SECURITY PRACTICES GUIDELINES
NATURAL GAS INDUSTRY
TRANSMISSION AND DISTRIBUTION

Prepared for:

AMERICAN GAS ASSOCIATION
AND
INTERSTATE NATURAL GAS ASSOCIATION OF AMERICA

Prepared by:

Process – Performance Improvement Consultants, AGA Natural Gas Security Committee,
and
INGAA Security Committee

Revised May 2008
This document provides an overview of the recommended security practices and procedures for the transmission and distribution segments of the natural gas industry. Individual companies will assess their own security needs and implement security measures they consider appropriate. This document is not intended to supplant the measures adopted by individual companies or to offer commentary regarding the effectiveness of individual operator efforts. With respect to particular circumstances, local, state and federal laws and regulations should be reviewed.

Information concerning security risks and proper precautions with respect to particular materials and conditions should be obtained from individual companies or the manufacturer or supplier of a particular material.

AGA and INGAA are not undertaking to meet the duties of employers, manufacturers, or suppliers to warn and properly train and equip their employees, and others exposed, concerning security risks and precautions, nor undertaking their obligation under local, state or federal laws.

To the extent this document contains company specific information; such information is to be considered confidential.

This document should not be made available on the Internet. Member companies, trade associations, and governmental agencies should control and track who is given copies (electronic or hard) of these Security Guidelines.
# TABLE OF CONTENTS

Security Practices Guidelines  
Natural Gas Industry  
Transmission and Distribution  
*American Gas Association,*  
*and*  
*Interstate Natural Gas Association of America*

<table>
<thead>
<tr>
<th>TABLE OF CONTENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>VISION STATEMENT</strong>……………………………………………………….</td>
</tr>
<tr>
<td><strong>EXECUTIVE SUMMARY</strong>……………………………………………………….</td>
</tr>
<tr>
<td><strong>1.0 OVERVIEW</strong>……………………………………………………….</td>
</tr>
<tr>
<td>1.1 National Infrastructure Protection Plan……………………………</td>
</tr>
<tr>
<td>1.2 Authorities, Roles, Responsibilities and Sector Specific Plans</td>
</tr>
<tr>
<td>1.3 Security Partners……………………………………………………….</td>
</tr>
<tr>
<td>1.4 Information Sharing……………………………………………………….</td>
</tr>
<tr>
<td>1.5 Security Incident Reporting…………………………………………….</td>
</tr>
<tr>
<td><strong>2.0 BACKGROUND</strong>……………………………………………………….</td>
</tr>
<tr>
<td>2.1. Pipeline Industry Practices………………………………………….</td>
</tr>
<tr>
<td><strong>3.0 VULNERABILITY AND RISK ASSESSMENT</strong>……………………….</td>
</tr>
<tr>
<td><strong>4.0 CRITICAL FACILITY DETERMINATION</strong>……………………….</td>
</tr>
<tr>
<td><strong>5.0 PRESCRIPTIVE OR PERFORMANCE DETERMINATION</strong>………….</td>
</tr>
<tr>
<td><strong>6.0 PRESCRIPTIVE METHOD</strong>…………………………………………….</td>
</tr>
<tr>
<td>6.1. Approach……………………………………………………………….</td>
</tr>
<tr>
<td>6.2. Detection and Deterrent Methods…………………………………….</td>
</tr>
<tr>
<td>6.3. Operator Action Plan………………………………………………….</td>
</tr>
<tr>
<td>6.4. Response to Events…………………………………………………….</td>
</tr>
<tr>
<td>6.5. Recovery from Events………………………………………………….</td>
</tr>
<tr>
<td>6.6. Critical Spare Parts…………………………………………………….</td>
</tr>
<tr>
<td>6.7. Modifications to Approach……………………………………………</td>
</tr>
<tr>
<td>6.8. Information Control…………………………………………………….</td>
</tr>
<tr>
<td><strong>7.0 PERFORMANCE METHOD</strong>………………………………………….</td>
</tr>
<tr>
<td>7.1. Approach……………………………………………………………….</td>
</tr>
<tr>
<td>7.2. Threat Analysis and Assessment……………………………………….</td>
</tr>
<tr>
<td>7.3. Asset Criticality………………………………………………………….</td>
</tr>
<tr>
<td>7.4. Asset Attractiveness…………………………………………………….</td>
</tr>
<tr>
<td>7.5. Asset Vulnerability……………………………………………………….</td>
</tr>
<tr>
<td>7.6. Other Employee Protection and Facility Security Considerations</td>
</tr>
<tr>
<td>7.7. Implementation of Risk Controls……………………………………….</td>
</tr>
<tr>
<td><strong>APPENDICES</strong></td>
</tr>
<tr>
<td>APPENDIX 1 Pipeline Operations Background</td>
</tr>
<tr>
<td>APPENDIX 2 Department of Energy Executive Summary Sector Specific Plan</td>
</tr>
</tbody>
</table>
APPENDIX 3  Transportation Sector-Specific Plan Annex F: Pipeline Modal Annex: Executive Summary
APPENDIX 4  Coordinating Council Structures
APPENDIX 5  Information Technology Security in the Natural Gas Industry
APPENDIX 6  System Criticality Determination
APPENDIX 7  Pipeline Components
APPENDIX 8  Pipeline Security Detection and Deterrent Methods Requiring Capital Additions for Critical Facilities
APPENDIX 9  DOT *Pipeline Security Information Circular* and *Pipeline Security Contingency Planning Guidance*
APPENDIX 10 Current Pipeline Industry Spare Part Inventory Practices
APPENDIX 11 Links to Key Websites and Agency Contact Information
APPENDIX 12 List of Terms and Acronyms

Note: The security arena uses a myriad of acronyms that are reflected throughout these Security Guidelines. To help the reader a list of security related terms and acronyms are provided in APPENDIX 12.
VISION STATEMENT

Energy is the lifeblood of the United States economy, and natural gas comprises about one-fourth of the energy consumed annually. Natural gas heats America’s water, cooks our food, warms our homes and businesses, fuels our factories, powers many of our transportation systems, and even generates much of the electricity used daily. This clean and efficient fuel is transported and distributed through a vast network of natural gas pipelines, most of which are underground. The transportation of natural gas continues to be one of the safest and most reliable forms of transportation. The vast and robust network of underground natural gas pipelines also makes it one of the most secure forms of transportation.

The natural gas industry is proud of the numerous voluntary proactive steps it has taken in the last seven years to further enhance the security of its pipeline systems by:

- identifying its Critical Infrastructure and Key Resources CI/KR),
- partnering with government in developing and implementing enhanced security plans,
- developing regional impact studies,
- collaborating, both within industry and across other industries, in sharing information, ideas, and best practices, and
- updating these Security Guidelines for its membership to use.

Because the security of our pipeline systems is a top priority, the natural gas industry remains firmly committed to taking appropriate and measured actions to deter threats, mitigate vulnerabilities, and minimize consequences associated with a terrorist attack and other manmade and natural disasters.

EXECUTIVE SUMMARY

The first Security Guidelines for the Natural Gas Transmission and Distribution Industry were published by the Interstate Natural Gas Association of America (INGAA) Security Practices Group (now Security Committee) and the American Gas Association (AGA) Natural Gas Security Committee with input from American Public Gas Association (APGA) in September 2002. The Security Guidelines were created in recognition of an increased general threat environment, and the desire of the natural gas transmission and distribution industry to voluntarily strengthen its existing security practices and plans. At that time, the natural gas transmission and distribution industry committed significant resources and took specific actions to implement appropriate security procedures at its identified CI/KR.

The natural gas transmission and distribution industry has identified its CI/KR based on a risk-based approach that assesses consequence determination, potential threats and their outcomes, and a selection of appropriate risk mitigation controls for these facilities. The industry, through AGA, INGAA and APGA, began partnering with several branches of the federal government, including the U.S. Department of Energy (DOE), the U.S. Department of Transportation (DOT), the U.S. Department of Justice (DOJ), and the Office (now Department) of Homeland Security (DHS) to address security concerns. To develop and enhance the appropriate security
programs requires collaboration and communication from all segments of the natural gas industry, other energy groups, and federal and state regulators.

Specific security measures/programs undertaken by the industry in 2002 to enhance security at critical facilities included:

- Developed security plans for CI/KR.
- Strengthened emergency, contingency, and business continuity plans.
- Increased law enforcement liaison efforts.
- Increased employee awareness through training and communication protocols.
- Requested increased monitoring by local law enforcement officials.
- Increased visitor and vehicle monitoring.
- Enhanced physical security installations.

The Security Guidelines developed in September, 2002 have served the industry well in helping advance its security initiatives, and it has been accepted by the industry’s governmental security partners and referenced in numerous government documents, including the applicable Sector Specific Plans (SSPs) from both DOE and Transportation Security Administration (TSA).

Since the implementation of the Security Guidelines there has been significant progress made at the federal, state, and industry levels to better understand and share information about terrorist threats and other hazards; to build security partnerships to share information and implement CI/KR protection programs; to implement long-term risk management programs; and to maximize the efficient use of resources for CI/KR protection. Below are some highlights of the progress made in these areas since 2002 at both the government and industry level:

**Government -**

- Formation of the DHS.
- Creation of TSA within DHS.
- Publication of the National Infrastructure Protection Plan (NIPP).
- Establishment of Sector Specific Agencies (SSAs).
- Establishment of Government Coordinating Councils (GCCs).
- Publication of SSPs.
- Implementation of Corporate Security Reviews (CSR) by the TSA.
- Periodic security briefings by Homeland Infrastructure Threat and Risk Advisory Center (HITRAC) and others.

**Industry –**

- Development or enhancement of company security plans.
- Identification of CI/KR.
• Establishment of Oil and Natural Gas Security Coordinating Councils (ONGSCC).
• Development of regional impact studies.
• Partnered with SSAs in writing SSPs, in particular the Energy SSP and the Pipeline Modal Annex of the Transportation Systems SSP.
• Utilization of HSIN.
• Participation in TSA Pipeline Corporate Security Reviews.
• Implementation of numerous security Smart Practices as captured in the TSA’s Pipeline Security Smart Practices document.
• Continuation of active security committees (and network of industry security professionals) through AGA and INGAA.
• Participation in numerous government security workshops and exercises.

U.S. policy has focused on the importance of enhancing CI/KR protection to ensure that essential governmental missions, public services, and economic functions are maintained in the event of a terrorist attack, natural disaster, or other type of incident, and that elements of CI/KR are not exploited or used as weapons of mass destruction against people or institutions. These Security Guidelines were revised in May 2008 to reflect many of these changes, and to highlight the progress that has been made since they were first published. They continue to provide an overview of industry practices that are based on existing and enhanced operational regulations, practices, and processes within the industry. These Security Guidelines offer an example of a systematic “approach” for use by companies to determine security risks, to implement detection and deterrent practices, and to refine response and recovery practices. They use the concept of risk management and, in particular, consequence reduction to address and manage security issues. At the same time, there must be a clear recognition that many other risk management and vulnerability assessment models are available, and that each individual company must assess risk using the approach which is the most effective for that company.

These Security Guidelines provide practices that are general in nature and reflect the importance of flexibility in application by the company. Each operator/company must determine how best to apply these Security Guidelines to protect its CI/KR. It is important that all companies do something to protect their CI/KR, realizing each company is different and consequently what works for one company may not be appropriate for another. The industry will need to continue to work in concert with other industries as well as governmental agencies in order to effectively manage security of the industry’s CI/KR.

1.0 OVERVIEW

The natural gas pipeline industry comprises more than 880 companies, large and small, which operate approximately two million miles of natural gas pipelines and associated facilities. This transportation infrastructure connects natural gas production, storage, and gathering fields to transmission systems, which in turn connect to distribution systems throughout the nation (see APPENDIX 1).
Natural gas pipeline operators have always been concerned with the safety and security of their facilities. Originally, their concerns centered on possible vandalism and disruption of service. After September 11, 2001 it was made clear that natural gas pipeline operators had to also look to the prospect of large-scale, planned sabotage or terrorism. However, to have an effective security plan, operators should not only be concerned with large-scale sabotage or terrorism, but consider all induced threats, both cyber and physical, including criminal, insider, domestic, and international.

To further the effectiveness in managing this concern, the natural gas pipeline industry has sponsored the development and maintenance of these Security Guidelines. They provide an example of a systematic “approach” that may be used by companies to determine security risks and to implement detection and deterrent practices. It uses the concept of risk management and, in particular, consequence determination to address and manage security issues. In addition, these Security Guidelines also provide for a more rigorous vulnerability assessment when deemed appropriate by the operator, and represents many of the conclusions from recent studies of security practices, including current best practices and gaps identified in those practices.

Since these Security Guidelines were published, significant progress has been made at all levels – national, state, local and industry – to better protect the Nation’s CI/KR. The industry will continue to partner with other industries as well as governmental agencies in order to effectively manage security of the pipeline CI/KR as well as update its Security Guidelines to address needed changes or revisions to the industry’s security practices and programs. Figure 1 is a map identifying the larger interstate natural gas pipelines in the U.S.
1.1 National Infrastructure Protection Plan

In June 2006, the NIPP was released to the general public. The NIPP meets the requirements that the President set forth in the HSPD-7, for the identification, prioritization and protection of critical infrastructure, and provides the overarching approach for integrating the Nation’s CI/KR protection initiatives into a single national effort. The overarching goal of the NIPP is to:

“Build a safer, more secure, and more resilient America by enhancing protection of the Nation’s CI/KR to prevent, deter, neutralize, or mitigate the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit them; and to strengthen national preparedness, timely response, and rapid recovery in the event of an attack, natural disaster, or other emergency.”

The NIPP provides the unifying structure for the integration of existing and future CI/KR protection efforts into a single national program to achieve this goal. It will enable the prioritization of protection initiatives and investments across sectors to ensure that government and private sector resources are applied where they offer the most benefit for mitigating risks by lessening vulnerabilities, deterring threats, and minimizing the consequences of terrorist attacks and other manmade and natural disasters.
The NIPP sets forth actions to address a series of objectives that require a collaborative partnership between and among a diverse set of security partners, including the Federal Government; State, territorial, local, and tribal governments; the private sector; and nongovernmental organizations, such as AGA and INGAA.

1.2 Authorities, Roles, Responsibilities, and Sector Specific Plans

The Homeland Security Act of 2002 provides the basis for DHS responsibilities in the protection of the Nation’s CI/KR, and for developing a comprehensive national plan for securing the Nation’s CI/KR. The national approach for CI/KR protection is provided through the unifying framework established in HSPD-7. HSPD-7 not only establishes the U.S. policy for enhancing protection of the Nation’s CI/KR and mandates a national plan to actuate that policy, but it also outlines other key roles and responsibilities for security efforts to specific security partners. These include assigning responsibility for CI/KR sector to nine SSAs as shown in Table 1 below.

The SSAs have been tasked to implement the NIPP framework and guidance as tailored to the specific characteristics and risk landscapes of each of the CI/KR sectors designated in HSPD-7. HSPD-7 has designated DOE as the SSA for the Energy Sector as it relates to production, refining, storage, and distribution of oil, natural gas, and electric power, except for commercial nuclear power facilities. As the SSA for Energy, DOE is responsible to coordinate the preparation of the Energy SSP that is an annex to DHS’s NIPP. It calls for private sector owners and operators to undertake CI/KR protection, restoration, coordination, and cooperation activities, and provide advice, recommendations, and subject matters expertise to the federal government as needed.

Under the NIPP, TSA is assigned as a SSA for the Transportation Sector, including the Nation’s pipeline systems. The U.S. Coast Guard (USCG) is the SSA for the Transportation Sector maritime mode. All of the SSAs coordinate closely with each other on pipeline security issues, programs, and activities. In addition, DOT’s Pipeline Hazardous Materials Safety Administration (PHMSA) \(^1\) is responsible for administering a national program for the safety of natural gas and hazardous liquid pipeline transportation, and DOT and the SSAs collaborate on matters related to the transportation security and infrastructure protection.

An Annex to the Memorandum of Understanding (MOU) between the DHS and DOT concerning TSA and PHMSA cooperation on pipeline and hazardous materials transportation security was signed in August 2006. The Annex delineates clear lines of authority and responsibility, and promotes communications, efficiency, and eliminates duplication of effort between the two Departments’ in the area of

\(^1\) PHMSA also oversees the security requirements of LNG facilities which predate 9/11.
transportation security. Table 1 lists each of the SSAs and the assigned CI/KR as set forth by HSPD-7.

Table 1 - Sector-Specific Agencies and HSPD-7 Assigned CI/KR Sectors

<table>
<thead>
<tr>
<th>Sector-Specific Agency</th>
<th>Critical Infrastructure/Key Resources Sector</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department of Agriculture</td>
<td>Agriculture and Food</td>
</tr>
<tr>
<td>Department of Health &amp; Human Services</td>
<td></td>
</tr>
<tr>
<td>Department of Defense</td>
<td>Defense Industrial Base</td>
</tr>
<tr>
<td>Department of Energy</td>
<td>Energy</td>
</tr>
<tr>
<td>Department of Health &amp; Human Services</td>
<td>Public Health and Healthcare</td>
</tr>
<tr>
<td>Department of the Interior</td>
<td>National Monuments and Icons</td>
</tr>
<tr>
<td>Department of the Treasury</td>
<td>Banking and Finance</td>
</tr>
<tr>
<td>Environmental Protection Agency</td>
<td>Drinking Water and Water Treatment Systems</td>
</tr>
<tr>
<td>Department of Homeland Security</td>
<td>Chemical</td>
</tr>
<tr>
<td>Office of Infrastructure Protection</td>
<td>Commercial</td>
</tr>
<tr>
<td></td>
<td>Dams</td>
</tr>
<tr>
<td></td>
<td>Emergency Services</td>
</tr>
<tr>
<td></td>
<td>Commercial Nuclear Reactors, Materials, and Waste</td>
</tr>
<tr>
<td>Office of Cyber Security and Telecommunications</td>
<td>Information Technology</td>
</tr>
<tr>
<td></td>
<td>Telecommunications</td>
</tr>
<tr>
<td>Transportation Security Administration</td>
<td>Postal and Shipping</td>
</tr>
<tr>
<td>Transportation Security Administration, United States Coast Guard</td>
<td>Transportation Systems</td>
</tr>
<tr>
<td>Immigration and Customs Enforcement, Federal Protective Service</td>
<td>Government Facilities</td>
</tr>
</tbody>
</table>

The NIPP required that each SSP be completed and submitted by the SSAs within 180 days of issuance of the NIPP. The SSPs provide the means by which the NIPP is implemented across all sectors, as well as a national framework for each sector that guides the development, implementation, and updating of state and local homeland security strategies and CI/KR protection programs. SSPs are tailored to address the unique characteristics and risk landscapes of each sector while also providing consistency for protective programs, public and private protection investments and resources. Both DOE and TSA engaged the natural gas industry in the development and review of their SSPs prior to publication. Executive Summaries from both the Energy SSP and Transportation SSP Pipeline Modal Annex can be seen in APPENDIX 2 and 3, respectively.
Consequently the natural gas pipeline industry is covered within the scope of multiple SSPs, requiring coordination with more than one SSA as well as other federal, state and local agencies. To date, the federal government has utilized the SCC/GCC model (discussed in 1.3 below) to help coordinate the multiple federal agencies involved with natural gas pipeline security. The need for coordination between the multiple oversight agencies remains strong, and the challenge for the federal government is to continue to try and rationalize this more complex (multiple-agency) oversight structure – i.e. take coordinated rather than independent agency actions affecting pipeline security and the natural gas industry. This concern is particularly strong from the perspective of a combination natural gas-electric utility due to the many additional security considerations (and potential for redundancy and conflicts) added from agency oversight on the electric side.

1.3 Security Partners

To effectively protect the U. S. natural gas industry CI/KR, there is a required partnership for all key stakeholders working collaboratively towards a common set of objectives. The natural gas industry remains committed to voluntarily working with all its security partners to ensure a useful exchange of security related information occurs and to optimize its infrastructure protection efforts. The NIPP base plan called for the creation of a SCC which is comprised of owners and operators and is self-organized, self-run, and self-governed with a spokesperson designated by the sector membership. The natural gas industry is part of the ONGSCC which includes 22 related industries (See APPENDIX 4). Each member of the ONGSCC has two representatives on the Council; one from its respective trade association and another from its respective industry. A chairperson represents the ONGSCC at all Critical Infrastructure Partnership Advisory Council (CIPAC) meetings which is the partnership between government and private sector CI/KR that facilitate effective coordination of security programs. A Pipeline Working Group has been established within the ONGSCC to address pipeline issues. Since natural gas pipelines are a mode of transportation, to avoid duplication and eliminate the need for multiple meetings with the same security partners, the ONGSCC Pipeline Working Group also acts as the Pipeline SCC for the Transportation SCC.

As noted earlier, the government counterpart to the SCCs is the GCCs that is comprised of representatives from Federal and State governments. The Energy GCC has also established a Pipeline Working Group to address pipeline issues. The Working Group also acts as the Pipeline GCC for the Transportation GCC.

The establishment of the GCCs and SCCs is proving effective in exchanging information, discussing security issues and goals, and protecting CI/KR. The industry was involved in helping develop both the Energy SSP and Transportation SSP Pipeline Modal Annex via writing teams comprised of members of the ONGSCC and industry security committees. Likewise, DOE, TSA and PHSMA, our government security partners, reviewed these revised Security Guidelines prior to publication.
As a result of partnership between the GCCs and SCCS, strong intra-pipeline industry partnerships have formed as well. Both AGA and INGAA have very active security committees comprised of representatives and security experts from within their membership. Each committee meets on a regular basis to share information, to discuss best practices, to receive security briefings from HITRAC and others, to collaborate on key issues, and to interface with their government counterparts on security topics outside the regular GCC/SCC meetings. These two committees communicate and work with each other when appropriate, and several individuals serve on both committees. There is also a strong tie between AGA and Edison Electric Institute (EEI) Security Committees due to the existence of combination gas-electric utilities and the shared interests of the membership.

One area where partnering between the SCC and GCC has proven effective is in the development of Pandemic Planning Guidelines for the ONG Sector. Although, pandemic planning and preparedness don’t pose a direct security threat to the industry’s CI/KR, it does fall into the broader perspective of ensuring the industry is prepared for an “all hazards” threat. More importantly, to avoid an economic and social catastrophe in the U.S., pandemic preparedness demands full public- and private-sector participation. With that in mind, DHS Secretary Michael Chertoff joined Secretary Leavitt in May 2006 to ask the National Infrastructure Advisory Council (NIAC) to provide them and President Bush with recommendations regarding the prioritization and distribution of pandemic countermeasures to the essential workers in our nation’s CI/KR sectors. Representatives from the ONGSCC participated on the NIAC Working Group, and developed a pandemic planning and preparedness template that has been adopted by and shared with all members of the ONGSCC. Additionally, most, if not all, natural gas pipeline companies have developed their own detailed pandemic and preparedness guidelines. A copy of the NIAC Final Report and Recommendations for the Prioritization of Critical Infrastructure For A Pandemic Outbreak In The United States can be found at http://www.dhs.gov/xlibrary/assets/niac/niac-pandemic-wg_v8-011707.pdf.

1.4 Information Sharing

The robust sharing of meaningful security related information between industry and government is important to the continual improvement of the joint security efforts and to the protection of the Nation’s CI/KR. There is a number of information sharing mechanisms in place to share both general security information and specific threat information. To work effectively, information sharing must be robust, timely, credible, actionable, and flow in all directions.

Listed below is the four general security information sharing mechanisms utilized by the natural gas industry and the government today:

1. Trade Association Security Committees – As mentioned earlier, both AGA and INGAA have very active security committees that meet regularly either in person and/or by conference call. A large portion of these meetings is focused on sharing and exchanging security information to ensure member companies
are knowledgeable of, actively engaged in, and strategically aligned on
security initiatives. Representatives of these committees also serve on the
ONGSCC which allows them to keep their security committees apprised of
ONGSCC activities and efforts. These committees routinely invite its
government security partners to participate in the meetings.

2. ONGSCC – The formation of the ONGSCC has significantly increased the
information flow between the government and industry as well as within and
between sectors themselves. The ONGSCC now serves as the focal point and
principal entity for coordinating and communicating with the government on a
wide range of CI/KR protection activities and issues. The sector relies heavily
on the ONGSCC to get much of its general security information coupled with
other information sharing mechanisms that also are available.

3. TSA Pipeline Security Stakeholder Conference Calls – TSA started
conducting regular conference calls with the pipeline industry in March 2006.
These calls are used to share and exchange information, to educate industry on
new security initiatives and programs, and to give industry an opportunity to
ask questions and bring up security issues for discussion.

4. Homeland Security Information Network (HSIN) – HSIN is a secure internet-
based communications system DHS established to facilitate exchanging
information between DHS and other government, private sector, and non-
government organizations involved in anti-terrorism and incident management
activities. In May 2006, the ONG HSIN was established and efforts are
underway to incorporate pipeline security communications and information
sharing activities into the existing ONG HSIN system. Pipeline companies
can have individuals within their organizations who have a “need to know”
about security information granted access to the ONG HSIN network.

Below are some examples of how information is exchanged and brought to the
attention of industry via the four major information sharing mechanisms:

1. Trade Associations - TSA and other government agencies sometimes provide
general threat information to the appropriate Trade Association who in turn
shares it with its security committee.

2. TSA Pipeline Security Division – TSA Pipeline Security Division provides
general threat information directly to the Trade Associations’ Security
Committees normally during their Stakeholder Conference Calls.

