearly understood.

Guideline:

Investigate guidelines developed by Corporate Security will be reviewed and authorized by Corporate Legal and site management representatives.

7.8.2 All investigations must be conducted in compliance with all applicable laws regarding the conduct of private investigations.

7.8.3 All investigations will be documented as appropriate. Documentation should include, but not be limited to:

- Purpose/subject of investigation
- Person authorizing investigation
- Dates
- Investigator
- Interviewees
- Case summary
- Follow-up action

7.8.4 The director of corporate security, with authorization of the ABC Corporation vice president responsible for health, safety, environment, and security, can assume primary responsibility for an investigation related to security matters.

Guideline:

All security-related losses of over $2,000 (USD) will be reported to Corporate Security.

Resource 9-7: Crisis Management Guidelines

Essential Element

7.6 A documented process will be maintained to manage crises which occur within the company.

Expectations

7.6.1 A Corporate Crisis Management Team (CCMT) will be established to decide policy issues, to manage any crisis, and to work with Corporate Communications to develop a public relations strategy.

7.6.2 A Corporate Crisis Operation Center will be established to provide the proper support facilities for the management of crises.

7.6.3 Each site will develop a documented crisis management plan which addresses, at a minimum, response to the crisis, coordination with a Corporate Crisis Management Team, and public relations, political, and security aspects.

Guideline:

The plan shall:

1. Provide for periodic contact with local authorities, such as police, embassy officials, and government agencies.

2. Include conducting and critiquing tabletop exercises on various types of crises (kidnappings, industrial accidents, or labor or civil unrest), as appropriate, on a yearly basis.

3. Provide for sufficient dedicated support equipment, including telephones, commercial radios, computer, intraplant radios or cellular phones, and site engineering drawings, as appropriate.

10. Audits

Management Practice 10

Audits to assess security programs and processes and implementation of corrective actions.

Companies will periodically assess their security programs and processes to ensure that those programs and processes are in place and working. If the assessments identify opportunities for improvement, the company will promptly take corrective action. Based on risk, it may also be appropriate to assess the programs and processes of other companies with which the company conducts business, such as chemical suppliers, transportation service providers, or customers.

The following samples are intended to stimulate thinking and offer helpful ideas on code implementation. Other approaches not described here may be just as effective or even more effective for a particular company. If a company so chooses, it may adopt any of these sample strategies or may modify them to fit the company's unique situation.

Resource 10-1: General Policy on Security Self-Assessments

Security self-assessments are an important tool to bring our security systems and programs up to expectations and maintain them at that level. They should be used to identify gaps in security systems against. Security self-assessments are a very effective way of identifying areas where efforts should be focused to achieve the desired state of readiness, consistent with local levels of threat.

The corporate template for conducting security self-assessments should be tailored to the different business lines, as needed.

Resource 10-2: Specific Policy on Security Program Reviews

Security programs should routinely be reviewed and tested to ensure proper deployment, identify weaknesses, incorporate lessons learned, and develop corrective actions. A security business center advisor or the corporate security contact normally reviews program compliance on behalf of or in close cooperation with line management. These reviews should be fact-finding, not fault-finding, and should focus on normal operations. Areas for review should include these:

- Guard Force
  - Are written post orders in place?
  - Are post orders suitable?
  - Are post orders known and complied with by guards?
- Access Procedures
  - Are written access procedures in place?
  - Are they followed?
  - Are badges displayed?
  - Are visitors identified, processed and escorted?
  - Is there a provision for controlling vehicular movement/parking?
  - Are procedures in place to deal with lost or stolen id badges?
  - Are access records routinely updated and reviewed?
- Search Procedures
  - Are written procedures in place?
  - Are visitor packages and briefcases screened?
  - Are visitor vehicles checked in an effective manner?
  - Are random, unannounced contraband searches conducted?
- Badge Management
  - Are procedures in place to deal with lost or stolen ID badges?
  - Are access records routinely updated and reviewed?
- Restricted Areas
  - Is access to sensitive areas restricted?
  - Are data logs reviewed for anomalies and updated access?
- Perimeter
  - Is the perimeter fence in a good condition?
  - Is perimeter lighting suitable?

- Emergency Procedures
  - Are bomb threat procedures current and tested?
  - Do operators and telephone receptionists have bomb threat questionnaires?
  - Are operators and telephone receptionists trained to handle bomb threat calls?
  - Are activist guidelines in place?
  - Are alarms and response to alarm events tested?
- Information Security
  - Are procedures in place to protect information?
  - Are after-hour inspections conducted to ensure the proper safeguarding of information?
  - Is regular Management Protection of Information (MPI) awareness training conducted?
- Personnel Protection
  - Are drivers/escorts trained on defensive driving, and protective driving if required?
  - Are alarm systems properly tested?

Resource 10-3: Security Management Benchmark/Audit Protocol

Facility: _____ Date(s) of Audit: _____

Auditor: _____

Period Under Review: _____

This protocol serves as a guide for planning and conducting security management benchmarks and audits at ABC Corporation. This protocol is based upon the minimum requirements outlined in the corporate management standard CMS-HSE-06, Security Management. It may require modification to meet the needs of facility-specific benchmark and audit objectives or facility organization considerations. This protocol consists of the following sections:

A. Introduction

B. Understanding Management Systems

C. Protocol Topics Prioritization and Verification Planning

D. Testing and Verification

- General
- Management Commitment
- Access and Egress Control
- Asset Protection
- Security Incidents
- Corrective Action
- Reports and Recordkeeping

E. Summarize Audit Results

Attachment 1: Facility Findings Prioritization

A. Introduction

Background Information Review (Pre-Audit Preparation)

1. Review program procedures and other background information obtained from the facility to develop a general understanding of the security management system.

2. Review the report for the last corporate audit on this topic and any available internal assessments to identify prior issues identified with the facility program. Also review the action item closure status for these reports.

3. Review the facility organization chart and the initial interviews planned for this topic. Discuss with the audit team leader any additional interviews of key program contacts that should be scheduled for the first day of the audit.

Protocol Modifications (Pre-Audit Preparation)

4. Modify this protocol as appropriate (based on the review of the background information) to provide emphasis on the key issues. Add steps to the protocol and develop specific checklists, etc., as appropriate. Review the interview questions in sections B and D and modify as appropriate. It will be useful to group together on a single list the questions (in sections B and D) that are appropriate for each of the program contacts to be interviewed.

Safety Orientation

5. The standard safety orientation will be provided by the facility to any team members who require this or desire a refresher review of the key facility safety rules and emergency procedures. The team leader will discuss key safety considerations for auditors at this time or at the first team meeting prior to field activity.

Opening Meeting

6. The audit team leader will lead a brief opening meeting with the facility management in which the team members will be introduced to the staff. The purpose of the audit will be reviewed and the scope and schedule discussed. Any changes necessary in the pre-arranged interviews planned for the first day of the audit should also be noted. A short overview presentation by the facility on the processes at the site is an optional element of the opening meeting. The team leader will request this from the facility if it is deemed to be value added for the audit.

Orientation Tour

7. The audit team leader will have prearranged a facility tour with the site hosts for the purpose of general layout familiarization if this is needed for team members not familiar with the site. As an alternative, team members may choose to have a more focused tour with their facility topic contact to be arranged at a mutually convenient time.

B. Understand Management Systems

(Refer to the Auditor's Field Guide for key techniques and considerations in developing this understanding.)

1. After a review of company standards, facility program procedures and other background information (noted in A.1. above) has been completed, the program contact (and other pre-arranged key contacts) will be interviewed to develop an understanding of the facility systems in place relevant to the protocol topics. In addition to developing an overall understanding of how these systems are designed to work, the following information should be obtained from these interviews:

   - Identification of other individuals who should be interviewed that have key roles with any of the systems being reviewed.
   - Location of records and other documentation which will be reviewed.
   - Information which should be obtained from the key program contacts that is specified in the relevant test and verification steps for each protocol topic.

Specific points to include in the key program contact interviews are described below for each protocol topic:

Note: The designation as a key program contact means a contact with whom an interview is needed (and will typically be pre-scheduled for the first day of the audit) to complete the understanding of management systems phase in the audit process.

General

2. Develop an understanding of the content of the facility's security management system. The following questions are suggested along with others the auditor may develop during the protocol modification as described in Section A: (Note: As part of your pre-audit preparation, obtain and review any written procedures that the facility has developed for its security program.) Provided below are some suggested questions to ask the key program contact person(s):

   - What written procedures are used by the facility to communicate/ document its practices and requirements for security management, including such areas as general facility security, and intellectual property protection? Obtain copies of any procedures that you may not have for your review. Example documents/ written procedures may include:
     - Security procedures/plan
     - Security structure/organization chart
     - Security incident reporting procedures
     - Security incident report log
     - Site security training practices
     - Security training records
     - Outside law enforcement assistance and coordination plan

– Others

- How broad is the security program at the facility (e.g., access/egress control, intellectual property protection, other)? Ask key program contact(s) to describe the universe of coverage under the facility's program.

3. The auditor may also complete the portion of Testing and Verification in Section D, step 1.

IMPORTANT: Note of Interpretation Regarding Intellectual Property and IT (Computing Infrastructure) Portions of the Security Management Standard

A. The intent of the language in section 5.3.2.3 of the standard, which covers protection of intellectual property, is to ensure that Research and Development information (including patent information) and plant design information are protected. The level of control required for R&D information is three layers of protection, and for plant design information is at least two layers of protection.

The following are considered as layers of security protection:

- Good facility perimeter access control via barriers such as fences and routine patrols by security staff is one layer.
- Controlling access to buildings via keyed locks or card entry systems is one layer.
- Locking the door at the entrance of the room containing the sensitive information is one layer.
- Locking the cabinet containing the information is one layer.
- Diligence by responsible personnel while in possession of sensitive materials, in the room with the materials, or along a hallway containing rooms with sensitive information is one layer.

…

Management Commitment

4. Develop an understanding as to how the facility manages its security process. Review the following suggested discussion points and questions, along with others the auditor may develop:
   - How does the facility manage and update its security procedures/ plans?
   - What functions, and their respective persons, has the site identified as having responsibility and accountability for the security programs and systems, including such areas as:
     – General facility security?
     – Intellectual property protection/ controls?

  - Are any key responsibilities overlapping, shared or conflicting?
  - What training is provided to appropriate personnel?
- What systems are in place to maintain cooperative relationships with local law enforcement agencies?
- How does the facility review the overall implementation and effectiveness of its security plan? To what extent does facility management review, measure, and evaluate results achieved against established criteria?

5. The auditor may also complete the portion of Testing and Verification in Section D, step 2 (for key program contact interviews) during these initial interviews.

Access and Egress

6. Develop an understanding as to how the facility monitors and controls access and egress. The following discussion points and questions are suggested, along with others the auditor may develop:

   - What are the practices to ensure all points of access and egress are identified?
   - What are the practices to ensure:
     - Entry of all employees, contractors and visitors is controlled?
     - Egress of all employees, contractors and visitors is controlled?
   - What are the practices to:
     - Provide identification to employees, contractors, and visitors?
     - Define documentation necessary to obtain contractor or visitor identification and that they have legitimate business at the site?
   - What methods are used to notify appropriate site personnel in the event of a breach in security?
   - What are the procedures for regular inspections of the facility's perimeters?

7. The auditor may also complete the portion of Testing and Verification in Section D, step 4 (for key program contact interviews) during these initial interviews.

Asset Protection

8. Develop an understanding as to how the facility assets are protected. The following discussion points and questions are suggested, along with others the auditor may develop:

   - What processes are used for protection of physical and intellectual property assets? For example:
     - Control the removal of materials and equipment from site.
     - Assure return of company property to site.

  - Protect intellectual property.
- What processes are used to identify possible theft, fraud, or unauthorized access to company assets?

9. The auditor may also complete the portion of Testing and Verification in Section D, step 8 (for key program contact interviews) during these initial interviews.

Security Incidents

10. Develop an understanding of the facility's practices in response to security incidents. The following discussion points and questions are suggested, along with others the auditor may develop:

- What is the procedure for reporting security incidents at the site?
- What are the procedures for responding to security incidents?
- How and where are security incidents recorded?
- What site function(s) has ownership for filing and maintaining security incident reports/documents?
- Is there an incident log or other similar document for recording incidents? If so:
  - What types of incidents are included?
  - Where is it located?

11. The auditor may also complete the portion of Testing and Verification in Section D, step 11 (for key program contact interviews) during these initial interviews

Corrective Action

12. Develop an understanding of the facility's practices to ensure appropriate action is taken in response to security incidents. The following discussion points and questions are suggested, along with others the auditor may develop:

- What process is used at the site for taking corrective action in response to security incidents?
- Who is involved in this process?
- How well does this process seem to work?

13. The auditor may also complete the portion of Testing and Verification in Section D, step 14 (for key program contact interviews) during these initial interviews.

Reports and Recordkeeping

14. Develop an understanding how incident reports are maintained. The following discussion points and questions are suggested, along with others the auditor may develop:

    - Who has ownership for this process?
    - Where are the reports maintained?

15. The auditor may also complete the portion of Testing and Verification in Section D, step 16 (for key program contact interviews) during these initial interviews.

C. Protocol Topics Prioritization and Verification Planning

1. Using the knowledge gained from the review of program procedures and interviews with the key program contacts, prioritize the protocol topics using the matrix in Figure C1. This should be endorsed by the team leader.

2. The completed prioritization of topics will be presented to the team and a verification plan developed to execute the protocol, taking into account the priority of each topic. Also consider these priorities when developing the sampling strategy for records review and field tour steps for each topic and in defining the appropriate number of employee interviews for each topic. The verification plan should be endorsed by the team leader.

3. The team will discuss opportunities for cooperation between the auditors to improve the overall audit efficiency and minimize audit impact on the facility. Consider the following areas for cooperation:

    - Employee interviews
    - Records reviews
    - Field tour focus items

Figure C1 - Protocol Topics Prioritization

Strength of Management Systems	*Strong*	Fourth	Second
	Weak	Third	First
		Low	*High*
	Potential Impacts from Failure of Management Systems		

PROTOCOL TOPIC: PRIORITY

A) General _____

B) Management Commitment _____

C) Access and Egress Control _____

D) Asset Protection _____

E) Security Incidents _____

F) Corrective Actions _____

G) Reports and Recordkeeping _____

PREPARED BY: _____

APPROVED BY: _____
Team Leader, Date

Verification Strategy					
Person to be Interviewed or Document Reviewed	**Date/time of Interview**	**Time Required**	**Sample Technique, Size & %**	**Applicable Protocol Sections (Consider overlaps with other protocols)**	**Reason for Interview (Issue/gap anticipated from management review)**

D. Testing and Verification

General

Procedures Review

1. Obtain and review written procedures that the facility may have for its security management program. Procedures may include such areas such as:
   - General facility security
   - Intellectual property protection
   - Other

Management Commitment

Program Contact Interviews

(Important note: Where applicable, interviews conducted for the Management Commitment protocol topic can be most efficiently completed in conjunction with interviews needed for the access and egress control, asset protection, security incidents, corrective action, and report and recordkeeping protocol topics listed in Section D. This will eliminate the need to interview the same person(s) more than once for collection of information common to these protocol topics.)

2. Verify the following through interviews with the key program contact person, security manager, site management or other applicable personnel:
   - How are responsibilities and accountabilities for program implementation clearly defined, established, and communicated? Some suggested questions include:
     - Has the site identified persons as having responsibility and accountability for the site security program and systems?
       - General facility security?
       - Intellectual property protection/controls?

       If so, describe. Who are they?
     - Are systems in place to involve key functions in the above security processes? (5.1.3)
       - If so, how?
       - What are the key functions at the site that are involved?
   - Is training provided to appropriate personnel having security responsibility? Some suggested questions include these:
     - How does the site determine the level of training required?