3. TSA Office of Intelligence - The TSA Office of Intelligence acquires and
assesses intelligence information regarding threats to transportation and
disseminates it, as appropriate, to officials in the government and industry
with transportation security responsibilities. The TSA Office of Intelligence
provides 24/7 indications and warnings, creates Spot Reports for DHS, acts as
the intelligence liaison to the Transportation Security Operations Center
(TSOC), and provides intelligence support, coordination, and communication between TSA Headquarters, TSA field operations, the aviation industry, rail-based urban mass transit systems, and the maritime, highway, cargo/supply chain, and pipeline/energy sectors. The TSA Office of Intelligence compiles transportation-related current intelligence, distributes warnings, alerts, and advisories, develops special event assessments (e.g., Super Bowl), and produces the weekly TSA Suspicious Incidents Reports.

4. HITRAC - DHS established HITRAC to develop products to help inform infrastructure owners and operators of any threats they may potentially face. HITRAC conducts integrated threat analysis for all CI/KR sectors, and produces information that supports responses to both emergent and immediate threats. HITRAC coordinates closely with security partners outside the Federal Government, and provides unclassified security threat updates at most of the Trade Association Security Committee meetings. They also provide bi-annual classified security threat updates to those security partners who have security clearances.

5. Direct Contact – Security representatives at individual companies are routinely contacted by government entities regarding any company-specific threats.

1.5 Security Incident Reporting

This section is intended to provide guidance on what type of security incidents and suspicious activities should be reported and to which authorities. This is an area that remains unclear, and hasn’t been addressed in the NIPP or SSPs. Consequently, the natural gas industry doesn’t have a single centralized organization to which it is to report security related incidences. Therefore, a number of organizations, as shown below, expect to be independently notified when there is a security related incident or when a suspicious activity has been noticed. **The first three organizations are prioritized in notification order per TSA recommendations.**

Local law enforcement should always be contacted first. This may include, if it is a known or suspected terrorist incident, the local Joint Terrorism Task Forces (JTTF) and/or Fusion Center. The JTTFs have been formed by the Federal Bureau of Investigation (FBI) to maximize interagency cooperation and coordination to create cohesive units capable of addressing terrorism problems within the U.S. A National Joint Terrorism Task Force is currently under development as a multi-agency task force at FBI headquarters. It consists of personnel from the intelligence, law enforcement (state, local and other federal agencies), and public safety community for the purpose of multi-agency information collaboration and efficient sharing between the FBI, the intelligence, the law enforcement, and public safety community nationwide.

State and local authorities have created 38 Fusion Centers around the country that provide critical sources of unique law enforcement and threat information, facilitate sharing information across jurisdictions and functions,
and serve as a conduit between people on the ground protecting their local communities to state and federal agencies.

Fusion Centers blend relevant law enforcement and intelligence information analysis and coordinate security measures in order to reduce threats in local communities. Analysts from the DHS’s Office of Intelligence and Analysis work side-by-side with state and local authorities at Fusion Centers across the country. These analysts facilitate the two-way flow of timely, accurate, and actionable information on all types of hazards.

2. The National Response Center (NRC)\(^2\) - The NRC is staffed 24/7 by Coast Guard watch standers, and any incident related to suspicious activity, terrorism, and possible terrorist activity requires telephonic notification ONLY to the NRC Center at 800-424-8802 or 202-267-2675. DO NOT SEND AN ON-LINE REPORT. Incidents requiring reporting would include bombings, bomb threats, suspicious letters or packages, and incidents related to the intentional release of chemical, biological or radioactive agents. Watch standers have been trained to ask specific questions for such reports, and will immediately pass the information to the proper agencies for response.

3. The Transportation Security Operations Center (TSOC) - The TSOC serves as the 24/7 point of contact for all transportation security concerns, including aviation, rail, mass transit, maritime, pipeline, highway, and cargo issues. The TSOC correlates and fuses real-time intelligence and operational information across all modes of transportation, and coordinates with all homeland security agencies for prevention of, and response to transportation-security related incidents. The TSOC monitors the security status of the transportation network/infrastructure in real time and, on an almost daily basis, receives notifications of potential incidents from numerous sources and transportation entities. Upon notification, the TSOC Command Center Watch reaches out to federal, state, and local law enforcement and to stakeholders to gather additional information. They also distribute actionable intelligence information related to transportation security to appropriate departments, agencies, industries and associations. The reporting of all surface transportation security-related incidents, as well as questions or additional information, should be directed to the TSOC Surface Transportation Operations Officer at 866-615-5150, Fax: (703) 487-3573 or Email: TSOC.ST@dhs.gov.

4. HITRAC - HITRAC has been established for intelligence analysts and infrastructure specialists to work in identifying the threat to critical infrastructures, vulnerabilities and interdependencies, and the overall risk inherent in any potential attack against critical infrastructure. HITRAC works closely with critical infrastructure owners and operators to ensure that the most complete, actionable, and accurate information regarding private sector

\(^2\) NRC does not have FOIA protection.
assets is disseminated expeditiously to key stakeholders. HITRAC also provides recommended protective measures. As mentioned earlier, HITRAC is the reporting entity for the ONG HSIN tool, and they can be contacted at 202-447-3086.

5. National Infrastructure Coordinating Center (NICC) – The NICC, a key component of the Infrastructure Coordination Division (ICD), serves as an extension of the Homeland Security Operations Center. Its mission is to assess the operational status of the nation’s CI/KR, to support information sharing with the ISACs and the owners and operators of CI facilities, and to facilitate information sharing across and between the individual sectors. Please email the NICC at nicc@dhs.gov or call them at 202-282-9201, 9202 and 9203

6. For Jurisdictional Interstate Pipelines – The Federal Energy Regulatory Commission (FERC) issued Order 682 amending section 260.9(a) to require that interstate natural gas companies report at the earliest feasible time (1) damage to natural gas facilities from a hurricane or other natural disaster or terrorist activity that results in loss of or reduction in pipeline throughput or storage deliverability, and (2) when the damaged facilities' pipeline throughput or storage deliverability has been fully restored. Such reports must be made, regardless of whether service interruptions were avoided by rerouting natural gas supplies or other means. FERC requests these notifications be made by either email to pipelineoutage@ferc.gov or facsimile transmission.

2.0 BACKGROUND

2.1 Pipeline Industry Practices

Security of pipeline infrastructure has always been a concern for the industry. Vandalism, the primary concern historically, has been a real and ongoing issue but has been effectively managed due to its localized nature and limited scope. Redundancies of company facilities as well as the nature of the national grid provide excellent reliability of service.

Pipelines have been historically designed, constructed, operated, and maintained with full consideration of risk management principles. The Pipeline Safety Regulations and its predecessor, the American Society of Mechanical Engineers (ASME) B31.8 code, have different requirements based on consequence and likelihood of pipeline failures. There are several references used by the industry for pipeline construction, operation and maintenance. Concepts such as class location and high consequence areas focus on population density and require stronger pipe, more frequent inspections, and greater integrity management. These regulations provide the owners
and operators with detailed information about the location and density of population, and places where people congregate such as schools and hospitals. The concepts provide a preliminary tool for analysis when considering management of security events.

Planning for natural disasters such as hurricanes, floods and earthquakes as well as preparation for managing pipeline failures has provided the industry with the opportunity to be well prepared for large-scale outages. In addition, due to the consequence of a failure in the system, redundancies were built into the pipeline infrastructure including many interconnects between companies. This planning and interconnect capability have provided the American consumer with reliable service even during major natural disasters and other system failures.

The Y2K effort saw yet more security implications addressed and carried out. Virtually every organization in the industry was compelled to identify their individual company’s cyber security issues. Additionally, the entire energy infrastructure was examined and addressed globally. National plans were developed, mock drills were administered, significant resources were committed, and the effort was successfully managed. Much of the work for this effort was also readily transferable to the cyber-terror arena (see APPENDIX 5

### 3.0 VULNERABILITY AND RISK ASSESSMENT

The approach demonstrated in the original Security Guidelines followed to the extent practical the “Vulnerability and Risk Analysis Program, Overview of Assessment Methodology” report developed by the DOE’s Critical Infrastructure Protection as well as the system currently being implemented for DOE’s most critical nuclear weapons facilities under the direction of the National Nuclear Security Administration (NNSA).

The first step in the approach is to determine whether or not a facility is critical. This determination is based on the system configuration of individual companies and the definition of critical facilities as shown in Section 4.0. As recommended by the DOT’s Office of Pipeline Safety (OPS), the extent to which a facility is critical depends on three main factors: 1) whether it is a viable terrorist target; 2) how important the facility is to the Nation’s energy infrastructure; and 3) how likely the facility is to be used as a weapon to harm people. If facilities are not deemed to be critical, normal operations and maintenance should be performed.
4.0 CRITICAL FACILITY DETERMINATION

Currently, other than the 2002 DOT Pipeline Security Contingency Planning Guidance, (see APPENDIX 9) there had been no published guidance from the government to define a critical facility. Both the NIPP and DOE Energy SSP discuss CI/KR extensively, but neither plan clearly defines it. In addition, the TSA SSP Annex F: Pipeline Modal Annex does not define it either, but does indicate critical assets include pipeline components such as:

- Pipeline interconnections
- Hubs or market centers
- Metering stations
- Pump stations
- Compressor stations, terminals
- Operational control facilities
- Pipeline bridge crossings
- Critical above ground piping
- Storage facilities

Therefore, each operator must determine, based on the general guidance provided by the Energy and Transportation SSPs coupled with their own knowledge of and familiarity with their system, what are the critical facilities of their own systems. Operators should factor in consequences, threats, and vulnerability when evaluating their facilities. Work done in recent years regarding high consequence areas for integrity programs should be considered along with numerous other factors such as throughout, single-line service, line pack, automation, etc. in determining the operator’s critical facilities. Some operators may find it appropriate to have two classes of critical facilities: DOT critical and company critical.

For purposes of security planning when the guidelines were originally published in 2002, a facility is a critical facility if it meets one or more of the following criteria as developed by DOT in the 2002 Pipeline Security Contingency Planning Guidance (see APPENDIX 9):

1. A pipeline facility or combination of facilities that may be considered a viable terrorist target and (a) intelligence information indicates that the facility, or facilities like it, is being targeted for attack or (b) a release from the facility has the potential for mass casualties or significant impact on public drinking water affecting a major population center;

2. A facility or a combination of facilities that, if damaged or destroyed, would have a detrimental impact on the reliability or operability of the pipeline system, significantly impairing the operator’s ability to serve a large number of customers for an extended period;
3. A facility or combination of facilities that, if damaged or destroyed, would significantly impair the operator’s ability to serve installations critical to National defense; or

4. A facility or combination of facilities that, if damaged or destroyed, would so impair other modes of transportation or other critical infrastructures (such as electric power generation, telecommunications or public utility) that it would cause major economic disruption.

This definition could be applied to ALL facilities, regardless of type, (i.e., distribution, transmission, natural gas, liquid, liquefied natural gas (LNG), etc.). With respect to natural gas distribution and transmission, the following facilities, might be considered for review. See APPENDIX 7 for more details.

- Main line block valves, launchers and receivers
- Communication facilities (phones, microwave, radio, voice/data)
- Supervisory Control And Data Acquisition (SCADA) systems
- Offshore platforms
- LNG terminal and land-based facilities
- Customer Call and Emergency Response Centers
- Other operator specific facilities

Operators have identified their critical facilities, and these determinations have been extensively reviewed to-date by TSA through their CSR program. Individual operators will continue to update and refine such critical facility determinations based on changes to their systems, and input from TSA and DOE under their respective SSP/SSA activities.

5.0 PRESCRIPTIVE OR PERFORMANCE DETERMINATION

After the determination that a facility is critical, the operator may choose to follow a prescriptive approach or a performance approach (or even a hybrid approach using parts of both the prescriptive and performance approaches) to determine the detection and deterrent methods as well as the response and recovery methods.

The prescriptive approach is described in detail in Section 6.0. This approach requires the operator to determine the permanent facility detection and deterrent methods and to develop an operational action plan that provides for the temporary actions the operator would take based on the threat condition. APPENDIX 8 is provided as a reference for the minimum suggested detection and deterrent methods requiring capital expenditure. The minimum action items to be incorporated in the operator’s action plan are listed in APPENDIX 9 as issued by DOT for critical facilities. Finally, responses to events are developed and recovery from events is planned for. Feedback
in the form of a comparison to actual events or performance testing should be used to modify the plan.

Note that the DOT guidance in APPENDIX 9 establishes guidelines for protective measures under specified threat conditions to help pipeline operators prepare and implement effective security. The protective measures listed in that guidance are intended to be applied only to critical facilities, although several of the countermeasures require company-wide actions. DOT and TSA expect that operators will use good judgment in incorporating these measures into their security plans, recognizing that not all countermeasures are appropriate for all types of facilities.

The performance approach as depicted in this guideline requires the operator to conduct a vulnerability assessment and is detailed in Section 7.0. An example of such a vulnerability assessment method is also provided in Section 7.0. The results of a vulnerability assessment will delineate any permanent facility detection and deterrent methods, temporary operators’ actions based on threat condition and response and recovery actions to follow. It should be noted that the approach presented in Section 7.0 requires the application of a vulnerability assessment. There are other equally acceptable performance methodologies presently in use among security professionals that do not require such an assessment.

The operator may choose to follow different options for different facilities or facility type. For example, the operator may choose to follow the performance path for compressor stations and LNG terminals and follow the prescriptive path for all other facility types. An operator may also decide to follow the performance path for one compressor station and the prescriptive path for another compressor station. Finally, an operator can choose to follow both paths.

Although the two paths ultimately lead to an acceptable level of protection for facilities with respect to security, the assessments differ in rigor and flexibility. The prescriptive path is easier to use but has less flexibility while the performance path requires more rigor in the analysis but provides more flexibility when initiating detection and deterrent options as well as response and recovery options.

**6.0 PRESCRIPTIVE METHOD**

**6.1 Approach**

Figure 1 represents the approach for the prescriptive method. It does NOT represent a vulnerability assessment approach, which is discussed in Section 7.0. Each element of the approach is briefly discussed in this section and discussed in detail in subsequent sections. By following the approach, the operator may systematically account for the security risk. Documentation of the approach and the results allow for systematic changes based on new information.
Critical Facility Definition - In this step, the operator determined the criticality of an individual facility, or by groups of like facilities for each facility type, or by facility type, whichever is the most appropriate for the operator. This determination is based on the criteria for critical facilities as defined in Section 4.0.

Detection and Deterrent Methods - After a risk assessment, the operator identifies and selects appropriate detection and deterrent methods based on the risk category for the facility. The detection and deterrent methods may vary depending on several factors and would include permanent physical changes to the facilities.

Operational Response Plan - In this step, the operator develops a plan that addresses the risk category from the risk assessment and details the temporary detection and deterrent methods selected. This plan also considers the threat or condition-state as determined by the government.

Response to Events - There are typically three elements to consider in responding to events: Emergency Plans, Incident Management Plans, and Regional Management Plans. The Emergency Plan deals with the emergency on a local level while the Incident Management Plan addresses the event on a large scale and involves resources across the company. Additionally, the Regional Management Plan focuses on the significant regional or national implications of an event.
Recovery from Events - There are typically three elements to consider in recovery from events: Operations and Maintenance Manual, Disaster Recovery Plan, and Regional Emergency Recovery Plan. The Operations and Maintenance Manual details the repair and return of a facility to normal operations. The Disaster Recovery Plan addresses the restoration of service after the loss of primary locations and processes. The Regional Emergency Recovery Plan involves significant variances from accepted practices and regulations in order to reinstate or maintain service.

Modifications to Approach - This feedback mechanism considers the specifics of any security event in order to improve this plan. In addition, the plan is periodically updated and/or verified through the conductance of mock emergencies and table top exercises.

6.2 Detection and Deterrent Methods

Based on results provided by the AGA/INGAA Security Committees, detection and deterrent methods were identified. A list of these methods was developed and is provided in APPENDIX 8. The methods listed in Appendix 8 are not intended to make facilities defendable from determined physical attacks but are designed to deter and detect an event and assist in the operator’s response to a security situation.

Certain options can serve as both detection and deterrent methods. For example, patrolling of facilities provides for detection of tampering and perhaps identification during the act. Patrolling also serves as a deterrent in that a saboteur recognizes that the act or the planning of the act may be discovered.

The operator should implement the methods in APPENDIX 8 for each facility type that meets the criteria for critical.

6.3 Operator Action Plan

Based on the Department of Homeland Security Threat Advisory System, industry will respond along the following lines:

Low Condition - Green

Low risk of terrorist attacks - the following Protective Measures may be applied:

- Refining and exercising preplanned Protective Measures
- Ensuring personnel receive training on Office of Homeland Security Threat Advisory System, departmental, or agency-specific Protective Measures
- Regularly assessing facilities for vulnerabilities and taking measures to reduce them

Guarded Condition - Blue

General risk of terrorist attack - in addition to the previously outlined Protective Measures, the following may be applied:
• Checking communications with designated emergency response or command locations
• Reviewing and updating emergency response procedures
• Providing the public with necessary information

Elevated Condition - Yellow

Significant risk of terrorist attacks - in addition to the previously outlined Protective Measures, the following may be applied:
• Increasing surveillance of critical locations
• Coordinating emergency plans with nearby jurisdictions
• Assessing further refinement of Protective Measures within the context of the current threat information
• Implementing, as appropriate, contingency and emergency response plans

High Condition - Orange

High risk of terrorist attacks - in addition to the previously outlined Protective Measures, the following may be applied:
• Coordinating necessary security efforts with armed forces or law enforcement agencies
• Taking additional precaution at public events
• Preparing to work at an alternate site or with a dispersed workforce; and restricting access to essential personnel only

Severe Condition - Red

Severe risk of terrorist attacks - in addition to the previously outlined Protective Measures, the following may be applied:
• Assigning emergency response personnel and pre-positioning specially trained teams
• Monitoring, redirecting or constraining transportation systems
• Closing public and government facilities
• Increasing or redirecting personnel to address critical emergency needs

It is anticipated should the industry go this alert level, that specific and credible information would be communicated to the industry or a particular company by the appropriate government agency or agencies through the communication channels referenced earlier in Section 1.5. Industry information would be posted and kept updated on HSIN.

The operator action plan should be used to document the results of the risk category and Condition State risk assessment. The plan should list the temporary actions to be taken for detection and deterrence of security events. The plan should identify the
threat condition-state; the initiating event necessitating a response by the operator; and the operator’s response.

The operator’s actions are identified in the plan and vary depending on the condition state. The responses are typically temporary and usually do not involve facility modifications.

The operator’s plan should include the applicable protective measures shown in APPENDIX 8.

6.4 Response to Events

Responses to events were determined by the AGA/INGAA Security Practices team to contain three elements. The first element is already well developed, tested and accepted, and is required by the Pipeline Safety Regulations. Each operator currently has an Emergency Plan in place. These plans, which are facility specific, are intended to deal with facility specific events and include isolation of facilities, protection of the public and company personnel, etc. Local operating personnel, who are trained on the plan and practice implementation, will execute the plan. Also, these plans are reviewed with local emergency responders and law enforcement agencies in order to ensure timely and effective event response. Communication with law enforcement agencies and emergency responders during an emergency are detailed in the plan.

The second element is a plan designed to address all issues beyond the local area of concern. These plans should include actions to be taken on a local and corporate level for such things as floods, hurricanes, earthquakes, major system outages, catastrophic loss of facilities and company personnel, loss of communications, control and response capabilities. These plans should be developed and practiced by a large portion of the company’s management and personnel. These plans should provide for communications with a wide variety of government agencies, emergency response organizations, law enforcement agencies, etc. Such plans were used during the Y2K event and Hurricanes Katrina and Rita.

The third element is a state or regional management plan that would be invoked if there were significant state, regional, or national implications from a security event. This plan would provide for such contingencies as re-routing and/or curtailment of gas supplies in some markets in order to continue gas supply in other markets.

6.5 Recovery from Events

Recovery from events was determined by the AGA/INGAA Security Practices Committee to contain three elements. The first element is already well developed, tested and accepted, and is required by the Pipeline Safety Regulations and its predecessor, the ASME B31.8 code. Each operator currently has Operation and Maintenance Procedures in place that deal with restoration of a facility and returning it back into service. These procedures, which are facility specific, are intended to
deal with facility specific events and include repair and restoration of service. These procedures are carried out by local operating personnel who are trained and have experience on the procedures.

The second element is a plan designed to address issues beyond the local area of concern. These plans should include actions to be taken on a local and corporate level for such things as restoring operation of primary locations and processes. These plans should be developed and practiced by a large portion of the companies management and personnel and include processes for operating the company from remote locations given the loss of the primary location and backup of critical processes and records.

The third element is a state or regional emergency recovery. This would involve obtaining significant variances from accepted practices and regulations in order to reestablish or maintain strategic natural gas service. These include, but are not limited to, permits, land acquisition, and strategic inventory stockpile.

6.6 Critical Spare Parts

The natural gas industry has experience with large-scale outages caused by natural disasters, third-party incidents, and vandalism. This experience has enabled the industry to reasonably determine that if an incident such as a terrorist attack were to occur, the incident most likely would not cause mass destruction to the entire “critical facility.” However, the attack could impact specific critical parts imperative for the operations of a facility.

Current industry spare part inventory practices and the practice of obtaining or sharing parts and supplies between companies or from suppliers are key aspects of safety and security initiatives. Inventories of emergency and critical spare parts are stored in centralized warehouse locations and other physical locations such as compressor stations. Materials in inventory include long lead-time items such as parts for engines and compressor station auxiliary systems, pre-tested pipe, valves and high yield fittings. In addition, pipeline companies have alliance agreements with vendors to utilize their inventory for short lead-time items and for major construction materials. The natural gas transmission industry typically doesn’t have “mutual assistance” agreements like those often found among natural gas distribution companies, but transmission companies do share parts and equipment during emergencies, if possible. A good example of parts and equipments sharing occurred during Hurricanes Katrina and Rita. A more detailed description of the industry’s spare part inventory practices along with sharing practices is found in APPENDIX 10 of these Security Guidelines.

6.7 Modifications to Approach

Security plans should be periodically internally reviewed and updated. Training of all individuals that would be involved in the process must occur. Testing of the plan through mock exercises and drills is a common practice and should be considered by
the operator. In addition, at the conclusion of a security event, the plan should be reviewed and modified as necessary. Companies should also modify their security plans based on information shared from:

- TSA CSRs
- Trade Association Security Committee Meetings
- ONGSCC/GCC Meetings and activities
- State and local security reviews
- New security technology advancements
- TSA Pipeline Security Smart Practices

In 2007, TSA distributed its list of 130 Pipeline Security Smart Practices that were broken down into 12 categories. It is not intended that each company incorporate all the Pipeline Security Smart Practices, but only those that make sense for a particular company based on factors such as practicality, risks, economics, etc.

6.8 Information Control

The control of information is essential for security purposes. It is recommended that companies closely control all data and information used and developed for performing security assessments as well as implementation of plans and procedures. It’s important that critical security information only be shared with those government agencies that have protection from the Freedom of Information Act (FOIA). The sharing of critical and sensitive security information is a concern of the industry, particularly when the information may be in a National Asset Database (NAD) or when states are requesting the information. When providing information to organizations and agencies outside of the control of the operator, refer to API 1162 “Public Awareness Programs”.

7.0 PERFORMANCE METHOD

7.1 Approach

As a best practices approach, this methodology is adapted from similar ones now in use within government (DOE, Department of Defense (DOD), and Department of Agriculture) for its most critical facilities and operations. The approach also takes into account existing security, safety and natural disaster recovery programs. It should be noted that the approach presented here requires the application of a vulnerability assessment. There are other equally acceptable performance methodologies presently in use among security professionals that do not require a vulnerability assessment. Thus what follows serves as one example of a performance method and should not be misconstrued as the recommended methodology.
Operators should proactively establish and continually reinforce their liaisons with federal, state, and local law enforcement. These existing intelligence resources are responsible for threat information gathering and analysis. Note that in most cases to obtain any level of detail from such organizations, the operator may need to obtain security clearance. The information in Section 7.0 is provided to educate the operator of the type of information to be aware of. By obtaining from established government or private sources the type of information listed below, the operator can more effectively assess the significance of the threat.

Sustainability is a core objective, as the U.S. is likely to face an evolving threat for the long-term. With a best practice methodology established at the industry level, companies will also have a resource base and access to expertise with which they can pursue implementation in a manner that is observably uniform across industry.

Figure 2 represents the process typically used in a vulnerability assessment approach. Each element of the approach is briefly discussed in this section. By following the approach, the operator systematically accounts for the security risk, documents the findings and implements the appropriate risk controls.
These considerations focus attention on those key assets (personnel and operating systems), threats, protection system elements, and consequences expected to be predominant in a heightened threat environment.

The information gathered will be used to determine the adequacy of protective systems in place and the need (if any) for enhancements. Also, in normal periods the process can be utilized to identify and prioritize where cost effective upgrades can be made, and during high threat periods, to rapidly direct security efforts and resources into the most appropriate areas.

7.2 Threat Analysis and Assessment

Threat monitoring is essential to the success of any sustained security effort. A “threat review” is comprehensive look at all available information in order to help evaluate the security posture of the system with regard to various threats, possible targets, and associated vulnerabilities.

The threat review should be continual since it’s difficult to know about all possible threats. While current security needs are addressed, the threat situation may be changing and new threats may be arising. Failure to update the threat assessment on a continuing basis may constrict a company’s ability to protect itself.

Successful analysis will not only rely on research and analysis alone but also will include continuing, up-to-the-minute liaison with local, state and federal law enforcement and intelligence agencies.

Operators using this method will comprehensively look at all available information in order to evaluate the security posture of the system with regard to the threats, targets, and vulnerabilities. The components of a thorough threat analysis include:

- Researching the threat to identify threat groups.
- Gathering information and intelligence that provides the answers about goals, methods of operation, techniques, strategies, tactics and potential targets of the adversaries.
- Studying the vulnerabilities to understand weaknesses in the existing security program, as well as the high-risk targets.