- Who is responsible for ensuring that appropriate personnel have the required training?
- What personnel require such training?
- What specific training is required?
- Is refresher training required to maintain proficiency?
  - If so, how is this accomplished?
  - Who is responsible for ensuring appropriate personnel have the required refresher training?
  - What personnel require such training?
- Interview a sample of affected personnel (e.g., security personnel) to verify status of training.

- How are cooperative relationship established and maintained with local law enforcement agencies?

Documentation and Records Review

(Important dote: This documentation and records review step can be most efficiently completed in conjunction with a review of documents and records needed for the access and egress control, asset protection, security incidents, corrective action, and report and recordkeeping protocol topics.)

3. Develop a list of applicable training records that may be on file. Review the records to verify the delivery/receipt of training.

Access and Egress Control

Program Contact Interviews

4. Review the facility's security management practices/systems for preventing unauthorized entry and exit of personnel and materials into and out of the facility. Verify the following through interviews with the key program contact person, security manager, site management, or other applicable personnel:

   - That points of access and egress are identified. Some suggested questions include:
     - How is this accomplished?
     - What are the points of access and egress into and out of the facility?
     - Are they controlled?
   - That access and egress are controlled:
     - Are access/ egress points controlled by gates? (5.2.1.2)
     - Is there perimeter fencing? (5.2.1.2)

- How are maintenance and monitoring of access/ egress controls accomplished? (5.2.1.2)
- Are facility perimeters inspected regularly? (5.2.1.6) Some suggested questions include:
  - At what frequency?
  - Is there a formal inspection schedule?
  - Who has responsibility for these inspections?
  - How are deficiencies documented and corrected?
    - Is there formal documentation?
    - Where is the documentation kept?
    - What is the process to correct deficiencies?
- During field verification, review the existence and condition of gated areas, perimeter fencing, and other such controls.
  - Practices to check incoming materials (e.g., random inspections of incoming and outgoing personnel and vehicles, check of incoming materials against authorizing paperwork, etc.).

- That a system is in place to ensure identification is provided to employees, contractors, and visitors. Some suggested questions include:
  - Who provides this identification to:
    - Employees?
    - Contractors?
    - Visitors?
  - What form of identification is provided?
  - What are the requirements to display/ wear this identification?
  - When does the person receive and return this identification?
- That a process is in place that defines the documentation necessary to obtain contractor or visitor identification and that the person has legitimate business at the location. Some suggested questions include:
  - What is the process used by the facility to determine what documentation is required?
  - What type of documentation is required before entry into the site?
  - Is a site person to be contracted for further verification at the time of entry?
- That procedures are in place that define actions to be taken in response to unauthorized access. Some suggested questions include:
  - What are the procedures in response to unauthorized access?

- What action does the site take?
- Who is contacted on site?
- Under what circumstances is an outside law enforcement agency contacted?

Security Employee Interviews

5. Interview a sample of security personnel to verify that:

   - Facility perimeter inspections are conducted. Some suggested questions include:
     - Who conducts them?
     - What areas are inspected?
     - At what frequency?
   - Deficiencies are documented.
   - Corrective actions are taken.

Employee Interview

6. Interview a sample of employees and contractors. Some suggested questions include:

   - How is access and egress controlled for employees, contractors, or visitors entering or leaving the facility?
   - How well does the process seem to work?
   - Are you aware of any problems with the process? If so, describe.
   - What are the facility's requirements to display/wear identification?

Documentation and Records Review

(Important note: This documentation and records review step can be most efficiently completed in conjunction with a review of documents and records needed for the management commitment, asset protection, security incidents, corrective action, and report and recordkeeping protocol topics.)

7. Develop a list of security inspection records and deficiencies reports that may be on file. Review the records and reports to verify that:

   - Facility inspections are conducted.
   - Frequency inspections are conducted.
   - Deficiencies from inspections are identified and documented.
   - Deficiencies are corrected.

Asset Protection

Program Contact Interviews

8. Review the facility's security management practices/ systems for protection of physical and intellectual property assets. Through interviews with the key program contact person, security manager, site management or other applicable personnel, verify the following:

    - That processes are in place to account for materials and equipment and to identify possible theft or fraud. Some suggested questions include:
        - Who oversees this responsibility at the site?
        - What are the procedures in the event of possible theft or fraud?
    - That processes are in place to ensure that company assets taken off-site are returned. Some suggested questions include:
        - What procedures are used to:
        - Control unauthorized removal of company assets from the site?
        - Assure the return of company assets (e.g., property pass system)?
    - That processes are in place to protect intellectual property and identify attempts to access such information by unauthorized individuals. (5.3.2.3) Some suggested questions include:
        - Who oversees this responsibility at the site?
        - What practices are used at the site to identify the existence of intellectual property and the location(s) where such property is stored?
        - How does the site ensure that such property is securely stored?

Employee Interviews

9. Interview a sample of employees and contractors. Some suggested questions include:

    - What procedures are used to control unauthorized removal of company assets/property from the facility?
        - What authorization is required before removal of company assets/property?
        - How is this authorization obtained?
        - How does the facility ensure that company assets taken off site are returned?
    - For holders of intellectual property:
        - How is the security of such property managed?

- Are you aware of any instances where this security was breached? If so, was it properly reported to management?

Documentation and Records Review

(Important note: This documentation and records review step can be most efficiently completed in conjunction with a review of documents and records needed for the management commitment, access and egress control, security incidents, corrective action, and report and recordkeeping protocol topics.)

10. Determine the types of records that may be available for:
    - Authorizing removal of company assets/property from the site.
    - Documenting return of company assets/property.

Review a sample of these records to assess effectiveness of procedures/ processes.

Security Incidents

Program Contact Interviews

11. Verify that the following action steps are in place for addressing security incident through interviews with the key program contact person, security manager, site management, or other applicable personnel:
    - Procedures or processes are in place and communicated for reporting security incidents at the facility.
    - Procedures are in place for responding to security incidents.
    - Security incidents are recorded and reported to facility management in a timely manner.
    - Systems are in place to maintain records and analyze data to evaluate performance, determine trends, and identify areas for improvement.

Employee Interviews

12. Interview a sample of employees and contractors. Some suggested questions include:
    - What is the procedure for reporting security incidents (e.g., incidents such as unauthorized facility entrance/ exit, missing property, possible property theft, company/ personal fraud, attempts to access intellectual property by unauthorized individuals, etc.
    - Are you clear on what to do if you observe a possible breach of security, suspect property theft, notice property missing, etc.?

Documentation and Records Review

(Important note: This documentation and records review step can be most efficiently completed in conjunction with a review of documents and records needed for the management commitment, access and egress control, asset protection, corrective action, and report and recordkeeping protocol topics.)

13. Determine the types of records that may be available for:

    - Reporting security incidents at the facility, including such incidents such as unauthorized facility entrance/ exit, missing property, possible property theft, company/ personal fraud, attempts to access intellectual property by unauthorized individuals, etc.
    - Recording such incidents in a log or other similar document.
    - Incident investigations.
    - Incident analysis, trend assessment, or other records for evaluating performance.

Review a sample of these records to assess effectiveness of the procedures/processes.

Corrective Action

Program Contact Interviews

14. Review the facility's corrective action system. Verify through interviews with the key program contact person, security manager, site management, or other applicable personnel:

    - That a system is in place to assure appropriate action is taken in response to security incidents.
    - That the system will ensure the prompt communication and coordination of security incidents with appropriate management groups for resolution.

Documentation and Records Review

(Important note: This documentation and records review step can be most efficiently completed in conjunction with a review of documents and records needed for the management commitment, access and egress control, asset protection, security incidents, and report and recordkeeping protocol topics.)

15. Review facility records for incident communication with appropriate management groups.

Reports and Recordkeeping

Program Contact Interviews

16. Interview the key program contact person, security manager, site management or other applicable personnel to develop an understanding of the facility's practices for retention of security incident reports. Verify that appropriate records are kept and available. Some suggested questions (along with others the auditor may develop) include:
    - How does the site manage its recordkeeping practices for incident reports?
    - Where are incident records kept?
    - What site function(s) has ownership for filing and maintaining these reports?

Documentation and Records Review

17. Use protocol step 13 above for this review.

E. Summarize Audit Results

1. Record in your working papers for each protocol step the information reviewed (or individuals interviewed by name or position). If no issues were noted for the protocol step, only a notation to that effect is required. If issues are noted, describe the deficiency noted and the basis for that determination. Alternatively, the finding or local attention item can be referenced without duplicating this description in the working papers. If the finding does not detail the facts behind the conclusion, this should be in the working papers, however.

2. Review all issues believed to be findings with the appropriate facility contacts and the team leader. If the conclusions change as to an issue being a legitimate finding during this review process, the basis for the different conclusion should be reflected in the working papers.

3. As a team, develop a complete listing of findings, recommendations (these may not be required on some audits), and local attention items which are clearly and concisely written and substantiated by audit data gathered.

4. Prioritize the findings for this topic using the Findings Prioritization Worksheet.

5. Prepare summary strengths and weaknesses of the standards in the protocol for the team leader.

6. Identify good practices for the topic and document. Review with the team leader.

7. Organize and collect your working papers, any relevant attachments, and your field notes for retention by the team leader. Complete your protocol and audit process feedback forms for the team leader.

ALL PROTOCOL STEPS CONFIRMED
FOR COMPLETION BY AUDITOR(S): _____

COMPLETION REVIEWED WITH: _____
Team Leader or Designate _____

Resource 10-4: Baseline Audit Questions

Source: *Security Guidance for the Petroleum Industry*, American Petroleum Institute, 2002.

From time to time operators should audit their security management program to determine the effectiveness of the program, and to ensure that the program is being conducted according to the operator's security management plan and in compliance with all applicable regulations. Audits may be performed by internal staff or outside consultants. While the audit will be based on local conditions, below are a series of questions that each operator can use as a starting point in developing a company-specific audit program:

- Is there a written policy/program for security management?
- Are there written procedures for tasks relating to security management?
- Are activities being performed as outlined in the operator's program documentation?
- Is someone assigned responsibility for each subject area?
- Are appropriate references available to those who need them?
- Are the people who do the work trained in the subject area?
- Are qualified people used when required?
- Are activities being performed using an appropriate integrity management framework as outlined in this guideline?
- Are all required activities documented by the operator?
- Are action items followed up?
- Is there a formal review of the rationale used for developing the risk criteria used by pipeline operator?
- Are there established criteria for responding to security events? Are criteria established for these activities stated above for terminals, pump stations, associated piping, and pipeline segments?

Resource 10-5: Asset-Based Vulnerability Checklist

Source: *Asset-Based Vulnerability Checklist for Wastewater Utilities*, Association of Metropolitan Sewerage Agencies, 2002.

I. Asset: Physical Plant

Perimeter

- Perimeter physical barriers, such as a fence or wall
- Locking of perimeter gates
- Patrolling perimeter by guards or electronic monitoring

Entry/Access Control

- Limiting access to employees or people having valid business at the facility
- Controlling access by a posted guard or through electronic means
- Locking of doors and windows
- Strength of doors, windows and locks
- Entry codes and locksets
- Control of visitors, photo identification, sign in and out, and facility escorts
- Facility tours
- Security of fill and vent pipes of chemical and fuel storage tanks

Surveillance

- Alarming of buildings and critical structures to detect intrusion
- Alarming of emergency exit doors
- Monitoring interior of buildings by closed circuit television (CCTV)
- Site monitoring by CCTV
- Continuous monitoring of alarms and CCTV with a reporting protocol
- Connecting alarms and monitoring systems to an uninterruptible power supply
- Night lighting throughout the facility for surveillance
- Emergency lighting for evacuation of premises
- Public address or other warning system to notify people within a facility of an incident
- Overgrowth of trees and shrubs that may block views of doors and windows

Vehicle and Materials Delivery Management

- Parking of private vehicles near buildings and other structures
- Locking and storage of utility's vehicles
- Policies for the use and operation of utility's vehicles
- Monitoring of utility's vehicles via a real-time tracking system
- Inspection of delivery vehicles
- Designation of distinct delivery areas for receiving and screening packages prior to their distribution within a facility

…

Hazardous Material Control

- Identification of hazards from process chemicals and other acutely hazardous materials
- Identification of acutely hazardous materials (AHMs) from adjacent establishments and facilities
- Tracking mechanism to account for all process chemicals and other acutely hazardous materials received and used at utility facilities
- Gas detection equipment
- Information available to employees or others responding to hazardous chemicals or toxins that may be introduced into the sewer system or treatment plant

II. Asset: People

Human Resource Policy

- Policies on background checks for potential employees before hiring
- Policies on periodic criminal checks for existing employees
- Procedures for employees who may be called to active duty in the military
- Legal rights afforded to employees who are reservists and members of the National Guard that are called for active military duty
- Policy to address compensation and benefits for employees who are called to active duty
- Policy to address compensation and benefits for employees who remain on-the-job for elongated periods during an incident
- Plan for management to effectively react when some employees may refuse to come to work during an incident

- Plan to transport personnel to and from their place of work if roads and streets are closed due to police order or physically blocked as a result of an incident
- Plan to mitigate the concern employees may have for their families' well being during a disaster
- Management discussion of security issues, emergency response plan, and disaster plan with union representatives

Personnel Identification and Personal Welfare

- Employees' photo identification badges
- Employee communications equipment to rapidly report incidents
- Employee monitors for radiation, chemical or biological detection
- Periodic changes in employee keys and pass-codes
- Biometric devices to control access to sensitive areas
- Contractors, vendors, and visitors
- Personal protection devices and first-aid materials at worksites
- Provisions for food, water, and rest for employees who remain on the job for extended periods of time
- Up-to-date list of all employees, their phone numbers and emergency contact information
- An employee assistance program to counsel employees and their families on life-crisis management
- Weapons at utility facilities

Planning and Training

- Employee training to properly handle a threat that is received in-person, by phone, by e-mail, by U.S. mail, or by other delivery service
- Employee knowledge of procedures to follow should an incident occur
- Management knowledge of whom to contact to report a threat or emergency
- Procedures for determining when and how to evacuate a building
- Employee training in security measures
- Employee training in emergency preparedness in accordance with the utility's adopted plan
- Employee training to detect symptoms of a chemical or biological attack
- First aid training for employees

Resource 10-6: Audit Checklist

Source: *Site Security Guidelines for the U.S. Chemical Industry*, American Chemistry Council, Synthetic Organic Chemical Manufacturers Association, and The Chlorine Institute, Inc., 2001.

Item #	Question	Response	Recommendations
A. Risk Assessment and Prevention Strategies			
1	Have we identified all key facility assets?		
2	Have we performed a chemical hazards evaluation?		
3	Have we performed a process hazard analysis?		
4	Have we performed a consequence assessment?		
5	Have we performed a physical factors assessment?		
6	Have we performed a mitigation assessment?		
7	Have we performed a security assessment/gap analysis?		
8	Have we developed rings of protection?		
B. Management Issues			
1	Does the company's top management visibly support security efforts?		
2	Have clear security policies been developed and promulgated?		
3	Have we established partnerships with local, state, and federal law enforcement agencies, other public safety agencies, and surrounding communities?		
4	Have we clarified relationships and procedures with other management functions to provide a more coordinated response to security incidents?		
5	Do we have a well-understood system for employees to report security incidents?		
6	Do we have a system for collecting and analyzing reports of security incidents?		
7	Have we developed security awareness programs for employees and contractors?		
8	Have we developed a procedure for referring suspicious incidents and breaches of company policy to corporate counsel or		