After examining the different adversary categories [e.g. crusaders/professionals, criminals/semi-professionals and crazies/amateurs which can be disgruntled employees] and the attack planning considerations, they are likely to employ a thorough knowledge of the characteristics of each threat group in order to arrive at a determination of the threat they pose to each key asset within an operating company or the energy system as a whole. Areas of review include:
- Threat Organizational Characteristic - An examination of the adversary’s structure and how it sustains itself. Understanding the threat's organizational characteristics is essential in determining the potential threat posed to the system. These characteristics should be analyzed in terms of organization, recruitment, financing, and international connections.

- Threat Operational Characteristics - An examination of how the threat will likely carry out their acts of aggression. Gathering information on the threat's operational capabilities is necessary in order to develop a base for planning countermeasures. Operational characteristics should be reviewed in terms of threat planning, timing, tactics, and insider threat potential.

- Threat Behavioral Characteristics - An examination of the threat's psychological profile to see how it affects their ability to commit aggressive acts against a system. This should be studied in terms of motivation, dedication and discipline.

- Threat Resources Characteristics - An examination of the threat's ability to obtain the resources needed to threaten a system. Evaluating the resources available to the threat group may represent the most important factor in evaluating their capability to successfully threaten a system key asset. Resource capabilities should be analyzed in terms of training and skills, group size, weapons and equipment, and transportation.

7.3 Asset Criticality

The first step in deciding the level of protection that a key asset would require is determining how critical that key asset is to the functioning of the system. This should be determined from the point of view of system operations. To measure the criticality of any single key asset, it is necessary to examine the consequences to the system of a successful attack against that key asset. The following information may be sought from existing government and/or private intelligence resources responsible for threat information gathering and analysis. These consequences to the system should be analyzed by examining the loss of a key asset in terms of the following three factors:

1. System Analysis - How the system would function or perform if the key asset is destroyed, damaged, or degraded. The loss of certain assets may not only reduce immediate system production capacity, but also may reduce system reliability by reducing system reserves, leading to fewer options and less resilience in the case of further attacks.

2. Ease of Replacement - This should be viewed in terms of availability of spare parts are available and the time required to manufacture replacement components if spare parts are unavailable. Also considered is the time it would take to install any replacement parts, once they can be obtained.
3. Redundancy of Asset Function - This analysis looks at whether there are other means available to perform the function if the key asset is damaged or destroyed. These alternative means may come from the effected company's own resources, from other companies or even governmental agencies.

Once the above three-part analysis has been completed, the resulting information is used to determine the overall impact on production from loss of this particular key asset.

7.4 Asset Attractiveness

Adversaries will usually evaluate a number of similar targets that potentially meet their objectives. Through a process of elimination the adversary will select the facility that offers the best probability of success with minimal effort, resources and organizational exposure. A target’s attractiveness is directly proportional to how effective the attack is in achieving the threat’s goals. So, while a key asset may be vulnerable to attack by a given threat, it may not be an attractive target.

To determine the attractiveness of any key asset to a given threat group requires the use of information from both the Threat Analysis as identified in Section 7.2 and Asset Criticality identified in Section 7.3. Information about the threat's goals, motivations, and objectives, combined with the asset's importance to the operation of the system are used to determine the attractiveness of the key asset. This two-part process is based on:

- Historical Incident Analysis
- Current Goals Analysis

Once again, this information may be sought from existing government and/or private intelligence resources responsible for threat information gathering and analysis. One of the most important pieces of evidence is the historical data on whether any given threat group has attacked this type of key asset in the past, and if so, how often. In most cases this is a strong indication if the threat will continue to view attacks on this type of target as an effective method of achieving the threat goals. Simply put, if a given target was attractive to a threat in the past, it is likely to remain attractive to him in the future. However, the threat assessment must be kept current since adversary goals can change, evolve or become more refined.

Therefore, historical information must be combined with a current goal analysis. Utilizing current intelligence and information, threat group motivations, and objectives should be analyzed in order to decide how attractive a key asset is in terms of accomplishing current threat goals. Many threat groups typically have overlapping goals. Threat goals and their relationship to a given key asset should be analyzed in terms of these potential threat objectives:
- Causes injury and death of personnel - Often a goal of Terrorist Groups seeking the most effective way to create terror, but can also be the goal of criminals, disgruntled employees or disoriented persons.

- Enrichment - The primary goal of the criminal, but also a favorite objective of the disgruntled employee who rationalizes that the money or other benefits gained will even the score.

- Social and economic disruption of the area - A prime terrorist goal in many cases and one in which the criticality of the key asset would be important in determining how attractive that key asset would be to the terrorists. Disgruntled employees and disoriented persons may also have an interest in this goal.

- Publicity and political statement - Although often a terrorist goal, this type of objective can also be sought by extremist protest groups.

- Increase public support for threat - Almost exclusively a goal of extremist protest groups.

- Destroy public confidence and feeling of safety - This objective is generally found only with the terrorist groups.

- Embarrass the company - This objective is associated not only with extremist protest groups, but also with disgruntled employees.

- Force change to operator/company policies - A typical goal of extremist protest groups.

- Vengeance - An objective generally found only with disgruntled employees and disoriented persons.

When analyzing attractiveness issues it is important to view the company's key assets in their total domestic and international environment. A company, particularly one that is part of or has large diversified interests, may be an attractive target for secondary reasons that do not directly relate to the company itself. Additionally, important industries or national security interests in the customer service area that could be disrupted by an attack should be considered.

After reviewing the historical data and analyzing the current information on threat goals, the process of determining the overall attractiveness rating of any given key asset can be depicted.
7.5 Asset Vulnerability

Typically, when an adversary analyzes a potential target, the threat group will attempt to determine if the asset is vulnerable to the means of attack at the disposal of the threat group.

To prepare for a vulnerability assessment of specific assets, operations managers should obtain all information about the security posture of the system that may have a potentially protective effect with regard to the asset. Such information may be sought from existing government and/or private intelligence resources responsible for threat information gathering and analysis. Security system effectiveness for each key asset can be discerned from the following areas of review:

1) Asset Characteristics:
   a) Site and geographical location
   b) Local social factors
   c) Utilities and outside support
   d) Adversary escape possibilities
   e) Ease of key asset recognition

2) Security System Characteristics:
   a) Graded approach
   b) Adversary deterrence (Barriers; Signs; Lighting; Patrols; Local Law Enforcement Presence; Deception, etc.)
   c) Pre-Incident indicator capability
   d) Accurate assessment of adversary
   e) Timely detection of adversary
   f) Adversary delay
   g) Adversary interruption
   h) Adversary neutralization

3) Physical Security Characteristics:
   a) Access controls (Badge compliance; Escorting; Entry and exit searches; Key control)
   b) Employee security education and awareness
   c) Facility lighting
   d) Facility barriers
   e) Contract guard force and response

From a review of these three areas, a picture will emerge of the relevant security weaknesses for each asset identified as critical to system operations.

7.6 Other Employee Protection and Facility Security Considerations

During the risk analysis and evaluation process, additional factors that apply to the protection and security of all key assets (employee and facility operating system) should be identified for which policies, procedures, and operating practices need to be
reviewed or developed to provide enhanced protection. Review of these activities, which should be ongoing, would further assist in determining security vulnerabilities.

7.7 Implementation of Risk Controls

To be valuable, the analysis should provide management with a bottom-line result that describes the amount of risk to which the asset being evaluated is exposed. Assets once considered critical may receive a lower rating because of recovery, redundancy, or protection. Some assets thought less important may receive a higher risk rating and may be in need of immediate attention.

This allows management to prioritize security enhancements during normal periods and to allocate resources during high threat periods.

Security recommendations usually fall into four areas:

1. Critical enhancements requiring immediate attention.

2. Risk reduction enhancements (cost-benefit analysis).

3. Cost reduction enhancements designed to maintain security at the current acceptable level, but do so at a lower cost.

4. No enhancements - Current system meets and/or exceeds providing adequate security in a cost effective way.

Companies then adopt a security strategy based upon facility characterization, threat capabilities, risk acceptance, and cost-effectiveness. Similar to the concept of “Protection-in-Depth,” multiple layers of different barrier types are put into place along all possible adversary paths in order to complicate adversary planning and provide additional time for the response forces to interrupt. Example elements of a protective system are: Physical Security; Protective Force; Personnel Security; Information Security; Communications Security; Damage Assessments; and a Security Discrepancy and Infraction Program.
APPENDIX 11

Pipeline Operations Background

1.1 Natural Gas Transmission Pipeline Operation

As reported by the Energy Information Administration (EIA) natural gas provides approximately 25 percent of the energy needs of the United States. The natural gas is principally transported through a complex network of nearly 290,000 miles of high-pressure pipelines, called transmission pipelines that crisscross America.

The transmission network receives the natural gas from gathering systems and processing plants and delivers the gas to investor-owned utilities, municipalities, and end-use customers.

It is important to realize that natural gas is only delivered to consumers by pipelines operating on a real time basis. This is significantly different than the national oil delivery system that utilizes pipelines, railroads, barges and trucks. The natural gas system operates very similarly to the electrical grid system, but the reaction time to consumers from outages is significantly greater. There are storage facilities for short-term and winter peaking use at selected locations in the country that permit the temporary storage and retrieval of natural gas. These are minimal as compared to the oil delivery system that has terminal tanks, gasoline storage tanks, and storage tanks at individual houses and businesses. This system design demands constant utilization of the pipeline system capacity to prevent shortages and to prevent consumer price spikes.

In addition, the transmission systems move large amounts of gas from the production areas where the natural gas is gathered and processed to local distribution companies (LDCs). Many of these pipeline systems contain multiple lines that run parallel to each other in the same right-of-way.

The amount of natural gas that can be delivered per day by a natural gas transmission system to a market depends on four variables.

Number of Pipelines - The capacity of the natural gas pipeline system is the summation of the capacity of individual pipelines emanating from supply sources. Some markets have one pipeline (sole source), others may have multiple pipelines emanating from the same supply source, and some may have multiple pipelines emanating from multiple sources.

Diameter of a Pipeline - This factor determines the cross sectional area of the pipeline through which the natural gas passes. Typical transmission pipelines range in diameter from 8 inches to 48 inches.
Pressure of Natural Gas - This determines the true volume of natural gas that is compressed into the confined space of the pipeline. Unlike a liquid, if natural gas is compressed to a higher pressure there are additional molecules within the same space, and therefore more molecules can pass through the same cross sectional area at a given velocity. Typical operating pressure in transmission pipelines range from 100 pounds per square inch (psig) to 1,440 psig.

Velocity of Natural Gas - The amount of natural gas that can be passed through a given cross sectional area at a given pressure is dependent on how fast the natural gas is moving through the pipeline. Typical velocity is 10 to 15 miles per hour in a natural gas transmission pipeline.

If either one of these variables is adjusted, the capacity of the pipeline system (ability to supply consumer demand) is altered. During normal operation, pressure and velocity of the natural gas being transported is adjusted to track the instantaneous demand of consumers. In periods of low demand, a given pipeline can be removed from service (no flow), if the remaining pipelines are operating at enough pressure and velocity to satisfy the demand.

The natural gas delivery infrastructure is designed to adjust for short-term losses in pipeline capacity, but it is not intended to accommodate long-term repetitive reductions in capacity, such as periodic integrity inspections at an accelerated rate.

1.2 Gathering

From the well, the natural gas goes into "gathering" lines, which are like branches on a tree, getting larger as they get closer to the central collection point. A gathering system may need one or more field compressors to move the natural gas to the pipeline or the processing plant. A compressor is a machine driven by an internal combustion engine, turbine, or electric motor that creates pressure to "push" the natural gas through the lines. Most engines and turbines in the natural gas delivery system use a small amount of natural gas from their own lines as fuel.

1.3 Processing

Some natural gas gathering systems include a processing facility, which performs such functions as removing impurities like water, carbon dioxide or sulfur that might corrode a pipeline, or inert gases, such as helium, that would reduce the energy value of the gas. Processing plants also can remove small quantities of propane and butane. These gases are used for chemical feedstocks and other applications.

1.4 Compressor Stations

Compressor stations are typically located approximately every 60 to 90 miles along each pipeline to boost the pressure that is lost through the friction of the natural gas moving through the steel pipe. Many compressor stations are completely automated, so the
equipment can be started or stopped from a pipeline's central control room. The control center also can remotely operate shut-off valves along the transmission system. The operators of the system keep detailed operating data on each compressor station, and continuously adjust the mix of engines that are running to maximize efficiency and safety.

Natural gas moves through the transmission system at up to 30 miles per hour, so it takes several days for natural gas from Texas to arrive at a utility receipt point in the Northeast. Along the way, there are many interconnections with other pipelines and other utility systems, which offer system operators a great deal of flexibility in moving natural gas.

1.5 Linepack

A 50-mile section of 42-inch transmission line operating at about 1,000 psig contains about 200 million cubic feet of natural gas -- enough to power a kitchen range for more than 2,000 years. The amount of natural gas in the pipe is called the linepack. By raising and lowering the pressure on any pipeline segment, a pipeline company can use the segment to store natural gas during periods when there is less demand at the end of the pipeline. Using linepack in this way allows pipeline operators to handle hourly fluctuations in demand very efficiently.

Natural gas pipelines use very sophisticated computer models of customer demand for natural gas, which relate daily and hourly consumption trends with seasonal and environmental factors.

1.6 Storage

A. Above Ground Storage

Natural gas is stored above ground for diverse purposes.

Within a distribution system, the gas may be stored in tanks or in pipe and bottle type holders. Tanks are typically low pressure while pipe and bottle type holders are medium pressure. Gas is stored during low demand times such as at night for delivery during higher demand times such as early morning and evening. These are typically defined as peak shaving facilities

Tanks and pipe and bottle type holders contain a small and definable footprint and are typically located near the city gate meter and distribution station. The volume in these facilities varies throughout the day.

Natural gas is sometimes compressed to very high pressures for use in natural gas fueled vehicles including buses and cars. These storage facilities are typically co-located with the vehicle parking facilities. The gas is received from the pipeline company, compressed to high pressures and stored in vessels. The vehicle is hooked up to the tank and filling commences.
Natural gas can also be liquefied and stored in large vessels. The gas is cooled to a liquid state and stored as LNG. The LNG is gasified and transported via pipeline from the storage location to the customer. LNG facilities may be located in order to receive LNG from ship and sometimes from rail or truck. Other LNG facilities receive gas from pipelines, liquefy the gas for storage, and re-gasify the LNG for pipeline transportation. LNG is stored under low pressure.

Access to the stored material for above ground facilities can be through the valves and piping associated with the tank or vessel. Access to the stored material can also be gained by damaging the piping or vessel.

Modeling of escape of the stored material for tanks and vessels can be accomplished using a variety of programs provided by Federal agencies. Modeling of escape of stored material for pipe and bottle type holders can alternatively be modeled as provided in the Pipeline Safety Regulations using as the variables, diameter and pressure and heat content of the gas.

B. Underground Storage

Natural gas is stored below ground in order to provide seasonal capacity to supplement supply when demand is high. Natural gas is stored under very high pressure.

There are approximately 400 underground storage facilities in the US. These facilities contain approximately 4,400 Billion Cubic Feet (BCF) of base gas and comprise several thousand wells. This gas remains in the formation on a continual basis and is not used over the life of the facility. These facilities also contain approximately 3,200 BCF of gas as storage gas (total at end of October, 2007). The amount of gas in storage varies throughout the year as well as year-to-year.

Natural gas is stored underground in three different types of storage facilities. 86% of the storage is in depleted reservoirs where oil and/or gas were removed during production. 10% of the storage is in aquifers that once contained water. 4% of the storage is in salt caverns where the caverns were created for the sole purpose of storing gas. These storage facilities can be anywhere from several hundred to several thousand feet underground.

Access to the stored material for below ground facilities can only be through perforation of the formation containing the gas. There is no way to access these facilities other than through the wells. The storage cannot be penetrated except by drilling.

On April 9, 2007, the DHS issued the Chemical Facility Anti-Terrorism Standards (CFATS). Congress authorized this interim final rule (IFR) under Section 550 of the DHS Appropriations Act of 2007, directing the Department to identify, assess, and ensure the effective security at high-risk chemical facilities. DHS will require applicable facilities to conduct a security vulnerability assessment (SVA) and then develop and
implement a Site Security Plan (SSP) that meet the Risk Based Performance Standards (RBPS) that the Department identified in the IFR.

On November 20, 2007, the final rule was published in the Federal Register. This publication marked a significant departure from the April 2007 draft Appendix A by revising the list of chemicals of interest (COI) that meet CFR 27. It requires that any facility that possesses (or later comes into possession of) a COI that meet or exceed the corresponding screening threshold quantity (STQ) for any applicable security issue must complete and submit a preliminary screening assessment, referred to as a Top-Screen by January 22, 2008.

In June 2008, DHS completed its review of the Top Screens and other available information and issued preliminary tiering letters to all Top Screen responders. There were a total of approximately 32,000 top screens received by DHS, and approximately 7,000 of these chemical facilities were assigned a preliminarily Tier level of 1 through 4. The approximately 25,000 non-regulated facilities received letters stating they do not “present a high level of security risk” and are not currently subject to CFATS. However, a material modification to even a non-regulated facility may require a new Top Screen submission.

Facilities that were preliminarily tiered are subject to additional review and must complete a Chemical Security Assessment Tool (CSAT) SVA within a specified time period. DHS will use the SVA data to make the final risk-based tier determinations, and provide final tiering letters the responders.

It is still unclear at the time of the publication of these revised Guidelines the final risk-based tiers determinations have not been completed and the exact impact CFATS will have on these facilities is unknown. Consequently, member companies should continue to monitor discussions between our industry trade associations and government agencies on this matter. You can find information on CFATS at http://www.dhs.gov/xprevprot/laws/gc_1166796969417.shtm, and the link for completing the on-line Top Screen analysis for your facilities is www.dhs.gov/xprevprot/programs/gc_1169501486197/shtm. It is suggested you consult with your corporate counsel as you make decisions regarding these filings.

1.7 Gate Stations

When the natural gas in a transmission pipeline reaches a LDC, it normally passes through a "gate station” also know as a “citygate point”. LCDs frequently have gate stations receiving gas at many different locations and from several different pipelines. Gate stations serve three purposes. First, they reduce the pressure in the line from transmission levels (200 to 1,500 psig) to distribution levels, which range from ¼ pound to 200 psig. Then an odorant, the distinctive sour scent associated with natural gas, is added, so that consumers can smell even small quantities of natural gas. Finally, the gate
station measures the flow rate of the gas to determine the amount being received by the LDC.

1.8 Distribution System

From the gate station, natural gas moves into distribution lines or "mains" that range from 2 inches to more than 24 inches in diameter. Within each distribution system, there are sections that operate at different pressures, with regulators controlling the pressure. Some regulators are remotely controlled by the LDC to change pressures in parts of the system to optimize efficiency. Generally speaking, the closer natural gas gets to a customer, the smaller the pipe diameter is and the lower the pressure is. The LDC’s central control center continuously monitors flow rates and pressures at various points in its system. The operators must ensure that the natural gas reaches each customer with sufficient flow rate and pressure to fuel equipment and appliances. They also ensure that the pressures stay below the maximum pressure for each segment of the system. Distribution lines typically operate at pressures far below their design pressure.

As natural gas flows through the system, regulators control the flow from higher to lower pressures. If a regulator senses that the pressure has dropped below a set point it will open accordingly to allow more natural gas to flow. Conversely, when pressure rises above a set point, the regulator will close to adjust. As an added safety feature, relief valves are installed on pipelines to vent natural gas harmlessly, if a line becomes over pressured and the regulators malfunction.

Sophisticated computer programs are used to evaluate the delivery capacity of the network and to ensure that all customers receive adequate supplies of natural gas at or above the minimum pressure level requirements.

Distribution mains are interconnected in multiple grid patterns with strategically located shut-off valves, so the LDC can perform maintenance of its lines with minimum disruption to its customers.

1.9 Natural Gas into the Home

Natural gas runs from the main distribution lines into a home or business in what's called a service line. Today, this line is likely to be a small-diameter plastic line of about an inch or less in diameter, with natural gas flowing at a pressure range of over 60 psig to as low as ¼ psig. When the natural gas passes through a customer's gas meter, it becomes the property of the customer. Once inside the home, natural gas travels to equipment and appliances through piping installed by the homebuilder, and owned by the customer who is responsible for its upkeep.

Most natural gas meters are connected to an inner or outer wall of a home or business. In some instances, however, meters are located next to the point where the service line meets the main distribution line. In this case, the piping from the meter to the structure is
the customer's property, not the natural gas companies. These are called "customer-owned" lines and their maintenance is the responsibility of the customer.

When the natural gas reaches a customer's meter, it passes through another regulator to reduce its pressure to under ¼ psig, if this is necessary. (Some service lines carry natural gas that is already at very low pressure.) This is the normal pressure for natural gas within a household piping system, and is less than the pressure created by a child blowing bubbles through a straw in a glass of milk. When a gas furnace or stove is turned on, the natural gas pressure is slightly higher than the air pressure, so the natural gas flows out of the burner and ignites in its familiar clean blue flame.

2.0 Consequences of a Pipeline Failure

The consequences of a failure of a pipeline system or component can be categorized into one of two categories:

**Escape of Gas from the Pipeline** - Natural gas is considered non-toxic, but can displace oxygen in enclosed areas. It is flammable and will ignite in the correct concentrations in the presence of ignition sources. Natural gas is lighter than air, and if ignited affects a small defined area at the facility.

**Incorrect Delivery of Product** - In general, this is the impaired or non-delivery of product, but in some cases it can be the over-delivery of product.
In June 2006, the U.S. Department of Homeland Security (DHS) announced completion of the National Infrastructure Protection Plan (NIPP) Base Plan, a comprehensive risk management framework that defines critical infrastructure protection (CIP) roles and responsibilities for all levels of government, private industry, and other security partners. The U.S. Department of Energy (DOE) has been designated the Sector-Specific Agency (SSA) for the Energy Sector, and is tasked with coordinating preparation of an Energy Sector-Specific Plan (SSP) that will be an annex to DHS's NIPP.

In its role as Energy SSA, DOE has worked closely with dozens of government and industry security partners to prepare this 2007 Energy SSP. Much of that work was conducted through the Sector Coordinating Councils (SCC) for electricity and for oil and natural gas, as well as through the Energy Government Coordinating Council (GCC). The electricity SCC represents more than 95 percent of the electric industry and the oil and natural gas SCC represents more than 98 percent of its industry. The GCC, co-chaired by DHS and DOE, represents all levels of government—Federal, State, local, and tribal—that are concerned with the Energy Sector.

The Energy Sector has developed a vision statement and six sector security goals that will be used as the framework for developing and implementing effective protective measures.

### Vision Statement

The Energy Sector envisions a robust, resilient energy infrastructure in which continuity of business and services is maintained through secure and reliable information sharing, effective risk management programs, coordinated response capabilities, and trusted relationships between public and private security partners at all levels of industry and government.

### Sector Security Goals

<table>
<thead>
<tr>
<th><strong>Information Sharing and Communication</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Goal 1</strong>: Establish robust situational awareness within the Energy Sector through timely, reliable, and secure information exchange among trusted public and private sector security partners.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Physical and Cyber Security</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Goal 2</strong>: Use sound risk management principles to implement physical and cyber measures that enhance preparedness, security, and resiliency.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Coordination and Planning</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Goal 3</strong>: Conduct comprehensive emergency, disaster, and continuity of business planning, including training and exercises, to enhance reliability and emergency response.</td>
</tr>
</tbody>
</table>

| **Goal 4**: Clearly define critical infrastructure protection roles and responsibilities among all Federal, State, local, and private sector security partners. |

| **Goal 5**: Understand key sector interdependencies and collaborate with other sectors to address them, and incorporate that knowledge in planning and operations. |

<table>
<thead>
<tr>
<th><strong>Public Confidence</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Goal 6</strong>: Strengthen partner and public confidence in the sector’s ability to manage risk and implement effective security, reliability, and recovery efforts.</td>
</tr>
</tbody>
</table>
Each day, thousands of businesses and millions of people rely on the safe, secure, and efficient movement of commodities through the transportation system. Manmade or natural disruptions to this critical system could result in significant harm to the social and economic well-being of the country. The Nation’s pipeline system is a mode of transportation with unique infrastructure security characteristics and requirements.

As required by Executive Order 13416, the Pipeline Modal Annex implements the Transportation Sector Specific Plan (TSSP) and was developed to ensure the security and resiliency of the pipeline sector. The vision of this plan is to ensure that the pipeline sector is secure, resilient, and able to quickly detect physical and cyber intrusion or attack, mitigate the adverse consequences of an incident, and quickly restore pipeline service.

The TSSP and the Pipeline Modal Annex were developed, reviewed, and updated using both the Transportation Sector and the Energy Sector Government Coordinating Council (GCC) and Sector Coordinating Council (SCC) frameworks. In accordance with the National Infrastructure Protection Plan (NIPP), a Critical Infrastructure Partnership Advisory Council (CIPAC) Oil and Natural Gas (ONG) Joint Sector Committee was established to provide a legal framework for members of the Energy Sector GCC and ONG SCC to engage in joint critical infrastructure protection discussions and activities, including those involved with pipeline security. Under this CIPAC committee, a Pipeline Working Group writing team was formed to develop and review applicable Sector-Specific Plans (SSPs), including the Energy SSP and the TSSP. The writing team reviewed and commented on the draft TSSP Base Plan and drafted the Pipeline Modal Annex. The draft plans were distributed to the pipeline industry via the GCC and SCC memberships for another level of review and input before finalizing the documents.