Item #	Question	Response	Recommendations
	corporate security management?		
9	Have we developed a policy of referring all suspected illegal activity to law enforcement?		
10	Have we developed procedures for emergency response and crisis management?		
11	Do we periodically reassess the site's security posture (threats, vulnerabilities, risks, and countermeasures)?		
C. Physical Security			
1	Have we implemented appropriate access control measures, such as signs, secure doors and windows, locks, card-based access control systems, parcel inspection, and control of gates and docks?		
2	Do we have appropriate perimeter protection, using, for example, fences, bollards, trenches, turnstiles, and security lighting?		
3	Do we need security officers, on patrol or at fixed locations? If so, do they have written post orders to direct their activity?		
4	Have we appropriately protected crucial communications equipment and utilities?		
D. Employee and Contractor Security			
1	Have we developed appropriate security practices for voluntary and involuntary terminations of employment?		
2	Have we adopted policies and established procedures to prevent and respond to workplace violence?		
E. Information, Computer, and Network Security			
1	Have we taken steps (through the Operations Security, or OPSEC, process) to protect information that could be of use to our adversaries?		
2	Do we follow procedures to reduce the likelihood that spoken information (in face-to-face conversations, phone calls, and radio communications) could be picked up by adversaries?		
3	Do we follow appropriate procedures for protecting and destroying sensitive documents?		
4	Are we using appropriate hardware, soft-		

Item #	Question	Response	Recommendations
	ware, and procedural techniques for protecting our computers and networks?		
5	Do we periodically analyze computer transaction histories to look for irregularities that might indicate security breaches?		

Resource 10-7: Stages Leading to Excellence

Stage 6. External political trends and/or conditions are monitored and evaluated to determine their potential impact on company security. Technical advancements are periodically incorporated into security systems. Employees take ownership for the facility security plan and are comfortable in their roles. Employee security training includes advanced level techniques in violence and theft prevention, intervention and/or reporting.

Stage 5. Teams of company security personnel and law enforcement agencies and/or qualified individuals conduct information and training sessions. Employees are able to identify and respond to warning signs of potentially violent situations. All employees share responsibility for site security and contribute to improvements. Drills are conducted in cooperation with local law enforcement and emergency response agencies.

Stage 4. Employees, contractors, and visitors submit to security clearance procedures that are appropriate for their positions. The security plan includes procedures to incorporate change, such as physical plant, personnel and area conditions. A confidential system is in place for employees to report security issues. Security personnel are proficient in identifying and controlling potential threats and breaches of security. Security systems, including surveillance cameras and metal detectors, are used to monitor critical areas where practical. Refresher training is conducted for security officers on a periodic basis. Employees traveling on company business are trained on the company's travel security plan.

Stage 3. Security planning is done in cooperation with applicable law enforcement, security agencies and emergency responders. Appropriate information is shared among responders. A policy controlling workplace violence is in place and consistently enforced. Access levels are established for all employees, contractors and visitors. Facility access is dependent upon the successful completion of orientation and pre-determined requirements. Employees are encouraged to help visitors and contractors comply with identification requirements. Designated personnel monitor chemicals, equipment and intellectual property to ensure that they are not improperly used. Internal investigations are conducted for reported security incidents. All contractors and visitors wear identification badges while on company property. Measures are in place in the event utilities (such as electricity, telephone, etc.) are not working. Communications to the facility emergency management team, critical personnel and local emergency responders are ensured by multiple communication methods.

Stage 2. Procedures are in place for all aspects of the site security plan. A facility security plan includes detailed responses to possible events. All employees are trained in emergency procedures and participate in drills to con-

firm knowledge of their roles. A designated security administrator oversees security operations as specified in the facility security plan. Fencing, gates, security guards, etc., secure facility property. Firearms and weapons are controlled through written policy and enforcement procedures. Responses to reports of threats, theft and other security concerns are prompt and thorough. Employee identification is required. A formal training program is in place for security officers. A screening mechanism is in place to check security personnel's criminal and credit background and to handle initial and random drug screening (where appropriate). Employees are subject to security evaluations appropriate to their positions, such as initial drug testing and criminal, background and credit checks.

Stage 1. All requirements of the Responsible Care® Security Code of Management Practices have been met. Self-evaluation ratings have resulted in all 5's for a minimum period of one year.

11. Third-Party Verification

Management Practice 11

Third-party verification that, at chemical operating facilities with potential off-site impacts, companies have implemented the physical site security measures to which they have committed.

Chemical industry security starts at our facilities. Companies will analyze their site security, identify any necessary security measures, implement those measures, and audit themselves against those measures. To help assure the public that our facilities are secure, the companies will invite credible third parties—such as firefighters, law enforcement officials, insurance auditors, and/or federal or state government officials—to confirm that the companies have implemented the enhanced physical security measures that they have committed to implement. In addition, companies should consult with these same parties as enhanced physical security measures are being considered and implemented.

The following samples are intended to stimulate thinking and offer helpful ideas on code implementation. Other approaches not described here may be just as effective or even more effective for a particular company. If a company so chooses, it may adopt any of these sample strategies or may modify them to fit the company's unique situation.

12. Management of Change

Management Practice 12

Evaluation and management of security issues associated with changes involving people, property, products, processes, information, or information systems.

Our employees and our processes contribute to, and rely upon, changes and innovations in products and technologies. As any changes are considered, our companies will evaluate and address related security issues which may arise. This can include changes ranging from new personnel assignments to installation of new process equipment or computer software or hardware.

The following samples are intended to stimulate thinking and offer helpful ideas on code implementation. Other approaches not described here may be just as effective or even more effective for a particular company. If a company so chooses, it may adopt any of these sample strategies or may modify them to fit the company's unique situation.

Resource 12-1: Notification of Change

Scope and Objectives. A process should be in place to ensure that security business centers are informed at the earliest opportunity of changes to existing operations and processes. The implications will be assessed by Security, vulnerabilities identified, and recommendations made to reduce the impact of future threats.

Key Procedures. Security will ensure that an effective communication process is in place to facilitate exchange of information with line management. Both internal and external changes that affect company operations will be assessed to establish if any changes to security operations or procedures are required.

Management of Change. Line management is responsible for ensuring that Security is informed of new operations and process and of changes to current operations and processes. Security will assess the changes, identify security vulnerabilities, and recommend cost-effective countermeasures.

Security will provide line management with generic security issues that should be considered during the management of change.

Verification and Measurement. Security business centers will meet with line management on a regular basis to assess both the effectiveness of the communication process and management of change. External assessments, security risk assessments, operational reviews, and internal reviews should evaluate the effectiveness of the notification process to security business centers of changes to operations and processes.

Feedback. The outcome of internal and external assessments should be communicated to line management and lessons learned should be implemented.

Resource 12-2: Updating Risk Assessments

Project Risk Assessment (RA) Planning. RA should be planned and scheduled "regularly" for ongoing operations and activities. It can be triggered by perceived changes in risk and at key milestones on major projects. Risk management coordinators (RMCs) or security business center managers should define the frequency for each ongoing operation or activity and communicate such timing to management, which, in turn, must make plans as to the actual timing and availability of resources. RMCs should also develop an annual RA plan (which documents both short-term and strategic assessment work plans) for review by organizational management.

An RA should be completed:

- As required by schedule and/or the execution of new projects,
- Prior to any significant change in a facility or operation,
- After a serious security incident, and
- Whenever new scenarios—not originally identified by risk assessment teams—are identified.

It should be recognized that other elements might require risk assessments in accordance with legal requirements, insurance considerations, and integrity-critical processes. Managers should monitor these activities and be aware of identified risks that may have an impact on security planning.

Risk Assessment Short Form

Initiated by _____ Telephone No. _____ Date _____

Change request no. _____ (leave empty if not applicable, i.e., for newly identified risks)

Description _____

_____

_____

Is the description provided above relevant to existing risk assessment scenario? Y / N

If yes, provide risk assessment name and scenario number _____

Describe the risk scenarios for the new situation. Refer to Risk Category Matrix at the back of this form for definitions and fill in this table based on your assessment / experience.