TSA will work with its security partners in both the transportation and energy sectors to update the TSSP and Pipeline Modal Annex regularly, as called for in the NIPP and Executive Order. The updating process is a responsibility shared with pipeline security partners collaboratively through the GCC/SCC/CIPAC framework.

The core of the plan is a pipeline system relative risk assessment and prioritization methodology. This methodology provides a logical prioritization process to systematically list, analyze and sort pipeline systems and critical pipeline components within those pipeline systems. By prioritization, security resources can be effectively used to manage risk mitigation in order to protect critical pipelines from terrorist threats. The methodology is based on the Transportation Sector Systems-Based Risk
Management (SBRM) methodology, which is in turn based on the Risk Management Framework presented in the NIPP.

With a view toward this end-state, the TSSP and this Pipeline Modal Annex specifically focus on how the Transportation Sector will continue to enhance the security of its critical infrastructure and key resources. Programs to protect the Nation’s Pipeline System(s) are key to making the nation safer, more secure, and more resilient in the face of terrorist attacks and other hazards.
APPENDIX 4

Oil and Natural Gas SCC and GCC Membership and Participation

US Department of Energy
US Department of Homeland Security, Transportation Security Administration
US Department of Homeland Security, United States Coast Guard
US Department of the Interior, Minerals Management Service
US Department of State, International Boundary and Water Commission
US Department of Transportation, Committee on the Marine Transportation System
US Department of Transportation, Pipeline and Hazardous Materials Safety Administration
US Department of the Treasury
US Environmental Protection Agency
Federal Energy Regulatory Commission
National Association of Regulatory Utility Commissioners
National Association of State Energy Officials

American Gas Association
Association of Oil Pipe Lines
American Public Gas Association
Canadian Association of Petroleum Producers
Center for Liquefied Natural Gas
Domestic Petroleum Council
Gas Producers Association
International Association of Drilling Contractors
Independent Liquid Terminals Association
Independent Petroleum Producers Association of America
National Association of Convenience Stores
National Ocean Industries Association
National Petrochemical & Refiners Association
National Propane Gas Association
Offshore Marine Service Association
Petroleum Marketers Association of America
Society of Independent Gasoline Marketers of America
US Oil & Gas Association
Western States Petroleum Association

Partnership for Critical Infrastructure Security
Sector Representation

- Banking and Finance
- Chemical
- Commercial Facilities
- Communications
- Dams, Locks and Levees
- Defense Contractors
- Emergency Services
- Energy – Electricity
- Energy – Oil and Natural Gas
- Food and Agriculture
- Healthcare
- Information Technology
- Nuclear Reactors, Materials and Waste
- Postal and Shipping
- Transportation – Public Transport
- Transportation – Rail
- Water
APPENDIX 5

Information Technology Security in the Natural Gas Industry

As outlined in the National Petroleum Study of June 2001 (See Appendix A of that study), the natural gas industry, like most other segments in the energy sector, is relying more and more on e-commerce, commodity trading, business-to-business systems, and enterprise network systems. Further, SSCADA Systems, which operate pipeline systems, distribution systems, and other critical components, are migrating to more open protocol based architectures. These new developments offer new opportunities to the industry, but they also represent serious challenges with regard to critical infrastructure protection.

The industry recognizes the importance of information technology security. The natural gas industry is one of the nation’s critical infrastructures and is crucial to government, business, and personal life. Further, to maintain consumer confidence, the industry must be able to handle financial transactions securely and efficiently and constantly have the ability to protect corporate and customer data.

Elements of a Cyber Security Vulnerability Assessment

As companies assess the elements that could possibly be vulnerable to cyber attack, a risk assessment should be performed which determines the critical information assets and identifies the potential risks. The components of an enterprise-wide information technology solution that should be considered include:

- Network Security (internal and external view)
- Data Security
- Systems Administration (user or system, desktops, servers)
- Data Classification and Disposal
- Detection and Response
- Policies and Procedures
- User Awareness and Compliance
- Information System Dependencies and Interdependencies
- Vendor, Partner, and Supply Chain
- Physical security surrounding cyber components
- Environmental systems in support of cyber components (UPS, HVAC, etc.)
- Disaster Recovery
- SSCADA

Energy company networks have similar characteristics. There are two basic networks – the corporate network and the operational network. The corporate network is characterized by business applications that facilitate corporate communications and have an Internet presence. The operational network is focused on the generation, transmission, and distribution of energy and uses SCADA systems. Security policies, personnel and
procedures exist for each network. Depending upon the size of the system, these networks could potentially be large and increasingly dependent on “open systems.”

With the increasing levels of information sharing between business units, external partners, and customers, there are more access points to corporate information. Also, with the evolution of the structures within the industry (i.e., mergers, new telecom and trading ventures), the scope at which information is shared is increasing.

21 Steps to Improve Cyber Security of SCADA Networks

The President’s Critical Infrastructure Protection Board and the DOE have developed the steps outlined below to help any organization improve the security of its SCADA networks. These steps are not meant to be prescriptive or all-inclusive. However, they do address essential actions to be taken to improve the protection of SCADA networks. The steps are divided into two categories: specific actions to improve implementation, and actions to establish essential underlying management processes and policies.

The following steps focus on specific actions to be taken to increase the security of SCADA networks:

1. Identify all connections to SCADA networks.
2. Disconnect unnecessary connections to the SCADA network.
3. Evaluate and strengthen the security of any remaining connections to the SCADA network.
4. Harden SCADA networks by removing or disabling unnecessary services.
5. Do not rely on propriety protocols to protect the system.
6. Implement the security features provided by device and system vendors.
7. Establish strong controls over any medium that is used as a backdoor into the network.
8. Implement internal and external intrusion detection systems and establish 24-hour-a-day incident monitoring.
10. Conduct physical security surveys and assess all remote sites connected to the SCADA network to evaluate their security.
11. Establish SCADA “Red Teams” to identify and evaluate possible attack scenarios.

The following steps focus on management actions to establish an effective cyber security program:

12. Clearly define cyber security roles, responsibilities, and authorities for managers, system administrators, and users.
13. Document network architecture and identify systems that serve critical functions or contain sensitive information that require additional levels of protection.
14. Establish a rigorous, ongoing risk management process.
16. Clearly identify cyber security requirements.
17. Establish effective configuration processes.
19. Establish system backups and disaster recovery plans.
20. Senior organizational leadership should establish expectations for cyber security performance and hold individuals accountable for their performance.
21. Establish policies and conduct training to minimize the likelihood that organizational personnel will inadvertently disclose sensitive information regarding SCADA system design, operations, or security controls.

Here is a link to the 21 steps report:
www.oe.energy.gov/DocumentsandMedia/21_Steps_-_SCADA.pdf

Control System Security

DHS has developed a Catalog of Control System Security Requirements to help facilitate the development of control systems cyber security industry standards. The author team consisted of representatives from the DOE National Laboratories (Argonne National Laboratory, Idaho National Laboratory, Pacific Northwest National Laboratory, and Sandia National Laboratory) and the National Institute of Standards and Technology. The document provides a catalog of requirements to facilitate the development and implementation of control system cyber security standards to be applied to the CI/KR of the U.S. and other nations.

The catalog presents a compilation of practices that various industry bodies have recommended to increase the security of control systems from both physical and cyber attacks. The recommended set of requirements in this catalog is grouped by 18 families, or categories, that have similar emphasis. The requirements within each family are displayed with a summary statement of the requirement, supplemental guidance or clarification, and a requirement enhancements statement providing augmentation for the requirement under special situations. The catalog is not limited for use by a specific industry sector but can be used by all sectors to develop a framework needed to produce a sound cyber security program. It should be viewed as a collection of requirements to be considered and judiciously employed, as appropriate, when reviewing and developing cyber security standards for control systems. The requirements in the catalog are intended to be broad enough to provide any industry using control systems the flexibility needed to develop sound cyber security standards specific to their individual security requirements.

Here is a link to the Catalog:
Cyber Security Plans

There are a series of excellent cyber security standards that provides a framework for organizations to use in the development of their operational cyber plan.

One of the most widely used security standards today is International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27002 which started in 1995. This standard consists of two basic parts: British Standard (BS) 7799 part 1 and BS 7799 part 2 both of which were created by the BSI. Recently this standard has become ISO 27001. This standard is endorsed by the natural gas industry as a framework and voluntary guidance in protecting the industry against cyber attacks.

The National Institute of Standards and Technology (NIST) has released several special papers addressing cyber security. One of these special papers is relevant to control systems; “Applying NIST SP 800-53 to Industrial Control Systems”. Three of these special papers are very relevant to cyber security: the NIST SP800-12 titled “Computer Security Handbook;” NIST SP800-14 titled “Generally Accepted Principals and Practices for Securing Information Technology;” and the NIST SP800-26 titled “Security Self-Assessment Guide for Information Technology Systems”.

Another good reference document is International Standard Architecture (ISA)-99 which provides standards for manufacturing and control systems security.

Here are some key components that companies should consider as part of their Cyber Security Program:

- Establish guidelines on handling and protecting data.
- Incorporate guidelines into the overall security plan of the organization (which includes physical).
- Educate employees and raise awareness.
- Enhance and enforce authentication (passwords) method.
- Utilize filtering technology at Internet connection points and install software to protect against malicious code executing on systems. Such software systems include virus protection and firewalls intrusion detection systems.
- Monitor the networks by reviewing firewall logs to identify suspicious patterns.
- Monitor emerging threats and regularly upgrade firewalls and cyber security software products.
Consider the replication of mission critical systems and data in multiple sites to ensure the ability to recover from damaging cyber (and physical) attacks.

Perform regular security assessments that possibly include penetration testing, architecture review, and a review of security policies and procedures.

Consider a security audit performed by an independent third party. This includes both audits of policy and attempting to compromise the actual corporate network.

Industry Activities in Cyber Security

As mentioned earlier, the natural gas industry is becoming more reliant on information technology for the operation of its business and has taken steps to strengthen its ability to withstand potential cyber attacks. Companies within the industry use firewalls, intrusion detection systems and other cyber security methods to safeguard their systems. Companies are participating in association and commercial forums to stay abreast of new threats and protection tools. With the increased level of cyber attacks, companies have been closely monitoring virus protection software versions and activity in the corporate firewalls.

In addition to the general cyber security measures mentioned above, specific natural gas industry initiatives currently underway include:

To provide a unified framework for control systems research efforts, DOE has partnered with industry to create a Roadmap to Secure Control Systems in the Energy Sector. This vital document identifies critical challenges and priorities for improving security, reliability, and functionality of energy control systems. The Roadmap will guide technology investments by government and industry and enhance operating practices in the electric, oil, and gas sectors. An Energy Sector Control Systems Working Group (ESCSWG) has been created to provide advice and guidance to help implement the Roadmap. The efforts of the ESCSWG are designed to foster private and public collaboration to improve control system security in the energy sector. The Working Group consists of senior representatives from the electric, oil and gas, and government sectors, as designated by the Energy SCC (Electric and Oil & Natural Gas) and the GCC for Energy. In addition, members may be invited as appropriate from other sectors, such as Communications and Information Technology. The Roadmap can be downloaded at www.controlsystemsroadmap.net.

The gas industry continues to have discreet discussions with the DOE labs about new and on-going initiatives and studies where industry can foster awareness and participation where applicable.
APPENDIX 6

System Criticality Determination

Purpose

Due to a magnified threat situation, industry’s security programs have taken on increased intensity and sophistication at every phase. Industry is focused on:

Public Safety
- Loss of life or injury to the public or to employees.
- Property damage to non-company structures near pipeline facilities.
- Highly visible events that may cause panic such as near public places.
- Sensational events with immediate media exposure.

Public Service
- Disruption in necessary gas service to a large customer base.
- Disruption in necessary gas service to other infrastructure (power plants, manufacturing, etc.).
- Collateral disruption on strategic infrastructure/national security.
- Single line service to necessary end users (hospitals, schools, etc.).
- Significant implications resulting in customer curtailments.

Critical Assets

In order to properly respond to this new threat environment, companies must conduct facility specific assessments oriented to an appraisal of key components of individual facilities on a prioritized basis.

As a general definition, key assets are resources that have sufficient value to the company’s operations to merit some type of protection. These important system components can either be tangible, e.g., compressor stations, control centers and the facilities that house them, or intangible assets such as sensitive information, company executives, etc.

To measure the criticality of any single asset, it is necessary to examine the consequences to the system of a successful attack against that asset. These consequences to the system are analyzed by examining the loss of the asset in terms of:
2. Ease of Replacement.
3. Redundancy of Asset Function.

As a result of this review, facilities are prioritized for risk control measures, including any singled out for exceptional levels of risk control. Companies manage security systems as part of efforts to ensure design effectiveness of those systems is sustained. For exceptions to results requested by appropriately authorized government entities, risk control resource requirements should be addressed jointly with the company in the same manner as exceptions made within company or government programs.

However, even if a critical asset is vulnerable to an attack by a given threat, the asset may still not be an attractive target.

**Threat Analysis**

*The following is provided to educate the operator of the type of information to be aware of for an improved understanding of the threat. Companies should proactively establish and continually reinforce their liaisons with federal, state and local law enforcement. These existing intelligence resources are charged with threat information gathering and analysis. Note that in most cases to obtain any level of detail from such organizations, the operator may need to obtain security clearance. By obtaining from established government or private sources the type of information listed below, the operator can more effectively assess the significance of the threat.*

Unprecedented attacks are becoming less rare. There has been no major terrorist attack on U.S. domestic energy systems. There have been significant and sustained attacks on energy systems elsewhere in the world; but they have usually been conducted during civil conflict or insurgent warfare, such as in Colombia and El Salvador. In order to force operations to be suspended at the Cano-Limon pipeline, Colombian guerrilla groups attacked the pipeline an estimated 170 times in 2001. Attacks on the pipeline continued through 2004, but the number of attacks dropped compared to 2001. In the last few years, routine attacks on pipelines have occurred in war torn Iraq and Chechnya. Closer to the U. S., Mexico’s state owned Petroleos Mexicanos’ natural gas pipeline has been attacked twice in 2007 by a leftist guerrilla group who is claiming responsibility for the attacks.

As was proven with man-made disruptions and natural disasters, an energy system is very resilient and generally requires sustained attacks in order to be successful. It can be assumed that an attack on an energy system would leave signatures, and given U.S. law enforcement’s significant post-blast investigative capabilities, would probably result in the attacker’s arrest. This further decreases the attractiveness of energy targets.

Be that as it may, the fact remains that energy is the basis on which our modern industrialized society rests. Energy assets are easily recognizable given that their design, construction and basic operations are based on almost universally applicable physical
principles. However, foreign-based “crusader” threat groups do not generally view energy targets as having inherent symbolic or iconic value, which is their preferred target type.

The Threat

In general, adversaries or threats can be grouped into three general categories:

The series of terrorist incidents in the United States beginning in 1993 and continuing today indicates a new model of terrorism is emerging: a loose aggregation of like-minded individuals sharing a common religion, the same contacts, and a collective extreme political and religious vision of the world. We are now facing crusaders - professional terrorist groups motivated by a religious imperative and bound by a common vision of militant Islam.

Attack Planning

There are an impressive number of specific targets in the United States from which a terrorist group may choose. Once a target has been selected, terrorists will most likely follow certain attack planning and attack principles that allow their efforts to be more efficient and ensure a greater margin of success. A professional adversary is likely to consider the following:

1. Criticality - Importance of the target to the operating system.
2. Accessibility - Ease of reaching the target.
3. Restoration & Recovery - Ability of the company to repair or by-pass damage from both a time and spare part point of view.
4. Vulnerability - Whether or not the target is susceptible to the means and the resources that the adversary possesses.
5. Effects - If attack will achieve the effects desired by the adversary group in political, psychological, social and economic terms.
6. Recognition - If the key asset can be easily identified.

Terrorists will also try and determine if the asset is vulnerable to the means of attack at the disposal of the threat group. The two areas to be reviewed are:

1. Characteristics of the asset, i.e., the environment and geographic location.
2. Characteristics of the security system, with an emphasis on the physical security elements.

Target Attractiveness

One of the most important pieces of evidence is the historical data on whether any given threat group has attacked this type of key asset in the past, and if so, how often. In most cases this is a strong indication if the threat continues to view attacks on this type of target as an effective method of achieving his goals.
Historical information must be combined with a current goal analysis in order to decide how attractive a key asset is in terms of accomplishing current goals. Many groups typically have overlapping goals. Threat goals and their relationship to a given key asset should be analyzed in terms of these potential threat objectives:

- **Causes Injury and Death of Personnel** - Often a goal of terrorist groups seeking the most effective way to create terror, but can also be the goal of criminals, disgruntled employees or disoriented persons.

- **Enrichment** - The primary goal of the criminal, but also a favorite objective of the disgruntled employee who rationalizes that the money he gains evens the score.

- **Social and Economic Disruption of the Area** - A prime terrorist goal, and one in which the criticality of the asset would be important to determine attractiveness to the terrorists. Disgruntled employees and disoriented persons may also have an interest in this goal.

- **Publicity and Political Statement** - Although often a terrorist goal, it is also almost always an objective sought by extremist protest groups.

- **Increase Public Support for Threat** - Almost exclusively a goal of extremist protest groups.

- **Destroy Public Confidence and Feeling of Safety** - This objective is generally found only with the terrorist groups.

- **Embarrass the Company** - This objective is associated not only with extremist protest groups, but also with disgruntled employees.

- **Force the Company to Change Its Policies** - A typical goal of extremist protest groups.

- **Vengeance** - An objective generally found only with disgruntled employees and disoriented persons.
APPENDIX 7

Pipeline Components

The determination in the approach described in the report is made for each pipeline component. The pipeline components are listed and described below with the description expanded to show the redundancies built into the grid.

Components:
- Large diameter pipelines
- Main-line block valves, launchers and receivers
- Large meter and regulator stations (City gate deliveries)
- Main-line compressor station
- Communication facilities (Phones, microwave, radio, voice/data)
- Gas pipeline flow control facility
- SCADA system
- Offshore platform
- LNG terminals and land-based facilities
- Reservoir or cavern storage wells
- Customer call, dispatching and Emergency Response Centers
- Other operator specific facilities

Description of Components

- Large diameter pipelines - The pipeline is a network of pipe of various sizes and operating at various pressures. This is the backbone of the transmission system. The nature of the pipeline grid is one where there is considerable redundancy. Redundancy is inherent in the multiplicity of pipes running parallel in the right-of-way as well as the many right-of-ways managed by different companies.

- Main-line Block Valves, Launchers and Receivers - Block valves are located along the pipeline backbone and spaced at least every 20 miles. These valves are used to isolate sections of pipe. Inherent in the design of a block valve setting is crossovers and blow-downs. Crossovers allow gas to cross from one pipe to another. Crossovers are located at block valve locations. Blow-downs provide for the planned evacuation of the gas from the pipe. Ability to move within the redundant pipelines is beneficial to managing outages.

- Large meter and regulator stations (City gate deliveries) - The transfer between transmission and distribution usually takes place at the city gate. Depending on the size of the community, many city gate stations are in service. These stations are located around the distribution grid. Many of the city gate stations can receive gas from different transmission pipelines.
Ability to keep gas flowing to the customer during outages is typically designed into the facilities.

- **Main-line compressor stations** - Stations usually contain several compressors located in groups and often in separate buildings. The nature of the stations is such that the outage of several units or a group of units will not significantly affect gas transportation. The design of the pipeline network was also done in such a manner that the outage of one or more compressor stations would not significantly affect transportation. The station can be bypassed and blown-down,

- **Communication facilities (Phones, microwave, radio, voice/data)** - Companies utilize many communication capabilities. Cell phones and satellite phones, hard wire lines and the company’s own microwave allow transmission of voice. Fiber optics, traditional wire, satellite and microwave allow transmission of data. SCADA systems are designed to work without communication if necessary. Also most facilities can be operated manually when necessary. Communication provides efficiency but operation is not dependent on it for pipeline systems.

- **Natural gas pipeline flow control facilities** - These facilities manage the transportation of gas. These facilities have been designed with backup systems either centrally located backup or distributive backup. The outage of gas control has always been planned for in pipeline operations.

- **SCADA systems** - See Communication facilities (above).

- **Offshore platforms** - These facilities, manned and unmanned, are the juncture of offshore gathering to offshore transmission from the platform to the onshore line pipelines. These facilities are remote, difficult to access and patrolled by the coast guard. Loss of one or more of these facilities would not hamper the transportation of gas to customers.

- **LNG terminals and land-based facilities** - By design, these are peak shaving facilities and as such utilized rarely. Security of these systems is mandated by DOT in the LNG regulations and NFPA 59A.

- **Reservoir and cavern storage wells** - Most storage systems have a multiplicity of wells for injection and withdrawal of gas from storage. Loss of one or more wells in a field would not impact gas transportation. Additionally there are many fields; the loss of any one would have minimal affect on transportation. Again this is a redundant system.

- **Customer call, dispatching and Emergency Response Centers** – These facilities manage calls from customers and non-customers related to gas leaks and other suspected gas distribution-related incidences.
APPENDIX 8

Pipeline Security Detection and Deterrent Methods Requiring Capital Additions for Critical Facilities

Large diameter pipelines
- Perimeter fence with secured gates or controlled access
- Signage

Main-line block valve, launcher and receiver
- Perimeter fence with secured gates or controlled access or tamper proof
- Signage

Large meter and regulator stations (City gate deliveries)
- Perimeter fence with secured gates or controlled access or tamper proof
- Secured buildings
- Security lightning
- Signage
- SCADA

Main-line compressor stations
- Perimeter fence with secured gates
- Secured buildings
- Security lightning
- Signage
- SCADA
- Voice communication capability
- Camera surveillance capability

Communication facilities (Phone, microwave, radio, voice/data)
- Perimeter fence with secured gates
- Secured buildings
- Security lighting
- Signage

Gas pipeline flow control facility
- Secured buildings
- Back-up capability

**SCADA systems – Covered in Appendix 5**

**Offshore platforms**
- Follow Coast Guard requirements
- Maritime Transportation Security Act

**LNG terminal and land-based facilities**
- [NFPA 59A](https://www.nfpa.org)

**Reservoir and cavern storage wells**
- Covered in state drilling and completion requirements
- Perimeter fence with secured gates or controlled access or tamper proof

**Customer call and Emergency Response Centers**
- Secured buildings
- Back-up capability

**Other Operator specific facilities**
- Specific to operator

**Notes:**

**PIPELINE SAFETY REQUIREMENTS:**
The current pipeline safety regulations (49 CFR Parts 192 and 193) presently contain many security requirements. Pipelines are buried which prevents access. Many safety and backup devices are required such as valves, regulators, and overpressure protection. Above ground pipelines are designed with more conservative safety margins providing additional protection from external damage. Patrolling, surveillance, testing and inspections are required ensuring the work force is constantly monitoring the facilities.

**PERIMETER FENCE WITH SECURED GATES:**
The intent of this requirement is to provide for the deterrence of unauthorized entry into the facility area. The specifications for fencing and gates are to be determined by the operator.

**SECURED BUILDINGS:**
The intent of this requirement is to provide buildings containing equipment and controls
to be secured for the deterrence of unauthorized entry into the buildings. The
specifications for securing buildings are to be determined by the operator.

SECURITY LIGHTING:
The intent of this requirement is to provide lighting of the station buildings and the area
near the buildings for deterrence of unauthorized entry. The specifications for security
lighting are to be determined by the operator.

SIGNAGE:
The intent of this requirement is to provide signage for the deterrence of unauthorized
entry. The specifications for signage are to be determined by the operator.

SCADA:
SCADA (Supervisory Control and Data Acquisition) provides for collecting operating
parameters as well as controlling certain equipment functions. All monitored conditions
are provided to central control and may provide detection of unintended actions.

VOICE COMMUNICATION CAPABILITY:
The intent of this requirement is to insure that personnel have communication equipment
available in order to report security conditions.

CONTROLLED ACCESS:
The intent of this requirement is to provide alternatives to fencing and gates around
facilities. Controlled access would be provided through a means equal to the level of
protection as afforded by fencing and gates.

TAMPER PROOF:
The intent of this requirement is to provide alternatives to fencing and gates around
facilities. The ability to affect security would be diminished through the tamper proofing
of the facilities through a means equal to the level of protection as afforded by fencing
and gates.

BACK-UP CAPABILITY:
The intent of this requirement is to provide the ability to remotely operate the functions
of the facilities. This control would be through either a backup centralized or
decentralized operation.

49 CFR PART 193 REQUIREMENTS:
Security requirements for LNG facilities are specified in 49 CFR Part 193, Subpart J -
Security.

NFPA 59A
Security requirements for LNG facilities are specified in NFPA 59A (National Fire
Protection Association)
STATE REQUIREMENTS:
States presently have requirements relating to the drilling and completion of storage wells. These requirements significantly reduce the risk of storage gas getting into drinking water sands or shallow coal seams.

COAST GUARD REQUIREMENTS:
The Coast Guard presently has requirements for protection of platforms.
Note: This Appendix will be updated in late 2008 to include a Circular that is being developed by TSA Pipeline Security Division that will supersede the DOT Circular below.

DOT Pipeline Security Information Circular and Pipeline Security Contingency Planning Guidance

FOR OFFICIAL USE ONLY: PUBLIC AVAILABILITY TO BE DETERMINED UNDER 5 USC 552.

PIPELINE SECURITY INFORMATION CIRCULAR

Information of Concern to Pipeline Security Personnel

Security Guidance for Natural Gas, and Hazardous Liquid Pipelines and Liquefied Natural Gas Facilities

Subject: PIPELINE SECURITY GUIDANCE

Issued: September 5, 2002

Summary:

Pipelines represent an important part of the nation’s critical infrastructure. Therefore, it is incumbent upon pipeline operators to take appropriate steps to protect critical pipeline facilities. The Research and Special Programs Administration’s Office of Pipeline Safety (RSPA/OPS) developed the attached guidance document in cooperation with energy and pipeline trade associations and state pipeline safety programs. This circular and the attached document define critical pipeline facilities, identify appropriate countermeasures for protecting them, and explain how RSPA/OPS plans to verify that operators have taken appropriate action to implement satisfactory security procedures and plans.

These guidelines represent the next step on a continuum of efforts by industry and the federal government to improve the security of the nation’s pipelines. The Transportation Security Administration (TSA) is responsible for ensuring the security of the transportation infrastructure and for fostering equivalent levels of protection across all modes of transportation. Because pipelines are an integral part of the nation’s energy and transportation infrastructures,
RSPA/OPS, the Department of Energy, and TSA are working together to achieve these goals. Pipeline operators rely on RSPA/OPS as their primary source of information for matters related to pipeline safety, including security issues, based on close working relationships forged over many years of daily interaction. While these guidelines may be revised as additional information becomes available, changes will be made only after appropriate consultation with industry. TSA will work with RSPA/OPS to avoid inconsistencies in guidance or unnecessary changes.

An operator’s security procedures may be included with a plan for operations, maintenance, and emergency response or in a separate document. OPS does not expect an operator to create redundant plans. We do suggest a cross reference to existing plans. RSPA/OPS and our State pipeline safety partners will not require operators to submit copies of their corporate security plans. Instead, RSPA/OPS and states will review the plans on site at the operator’s offices, and conduct spot checks of selected critical facilities in the field to verify that the operator is implementing its plan as written. RSPA/OPS understands that corporate security plans will likely be limited in their distribution and that field personnel may not be aware of all the details of their employer’s security plan. However, when spot-checking facilities that the operator has identified as critical, RSPA/OPS intends to verify the extent to which the operator has implemented the protective measures and security training described in their security plan.

The purpose of this information circular is to encourage operators to identify their critical facilities and to begin to implement appropriate measures for such facilities. RSPA/OPS does not imply that operators must implement every measure identified for each of the various threat levels. Because pipeline facilities may be attractive terrorist targets, operators need to make a good faith effort to implement security measures to protect the safety of the public and their critical facilities, and to ensure reliability of the nation’s energy supply both for national defense and to sustain the economy. For facilities that do not meet the threshold for being designated critical, operators may still want to implement some security measures.

**Recommendations:**

In the current threat environment, all natural gas and hazardous liquid pipeline and liquefied natural gas facility operators should continue and strengthen their security efforts. The following measures or their equivalents are basic:

1. Identify any of its facilities that could be defined as “critical facilities.” If an operator considers none of its facilities to be critical, document the basis for the conclusion. The operator should maintain a list of facilities that are identified as critical in a secure place at corporate headquarters. This list should be available to RSPA/OPS and State representatives for on-site verification. RSPA/OPS does not intend to require operators to distribute this list outside the corporation.

2. Develop a corporate security plan that is consistent with the security guidance published by the trade association for the operator’s segment of the pipeline industry.
3. Begin to implement their corporate security plan as soon as possible.

4. Review their corporate security plan on an annual basis and revise it as necessary to reflect changing conditions.

Submission of Operator’s Statement:

RSPA/OPS requests that within six months of the date of this circular, each operator should submit a written statement to confirm that the operator has:

- Reviewed this information circular and the accompanying Pipeline Security Contingency Planning Guidance;
- Reviewed the consensus security guidance appropriate to its portion of the pipeline industry;
- Identified its critical facilities;
- Developed a corporate security plan; and
- Begun implementing its corporate security plan as necessary to protect the physical and cyber security of its critical facilities.

For operators under the authority of RSPA/OPS, the statement should be submitted to the Associate Administrator for RSPA/OPS. For intrastate operators, the statement should be submitted to the State pipeline safety regulatory agency. Operators’ written statements are needed to confirm that operators are making progress and fully understand what is expected of them, and to enable RSPA/OPS to measure the effectiveness of the current non-regulatory approach to pipeline security.

The statement may be sent to:
Associate Administrator for Pipeline Safety
Room 7128
Research and Special Programs Administration
U.S. Department of Transportation
400 Seventh Street, S.W.
Washington, DC 20590

Alternatively, it may be e-mailed to: pipeline.security@rspa.dot.gov

RSPA/OPS Follow-Up Actions:

RSPA/OPS intends to verify operators’ measures to secure their critical pipeline facilities, beginning with operators of the pipelines that present significant risks to people and are most important to the integrity of the national energy infrastructure. RSPA/OPS will not ask operators to submit copies of their corporate security plans. Instead, RSPA/OPS and states will verify the plans on-site, and conduct checks in the field to determine whether each operator is implementing its plan as written and whether the plan is consistent with the security guidance published by the trade association for that operator’s segment of the pipeline industry (see
If the verification audit identifies security deficiencies, RSPA/OPS will work with the operator to correct them. RSPA/OPS will not maintain documentation about the contents of an operator’s security program except to identify general deficiencies requiring correction. This documentation will not compromise the identity of critical facilities or the integrity of the security plan.

To assist RSPA/OPS in performing an on site security review, we request that an operator be prepared to discuss the following:

a. A list of an operator’s critical facilities;

b. The steps which an operator would take to decrease the attractiveness of each critical facility as a target;

c. Procedures explaining how an operator would work with federal, state, and local agencies to respond to attacks on its critical facilities;

d. An operator’s process for conducting vulnerability assessments (if needed) of its critical facilities;

e. Cyber security methods for protecting its computer systems that are essential for the safe operation of the pipeline;

f. Procedures for training employees, including contractors, to respond appropriately during a security incident;

g. Procedures explaining how an operator would receive threat notification (physical attack, cyber attack, etc) and how it would disseminate this information to its employees, contractors, FBI, RSPA/OPS or other appropriate public officials;

h. A process for controlling access to its facilities for both individuals and vehicles; (e.g. badging, visitor screening, vehicle searches);

i. Coordination with existing response plans, as necessary;

j. How an operator would expedite restoration of service with minimal disruption (e.g. establishing a spare parts inventory, procedures for rerouting product to other lines);

k. How the security plan conforms to the guidance developed by pipeline industry trade associations;

l. Procedures, if any, for conducting background checks on employees and/or contractors.

**Industry Consensus Security Guidance:**

In addition to the Pipeline Security Information Circular and Pipeline Security Contingency Planning Guidance, RSPA will use the following documents, which have been developed in concert with major industry groups, when evaluating operators’ security plans. Hazardous liquid pipelines will be evaluated according to the American Petroleum Institute’s “Guidelines for Developing and Implementing Security Plans for Petroleum Pipelines.” Natural gas transmission and distribution pipelines, including liquefied natural gas facilities, will be evaluated according to the “Security Guidelines: Natural Gas Industry, Transmission and Distribution,” developed by the American Gas Association and the Interstate Natural Gas Association of America. For
operators that do not belong to a trade association, RSPA/OPS will provide the appropriate
industry consensus security guidance documents to them upon request.

**Protection of Operators’ Security-Related Information:**

RSPA/OPS recognizes that operators have concerns about our ability to protect operator
security related information from disclosure. RSPA/OPS will withhold any security related
information in our possession if it is sought under FOIA, as long as it is either: (1)
commercial information that if released would likely cause an operator substantial
competitive harm; or (2) related directly to the security of an operator’s pipeline facilities.

**Communicating Pipeline Security Information to Operators:**

RSPA/OPS, the Department of Energy, and the FBI have systems in place to distribute
security-related information to industry. Also, RSPA/OPS has established a recorded
announcement at (202) 366-4532 that pipeline operators can call to check the latest threat
condition for pipelines. At the time of publication of this notice, the nation is at the yellow
alert level, as defined by the Office of Homeland Security. Any change in the nation’s
security posture will be reflected in the recorded announcement at that phone number.

If there is a change in the nation’s security posture, RSPA/OPS expects operators to use
good judgment in deciding what, if any, change in security measures are appropriate for
their critical facilities.

The Office of Homeland Security has proposed a tiered system that corresponds to five
threat levels:
- Low = green
- Guarded = blue
- Elevated = yellow
- High = orange
- Severe = red.

For each threat condition, there are suggested protective measures that correspond to that
threat level.

**Dissemination of Guidance and Updating of Operator Contact Information:**

RSPA/OPS is distributing the attached guidance document to pipeline operators, pipeline
industry trade associations, regulatory and public safety agencies, and others with a
demonstrated need to know. This document is not being made available to the general
public because of its security-sensitive nature.

To update our distribution list for urgent security related information, RSPA/OPS asks that
each operator e-mail the following information to: pipeline.security@rspa.dot.gov or mail
this information to RSPA/OPS at the address provided above. RSPA/OPS is requesting 24-
hour contact information for each operator’s Chief Executive Officer, Chief Operating
Officer and the person responsible for pipeline security. For each of these, we are
requesting office, phone, and fax numbers, e-mail addresses, and, if applicable, cell phone and pager numbers. Alternatively, an operator with a 24-hour operations center may prefer to make that the recipient of urgent security-related information. In such cases, RSPA/OPS requests contact information for the operator’s 24-hour operations center.

**PIPELINE SECURITY CONTINGENCY PLANNING GUIDANCE**

This pipeline security contingency planning guidance was developed by the U.S. Department of Transportation’s Office of Intelligence & Security, the Research and Special Programs Administration’s Office of Pipeline Safety (OPS), the Department of Energy, State pipeline safety agencies, and pipeline industry representatives. It is intended to ensure that pipeline owners and operators are able to discourage attacks and respond quickly and effectively if attacks occur.

In general, pipelines are robust and redundant systems. Most sections of pipeline systems are underground and less vulnerable to attack than aboveground facilities. Most damage to line pipes is relatively easy to repair in a few days. Major disruptions in energy supplies can be avoided by using interconnections between pipelines to move product around the site of a terrorist attack. Therefore, the industry’s security efforts should focus on the portions of pipeline system that are most critical to public safety and reliability of service, including systems for which interconnections may be very limited.

There is broad agreement between government and industry on how to address security. Consensus guidance on industry security practices recommends that each pipeline operator follow three steps: (1) assess the terrorist threats to its system; (2) assess the vulnerabilities of its system to these threats; and (3) develop and implement security, response, and recovery plans that address terrorism. Federal and State governments should work with operators to verify that adequate plans are in place and to test the effectiveness of their plans through exercises.

This document establishes guidelines for protective measures under specified threat conditions to help pipeline operators prepare and implement effective security. The protective measures listed in this document are intended to be applied only to critical facilities, although several of the countermeasures require company-wide actions. It is expected that operators will use good judgment in incorporating these measures into their security plans, recognizing that not all countermeasures are appropriate for all types of facilities. Unmanned facilities or small, distribution facilities, for example, may require countermeasures different from those required for manned facilities.

The extent to which a facility is critical depends on three main factors: (1) whether it is a viable terrorist target; (2) how important the facility is to the Nation’s energy infrastructure; and (3) how likely the facility is to be used as a weapon to harm people. In addition, individual operators can deviate from the protective measures listed below by performing and documenting a vulnerability assessment for a facility to estimate the attractiveness of the facility as a terrorist target in accordance with factors other than those just listed. In such cases, the operator would implement protective measures that are appropriate to the
facility’s specific vulnerabilities and commensurate with its attractiveness as a terrorist target.

Determining whether a specific pipeline facility is a critical facility may require the operator to do some research. To the extent permitted under anti-trust laws, pipeline operators should seek out information from the following sources:

- Other operators in a shared right of way;
- Other utilities in the area of the pipeline operator’s critical facilities (whose facilities may also be critical); and
- Specific customers (e.g. a military base).

Operators may be hampered in making determinations about specific critical facilities by the willingness of the other party to share information.

For purposes of security planning, a facility is a critical facility if it meets one or more of the following criteria:

1. A pipeline facility or combination of facilities that may be considered a viable terrorist target and (a) intelligence information indicates that the facility, or facilities like it, is being targeted for attack or (b) a release from the facility has the potential for mass casualties or significant impact on public drinking water affecting a major population center;

2. A facility or a combination of facilities that, if damaged or destroyed, would have a detrimental impact on the reliability or operability of the pipeline system, significantly impairing the operator’s ability to serve a large number of customers for an extended period;

3. A facility or combination of facilities that, if damaged or destroyed, would significantly impair the operator’s ability to serve installations critical to National defense;

4. A facility or combination of facilities that, if damaged or destroyed, would so impair other modes of transportation or other critical infrastructures (such as electric power generation, telecommunications or public utility) that it would cause major economic disruption.

Operators of critical facilities, as defined above, will need to be aware of the current threat conditions, which mirror the Homeland Security Advisory System (HSAS). Under the HSAS, there are five levels of threat conditions, each identified by a description and corresponding color. From lowest to highest, the levels and colors are:

- Low = Green
- Guarded = Blue
- Elevated = Yellow
The higher the threat condition, the greater the risks of a terrorist attack. Risk includes both the probability of an attack occurring and its potential gravity. Threat conditions may be assigned for the entire Nation, or they may be set for a particular geographic area or industrial sector.

The following threat conditions and protective measures are cumulative. Each successive level assumes that a facility is already implementing the protective measures associated with the preceding threat conditions, as appropriate. The threat conditions and the protective measures associated with each level represent an increasing risk of terrorist attacks. The levels are as follows:

**Low Condition (Green).** This condition is declared when there is a low risk of terrorist attack. The following measures under Low Condition (Green) should be maintained indefinitely:

**Measure 1.** All operators should verify the identity of all employees and visitors and control access to critical facilities at all times. Visitors should not be allowed access to critical facilities unless the operator is satisfied as to their identity and the visitor has a legitimate business purpose for their visit. The operator should be aware of any contractors working on a critical facility. Operators should use company-issued photo ID’s or government-issued photo ID’s.

**Measure 2.** Ensure that existing security measures such as fencing, locks, camera surveillance, intruder alarms, and lighting are in place and functioning. Identify additional security measures and resources that can enhance the security of critical facilities at the higher threat condition levels (e.g., increased surveillance).

**Measure 3.** Survey surrounding areas to determine how threats to neighboring facilities (e.g., airports, government buildings, industrial facilities, and other pipelines) could affect the facility.

**Measure 4.** Develop and implement hardware, software, and communications security for computer-based operational systems.

**Measure 5.** Establish local, regional, and system wide threat and warning dissemination processes, emergency communications capability, and contact information with law enforcement, including local FBI field offices, first responders, and State and regional pipeline safety representatives. Emergency communications should have redundancy for both hardware and means to contact law enforcement agencies.

**Measure 6.** Develop terrorism and security awareness and educate employees on security standards and procedures.
Measure 7. Advise all personnel at each facility to report the presence of unknown personnel, unidentified vehicles, vehicles in an unusual manner, abandoned parcels or packages, and other suspicious activities. Be alert to vehicles parked for an unusual length of time in or near a facility.

Measure 8. Provide security awareness information to land owners along the pipeline right of way (ROW) and to emergency response organizations.

Measure 9. Develop procedures for shutting down and evacuating the facility. Facilities located near critical community assets should be especially vigilant.

Measure 10. Ensure contingency and business continuity plans are current and include a response to terrorist threats.

**Guarded Condition (Blue).** This condition is declared when there is a general risk of terrorist attacks. In addition to the measures listed previously, the following measures should be implemented:

Measure 11. Continue all Low condition measures or introduce those that have not already been implemented.

Measure 12. Ensure that a company response can be mobilized and review facility emergency and security plans and procedures. Test security and emergency communication procedures and protocols.

Measure 13. Inspect perimeter fencing and repair all fence breakdowns. In addition, review all outstanding maintenance and capital project work that could affect the security of facilities.

Measure 14. Review all operations plans, personnel assignments, and logistical requirements that pertain to implementing higher threat conditions.

**Elevated Condition (Yellow).** An Elevated Condition is declared when there is a significant risk of terrorist attacks. In addition to the measures listed previously, the following measures should be implemented:

Measure 15. Continue all Low Condition and Guarded Condition measures or introduce those that have not already been implemented.

Measure 16. Close and lock gates and barriers except those needed for immediate entry and egress at critical facilities. Inspect perimeter fences regularly. Ensure that other security systems are functioning and available for use.
Measure 17. Limit visitation and confirm that every visitor is expected and has a need to be at a critical facility. All unknown visitors should be escorted while in the facility.

Measure 18. Secure all buildings and storage areas not in regular use. Increase frequency of inspections and patrols within the facility, including the interior of buildings and along the facility perimeter.

Measure 19. Check critical unmanned sites and remote valve sites more frequently than usual for signs of unauthorized entry, suspicious packages, or unusual activities. Increase ROW surveillance in critical areas.

Measure 20. Inspect on a more frequent than usual basis the interior and exterior of all buildings, the area around all aboveground storage tanks, and other vulnerable areas in critical facilities.

Measure 21. Direct that all personal, company, and contractor vehicles at critical facility sites be secured.

Measure 22. Do not open suspicious packages. Inspect all mail and packages coming into a facility. Review the USPS Publication 166 “Mail Center Security Guidelines” with all personnel involved in receiving mail and packages.

Measure 23. Ensure that a company response can be mobilized as appropriate for the increased security level. Review communications procedures and backup plans with all concerned.

Measure 24. Check to ensure that all telephone, radio, and satellite communication systems are in place and operational.

Measure 25. Increase the frequency of warnings required by lower threat conditions and inform personnel of additional threat information as available. Implement procedures to provide periodic updates on security measures being implemented.

Measure 26. As appropriate, review with facility employees the operations plans, personnel safety, security details, and logistical requirements that pertain to implementing increased security levels.

Measure 27. Confirm the availability of security resources that can assist with round-the-clock coverage of critical facilities.

High Condition (Orange). A High Condition is declared when there is a high risk of terrorist attack. In addition to the measures listed previously, the following measures should be implemented:
Measure 28. Continue all Low, Guarded, and Elevated Condition measures or introduce those that have not already been implemented.

Measure 29. Reduce the number of access points for vehicles and personnel to minimum levels at critical facilities and randomly spot-check the contents of vehicles at the access points.

Measure 30. Limit access to critical facilities to personnel who have a legitimate and verifiable need to enter the facility. Require positive identification of all personnel entering the facility; no exceptions.

Measure 31. Assign personnel at critical facilities to assist with security duties by monitoring personnel entering the facility, checking vehicles entering the facility, patrolling the area regularly, and reporting to facility management as issues surface.

Measure 32. Consult local authorities about control of public roads and access points that might make the facility more vulnerable to terrorist attack if they were to remain open.

Measure 33. Erect barriers to control direction of traffic flow and protect the affected facility from an attack by a parked or moving vehicle or company vehicles may be used for this purpose. Implement centralized parking and shuttle bus service where feasible.

Measure 34. Move automobiles and other non-stationary items at least 30 yards from critical facilities, particularly buildings and sensitive areas, unless doing so would create a safety hazard or impede other security measures in place at the facility. Identify areas where explosive devices could be hidden.

Measure 35. Resurvey the surrounding area to determine if activities near a critical facility (e.g., airports, government buildings, industrial facilities, railroads, other pipelines) could create hazards that could affect the facility.

Measure 36. Secure critical facilities round-the-clock using either contract or company personnel; ensure that all security personnel have been briefed on policies governing the use of force and pursuit (as appropriate).

Measure 37. Advise local police agencies that the alert level is at a High Condition (Orange) and advise them of the security measures being employed. Request police agencies to increase the frequency of their patrols of the facility.

Measure 38. Review all outstanding maintenance and capital project work that could affect the security of facilities.
Measure 39. Cancel or delay all non-vital facility work conducted by contractors, or have company personnel continuously monitor the contractors’ work.

Measure 40. Schedule more frequent visits to remote valve sites and other locations that could be affected.

Measure 41. Instruct employees working alone at remote locations or on the ROW to check in periodically.

Measure 42. Check all security systems such as lighting and intruder alarms to ensure that they are functioning. Modify lighting levels, as appropriate, to address changing security needs.

Measure 43. Implement frequent inspection of critical facilities including the exterior and roof of all buildings and parking areas. Increase patrolling at night and ensure that all vulnerable critical points are fully illuminated and secure.

Measure 44. Caution employees not to talk with outsiders concerning their facility or its operations.

Severe Condition (Red). A Severe Condition reflects a severe risk of terrorist attacks. Under most circumstances, the protective measures for a Severe Condition are not intended to be sustained for substantial periods of time. This condition represents the highest threat condition and, in all cases, this condition will require rapid response by Federal, State, and local agencies and departments. In addition to the measures listed previously, the following measures should be implemented:

Measure 45. Continue all Low, Guarded, Elevated, and High Condition measures or introduce those that have not already been implemented.

Measure 46. Activate emergency response plans for the critical facilities.

Measure 47. Reduce facility access points to the absolute minimum necessary for continued operation.

Measure 48. Augment security forces to ensure control of the facility and access to the facility and other potential target areas. Establish surveillance points and reporting criteria and procedures.

Measure 49. Inspect all vehicles entering critical facilities including the cargo areas, undercarriage, glove compartments, and other areas where dangerous items could be concealed.
Measure 50. Identify the owners of all vehicles at critical facilities and remove all vehicles whose owners have not been identified.

Measure 51. Increase security patrol activity at critical facilities to the maximum level sustainable. Increase perimeter patrols and inspections of facility.

Measure 52. Increase the frequency of call-ins from remote locations. Employees should not work alone in such areas.

Measure 53. Shut down affected facilities and operations in accordance with contingency plans unless there is a compelling reason not to, and evaluate the situation before resuming operations.

Measure 54. Request assistance from the local police agencies in securing the facility and access. Cooperate with local police or other authorities if they direct security measures.

Measure 55. Evacuate all nonessential personnel.

Measure 56. Implement business contingency and continuity plans as appropriate.
The U.S. natural gas pipeline industry has a long and admirable record of providing safe and highly dependable supplies of gas to customers. A key element in that dependable service is the maintenance of spare parts and equipment that allow rapid response to emergency situations and quick restoration of service in times of outages. A high-level summary of the current typical company practices follows below.

**Inventory**

- Inventory of emergency and critical spare parts are stored in centralized warehouse locations and physical locations such as compressor stations.
  - Materials in inventory include long lead-time items such as parts for engines and compressor station auxiliary systems, and pre-tested pipe, valves and high yield fittings.

- Inventory level is based upon usage requirements, and the need to maintain operational reliability with minimal interruption or downtime at the facilities they support.

- Inventory replenishment reports are generated on a routine basis and reviewed with the appropriate operations personnel prior to parts being reordered.

**Alliance and Supplier Partner Arrangements**

- Alliance agreements exist with several OEM vendors and material supply vendors to utilize their inventory for short lead-time items and for major construction materials.
  - Construction materials include pre-tested large diameter pipe, large valves, fittings, meter tubes, control valves, etc.

- Arrangements include delivery time commitments and in some cases, vendors reserving inventory.

**Other Resources and Arrangements**

- RUPE (Responding to Underwater Pipeline Emergencies) - Consortium of companies stock long lead-time items such as repair clamps and other fittings needed for offshore pipeline maintenance.
• Maintenance arrangements with turbine suppliers to provide replacement engines on a timely basis, as well as temporary horsepower for emergency use.

• Relationships exist with other companies to assist each other in times of an emergency and to replace items used with one of like kind. Equipment lists are available to determine similar equipment and contact personnel in other companies.

• Internal analysis exists for the possibility of temporarily removing an item from another site with like equipment, in a less critical location. This allows a company to maintain service until a suitable replacement is secured.

Critical Spare Parts

Foremost, it is necessary to make the distinction between a “critical facility” and a “critical part.” Since a “critical facility” can be defined as having substantial implications to the national infrastructure, critical parts would be parts located at those facilities. The natural gas industry has experience with large-scale outages caused by natural disasters, third-party incidents and vandalism. This experience has enabled the industry to reasonably determine that if a terrorist attack were to occur, the attack most likely would not cause mass destruction to the entire “critical facility.” However, the attack could impact specific critical parts imperative for the operations of a facility.

Critical parts of the facility types listed above could consist of the following:

• Pipeline - no critical parts due to redundancy of parallel pipelines and underground location.

• Block valves - no critical parts due to crossovers, blow-downs and ability to move between parallel pipelines.

• Compressor station - critical parts could consist of water, gas and oil coolers; reciprocating heads; instrumentation; emissions control; and possibly large diameter pipe, valves, and fittings.

• Meter and regulator stations - instrumentation, fittings.

• Communication facilities - no critical parts due to expandability of components (phones, satellite and microwave).

• Gas control facilities - similar to Compressor stations.

• Offshore platforms - critical parts consist of pipe, valves, fittings and clamps.

• LNG facilities - vaporizers and auxiliary tanks; temperature controls.
• Storage facilities - above ground compressor parts and instrumentation.

Further review should be given to critical facilities that could come under attack from cyber terrorism. Particular attention should be focused on the industry dependence on information technology and communication, specifically SCADA systems. These systems are sometimes interlinked with parts suppliers and transportation vendors via extranets. Caution should arise not so much from the operator’s system, but from external infiltration’s via vendor systems. For example, in order to respond to an incident or an event, an operator would often be notified of a potential leak or break by looking at its SCADA system. A hacker could enter the system and bypass the alert system making it seem to the operator as if all systems are working efficiently.