Scenario No.	Scenario Description	Probability Category	Consequence Category
1			
2			
3			
4			

A Do these scenarios imply a change from previously defined scenarios? Y / N / New Risk

B Does the consequence or probability category change? Y / N / New Risk

C Does the risk fall in the 1 or 2 risk category? Y / N

If you answer YES to question C and it is either a new risk or a change in risk category, line management must discuss with security risk management coordinators whether this warrants formal assessment by new team.

Assessment team required? Y / N

If no, complete the following:

D Does the above require new or revised action items for risk prevention / mitigation? Y / N
If yes, define new action items:

Number	Method of Addressing	Who is Responsible	Timing
1			
2			
3			

Approved by _____ Date _____

Send copy of this form to Security Risk Management

Modifications in operations may require a recycle of previous RAs or an entirely new assessment when a change results in a situation (e.g. creates new vulnerabilities) that has not been addressed by earlier assessments. The change procedure should document risk aspects of change. If change is considered significant, constitution of a formal RA team may be required. Examples of "significant change" include major modifications; new standards, regulatory mandates, or laws; political/community changes; and new technology. A revision process should be also initiated when new information alters planned follow-up activities.

Transition Management. An important element is transition of risk findings from one operational or activity phase to another. This transaction ensures that responsible individuals continue to be assigned to follow-up and close-out risk mitigation activities throughout the entire life cycle of the project. The owner should prepare a memorandum documenting or referring to all necessary follow-up and close-out activities and forward to the new owner, assignee, security management, and the RMCs.

Resource 12-3: Assessing New Sites

Essential Element

7.5 Security assessments will be conducted under the direction of Corporate Security.

Expectations

7.5.1 The Corporate Security survey form will be used for the initial assessment of all facilities, both manufacturing and office sites.

7.5.2 Security assessments will be conducted in advance of the purchase, lease, or rental of a manufacturing site or office space, or for use in the analysis of an entity for acquisition.

7.5.3 Compliance or inspection schedules and standard formats will be developed and used by Corporate Security and other assessment groups to ensure that manufacturing and office sites are in compliance with company policies and minimum standards.

7.5.4 Periodic on-site inspections by a security professional will be conducted at each site as appropriate.

- Findings will be documented and reported to the appropriate site manager.
- Each site will develop corrective action plans, which will be tracked to ensure prompt implementation.

Essential Element

7.7 A threat analysis will be made at proposed sites for new plant or office locations, or at an existing site for new acquisition, prior to the commitment of financial resources.

Expectations

7.7.1 The director of corporate security or a designated representative will conduct a site selection threat analysis. The threat analysis should include an actual site visit and interviews with appropriate sources within the country in which the facility is to be located and at the specific site location.

7.7.2 The analysis should determine the current and projected threats related to:

- Political climate
- Possibility of civil unrest
- History of terrorism, strikes, or criminal activity
- Incidents of extortion
- Industrial and state sponsored espionage

- Threat of kidnapping
- Competency, efficiency, and responsiveness of local police, fire, and medical facilities
- Other related risk categories

7.7.3 A threat level will be established based on the analysis and will be used to develop an appropriate site security plan.

Resource 12-4: Change Management Cycle

Source: *Security Guidance for the American Petroleum Industry*, American Petroleum Institute, 2002.

Managing Change. A systematic process should be used to ensure that changes to a facility or its operations are evaluated for their potential risk impacts prior to implementation, and to ensure that changes in the environment in which the facility operates are evaluated. Furthermore, and after these changes have been made, they should be incorporated, as appropriate, into future risk assessments to be sure the risk assessment process addresses the facility as it is currently configured.

As this final element indicates, managing security is not a one-time process. …[A] security management program involves a continuous cycle of monitoring conditions, identifying and assessing risks, and taking action to minimize the most significant risks. Risk assessments must be periodically updated and revised to reflect current vehicle or facility conditions so operators can most effectively use their limited resources to achieve the goal of controlling risks and minimizing their impact.

…

8.14 Managing Change in a Security Program

Once a pipeline security program is established, it is critical that the pipeline operator keep the program current. Changes to the pipeline system made by the operating company and changes affecting the pipeline system made by others could affect the priorities of the security program and the risk control measures employed. To ensure continued validity of the program, operators must:

- Recognize changes before or shortly after they occur
- Ensure that those changes do not unnecessarily increase risks
- Update the affected portion(s) of the pipeline security program

Operators with an existing management of change (MOC) program should verify that the types of changes mentioned in this section are included in their MOC program. For other operators, a system should be established to recognize and manage changes relevant to their pipeline security program.

8.14.1 Recognizing Changes That Affect the Security Program

To keep the pipeline security program current, the operator should identify the ways a pipeline system may be modified that could impact any of the risk factors identified in the pipeline security program. Examples of such changes are:

- Adding, deleting, or otherwise modifying the pipeline segments or facilities.

- Changes in the fluid transported and/or its operating conditions in the pipe that may also affect the risk prioritization and any mitigation measures employed.
- Restarting equipment or systems that have been out of service for an extended time and/or systems that have not been maintained.
- Changes to existing procedures, or addition of new procedures.
- Changes along the right-of-way, such as changes in land use.
- Regulatory changes.

The operator is responsible for recognizing these changes and ensuring that the changes are appropriately reviewed.

8.14.2 Updating the Pipeline Security Program

A change may impact any or all [parts] of the pipeline security program.… As part of managing a change, the operator should evaluate security program issues such as these:

- Have the potential impacts or affected impact zones been altered?
- Should data be added, deleted, or modified?
- Does this change impact data that was input or assumptions that were made during the risk assessment?
- Does this change affect mitigation plans?
- Does this change impact the security program for pipeline segments or facilities?
- Should this change lead to a revision of the security management plan?
- Does this change impact any performance indication or auditing criteria?

Any change that affects the pipeline security program should be documented. Affected parts of the pipeline security program should be modified as necessary to reflect the change.

Resource 12-5: Tracking Change (1)

Site Security: Stages Leading to Excellence

External political trends and/or conditions are monitored and evaluated to determine their potential impact on company security. Technical advancements are periodically incorporated into security systems. Employees take ownership for the facility security plan and are comfortable in their roles. Employee security training includes advanced level techniques in violence and theft prevention, intervention and/or reporting.

Resource 12-6: Tracking Change (2)

Source: *Site Security Guidelines for the U.S. Chemical Industry*, American Chemistry Council, Synthetic Organic Chemical Manufacturers Association, and The Chlorine Institute, Inc., 2001.

To be effective in a security leadership role, a manager must be proactive and be able to plan for and manage risk. Knowledge of whether and when the risks may change is critical. Other company departments can be a source of such information.

For example, a chemical company's public affairs department may be able to inform the security-responsible manager that a group is planning a protest at his or her facility and may even be able to obtain the protest's agenda and expected number of protesters. The human resources department may be able to contact managers about evolving security-related personnel issues, such as suspensions, terminations, labor unrest, or employees exhibiting unusual behavior. The purchasing or procurement department may be able to provide information about contractor or vendor changes that might have security implications (such as theft of equipment or tools). The legal and accounting departments may be able to inform managers about investigations of conflict of interest or misappropriation of funds.

At one chemical facility, the information technology (IT) department contacted managers responsible for security when the IT department began to plan a major computer equipment transition. Security concerns were taken into consideration early in the process. The new equipment was then properly secured during transport, upon arrival at the site, and while being installed, and the old equipment was accounted for and properly disposed of.

…

The conditions surrounding a security effort change constantly. Employees come and go, a facility's contents and layout may change, various threats wax and wane, and plant operations may vary. Even such mundane changes as significant growth of bushes or trees around a facility's exterior may affect the security plan (for example, by providing cover for intruders).

Therefore, managers should review their security measures periodically, as well as when-ever facilities or other conditions change significantly. It may also be useful to do the following at appropriate intervals:

- Update risk assessments and site surveys.
- Review the level of employees' and contractors' compliance with security procedures.
- Consider whether those procedures need modification.