The Risk of Explicitly Defining

Broad public access to information on critical parts, facilities, emergency response plans and other data could increase vulnerability to critical components of the national infrastructure by providing an easily accessible “road map.” Vital industry information, such as critical items, should be exempt from releases under the Freedom of Information Act. Similarly, any definition of “critical” or “ultra-critical” facilities should be kept as confidential as possible by both industry participants and regulatory bodies.
APPENDIX 11

Links to Key Websites and Agency Contact Information/Security and Primary Security Liaison

AGA  
www.aga.org  
202-824-7000  
Kimberly Denbow - kdenbow@aga.org

APGA  
www.apga.org  
302-655-7100

DHS  
www.dhs.gov  
202-282-8000

DOE  
www.doe.gov  
800-dial-DOE  
Ken Friedman – Kenneth.Friedman@hq.doe.gov

FERC  
www.ferc.gov  
866-208-3372

INGAA  
www.ingaa.org  
202-216-5900  
Terry Boss – tboss@ingaa.org

NIPP  
www.dhs.gov/xprevprot/programs/editorial_0827.shtm

NRC  
www.nrc.uscg.mil/report.jhtml

PHSMA  
www.phmsa.dot.gov  
202-366-4433  
John Hess – john.hess@dot.gov

TSA  
www.tsa.gov  
Jack Fox – jack.fox1@dhs.gov

---

1 To open link, right click on link and click on open hyperlink. Please see Section 1.5 for Security Incident Reporting information and telephone numbers.
APPENDIX 12

List of Terms and Acronyms
(Originally developed by ASIS International but condensed for these Security Guidelines)

Abet: To aid, encourage, or incite another person to commit a crime. The term implies that at least two persons are concerned in the commission of the offense: one who directly commits the act and a second who abets its commission. An abettor can be, but not always, charged in a crime as a principal.

Abuses of trust: Type of white collar crime. Committed by people in organizations against organizations, for example, embezzlement, bribery, and kickbacks.
2005 Fraud Examiners Manual (Canada).

Access Control: The control of persons, vehicles and materials through entrances and exits of a protected area; an aspect of security that often utilizes hardware systems and specialized procedures to control and monitor movements into, out of, or within a protected area. Access to various areas may be limited to place or time, or a combination of both.

Access Control Systems: Include all forms of locks and barriers, including doors, walls, floors, and ceilings, as well as electronic access control systems.

Access Mode: A feature of an alarm monitoring system which allows sensors to be shunted by automatic or manual command. An alarm signal is silenced when a protected area is in the access mode. However, if the system is tampered with during the access mode, an alarm is annunciated.

Accident Analysis: The critical examination of facts for the purpose of identifying causal factors and prescribing measures designed to prevent recurrence.

Accident Severity: A measure of the severity or seriousness of losses, rather than the number of losses. It can be measured in terms
of dollar loss or injuries sustained rather than the number of individual accidents.


Accumulator Circuit: A circuit that initiates an alarm signal as a function of accumulated information; a circuit programmed to send a signal when a door remains unclosed after a specified number of seconds, or when a specified number of sensors activate in one zone within a given period of time.


Acoustic Fuse: The fuse of a bomb sensitive to minute sonic or subsonic variations. The fuse operates from an influence exerted by the target on a sensitive detecting device within the fuse itself.


Acoustic Pickup: A conventional or a specially designed microphone used for the detection of sounds such as noise made by a burglar breaking into protected premises.


Active Imaging: Forming a visual image on a screen of low light scene by using an infrared illumination source. The technique is not dependent on available light energy to electronically form the image.


Ad hoc violations: Type of white collar crime. Committed for personal profit on an episodic basis, for example, tax cheating. 2005 Fraud Examiners Manual (Canada).

Adversary: Any individual, group, organization, or government that conducts activities, or has the intention and capability to conduct activities detrimental to critical assets. An adversary could include intelligence services of host nations, or third party nations, political and terrorist groups, criminals, rogue employees, and private interests. Adversaries can include site insiders, site outsiders, or the two acting in collusion. Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries, Second Edition, American Petroleum Institute (API), October 2004.
al Qaeda Core: The group of individuals and cells directly in contact with, and under the control of, al Qaeda Senior Leadership (e.g. al Qaeda East Africa Cell).

al Qaeda Influenced: Groups, networks, cells and individuals who share the AQ ideology but have no current contact (or personnel with strong historical links) with the al Qaeda Core (e.g. Madrid Cell, Hofstadt Group).

al Qaeda Linked: Groups, networks, or cells with (at times intermittent) contact with al Qaeda Core and who accept the al Qaeda ideology, but who are not under direct operational control (e.g. IJU,JI, AQAP, AQ-I).

al Qaeda Movement: Overarching term for al Qaeda Core, Linked, and Influenced groups, networks, or cells. Also called the “Global Jihad” Community.

al Qaeda Senior Leadership: Osama bin Laden and his senior lieutenants. This relatively small group of people are primarily based in the Pakistan/Afghanistan border region.

Alarm Assessor: A device or system that allows an operator of an alarm system to evaluate or assess a reported alarm. For example, alarm assessment can be made possible with the use of a CCTV system that permits visual observation at a protected area where a motion sensor has activated.

Alarm Discriminator: A device used to minimize or eliminate the possibility of false alarms caused by extraneous sounds or vibrations. It can be adjusted to provide alarm discrimination under any job conditions. It may be either a special circuit incorporated in a detector or a device that is added to a system.

Alarm Line: An electrically supervised wire circuit used for the transmission of signals from a protected area to a central receiving point.
Alarm Receiver: An annunciator that also provides supervision of the alarm line and may or may not include an audible alarm device. Various circuit and contact arrangements are usually available to provide auxiliary functions upon receipt of an alarm signal. *Protection of Assets Manual, Volume I, 2001.*

Alarm Screen: A window screen, usually laced with fine wire, used as an intrusion detection device. Cutting or breaking the screen causes an open circuit and trips the alarm. [www.asisonline.org](http://www.asisonline.org), 2006.

Alarm Sequential Switcher: A device in a CCTV system which activates when sensors in a viewing zone detect an alarm condition. The switcher also automatically displays views from the affected zone. [www.asisonline.org](http://www.asisonline.org), 2006.

Alarm Station: Any of a wide variety of switched that depend upon human operation for the reporting of an alarm condition. Examples include fire alarm pull stations, holdup alarms, and medical emergency alarms. [www.asisonline.org](http://www.asisonline.org), 2006.

Alarm Signal: An audible and/or visual signal indicating an emergency, such as an intrusion, fire, smoke, unsafe equipment conditions, equipment failure, reporting line tamper or failure and so forth, that requires immediate action. *Protection of Assets Manual, Volume I, 2001.*

Alarm System: A combination of sensors, controls, and annunciators arranged to detect and report an intrusion or other emergency. [www.asisonline.org](http://www.asisonline.org), 2006.

Alert Levels: Describes a progressive, qualitative measure of the likelihood of terrorist actions, from negligible to imminent, based on government or company intelligence information. Different security measures may be implemented at each level based on the level of threat to the facility. *Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries, Second Edition, American Petroleum Institute (API), October 2004.*

Alternate Worksite: A work location, other than the primary location, to be used when the primary location is not accessible.
Altimeter Bomb: A bomb (frequently homemade) triggered by the change in atmospheric pressure relative to the altitude and the earth’s surface.  

American Gas Association (AGA)  Founded it 1918, represents 197 local energy utility companies that deliver natural gas to more than 56 million homes, businesses and industries throughout the United States. AGA’s members account for roughly 83 percent of all natural gas delivered by the nation’s local natural gas distribution companies. AGA is an advocate for local natural gas utility companies and provides a broad range of programs and services for member natural gas pipelines, marketers, gatherers, international gas companies and industry associates. AGA’s vision is to be the most effective and influential energy trade association in the United States while providing clear value to its membership.  

American Petroleum Institute (API)  The only national trade association that represents all aspects of America’s oil and natural gas industry. Over 400 corporate members, from the largest major oil company to the smallest of independents, come from all segments of the industry. In recent years, API’s work has expanded to include a growing international dimension, and today, API is recognized around the world for its broad range of programs including: advocacy, research and statistics, standards, certification, and education.  

American Public Gas Association (APGA)  APGA is a nonprofit trade organization representing America’s publicly owned natural gas local distribution companies (LDCs). APGA represents the interests of public gas before Congress, federal agencies and other energy-related stakeholders by developing regulatory and legislative policies that further the goals of members. APGA also organizes meetings, seminars, and workshops with a specific goal to improve the reliability, operational efficiency, and regulatory environment in which public gas systems operate.  
<table>
<thead>
<tr>
<th><strong>American Society for Industrial Security:</strong></th>
<th>See “ASIS International”.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ANFO:</strong></td>
<td>A low explosive made of ammonium nitrate fertilizer and fuel oil. <a href="http://www.asisonline.org">www.asisonline.org</a>, 2006.</td>
</tr>
<tr>
<td><strong>Anthrax:</strong></td>
<td>One of the most lethal and hardy bacterial pathogens. It can infect by inhalation, ingestion, or absorption through cuts. Infection by inhalation can be lethal. <em>Protection of Assets Manual, Volume I, 2006.</em></td>
</tr>
<tr>
<td><strong>Anti-disturbance Device:</strong></td>
<td>A device built into a homemade bomb so as to trigger the bomb if it is jarred, moved, or disturbed in any way. <a href="http://www.asisonline.org">www.asisonline.org</a>, 2006.</td>
</tr>
<tr>
<td><strong>Anti-passback:</strong></td>
<td>A feature of an access control system which prevents successive use of one card to pass through any portal in the same direction. To attain this protection, a separate reader is required at each entrance and exit. Anti-passback prevents a card from being passed back to another person for the purpose of gaining unauthorized entry. <a href="http://www.asisonline.org">www.asisonline.org</a>, 2006.</td>
</tr>
<tr>
<td><strong>Anti-personnel Bomb:</strong></td>
<td>A bomb intended to primarily injure or kill people, frequently home-made as in a pipe bomb, and designed to fragment upon explosion. <a href="http://www.asisonline.org">www.asisonline.org</a>, 2006.</td>
</tr>
<tr>
<td><strong>Apostasy:</strong></td>
<td>In an Islamic context, to purposefully cease to be Muslim. The term <em>apostate</em> is used by Islamic extremists to designate Muslim individuals, groups or nations that have, in their eyes, committed acts that go against their interpretation of <em>Sharia law</em>. <em>JTAC Terrorism Report, June, 2007.</em></td>
</tr>
<tr>
<td><strong>Area Detection:</strong></td>
<td>A technique for detecting an intruder’s presence anywhere within a specifically defined, protected area, as opposed to detection at a specific point such as a door. <em>Protection of Assets Manual, Volume I, 2001.</em></td>
</tr>
<tr>
<td><strong>Area Maritime Security:</strong></td>
<td>Existing regulatory standards relating to Coast Guard requirements for natural gas facilities in their jurisdiction. Refer to 33 CFR Part 103.</td>
</tr>
<tr>
<td><strong>Arming Signal:</strong></td>
<td>A coded message or signal transmitted from a protected premises to a central station or other monitoring location which informs that the alarm system has been armed by an authorized person.</td>
</tr>
</tbody>
</table>
Arming Station: A switching device from which an alarm system is placed into operation.

Assessment Guideline: risks at a specific location can be identified and communicated,

Asset: Any person, environment, facility, material, information, business reputation, or activity that has a positive value to an owner. The asset may have value to an adversary, as well as an owner, although the nature and the magnitude of those values may differ. Assets in the SVA include the community and the environment surrounding the site. 


Asset Attractiveness: An estimate of the value of an asset to an adversary. Experience has shown that, particularly for terrorist attacks, certain targets better accomplish the objectives of the adversaries than do others. 


Asset Category: Assets may be categorized in many ways. Among these are: 
- People 
- Hazardous materials (used or produced) 
- Information 
- Environment 
- Equipment 
- Facilities 
- Activities/Operations 
- Company reputation 


Assets Protection: The function of shielding from danger or harm the money, receivables, information, resources, rights, property and other valuables of an owner.

Assistant Secretary of Infrastructure Protection (ASIP)  
Within the Department of Homeland Security (DHS) Office of Infrastructure Protection (OIP), the ASIP leads the coordinated national effort to reduce the risk to the Nation’s critical infrastructures and key resources (CI/KR) from terrorist acts, and to strengthen national preparedness, response, and recovery in the event of an attack, natural disaster, or other emergency.

Astro-pak:  
The trade name for a two-part explosive used in blasting. A two-part explosive is composed of two chemicals each of which is not explosive until joined together.  

Audio Listen-in Device:  
A device that monitors the sounds at a protected facility to determine where an intrusion occurs and/or to determine the nature of the intrusion after it has been detected by other means. Audio monitoring is typically an arrangement of microphone, amplifier, and receiver that allows a person at a separate location to listen for suspicious sounds.  

Autoclave Bomb:  
A bomb designed to explode when atmospheric conditions change.  

Automated Identification System (AIS):  
A computerized fingerprint identification system used by the FBI that provides speedy and efficient identification services.  

Automatic Shutdown:  
A system in which certain instruments are used to control or maintain the operating conditions of a process. If conditions become abnormal, the automatic shutdown feature stops the process.  

Auxiliary Lock:  
A lock installed on a door or window to supplement a previously installed primary lock. It is typically a mortised board or rim lock.  

Background Investigation:  
An inquiry into the background of an individual under consideration for employment, credit, access to sensitive assets (such as national defense information), and other reasons. A background investigation can vary widely, from merely checking prior employment experience and
educational credentials to civil, criminal, and medical histories.  


**Background Screening:** An inquiry into the history and behaviors of an individual under consideration for employment, credit, access to sensitive assets (such as national defense information), and other reasons. 

*Preemployment Background Screening, ASIS, 2006.*

**Bangalore Torpedo:** A dynamite-filled length of pipe detonated by a blasting cap or a fuse.  


**Barometric Bomb:** A bomb triggered by a change in air pressure.  


**Barrier:** A natural or manufactured obstacle to the movement of persons, animals, vehicles or materials. A properly installed barrier should clearly warn a potential intruder to “Keep out” either explicitly or intuitively.  


**Best Practices:** Fundamental principles that add value to organizational performance; workplace behavioral standards that contribute to consistently excellent performance by employees and teams of employees; comparative research (i.e., benchmarking) that is intended to improve organizational performance. Best practices in the security field incorporate elements that have been found to be successful such as policy and planning as guides, work rules and procedures as directives, risk assessment, crime opportunity reduction, and training and re-training of employees.  


**Black Intelligence:** Information obtained through espionage.  


**Botulinum Toxin:** Produced naturally by the bacterium Clostridium botulinum. Commercially available through pharmaceutical sources, it is produced by a living organism. It is a chemical weapon, an extremely lethal neurotoxin. Theoretically, one ounce is enough to kill 60 million people. An ounce or two in a reservoir of 10 million gallons would kill anyone who drank a half-pint of water.  

**Breach:**
A break in a system’s security that results in admittance of a person or program.


**Break Alarm:**
An alarm signal produced by opening or breaking an electrical circuit, sometimes referred to as an open-circuit alarm. Trouble signals are generally open or break alarms.


**Breaking and Entering:**
The illegal and forcible entry of a premises, as by breaking a lock or a window, removing a door, or cutting through a rood or wall. When the entry is for the purpose of committing a theft, it is usually charged as burglary.


**Break-wire Sensors:**
Intrusion detection devices used on building heating, ventilating, and air-conditioning air intakes or in interstitial ceiling spaces.


**Buffer Zone Protection Program**
Provides federal resources to identify and mitigate vulnerabilities to critical infrastructure.

[www.ojp.usdoj.gov/odp/docs/FY06_BZPP_FINAL.pdf](http://www.ojp.usdoj.gov/odp/docs/FY06_BZPP_FINAL.pdf).

**Building Security Systems:**
A completely integrated system to protect against intrusion, espionage, vandalism, theft, smoke, fire, unsafe or faulty equipment operation, and any other condition or act that might endanger and installation, which includes the control of traffic and operation of doors and/or gates from a remote location. Use is made of human guards, or mechanical, electrical, and electronic devices, or combinations thereof, in sufficient quantities and varieties to assure the desired degree of protection.


**Bullet-resisting (BR) Glass:**
Laminated glass consisting of multiple piles of glass, polycarbonate and other plastic films to provide many levels of ballistic resistance.


**Burqa:**
A long woman’s veil that covers the body except for the eyes and tips of the fingers.

*JTAC Terrorism Report, June, 2007.*

**Buttress Lock:**
A lock that secures a door by wedging a bar between the door and the floor. Some incorporate a moveable steel
rod which fits into metal receiving slots on the door and
in the floor.

Cam: The part of a lock or cylinder which rotates to actuate the
bolt or latch as the key is turned. The key may also act
as the bolt.

Canine Security: The use of canine (dogs) in security, such as for
guarding property, protecting people, and detecting
drugs and explosives.

Capability: When assessing the capability of an adversary, two
distinct categories need to be considered. The first is the
capability to obtain, damage, or destroy the asset. The
second the adversary’s capability to use the asset to
achieve their objectives once the asset is obtained,
damaged, or destroyed.
Security Vulnerability Assessment Methodology for the
Petroleum and Petrochemical Industries, Second
Edition, American Petroleum Institute (API), October
2004.

Carbon Microphone: While larger than most spy audio devices, they provide
good pick-up if properly hidden and located. As with
other forms of listening equipment, these microphones
are usually equipped with a transmitter that relays
intercepted conversations off-site to a recorder.
2005 Fraud Examiners Manual (Canada).

Card Encoder: A device that places a unique access code on or within
an access control card.

Card Key: A plastic card that contains coded information capable of
being read by electronic devices placed at the entry and
exit points of the protected facility.

Card Master: A card key that will open all locks within a mastered
group of locks.

Card Reader: A device for reading a card containing a code or signal;
an intelligent reader that compares data on a card against
preprogrammed parameters. Entry or exit is granted or
denied by the card reader at the reader location.
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
<th>Source/Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Casement Window:</strong></td>
<td>A window that has one or two movable panels hinged at the side to the frame to provide a complete opening of the window.</td>
<td><em>Protection of Assets Manual, Volume I, 2002.</em></td>
</tr>
<tr>
<td><strong>CATV Alarm System:</strong></td>
<td>A central station alarm system which uses cable television lines to carry alarm signals.</td>
<td><a href="http://www.asisonline.org">www.asisonline.org</a>, 2006.</td>
</tr>
<tr>
<td><strong>CCTV Motion Detectors:</strong></td>
<td>Intrusion detection devices used in building stairwells and various locations where CCTV is used in the building.</td>
<td><em>Protection of Assets Manual, Volume IV, 2006.</em></td>
</tr>
<tr>
<td><strong>Cease and Desist Order:</strong></td>
<td>A ruling, frequently issued in unfair labour practice cases, which requires the charged party to stop conduct held to be illegal and take specific action to remedy the practice.</td>
<td><a href="http://www.asisonline.org">www.asisonline.org</a>, 2006.</td>
</tr>
<tr>
<td><strong>Cell:</strong></td>
<td>A small closely-knit cluster of people with a shared common operational goal.</td>
<td>JTAC Terrorism Report, June, 2007.</td>
</tr>
<tr>
<td><strong>Chain Bolt:</strong></td>
<td>A vertical spring-loaded bolt usually mounted at the top of a door, manually actuated by a chain.</td>
<td><a href="http://www.asisonline.org">www.asisonline.org</a>, 2006.</td>
</tr>
<tr>
<td><strong>Chain Referral Scheme:</strong></td>
<td>A scheme that typically involves sales of grossly overpriced products through false representation that the cost will be recovered by commissions the promoter will pay on sales to the purchaser’s friends, if only the purchaser will permit them to be contacted with the same proposition.</td>
<td><a href="http://www.asisonline.org">www.asisonline.org</a>, 2006.</td>
</tr>
<tr>
<td><strong>Chemical Explosion:</strong></td>
<td>An explosion that results from an extremely rapid conversion into gases of a solid or liquid explosive compound, characterized by an instantaneous change normally called a detonation or deflagration.</td>
<td><a href="http://www.asisonline.org">www.asisonline.org</a>, 2006.</td>
</tr>
<tr>
<td><strong>Chemical Facility Anti-Terrorism Security (CFATS)</strong></td>
<td>CFATS, enacted by Section 550 of the Homeland Security Appropriations Act of 2007, was published in the Federal Register on April 4, 2007. The rule authorizes implementing risk-based performance standards for the Nation’s high-risk chemical facilities. Under the rule, if DHS notified a facility it is “high</td>
<td></td>
</tr>
</tbody>
</table>
“risk”, officials will have 60 days in which to file Vulnerability Assessments and 120 days in which to file Site Security Plans. DHS will follow up with site inspections and audits.

**Chemical Sensor:**
A sensor that evaluates air in a protected area. If suspicious effluvia are detected, the sensor can read and record the change, and signal as programmed.  

**Chip-in Card:**
A plastic identification card embedded with an integrated circuit chip which has both a coded memory and microprocessor intelligence and can record card transactions and store data.  

**Christmas Ball Hazer:**
A homemade device in the shape of a baseball and made of Styrofoam or similar material. The sharp points of needles and nails protrude from the ball. It is sometimes soaked with urine or other irritant and thrown at police officers during disturbances.  

**Clandestine Operations:**
Intelligence, counterintelligence, and other information collection activities and covert political, economic, propaganda and paramilitary activities, conducted so as to assure secrecy.  

**Class A Circuit:**
A type of four-wire alarm circuit used to detect an alarm or line fault. The circuit allows reporting of an alarm condition even when a trouble condition has occurred. Two conductors run from the alarm panel to the sensor, and two return. A single break does not prevent the reception of an alarm signal, but does initiate a trouble condition.  

**Class B Circuit:**
A four-wire system in which two conductors travel from an alarm panel, connect with one or more alarm sensors, and return to the panel. One broken conductor prevents reception of an alarm signal from any point beyond the break, causing a trouble condition. A Class B Circuit can also consist of a two-wire system in which only one conductor travels from the panel to sensors and back again. A single break prevents all alarm transmissions and initiated a trouble condition at the panel.  
Clear Zone: An unobstructed area on both sides of a perimeter barrier. A clear zone is kept free of rubbish, weeds, bushes, trees or other material that might conceal anyone attempting to climb, tunnel or cut through a perimeter barrier.


Climb Detector: A type of intrusion sensor typically consisting of three low voltage wires strung across the top of a wall, fence, or building.


Closed Bomb: A bomb in which none of the component parts are visible to the naked eye.


Closed Buildings: Access to elevator banks is controlled by some form of credential checking, visitors are authenticated prior to proceeding to elevators, and sometimes a separate messenger centre, with controlled delivery of property, is provided.


Closed Circuit: A protective circuit consisting of all normally closed devices connected in a series. A break in the circuit or activation of one or more sensors triggers an alarm.


Closed Circuit Television (CCTV) A television installation in which the signal is transmitted to a defined number of receivers.


Coding Siren: A siren with the capability of emitting controlled bursts of sound.


Concentrated Explosion: An explosion characterized by an extremely rapid combustion, known as detonation reaction, which occurs through the action of explosives such as dynamite, TNT, nitroglycerin, pentaerythritoltetranitrate, and various plastic explosives.


Confidential: A designation generally applied to information or material the unauthorized disclosure of which could be reasonable expected to cause damage to the owner’s interest. In national security, examples of damage include the compromise of information that indicates strength of ground, air, and naval forces and overseas
areas; disclosure of technical information used for training, maintenance, and inspection of classified munitions of war; and revelation of performance characteristics, test date, design, and production data on munitions of war.

Contingency Planning: Problem solving before the fact; planning to counter emergencies or unexpected occurrences.

Contingency Procedures/Plans Contingency procedures are alternatives to normal procedures when an unusual but anticipated situation occurs. Contingency plans set forth organized, planned, and coordinated courses of action to be followed in case of an emergency event such as fire, explosion, or release of hazardous waste.

Contract Security: Protective services provided by one company, specializing in such services, to another company on a paid, contractual basis.

Control Elements: Software and data performing or supporting control functions such as access control, logging, and violation detection. Examples are password data sets, files of cipher-keys, and log files.

Control Panel: A centrally located assembly containing all power supplies, relays, amplifiers and any other equipment required to receive and interpret alarm signals from a protected area via reporting lines and to supervise these lines.

Controlled Access Area: An area which is clearly demarcated, access to which is controlled and which affords isolation of the material or persons within it.

Countermeasures: An action taken or a physical capability provided whose principal purpose is to reduce or eliminate one or more vulnerabilities. The countermeasure may also affect the threat(s) (intent and/or capability) as well as the asset’s value. The cost of a countermeasure may be monetary, but may also include non-monetary costs such as reduced operational effectiveness, adverse publicity,
unfavorable working conditions, and political consequences.


**Covert Meet Security:**
Measures taken to protect a covert meeting in terms of information about the event and physical protection of the meeting itself. It is a very broad term and may include such activities as encrypting information involved in setting up the meeting, using a safe house or other “secure” location, counter surveillance, armed security and other measures. It is designed to protect the conduct of the meeting itself and the people involved in the meeting.

[www.asisonline.org](http://www.asisonline.org), 2006

**Covert Surveillance:**
Observation by someone who is hidden from public view, usually to detect suspicious or illegal activity, and sometimes used by the police to aid in traffic enforcement.

[www.asisonline.org](http://www.asisonline.org), 2006

**Crisis Management Center**
A specific room or facility staffed by personnel charge with commanding, controlling, and coordinating the use of resources and personnel in response to a crisis.


**Crisis Management Planning:**
A properly funded ongoing process supported by senior management to ensure that the necessary steps are taken to identify and analyze the adverse impact of crisis events, maintain viable recovery strategies, and provide overall coordination of the organization’s timely and effective response to a crisis.


**Crisis Management Team:**
A group directed by senior management or its representatives to lead incident/event response comprised of personnel from such functions as human resources, information technology facilities, security, legal, communications/media relations, manufacturing, warehousing and other business critical support functions.
Chemical Facility Anti-Terrorism Standards (CFATS):
DHS promulgated CFATS on April 9, 2007. This program is designed to secure the nation’s chemical infrastructure by identifying high risk chemical facilities and requiring them to implement risk-based performance standards and other requirements. Facilities that manufacture, use, store or distribute certain types of chemicals will be covered by the new requirements. DHS has clarified that Appendix A does not apply to underground storage of natural gas in geological formations (to include, but not limited, to depleted reservoirs, salt caverns, domes, aquifers and other porous media). Operators are not required to quantify for the purposes of screening threshold quantity (STQ) for natural gas stored underground.

Critical Infrastructure:
Systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

Critical Infrastructure Information Act (CIIA)
Part of the Homeland Security Act of 2002, the CIIA consists of a group of provisions addressing circumstances under which DHS may obtain, use, and disclose critical infrastructure information as part of a critical infrastructure protection program. Under provisions of the CII Act, the information submitted voluntarily to DHS per those provisions will be protected from public disclosure until and unless the Protected Critical Infrastructure Information (PCII) Program Office determines the information does not meet the requirements for PCII. If validated as PCII, the information will remain exempt from public disclosure.

Critical Infrastructure and Key Resources (CI/KR)
CI/KR includes the assets, systems, networks, and functions that provide vital services to the Nation. CI/KR refers to assets, systems, and networks, whether physical or virtual, so vital to the United States that the incapacity or destruction of such assets, systems, or networks would have a debilitating impact on security,
national economic security, public health or safety, or any combination of those matters.

**Critical Infrastructure (CI)** Programs and activities to protect systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such assets would have a debilitation impact on security, national economic security, national public health or safety, or any combination of those matters.

**Critical Infrastructure Partnership Advisory Council (CIPAC)** CIPAC, which has been exempted from the requirements of the Federal Advisory Committee Act (FACA), is the mechanism to allow meaningful dialogue on key critical infrastructure protection issues and agreement on mutual action between government and owner/operator entities. CIPAC is a non-decisional body and includes sector members and government members. Sector members are the members of that sector’s SCC that are owners and/or operators and the trade associations that represent them. Government members are the Federal, State, local, and tribal government agencies (or their representative bodies) that comprise the GCC for each sector. The most current CIPAC membership list is maintained on the internet and can be found on DHS’ CIPAC website – [www.dhs.gov/cipac](http://www.dhs.gov/cipac).

**Critical Infrastructure Warning Information Network (CWIN)** Operational since 2003, CWIN is the critical, survivable link in the Homeland Security Information Network (HSIN) connecting DHS with the CI/KR sectors, State homeland security advisors, and the Sector-Specific Agencies (SSAs) during incidents of national significance. CWIN also connects emergency operations centres in all 50 States and the District of Columbia to the DHS Homeland Security Operations Centre (HSOC).

**Critical System:** Any electronic data processing system which if interrupted would cause substantial loss. [www.asisonline.org](http://www.asisonline.org), 2006

**Criticality Assessment:** A methodology for measuring the impact upon an organization that the loss of an asset would impose. [www.asisonline.org](http://www.asisonline.org), 2006

**Cumulative Evidence:** Additional or corroborative evidence to the same point; that which goes to prove what has already been established by other evidence. [www.asisonline.org](http://www.asisonline.org), 2006
**Criticality Rating:**
An arbitrary designation, applied to a particular loss event, which expresses the impact of the loss upon the organization. Examples of ratings might be: fatal to the business, very serious impact on the business, moderately serious, less than serious, and not serious.  
[www.asisonline.org](http://www.asisonline.org), 2006

**Crystal Microphone:**
A microphone that depends on the generation of an electric charge by the deformation of a crystal for its operation.  

**Cyber Isolation:**
The removal of an individual’s or entity’s computer network from access to the Internet.  

**Cyber Security:**
Security used to protect an individual’s or entity’s computer network access from criminal activity.  

**Cyber Storm II (CSII):**
Cyber Storm II represents the largest government-sponsored cyber security exercise of its kind, and it will incorporate international, Federal, State, and local government officials, as well as private sector players, including CI/KR sectors (IT, Communications, Chemical, and Transportation). The DHS-led exercise will focus on a cyber-specific scenario that rises to the level of an Incident of National Significance. The March 2008 test will be a follow-up to the February 2006 Cyber Storm test. Like the first Cyber Storm, this exercise will evaluate the ability of the public and private sector to provide a coordinated response to a large-scale cyber event.

**Department of Energy (DOE)**
The DOE's mission is to advance the national, economic, and energy security of the United States; to promote scientific and technological innovation in support of that mission; and to ensure the environmental cleanup of the national nuclear weapons complex. The Department’s strategic goals to achieve the mission are designed to deliver results along five strategic themes: energy security; nuclear security; scientific discovery and innovation; environmental responsibility; and management excellence.  
One primary reason for the establishment of the DHS was to provide the unifying core for the vast national network of organizations and institutions in efforts to secure America. In order to better do this and to provide guidance to the 180,000 DHS men and women who work every day on this important task, the Department developed its own high-level strategic plan. DHS leads the unified national effort to secure America and prevent and deter terrorist attacks and protect against and respond to threats and hazards to the nation. DHS aims to ensure safe and secure borders, welcome lawful immigrants and visitors, and promote the free-flow of commerce.


Detection:
A countermeasure strategy that is intended to identify an adversary attempting to commit a security event or other criminal activity in order to provide real-time observation as well as post-incident analysis of the activities and identity of the adversary.


Detection Range:
The maximum effective distance a sensor can detect an intruder. A specified figure for detection range is determined by repeatedly introducing fault conditions at varying distances.


Deterrence:
A countermeasures strategy that is intended to prevent or discourage the occurrence of a breach of security by means of fear or doubt. Physical security systems such as warning signs, lights, uniformed guards, cameras, bars are examples of countermeasures that provide deterrence.


Deviance:
Conduct, activity, or condition that is disapproved of, stigmatized, and subject to formal and informal punishment. Generally, it is behavior that varies markedly from the average or norm, usually pathological in nature, or which elicits condemnation in the social setting in which it takes place.

### DHS Homeland Information Threat Risk and Analysis Center (HITRAC)

HITRAC is a DHS entity that conducts integrated threat analysis for all critical infrastructure sectors. HITRAC works with the intelligence and law enforcement communities to integrate and analyze intelligence on security threats to homeland infrastructure.

### DHS Protective Security Advisor

To partner with state and local governments, as well as the private sector, DHS has placed security specialists in communities throughout the country to assist local efforts to protect critical assets and provide local perspective to national efforts.

### DHS Transportation Security Operations Center (TSOC)

Serves as critical national centre for transportation security information sharing and domestic incident reporting. TSOC is staffed 24/7 and serves as the point of contact for all transportation security concerns, including aviation, rail, mass transit, maritime, pipeline, highway, and cargo issues.

### DHS TSA Suspicious Incident Reports

These weekly reports contain suspicious activity reported by the six transportation sectors, Aviation, Maritime, Highway, Pipelines, Rail/Transit, and Cargo/Supply Chain, and are compiled by the TSA Office of Intelligence and are classified as Sensitive Security Information (SSI).

### Digital Electronic Scanning Software

Programs that allow a fixed camera to appear as if it were mounted to a mechanical pan/tilt device. This is accomplished by scanning across the imager in a predetermined path as opposed to physically moving the camera.


### Director of National Intelligence

The DNI serves as the head of the U.S. Intelligence Community. The DNI also acts as the principal advisor to the President; the National Security Council, and the Homeland Security Council for intelligence matters related to the national security; and oversees and directs the implementation of the National Intelligence Program. The President appoints the DNI with the advice and consent of the Senate.
Distributed Card Access: An access control system in which each card reader has all the intelligence and data required to make access decisions.

Distributed Intelligence Systems: Security systems that incorporate control and discrimination logic, which is programmable from either the console at the control centre or other operator’s terminals – such as guard posts in remote buildings. 

Dome Camera: A CCTV camera installed in a tinted dome-shaped housing, so that the camera and its direction are unseen.

Double-hung Window: A window that is divided into upper and lower sections that slide vertically past each other. They may be counterweighted with sash weights or spring balances to hold them at a desired open position.

Double-keying: A procedure requiring that two persons, each with a separate and different key, open locks that grant access to a sensitive item or location.

Dual Alarm System: A system that sounds a coded alarm signal for a fixed number of rounds at selected locations, and at the same time a constant and continuous alarm signal at all other locations until the system is restored to normal. The coded signal identifies the particular alarm-initiating device in operation. A dual alarm system facilitates evacuation of a building by announcing a fire alarm generally in all parts of the building and by simultaneously notifying response personnel so that evacuation and fire fighting can be started without delay at the fire-affected area.

Dual Rate Alarm Signal: An audible signal that begins with a slowly pulsed annunciation. When a pre-determined length of time has been reached or when a manually operated switch has been activated, the audible signal changes to a rapidly pulsed annunciation. The slow-pulse signal alerts emergency response personnel. The fast-pulse signal informs occupants to evacuate.
**Dual Technology Motion Detector**  
A sensor that utilizes two technologies, e.g., microwave and infrared, in a logical combination to reduce false alarms.  

**Duress Alarm:**  
A device that enables a person placed under duress to call for help without arousing suspicion.  

**Electric Deadbolt:**  
A solenoid (electro-magnet) moves a deadbolt, typically mounted on a door frame, either into or out of a strike plate on a door.  

**Electric Door Strike:**  
An electrically operated door lock with a solenoid and mechanical latch. Applying power causes the solenoid to withdraw the latch pin so that the door may be opened.  
www.asisonline.org, 2006

**Electrostatic Detection Apparatus**  
Allows examiners to detect indented writing from the top page of a pad of paper up to five pages below the original. The Electrostatic Detection Apparatus uses photocopier toner to develop the areas of indentation after a document has been covered with an electrically charged plastic film.  
*2005 Fraud Examiners Manual (Canada).*

**Electromagnetic Lock:**  
A type of lock that uses magnetic attraction to hold the latch in the locked position.  
www.asisonline.org, 2006

**Electronic Security Measures:**  
Include burglar and fire alarm systems for prevention, deterrence, and response.  

**Electronic Serial Number (ESN):**  
A number assigned to an electronic device that is connected to a computer. For example, a cellular phone may have an ESN that is automatically reported to the base station every time a call is made from the phone.  
www.asisonline.org, 2006

**EMS:**  
Emergency Medical Service.  
Energy Sector-Specific Plan for Critical Infrastructure Protection
U.S. Department of Homeland Security, Transportation Security Administration, final version was developed and released by DOE.

Exit Device:
Also known as a panic bar or crash bar, the exit device is commonly used on doors in the path of egress from structures with high occupancy. *Protection of Assets Manual, Volume I, 2002.*

FBI Joint Terrorism Task Force
Contact local FBI office for additional information on your local JTFF. www.fbi.gov/contact/jtff.

Federal Advisory Committee Act (FACA)
In 1972, Congress enacted the Federal Advisory Committee Act (FACA) to ensure that advice rendered to the executive branch by the various advisory committees, task forces, boards, and commissions formed over the years by Congress and the President, be both objective and accessible to the public. A FACA committee must follow certain rules including open meetings and records.

Federal Emergency Planning Guide For Business and Industry
This guide provides step-by step advice on how to create and maintain a comprehensive emergency management program. It can be used by manufacturers, corporate offices, retailers, utilities or any organization where a sizable number of people work or gather. www.fema.gov/pdf/library/bizindst.pdf.

Firewall:
A combination of hardware and software that filters computer network traffic from and to the Internet based upon network access control parameters. A firewall can mask internal network information as well as stop exploratory probes and denial of service attacks. *Threat Advisory System Response (TASR) Guideline, ASIS International, 2004.*

Fail Safe Lock:
A type of lock that automatically opens when a power failure occurs. Typically, a fail safe lock will have an electrically released strike plate or a solenoid operated bolt. www.asisonline.org, 2006
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
<th>Source</th>
<th>Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fail Secure Lock</td>
<td>A type of lock that automatically locks when a power failure occurs, as opposed a fail safe lock.</td>
<td><a href="http://www.asisonline.org">www.asisonline.org</a>, 2006</td>
<td></td>
</tr>
<tr>
<td>Federal Energy &amp; Regulatory Commission (FERC):</td>
<td>The FERC regulates and oversees energy industries in the economic, environmental, and safety interests of the American public. The FERC is an independent agency that regulates the interstate transmission of electricity, natural gas, and oil. The FERC also reviews proposals to build liquefied natural gas (LNG) terminals and interstate natural gas pipelines as well as licensing hydropower projects.</td>
<td><a href="http://www.ferc.gov">www.ferc.gov</a>, 2006</td>
<td></td>
</tr>
<tr>
<td>Fence Ribbon</td>
<td>Barbed metal tape, similar to barbed wire, used for perimeter protection.</td>
<td><a href="http://www.asisonline.org">www.asisonline.org</a>, 2006</td>
<td></td>
</tr>
<tr>
<td>Fencing</td>
<td>Physical barrier installed to delineate a boundary or to deter, delay, or prevent unauthorized access to a protected area.</td>
<td><a href="http://www.asisonline.org">www.asisonline.org</a>, 2006</td>
<td></td>
</tr>
<tr>
<td>Fire Bomb</td>
<td>An incendiary device, typically homemade, which when thrown will produce fire upon impact. A fire bomb usually consists of gasoline and a wick in a glass container. The wick is ignited, and the bomb is thrown. When the glass container breaks, a flash explosion occurs.</td>
<td><a href="http://www.asisonline.org">www.asisonline.org</a>, 2006</td>
<td></td>
</tr>
<tr>
<td>Firewall</td>
<td>Software or hardware that provides security by isolating a company’s computer network from the Internet. A firewall also prevents outsiders from connecting to the owner’s network.</td>
<td><a href="http://www.asisonline.org">www.asisonline.org</a>, 2006</td>
<td></td>
</tr>
<tr>
<td>Floor Sensor</td>
<td>A sensor installed under, in, or upon a floor and designed to trigger and alarm when an intruder moves across the floor. Typically, a floor sensor operates on a weight or pressure principle.</td>
<td><a href="http://www.asisonline.org">www.asisonline.org</a>, 2006</td>
<td></td>
</tr>
<tr>
<td>Fluoroacetates</td>
<td>Fluoroacetic acid and related compounds are sold commercially as rodenticides. The commercial form can easily be refined into more deadly compounds. As a dust or liquid, this poison can be absorbed by inhalation, by ingestion, through the eyes, and through cuts and abrasions.</td>
<td><a href="http://www.asisonline.org">www.asisonline.org</a>, 2006</td>
<td></td>
</tr>
</tbody>
</table>
Foil: Type of detector formerly widely used on surfaces, most often glass, to signal a surreptitious or forcible penetration. An electrical current flows in the foil and when the foil is broken or grounded, an alarm is initiated.

Forced Entry: Entry accomplished by the use of force upon the physical components of the premises using tools or muscle power.

Freedom of Information Act (FOIA) The U.S. Freedom of Information Act (FOIA) is a law ensuring public access to U.S. government records. FOIA carries a presumption of disclosure; the burden is on the government – not the public – to substantiate why information may not be released. Upon written request, agencies of the U.S. government are required to disclose those records, unless they can be lawfully withheld from disclosure under one of nine specific exemptions in the FOIA. This right of access is ultimately enforceable in Federal court.

Functional Exercise: Limited involvement or simulation by field operations to test communication, preparedness, and available/deployment of operational resources.

Fundamentalist: A person who upholds strict or literal interpretation of a traditional religious belief. Holding a fundamentalist viewpoint does not imply a willingness to use violence.

Glass Break Sensor: An electronic detector that evaluates the sound frequencies generated by breaking glass. Also called glass break detector. Contact-type sensors can be mounted directly on the glass; acoustical detectors listen for sound waves.

Global Jihad: The belief, espoused by Osama bin Laden, that to remove the apostate regimes in the Islamic world you must first force, by violence, the disengagement of the West from the Islamic world.

Government Accounting Copies of reports and testimonies.
Government Coordinating Council  GCCs are comprised of representatives across various levels of government as appropriate to the security landscape of each CI/KR sector. Chaired by the designated Sector-Specific Agency (SSA), each GCC is responsible for ensuring appropriate representation on the council and providing cross-sector coordination with State, local, and tribal governments. These councils work with the Sector Coordinating Council (SCC) to plan, implement, and execute sufficient and necessary sector-wide security to support the Nation’s homeland security mission.

Guard:  Onsite security officer who comprises the response function in a physical protection system.  
www.asisonline.org, 2006

Guard Bar:  A series of two or more cross bars, generally fastened to a common back plate, to protect the glass or screen in a door.  
www.asisonline.org, 2006

Guard Plate:  A piece of metal attached to a door frame, door edge, or over the lock cylinder for the purpose of reinforcing the locking system against burglary attacks.  
www.asisonline.org, 2006

Hard Target:  A target, normally of political, military, economic or symbolic importance, that is protected by a range of physical security measures. These measures make it difficult (i.e. hard) for a terrorist to gain access to the target.  

Hazard Analysis:  A process for determining loss exposure and loss potential by comparing loss history against applicable standards.  

Hazard Control:  A means of reducing the risk due to exposure to a hazard. Such means may include: safety-guarding and interlocking of equipment; barricading of pedestrian and vehicular traffic routes; controlling exposure to toxic materials; and using hazard annunciators.  

High Explosive: An explosive with a rapid burning rate. On detonation, a high explosive will have a shattering effect on objects in the immediate area. TNT, RDX, nitroglycerin, dynamite, pentaerythritoltetranitrate, and various plastic explosives are types of high explosives. www.asisonline.org, 2006.

High-order Explosion: An explosion characterized by an extremely rapid combustion, known as detonation reaction, occurring through the action of high explosives. High-order explosions are those manifesting a velocity of detonation greater than 1000 meters per second. www.asisonline.org, 2006.

High Risk Target: A person, object or place which because of actual value, symbolic value, or relative isolation is more likely to be attractive or accessible to criminal action. www.asisonline.org, 2006.

Hijab: “Partition:” in modern or popular usage it means the head covering or veil worn by some Muslim women. JTAC Terrorism Report, June, 2007.

Hijacking: Taking control of a vehicle by the use or threatened use of force or intimidation; taking a vehicle by stealth, without the use or threatened use of force, in order to steal its cargo. www.asisonline.org, 2006.

Historical Logging: The chronological recording of system events such as places entered, by whom and when, alarm activations, and similar occurrences. www.asisonline.org, 2006.

Hollerith Card: A very early form of an access card. Small holes in the card are read by a light source or contact brushes. www.asisonline.org, 2006.

Homeland Infrastructure Threat And Risk Analysis Center (HITRAC) HITRAC is a DHS entity that conducts integrated threat analysts for all CI/KR sectors. HITRAC brings together intelligence and infrastructure specialists to ensure a complete and sophisticated understanding of the risks to U.S. CI/KR. HITRAC works in partnership with the U.S. Intelligence Community and national law enforcement to integrate and analyze intelligence and
law enforcement information on the threat. HITRAC also works in partnership with the SSAs and owners and operators to ensure its specialists integrate their expertise on infrastructure operations into its threat analysis. HITRAC coordinates very closely with security partners outside the Federal Government through the SCCs, GCCs, and ISACs to ensure its analytic products are relevant to security partner needs, and that they are accessible to the partners who need them.

**Homeland Security Advisor (HAS)**
State Homeland Security Advisors are responsible for overseeing all State homeland security activities, including the coordination of statewide efforts to detect, prevent, respond to, and manage the consequences of a terrorist attack or other critical incidents.

**Homeland Security Advisory Council (HSAC)**
The HSAC is a FACA committee that provides advice and recommendations to the Secretary on matters related to homeland security. The Council is comprised of leaders from State and local government, first responder communities, the private sector, and academia.

**Homeland Security Information Network (HSIN)**
The HSIN is a national communications platform that allows the flow of real-time information among DHS, State, local, and private sector partners at the Sensitive-but-Unclassified level. [www.dhs.gov/xinfoshare/programs/gc_1156888108137.shtm](http://www.dhs.gov/xinfoshare/programs/gc_1156888108137.shtm).

**Homeland Security Operations Center (HSOC)**
The HSOC serves as the Nation’s nerve centre for information sharing and domestic incident management – dramatically increasing the vertical coordination between Federal, State, territorial, tribal, local, and private sector partners. The HSOC collects and fuses information from a variety of sources everyday to help deter, detect, and prevent terrorist acts. Operating 24/7/365, the HSOC provides real-time situational awareness and monitoring of the homeland, coordinates incidents and response activities, and, in conjunction with the DHS Office of Information Analysis, issues advisories concerning threats to homeland security, as well as specific protective measures. The HSOC shares information on domestic incident management with Emergency Operations Centers at all levels through the Homeland Security Information Network (HSIN).
Homeland Security Presidential Directive 7 (HSPD-7)  
HSPD-7 establishes the basis for a national coordinated approach to critical infrastructure protection and identifies the 17 CI/KR sectors. The primary intent of HSPD-7 is to prevent the exploitation, incapacitation, or destruction of these infrastructures and resources. However, a secondary goal is to foster the development of methods and technologies that can minimize the impact if an adverse event actually occurs. Federal departments and agencies have been instructed to work with State and local governments, and with the private sector, to accomplish the objectives laid out in this directive.

Horizontal Sliding Window:  
A window with a moveable sash or glass that slides in a horizontal direction.  

Howler:  
An alarm annunciator that emits a howling sound.  

Hustling:  
Nonviolent means of making money illegally, such as theft, prostitution, pimping, drug selling, and conning.  

Hypergolic:  
Self-igniting, a characteristic of certain explosives in which detonation will result from a combining of chemicals contained in a bomb.  

Hypergolic Initiation:  
An explosion or sudden burning that results when two or more chemicals are combined and consequently react upon one another.  

IED:  
Improvised explosive device.  
*JTAC Terrorism Report, June, 2007.*

Implementation of National Maritime Security Initiatives  
Existing regulatory standards relating to Coast Guard requirements for natural gas facilities in their jurisdiction. Refer to 33 CFR Parts 2, 101 & 102.

Incident Command System (ICS)  
An organized approach to take charge of a critical incident and coordinate the response. Joint private/public sector planning established a smooth transfer of authority from the private sector to the public sector.
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident Commander</td>
<td>Public sector official, usually fire or police, in charge of coordinating resources and developing strategies to resolve the critical incident.</td>
<td><a href="http://www.asisonline.org">www.asisonline.org</a>, 2006.</td>
</tr>
<tr>
<td>Incident Management</td>
<td>Also termed “Case Management.” Incident Management refers to the processes, strategies, and methods followed by a Threat Management Team to (a) receive reports of behaviors requiring assessment, (b) assess the cases, (c) develop and implement an intervention strategy, and (d) monitor the case until final resolution is achieved.</td>
<td>Workplace Violence Prevention and Response Guideline, ASIS International, 2005.</td>
</tr>
<tr>
<td>Incident Management Team (IMT)</td>
<td>The private sector response team at the scene to resolve the critical incident. Also called Emergency Response Team (ERT).</td>
<td><a href="http://www.asisonline.org">www.asisonline.org</a>, 2006.</td>
</tr>
<tr>
<td>Information Security</td>
<td>The protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional; the effort or the result of a system of administrative policies and procedures established for identifying, controlling, and protecting information from unauthorized disclosure.</td>
<td><a href="http://www.asisonline.org">www.asisonline.org</a>, 2006.</td>
</tr>
<tr>
<td>Information Sharing and Analysis Center (ISAC)</td>
<td>Privately owned and operated, ISACs are information-sharing mechanisms that disseminate information to sector stakeholders, often to stakeholders who are paying members of the ISAC.</td>
<td></td>
</tr>
<tr>
<td>Information Sharing Environment (ISE)</td>
<td>The ISE is focused on sharing information related to terrorism, homeland security, and law enforcement.</td>
<td></td>
</tr>
</tbody>
</table>
ISE will be comprised of policies, procedures, and technologies linking the resources (people, systems, databases, and information) of Federal, State, local, and tribal entities and the private sector to facilitate terrorism information sharing, access, and collaboration.

InfraGard:  
InfraGard is a Federal Bureau of Investigation (FBI) program and is an effort to gain support from the information technology industry and academia for the FBI’s investigative efforts in the cyber arena. InfraGard and the FBI have developed a relationship of trust and credibility in the exchange of information concerning various terrorism, intelligence, criminal, and security matters.  
www.infragard.net.

Infrared Card Reader:  
A card reader that uses an infrared light source to read information encoded in an access card. It operates on an optical density principle.  

In-house Security:  
Protective services provided to a company by its own employees; a system of security in which there is an employer-employee relationship between the owner of the protected premises and the persons who provide the protection.  

Inside Perimeter:  
A line of protection adjacent to a protected area and passing through points of possible entry into the area, such as doors, windows, skylights, tunnels or other points of access.  