It is also useful to establish ongoing testing and maintenance of security systems (such as access control, intrusion detection, and video surveillance).

13. Continuous Improvement

Management Practice 13

Continuous performance improvement processes entailing planning, establishment of goals and objectives, monitoring of progress and performance, analysis of trends, and development and implementation of corrective actions.

Our industry commitment to security calls for companies to seek continuous improvement in all of our security processes. That means companies continually will be tracking, measuring, and improving security efforts to keep people, property, products, processes, information, and information systems more secure.

The following samples are intended to stimulate thinking and offer helpful ideas on code implementation. Other approaches not described here may be just as effective or even more effective for a particular company. If a company so chooses, it may adopt any of these sample strategies or may modify them to fit the company's unique situation.

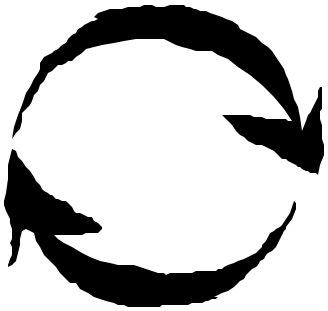
Resource 13-1: Continuous Improvement Cycle

The ABC Corporation Security Program uses a continuous improvement cycle designed to manage security risks. To be effective, this process must be an integral component of the facility's total business plan, not a special, stand-alone process. Each employee must be involved in the security program's continuous improvement cycle. Management leadership and involvement, too, are critical to success.

The continuous improvement cycle consists of these steps:

1. Plan
Develop Strategies
- Communicate the ABC Corporation security program to all employees.
- Obtain senior management commitment to the security program's continuous improvement process.
- Integrate continuous improvement of the security program into the company's overall strategic plan.

2. Do
Implement
- Conduct an initial assessment to determine status of and gaps in security.
- Identify specific objectives, assign responsibilities, and set completion dates for each selected management practice.
- Identify and prioritize management practices for implementation.
- Integrate continuous improvement activities into daily operations.



4. Act
Take Remedial Action
- Recognize teams and individuals.
- Communicate status.
- Identify opportunities for improvement.
- Develop improvement strategies for existing security measures and select additional measures for implementation..

3. Check
Evaluate
- Measure and evaluate implementation of objectives.
- Conduct annual self-evaluations.

Resource 13-2: Gap Analysis and Improvement Plan

- Review prevention and countermeasures needed to address the identified threats with existing systems.
- Identify existing systems; determine if discrepancies (gaps) exist.
- Develop and implement an improvement plan.
- Periodically review security plan.
  - Identify site security plan elements.
  - Audit actual site practice against this list of elements.
  - Reassess assets, vulnerabilities, and threats when audit reveals deficiencies, new information becomes available impacting the plan, or there are significant facility changes.

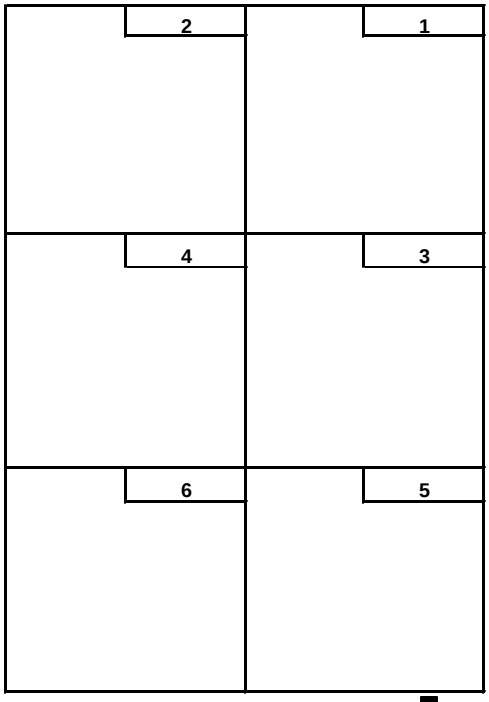
Resource 13-3: Security Program Reviews

Security program reviews, including penetration exercises, are a key component to ensure proper deployment, identify weaknesses, share lessons learned, and develop corrective actions. Such exercises should generally be coordinated and arranged by the line manager responsible for the facility or by a security business center advisor. Penetration exercises should be unannounced and should take place during both regular and off-hours. Discretion and good judgment should be applied when deciding on methods to be employed.

Resource 13-4: Prioritizing Audit Findings for Continuous Improvement

This table shows an approach for prioritizing the findings of a security audit as part of a continuous improvement process.

Attachment 1
FINDINGS PRIORITIZATION
Audit Topic_____



POTENTIAL IMPACT

High Impact

Hospitalization of employee(s), contractor(s) or members of the public for an overnight stay for more than observation
Fatality or life disabling injury
Fire or explosion that requires actual firefighting or other outside assistance (mutual aid) or results in major unit damage or downtime
Significant business interruption
Off-site safety or health impact
Major compliance issues
Major news event with extensive/substantial media or public attention
Significant environmental damage
Significant management system deficiency in a PSM element
Significant management system deficiency which impacts reliability

Medium Impact

Low Impact

Minor injury treatable by first aid
Minor recordkeeping or documentation issue
Incident with minimal environmental impact that is not reported or tracked
Shutdown covered by existing inventory
Minor agency inspection deficiencies not addressed
Minor deficiency in a PSM element
Minor management system deficiency which impacts reliability or cost control programs

Management System not in place or is not effective at mitigating risk associated with finding

Management Systems partially in place and partially effective at mitigating risk associated with finding

Prepared By:_____
Reviewed By:_____

Findings Priority	
Most Important (1)	
Very Important (2,3)	
Important (4)	
Less Important (5,6)	

4.0 Definitions

4.1 Potential Impact—The magnitude of the potential consequence associated with a particular finding, assuming the absence of interim administrative or other controls.

4.2 High Impact—Issues as identified are likely to have as direct result: hospitalization for an overnight stay for more than observation, fatality or life disabling injury, fire or explosion that requires actual firefighting, off-site safety or health impact, major compliance issues, major news event with substantial media or public attention, significant environmental damage or significant management system deficiency in a PSM element. High impact incidents are described as level three and four incidents.

4.3 Medium Impact—Issues as identified that do not meet the criteria for High or Low Impact. Also included in this category are issues which potentially could lead to High Impact events but are unlikely to occur. Medium impact incidents are described as level two incidents.

4.4 Low Impact—Issues as identified are likely to have as direct result: minor injury treated by first aid, minor recordkeeping or documentation issue, or plant shutdown covered by existing inventory. Also included in this category are issues which potentially could lead to Medium Impact events but are unlikely to occur.

4.5 Partially Functional—A measure of the facility system to mitigate the risk of the POTENTIAL IMPACT associated with a finding that describes one of the following situations:

4.5.1 Current management system for the audit finding partially mitigates risk.

4.5.2 Current management system for the audit finding does little or nothing to mitigate risk, but there are other systems and practices that do.

4.5.3 Current practice related to the audit finding does mitigate risk, but there is not a formal procedure and training where required.

4.6 Non-Functional—A measure of the facility system to mitigate the risk associated with a finding where the current management system for the audit finding does not mitigate risk and there are no other systems or practices that do.

5.0 Requirements

5.1 Complete the audit/benchmarking process defined in [company document].

5.2 Distribute a copy of the audit findings, Examples Of Findings Illustrating Potential Impact (Appendix I), Findings Prioritization Worksheet (Appendix II) and Risk Assessment of Most Important Findings (Appendix III) to each auditor and facility functional contact.

5.2.1 The audit team leader will distribute the material to all auditors and facility functional contacts and review the criteria for defining POTENTIAL IMPACT, PARTIALLY FUNCTIONAL, and NON-FUNCTIONAL management systems.

5.2.2 Each auditor and facility functional contact will review findings in their area and assign a consensus priority to each finding. In case of a lack of consensus, the facility will decide the priority.

Most important findings that are Priority 1 (requiring immediate controls) will be identified by the audit/benchmark team.

6.0 Reports and Recordkeeping

6.1 Give a copy of Findings Prioritization Worksheet using the draft report finding numbers to the facility manager at closing.

6.2 Distribute Findings Prioritization Worksheet to everyone receiving entire audit report.

…

Examples of Findings Illustrating Relative Potential Impact

The types of findings are categorized into two main groups: "High Impact" (level three and four incidents) findings and "Low Impact" findings. These two areas can be characterized easily, leaving all other findings in between as "Medium Impact" (level two incidents) findings. Again, the examples used are intended to be broad in an attempt to help focus on the impact without being too prescriptive.

High Impact

An audit finding could be considered a high impact finding if it has caused or has the potential to cause one or more of the following:

- Single fatality or permanent disabling injury to any person, or hospitalization for an overnight stay for more than observation purposes of one or more employees, contractors, or members of the public
- Fire or explosion that requires actual fire fighting or other assistance from organizations outside the facility (mutual aid) or results in major damage or downtime to the unit involved
- An incident that results in significant business interruption
- Release of materials that pose a potential threat to the health and safety of members of the public or results in a shutdown or evacuation outside the release area
- Major compliance issues
- An incident that has the potential to focus extensive adverse news media and public attention on the company
- Release of materials, which results in the evacuation of off-site facilities, restricts the navigational or recreational use of a waterway, or affects a source of drinking water
- Significant management system deficiency in a PSM element (such as inadequate process for MOC safety reviews)

- Significant management system deficiency which impacts reliability (such as lack of management approval for overdue inspections of critical equipment)

Low Impact

An audit finding could be considered a low impact finding if it is of the following nature:

- Minor injury treatable by first aid
- Minor recordkeeping or documentation issue
- Incident with minimal environmental impact that is not reported or tracked
- Shutdown covered by existing inventory
- Minor agency inspection deficiencies not being addressed
- Minor deficiency in a PSM element (such as inadequate documentation on training conducted for process changes)
- Minor management system deficiency which impacts reliability or cost control programs (such as maintenance key indicators not regularly issued to plant)

Resource 13-5: Program Evaluation

Source: *Security Guidance for the Petroleum Industry*, American Petroleum Institute, 2002.

Program evaluation should be conducted on an ongoing basis. Information should be accumulated and documented over time. Since the details of operator security management programs will vary, so too will the appropriate set of performance measures. Section 8.13.1 identifies performance measures that can be used by operators. Some operators may elect to have additional performance measures. Audits should be used as additional information sources for understanding the effectiveness of pipeline security programs. Recommendations for security management program improvement shall be developed based on the results of performance evaluation, including performance measures and audits. The performance measurement and audit results shall also be factored into future risk assessments.

The results of performance measurement and audits, including all follow-up recommendations, should be reported to those individuals within an operating company who are responsible for pipeline security. Performance should be reviewed at least annually and issues should be addressed.

8.12 Updating the Security Plan

Inspections and other security assessments conducted under an operator's pipeline security plan will result in data that must be analyzed and integrated with previously collected data. This is in addition to the other types of security related data that is constantly being gathered, updated, reviewed, and integrated into the operator's database. The result of this ongoing data integration and periodic risk assessment will result in revision of the plan in the form of new or modified mitigation plans and subsequent security assessments.

Analysis of inspection and other security assessment data will most likely result in a series of additional mitigation activities. Some of these mitigation activities may require immediate action while others may be scheduled in a long-term plan. The criticality of mitigation actions and how they are scheduled will depend on the results of integrating this information into an operator's risk assessment.

8.13 Plan Evaluation

The intent of this section is to provide system operators with a methodology that can be used to evaluate the effectiveness of security management. The goal of the operator of any pipeline system is to operate the pipeline in such a way that there are no adverse effects on employees, the environment, the public, or their customers as a result of their actions. Evaluations need to be performed on a periodic basis to review the effectiveness of the operator's security management program. In the most basic sense, a plan evaluation should help an operator answer the following questions:

- Did you do what you said you were going to do?

- Was what you said you were going to do effective in addressing the issues of security in your pipeline system?

8.13.1 Performance Measures

The operator should collect performance information and periodically evaluate the effectiveness of its security assessment methods and its mitigation risk control activities, including response. The operator should also evaluate the effectiveness of its management systems and processes in supporting security management decisions. A combination of performance measures and internal and external system audits is necessary to evaluate the overall effectiveness of a pipeline security plan.

Each operator should have performance measures. These performance measures should include a distribution of leading, lagging, and deterioration measures (see 8.13.2 for a discussion of the types of performance measures). These performance measures should be part of the operator's security management program and should be based on an understanding of the risks to the security for each pipeline system operated.

The following performance measures should be considered:

1. A performance measurement goal to document the percentage of security management activities completed during the calendar year

2. A performance measurement goal to track and evaluate the effectiveness of the operator's collaboration efforts with outside agencies

3. A performance measure based upon audits and drills of the operator's security plan

4. A performance measure based on operational events, e.g., security breaches, cyber attacks, alerts, and countermeasures employed, that have the potential to adversely affect pipeline security.

5. A performance measure to demonstrate that the operator's security management program reduces risk over time with a focus on high risk items.

6. A performance measure to demonstrate that the operator's security management program for pipeline segments and facilities reduces risk over time with a focus on high risk items.

8.13.2 Performance Measurement Methodology

All of the risk assessment and mitigation methods discussed earlier in this guideline are put forth with the intent of reducing the likelihood and consequences of a security event. Ultimately, the performance measurement of an operator's security management program is the degree to which security risks are eliminated. However, a typical security management program will contain many elements, and the program will op-

erate over long time horizons. Thus a security management program cannot be evaluated based on any one measure. This section describes an approach to monitoring performance of the components of a security management program with the expectation that component progress will correlate with overall program success. Performance measures actually form a continuum from leading indicators (before security events) to lagging (after security events), and include process measures and measures of actual security events.

…

These measures answer the question: "Once the program has been defined, how well are the details being executed?" Drills are an effective way to demonstrate awareness and understanding of security management programs. Activity measures must be thoughtfully selected since not all activity measures will effectively measure performance.

Security event measures—Operational and maintenance trends employed to indicate when the security of the system is reduced despite mitigation measures. Some performance measures of this type may indicate that the system condition is deteriorating despite well-executed mitigation activities. Other performance measures may indicate that predicted security events are within expected parameters or they are not within expected parameters. Security event measures should be evaluated over time to understand trends.

8.13.3 Measuring Performance Using Internal Comparisons

Every operator should evaluate its current performance against past performance and set specific goals. Internal comparisons over time are suitable for analyzing trends. For example, security audits and drills during the last 12 months can be plotted on a rolling basis once per quarter. An increasing trend would indicate that the average age of security data is improving.

Internal comparisons of one portion of a pipeline system against another portion of the same pipeline system (for example, portions of the system within designated high consequence areas versus other portions outside designated high consequence areas) may be used to evaluate the effectiveness of specific mitigation actions.

Internal comparisons from one geographic region to another geographic region within the same operating company, or from one business unit to another business unit may be helpful ways to identify areas with deficiencies.

8.13.4 Measuring Performance Using External Comparisons

External comparisons may be more difficult to obtain. This is particularly true for the metrics related to mitigation actions. Benchmarking among operators may prove practical when those operators are not in direct competition. Care needs to be taken to ensure that benchmarking is conducted such that information is comparable among the benchmarking operators or systems. Operators should also conduct periodic

evaluations of their own performance in comparison with industry-wide data sources. In order to ensure that operators have access to external databases, operators need to participate in data initiatives, both operator benchmarking and industry wide databases. Individual operators should collect internal incident information using standard incident data fields even if they do not choose to contribute operator information to external databases. Only by using standard data fields can comparisons be made external to individual operators.

In order to conduct trend analysis of incidents, system characteristics also need to be captured using a standard format (facility location, pipeline miles, miles by diameter, and volumes moved). Operators should collect infrastructure data for trend analysis using standard data fields even if they do not choose to contribute system infrastructure information to external databases.