Insider Trading:  
The purchase and sale of corporate securities by one with “inside” “confidential” non-public” material information (i.e., that which can affect the value of a corporation’s securities). Generally, individuals with insider information can trade securities within a corporation so long as they are not doing so as a result of material inside information.  
2005 Fraud Examiners Manual (Canada)

Insurgency:  
The overt actions of a minority group within a state that is intent on forcing political change by means of propaganda, subversion and military pressure, aiming to persuade or intimidate the broad mass of people to accept such a change.  
Integrity Seals: A seal that provides clear evidence that it has been tampered with or illegitimately opened and whose forcible removal would result in the visible destruction of its essential parts. *Threat Advisory System Response (TASR) Guideline, ASIS International, 2004.*

Interior Zone: A protective zone established inside a perimeter zone. Also called a secondary zone. *www.asisonline.org, 2006.*

Internal Control: A plan of organization and all of the methods and measures adopted within a business to safeguard its assets, check the reliability and accuracy of its accounting data, promote operational efficiency, and encourage adherence to prescribed managerial policies. *www.asisonline.org, 2006.*

International Jihadist: Someone who joins an armed *jihad* taking place outside their country of origin. *JTAC Terrorism Report, June, 2007.*

International Criminal Police Organization (Interpol): An international law enforcement organization consisting of 138 member countries. Interpol, headquartered in Saint Cloud, France, enables communication among law enforcement organizations and provides assistance in both domestic and foreign criminal investigative matters. Each member country, a point of contact and coordination is established within some component of the national police in the capital city. The designated entity is known as the National Central Bureau (NCB). *www.asisonline.org, 2006.*

Interrogating Zones: Distance zones between the interrogator and a respondent which are regarded as being influential in the success or failure of an interrogation. *www.asisonline.org, 2006.*

Interstate Natural Gas Association of American (INGAA) INGAA is a trade organization that advocates regulatory and legislative positions of importance to the natural gas pipeline industry in North America. INGAA represents virtually all of the interstate natural gas transmission pipeline companies operating in the U.S. as well as comparable companies in Canada and Mexico. Its members transport over 95 percent of the nation’s natural gas through a network of 180,000 miles of pipelines. Foundation membership is made up of pipelines as well as suppliers of goods and services to
the pipeline industry. The primary activity of the Foundation is the sponsorship of studies aimed at unlocking the potential of natural gas as North America’s premium domestic fuel.


Intrusion Detection System
A system combining mechanical or electric components to perform the functions of sensing, controlling, and announcing unauthorized entry into areas covered by the system.


Intrusion Switches:
Accessible openings such as doors, windows, and skylights may be protected with intrusion switches. This type of sensor is composed of a two part electrical contact—one installed on the opening surface and the other installed on the fixed surface. When the opening surface, such as a door, is in a closed position, the two contacts provide a closed circuit so there is a continuity of current flow. When the opening surface is moved, the contacts separate, the circuit is broken, there is an interruption in the current flow, and an alarm is signaled.


Isolation Zone:
An area adjacent to a physical barrier, clear of all objects which could conceal or shield an individual.


Jihad:
“Struggle”; in the context of political action, jihad is the armed defense of Islam against aggression. Participation in jihad can take a number of forms, ranging from taking part in combat to providing logistical support. See also Global Jihad.


Key Control System:
Special cabinets, trays or enclosures that store keys in an organized system, and protect them from unauthorized removal.

www.asisonline.org, 2006

Key Run:
A patrol route having key stations. A security officer follows the route and uses the key at each station to record the check-in time.

www.asisonline.org, 2006

Key Station:
A place along a route followed by a security or fire patrol officer. The station has a key which when inserted
into the watchman’s clock carried by the officer will record the check-in time.

**Key System:**
Any variety of systems that provide control and accounting of mechanical keys that unlock doors. Typically in a large building or group of buildings; any system or program for controlling the keys and/or locking hardware of a facility. Control usually includes conducting initial and periodic inventories of existing keys, maintaining indexes or records that reflect persons holding keys, and maintaining a limited-access key storage facility.

**Keyless System:**
An access system that uses a keypad and an electric door strike. Pressing the correct sequential combination of push buttons on the keypad releases the lock to allow entry.

**Lacing Sensors:**
A network of very fine wire placed in a concealed fashion around a protected object or at a point of entry such as a skylight or cellar window. If the lacing is broken, an alarm results.

**Laminated Safety Glass:**
Glass consisting of two layers of plate bonded with a plastic interlayer. When smashed, glass pieces tend to remain connected to the interlayer reducing the hazard of flying glass.

**Laser Intrusion Detector:**
A sensor that activates upon detection of a break in a beam generated by a low-power reset.

**Layered Security:**
A physical security approach that requires a criminal to penetrate or overcome a series of security layers before reaching the target. The layers might be perimeter barriers; building or area protection with locks, CCTV and guards; and point and trap protection using safes, vaults, and sensors.

**Lever Lock:**
A key-operated lock that incorporates one or more lever tumblers, which must be raised to a specific level so that the fence of the bolt is aligned with the gate of the tumbler in order to withdraw the bolt. Lever locks are
commonly used in storage lockers, and safety deposit boxes.
www.asisonline.org, 2006

Lever Tumbler: A flat metal arm, pivoted on one end with a gate in the opposite end. The top edge is spring loaded. The bitting of the key rotates against the bottom edge, raising the lever tumbler to align the gate with the bolt fence. Both the position of the gate and the curvature of the bottom edge of the lever tumbler can be varied to establish the key code.
www.asisonline.org, 2006

Light Bulb Bomb: An incendiary device made by drilling a small hole in a light bulb and filling it with a highly combustible material. The light bulb is placed in a socket. When the light switch is activated, the electrical arc in the bulb will ignite the combustible.
www.asisonline.org, 2006

Liquefied Natural Gas (LNG)
Federal Safety Standards Existing regulatory standards, including security provisions, enforced by the Pipeline and Hazardous Materials Administration: (PMSA). Refer to 79 CFR Part 193, specifically subpart J.

Local Alarm: An alarm that is annunciated in the immediate vicinity of the protected premises.
www.asisonline.org, 2006

Lock Cartridge: The portion of a card reader that compares the information encoded on the card with the code contained on the program board.
www.asisonline.org, 2006

Loose Surveillance: Targets need not be kept under constant observation. The surveillance should be discontinued if the person becomes suspicious.
2005 Fraud Examiners Manual (Canada).

Lye Bomb: A non-exploding, homemade anti-personnel device consisting of a thin-glassed container filled with a liquid lye. It is designed to be thrown and to break upon impact, causing burns to the skin and eyes of the targeted persons.
www.asisonline.org, 2006

Magnetic and Electret Useful when a microphone needs to be close to the speakers and
Microphones: hidden inside something small. Electret microphones also provide good close range coverage. Both types of microphones are smaller than the standard carbon microphone, though they tend to offer a lower range of coverage. 
2005 Fraud Examiners Manual (Canada).

Magnetic Contacts: Intrusion detection device used on perimeter exit doors, building stairwell doors, doors leading to maintenance spaces, and doors inside tenant areas. 

Magnetic Stripe Card: A plastic card with a data-encoded stripe on one face. 

Mantrap: Used where a high degree of access control is required and egress is low. It is typically a vestibule with card reader controlled doors on both ends, so that when one door is open the other automatically locks. 

Manual Evacuation: The physical removal of people and property by hand to another, more secure location. 

Manual Override: A feature that allows for manual shutdown of an access control system during emergencies or in other circumstances not covered by automatic programming. 

Maritime Security – Vessels: Existing regulatory standards relating to Coast Guard requirements for natural gas facilities in their jurisdiction. Refer to 33 CFR Part 104.

Master Combination: A universal code for unlocking digital mechanical locks. It serves the same function as a master key. 

Master Key: A single key configuration that opens any number of differently keyed locks in a system. There may be more than one level of master key for a locking system, with each level corresponding to a given set of locks. 

Master Key System: A keying system in which a single key will operate multiple locks, each of which also operates with an individual change key. 
**Match Head Bomb:**
An explosive device consisting of match heads packed tightly into a fragmentable container, such as a short length of pipe capped at both ends and drilled to allow insertion of a fuse.


**Mechanical Explosion:**
A result of a gradual build-up of heat and pressure inside a vessel until the resistance of the vessel is shattered and there is a violent escape of gases or steam.


**Mechanical Lock:**
A locking mechanism that does not require any electrical or electronic circuitry to operate. A true mechanical lock uses springs and rotating cams to move the major parts and the latch bolt. Combinations of internal slides or tumblers allow the lock to open.


**Metal Detectors:**
Function by generating an electromagnetic field. If a metal object capable of conducting electricity, is introduced into the electromagnetic field, it disrupts the pattern of the field. The disruption is announced by sound and/or other indicators.


**Metal Foil:**
A thin strip of meal usually installed on glass. A break in the foil results in an alarm.


**Microwave Motion Detection:**
A means for detecting the presence of an intruder through the use of radio frequency generating and receiving equipment operating in the range of 1 GHz to 300 GHz. This type of device is one in a family of radio frequency motion detection devices, which are classified according to frequency.

**Mitigation:**
Prevention activities, control or containment, forward planning, or risk reduction, to eliminate hazards in advance or lessen their impact if an incident occurs.


**Mitigation Strategies:**
Implementation of measures to lessen or eliminate the occurrence or impact of a crisis.


**MOA:**
Memorandum of Agreement.

Monitoring Station: A term used to indicate the remote area at which guards or other personnel monitor the security system annunciators or alarm receivers. *Protection of Assets Manual, Volume I, 2001.*

Motion Detector: Passive, low-power, area-protection device that detects a change in ambient temperature caused by movements of a body or objects within a protected zone. Sensor circuitry generates an alarm when a moving object causes a change in a radiated energy pattern covering the protected zone. For example, an intruder moving into a protected zone would introduce a heat change caused by the intruder’s body heat. Also called passive infrared or PIR. [www.asisonline.org](http://www.asisonline.org), 2006.

Moving Coil Microphone: A moving conductor microphone in which the movable conductor is in the form of a coil. An electric output results from the motion of the coil in a magnetic field at an audio frequency rate. *Protection of Assets Manual, Volume II, 1998.*


Multilevel Security Mode: A mode of operation that provides a capability for various levels and categories or compartments of data to be concurrently stored and processed in an automated data processing system and permits selective access to such material concurrently by users who have differing access privileges and need-to-know rights. [www.asisonline.org](http://www.asisonline.org), 2006.

Mushroom Button: A knob or disk, shaped like a mushroom, which is typically used for emergency purposes such as to deactivate a malfunctioning alarm, shut off power equipment, or summon help. [www.asisonline.org](http://www.asisonline.org), 2006.

Mutual Aid Agreement: A pre-arranged agreement developed between two or more entities to render assistance to the parties of the agreement. *Business Continuity, ASIS, 2005.*

National Asset Database (NADB) Property of DHS, the NAB is an evolving and comprehensive catalogue of the assets, systems, and networks that make up the Nation’s CI/KR. The NADB contains descriptive information regarding CI/KR and is
the primary Federal repository for CI/KR information. Although the NADB is not a listing of prioritized assets, it has the capability to help inform risk-mitigation activities across the CI/KR sectors and government jurisdictions. The NADB provides a coordinated and consistent framework to incorporate and display the CI/KR data submitted by Federal, State, and local agencies; the private sector; and integrated Federal or commercial databases.

**National Association of Regulatory Utility Commissioners**

NARUC is a non-profit organization whose members include the governmental agencies that are engaged in the regulation of utilities and carriers in the fifty States, the District of Columbia, Puerto Rico and the Virgin Islands. NARUC’s member agencies regulate the activities of telecommunications, energy, and water utilities. NARUC’s mission is to service the public interest by improving the quality and effectiveness of public utility regulation. Under State law, NARUC’s members have the obligation to ensure the establishment and maintenance of utility services as may be required by the public convenience and necessity, and to ensure that such services are provided at rates and conditions that are just, reasonable and nondiscriminatory for all consumers.  


**National Communication System**

Within DHS, NCS is responsible for coordinating restoration of national security and emergency preparedness telecommunications services and facilities.

**National Cyber Security Division (NCSD)**

Within DHS, NCSD works collaboratively with public, private, and international entities to secure cyberspace and America’s cyber assets.

**National Incident Management System (NIMS)**

DHS developed NIMS so first responders from different jurisdictions and disciplines have the ability to work together better to respond to natural disasters and emergencies, including acts of terrorism. NIMS benefits include a unified approach to incident management; standard command and management structures; and emphasis on preparedness, mutual aid, and resource management.

**National Infrastructure Advisory Council (NIAC)**

The NIAC is a FACA committee that provides the President through the Secretary of Homeland Security
with advice on the security of the critical infrastructure sectors and their information systems. The council is composed of a maximum of 30 members, appointed by the President from private industry, academia, and State and local government.

**National Infrastructure Operations Center (NOC)**

The NICC is one of four sub-elements of the DHS National Operations Centre (NOC), which serves as the Nation’s hub for domestic incident management, operational coordination, and situational awareness. As a CI/KR-focused element of the NOC, the NICC, a 24/7/365 watch operations centre, provides a centralized mechanism and process for information sharing and coordination between the government, SCCs, GCCs, and other industry partners.

**National Infrastructure Protection Plan (NIPP)**

The NIPP provides a coordinated approach to CI/KR protection roles and responsibilities for Federal, State, local, tribal, and private sector security partners. The NIPP sets national priorities, goals, and requirements for effective distribution of funding and resources which will help ensure that our government, economy, and public services continue in the event of a terrorist attack or other disaster.

**National Pipeline Mapping System**


**National Response Plan (NRP)**

The NRP establishes a comprehensive all-hazards approach to enhance the ability of the United States to manage domestic incidents. The plan incorporates best practices and procedures from incident management disciplines – homeland security, emergency management, law enforcement, firefighting, public works, public health, responder and recovery worker health and safety, emergency medical services, and the private sector – and integrates them into a unified structure. It forms the basis of how the Federal government coordinates with State, local, and tribal governments and the private sector during incidents.

**National Security Telecommunications Advisory Committee**

The NSTAC is a FACA committee composed of up to 30 industry chief executives representing the major
communications and network service providers and information technology, finance, and aerospace companies. The NSTAC provides industry-based advice and expertise to the President on issues and problems related to implementing national security and emergency preparedness communications policy. Since its inception in 1982, the NSTAC has addressed a wide range of policy and technical issues regarding communications, information systems, information assurance, critical infrastructure protection, and other NS/EP communications concerns.

**Natural Disaster:**
A naturally occurring calamitous event bringing great damage, loss, or destruction such as tornadoes, hurricanes, earthquakes, and related occurrences. *General Security Risk Assessment Guideline, ASIS International, 2003.*

**Network:**
A series of connected nodes united by a common ideology or aim. These nodes can be individuals, cells, or organizations so long as they are linked in a significant manner e.g. a support network. *JTAC Terrorism Report, June, 2007.*

**Nuisance Alarm:**
A false alarm; an alarm caused by equipment failure or a fault not related to an actual criminal event. *www.asisonline.org, 2006.*

**Office of Domestic Preparedness Incident Protocol**

**Office of Domestic Preparedness Homeland Security Exercise & Evaluation Program**
HSEEP are both doctrine and policy for designing, developing, conducting and evaluating exercises. HSEEP is a threat and performance-based exercise program that includes a cycle, mix and range of exercise activities of varying degrees of complexity and interaction. HSEEP includes a series of four reference manuals to help states and local jurisdictions establish exercise programs and design, develop, conduct, and evaluate exercises. *www.ojp.usdoj.gov/odp/docs/hseep.htm.*
Office of Infrastructure Protection

Within DHS, OIP leads the coordinated national effort to reduce risk to our CI/KR posed by acts of terrorism. In doing so, DHS increases the Nation’s level of preparedness and the ability to respond and quickly recover in the event of an attack, natural disaster, or other emergency. OIP facilitates the identification, prioritization, coordination, and protection of CI/KR in support of Federal, State, local, territorial, and tribal governments, as well as the private sector and international entities. By ensuring the sharing of information with its security partners, OIP communicates threats, vulnerabilities, incidents, potential protective measures, and best practices that enhance protection, response, mitigation, and restoration activities across the Nation.

Oil and Natural Gas Sector Coordinating Council (ONGSCC)

A private forum for coordination of oil and gas security issues across the broad oil and natural gas sector. Involves a broad spectrum of industry associations and provides a forum for interfacing with corresponding Government Coordinating Council (GCC). Various SCCs serve as the government’s principal point of contact into each sector. Oil and Natural Gas SCC utilizes HSIN as a communication interface / tool.

Open Bomb:

Bomb in which all of the component parts are visible to the naked eye. Also called a straight bomb.  

Open Buildings:

Access is typically unrestricted at the building entry level. Tenants, building employees, and visitors proceed directly to their destination floor, via building elevators, where the occupier of that space determines the level of entry control and security.  

Open Circuit Alarm:

An alarm signal produced by opening or break in an electrical circuit. Also called a break alarm.  

Operative:

A person who assumes a false identity for the purpose of obtaining information, usually concerning a criminal activity that cannot be discovered through conventional law enforcement methods.  
**Optical Card:** A type of access card containing rows of spots of varying transparency. The relative passage of light through the pattern of spots forms a readable code. [www.asisonline.org](http://www.asisonline.org), 2006.

**Optical Turnstile:** A turnstile used in conjunction with a badge or card reader and a CCTV camera. The turnstile has two upright columns with a beam passing between them. After an authorized person has been cleared for entry by the reader, the person passes through the turnstile and breaks the beam. The breaking of the beam can activate another device such as a CCTV camera that alerts a security officer as to the entry. [www.asisonline.org](http://www.asisonline.org), 2006.

**Outer Continental Shelf Facility Security** Existing regulatory standard relating to Coast Guard requirements for natural has facilities in their jurisdiction. Refer to 33 CFR Part 106.

**Outside Perimeter:** A line of protection surrounding but somewhat removed from a protected area, such as a fence. *Protection of Assets Manual, Volume I, 2001.*

**Overt Surveillance:** The observation in plain sight of the public or of a specific surveillance target by police. This tactic is usually applied in high crime areas as a means for discouraging criminal behavior. [www.asisonline.org](http://www.asisonline.org), 2006.

**Palmgeometry Reader:** An access control device that optically scans the geometry of the hand. [www.asisonline.org](http://www.asisonline.org), 2006.

**Panic Alarm:** A sensor or other device which reports a panic or emergency situation. In commercial applications, a panic alarm is usually called a hold-up alarm. [www.asisonline.org](http://www.asisonline.org), 2006.

**Partnership and Outreach Division** Formerly the Infrastructure Partnerships Division (IPD) of DHS, POD manages the NIPP Senior Leadership Council; manages NIPP process; supports and coordinates sector partnerships, including SCC, GCC, CIPAC, and advisory councils; facilitates and coordinates private sector operational information sharing and Sector Coordinator activities, including the NICC; and manages PCII submission and dissemination.
Partnership for Critical Infrastructure Security (PCIS)  
PCIS is a non-profit organization formed in 1999 to address cross-sector critical infrastructure protection and interdependency issues of concern to critical infrastructure owners and operators.

Passive Infrared (PIR) Sensors  
Intrusion detection device used to protect perimeters, areas, and objects; heating, ventilating, and air conditioning air intakes; interior tenant areas; and building main exit doors (to facilitate automatic opening).

Percussion Bomb:  
An exploding device that detonates upon impact or when struck.

Perimeter:  
An outer limit, or boundary that protects another area.

Perimeter Alarm System:  
An alarm system used on the outermost boundary of a protected area. The perimeter can consist of a wall, fencing, or open space. Typical perimeter alarm systems incorporate magnetic control switches, foil, alarm screen, fence sensors, pressure alarms, and video detectors.

Perimeter Barrier:  
A physical barrier used on the outside of a protected area to prevent, deter, or delay unauthorized entry.

Permanent “Trash Marks”:  
Uniquely identifiable markings on copies are usually caused by accidental deep scratches and imperfections in the copier’s glass surface or document cover, in the printing element surface, or other permanent machine parts which are not readily replaced of changed during servicing of the machine. These marks can be reproduced on copies for years until the machine is repaired or the part replaced.
2005 Fraud Examiners Manual (Canada).

Physical Barrier:  
A barrier, either natural or structural, that provides protection to an area. For example, a natural barrier would be a river and a structural barrier would be a fence.

Physical Security:  
Security systems and architectural features that are intended to improve protection. Examples include
fencing, doors, gates, walls, turnstiles, locks, motion detectors, vehicle barriers, and hardened glass. 


**Piggyback:**
To slip through an electronically controlled access door by following closely behind a person that the system has allowed to enter. Also called tailgating.


**Pintumbler Lock:**
A lock consisting of a plug which rotates with the key to throw or withdraw a bolt. Surrounding the plug is the shell, a fixed assembly into which the plug fits. A series of pins fit into matching cylindrical holes in these two lock parts. With the key withdrawn, the pins extend through the surface between the plug and the shell so that the plug cannot turn. Insertion of the correct key lines up pins in such a way that the outer end of each one matches the surface separating the plug from the shell, so the plug can turn to withdraw the bolt.


**Pipe bomb:**
A short length of pipe capped at both ends and drilled at one end to accept a fuse, which is used to detonate an explosive contained inside the pipe.


**Pipeline Security Smart Practices**
TSA Corporate Security Review (CSR) Program onsite review document utilized by DHS TSA when evaluating natural gas company pipeline security programs. Also used to identify and share pipeline security smart practices observed throughout the industry.

**Plug-in Card:**
A machine-readable entry card with a printed circuit and an electric contact at one end. When inserted into a reader, electrical contact is made.


**Ponzi Operation:**
A confidence scheme in which money is collected from investors and part of it is paid back with high profits to encourage the early investors and others to increase their investments. When the total amount becomes substantial, the swindlers abscond with the investments. This form of fraud is similar to the pyramid scheme in which investors purchase distributorships and rights to sell lower-level distributorships. The scheme collapses when there are no more investors willing to buy in.

**Portable Detector System:** A complete detector system, easily transportable from one place to another. The system normally has provisions for a local alarm device, alarm lines, and automatic or manual resetting. *Protection of Assets Manual, Volume I, 2001.*

**Predatory Vandalism:** Willful destruction or defacement of property committed for material gain; destructive acts which produce some form of financial reward for the perpetrator. Breaking into a vending machine to steal coins would be an example. *www.asisonline.org, 2006.*

**Pressure Mats:** Type of detector that may be used in front of a door or strategically installed under carpeting or on stair treads. It is commercially available in the form of a flat mat designed to initiate an alarm when a weight of from five to twenty pounds per square foot is applied to the mat surface. *Protection of Assets Manual, Volume I.*

**Prevention Model:** A model, program, project, campaign, or similar organized effort aimed at the prevention of an undesirable activity, e.g., crime or drug abuse. *www.asisonline.org, 2006.*

**Probability:** The chance, or in some cases, the mathematical certainty that a given event will occur; the ratio of the number of outcomes in an exhaustive set of equally likely outcomes that produce a given event to the total number of possible outcomes. *General Security Risk Assessment Guideline, ASIS International, 2003.*

**Probable Maximum Loss:** The amount of loss a target of criminal attack would likely sustain in a single successful attack. *www.asisonline.org, 2006.*

**Progressive Surveillance:** A technique in which a subject is followed during a particular phase of his/her daily routine or during a specific period of time in one day. The surveillance is resumed on a later occasion at a phase or time when the previous surveillance was broken off. The several phases of surveillance constituting the subject’s full routine are examined for the intelligence data they provide within the context of the investigation. *www.asisonline.org, 2006.*
Proprietary Information: Information owned by a company or entrusted to it which has not been disclosed publicly and has value. Information is considered proprietary when (1) it is not readily accessible to others, (2) it was created by the owner through the expenditure of considerable resources, and (3) the owner sought to keep the information confidential.

Proprietary System: A system in which the alarm signal is relayed to a central location that is owned, manned and operated by the building proprietor (owner) or his agents. This term is also used to describe a system, component, technology or software package supplied by only one manufacturer.

Protected Area: An area continuously protected by physical security safeguards and access controls.

Protected Critical Infrastructure Information

Protected Critical DHS designed the PCII Program to encourage private industry to infrastructure share its sensitive security-related business information with the
Program (PCII):

Federal government. An information-protection tool, PCII facilitates information sharing between government and the private sector. DHS and other Federal, State and local analysts use PCII to focus primarily on: (1) analyzing and securing critical infrastructure and protected systems; (2) identifying vulnerabilities and developing risk assessments; and (3) enhancing recovery preparedness measures.

Protective Security Advisor (PSA) To better partner with State and local governments, as well as private sector businesses, DHS has placed a cadre of highly experienced security specialists in communities throughout the country to assist local efforts to protect critical assets and provide a local perspective to the national risk picture. These critical infrastructure and vulnerability assessment experts provide a federally funded resource to communities and businesses in an effort to assist in the protection of critical assets.

Punch-coded Card: An access control card having a specific pattern of punched holes.
Punches Card Reader: A reader that senses the holes in a punches card, transforming the data from hole patterns to electrical signals.


Readiness: The first step of a business continuity plan that addresses assigning accountability for the plan, conducting a risk assessment and a business impact analysis, agreeing on strategies to meet the needs identified in the risk assessment and business impact analysis, and forming Crisis Management and any other appropriate response teams.


Remote Station System: An alarm system in which the alarm signal is transmitted to a remote location operated by an independent party.


Retarding Transmitter: An alarm transmitter that delays transmission of an alarm signal for a predetermined time, usually seconds.


Reversed Gas Meter Theft of Service: Theft of gas service in which the gas meter is disconnected from the gas line piping and is remounted in a reverse configuration. The gas flowing backwards through the meter will cause the meter readings to operate in reverse.


Risk: The potential for damage to or loss of an asset. Risk, in the context of process security, is the potential for a catastrophic outcome to be realized.


Risk Analysis: A detailed examination including risk assessment, risk evaluation, and risk management alternatives, performed to understand the nature of the unwanted, negative consequences to human life, health, property, or the environment; an analytical process to provide information regarding undesirable events; the process of quantification of the probabilities and expected consequences for identified risks.

Risk Analysis Management for Critical Asset Protection (RAMCAP) A risk assessment methodology designed to allow comparative risk analysis within a single sector and across all 17 sectors. First, RAMCAP defines a common risk framework that the owners and operators of the nation’s critical infrastructure can use to assess terrorist risk to their own assets and systems.

Risk Assessment: Risk (R) assessment is the process of determining the likelihood of an adversary (T) successfully exploiting vulnerability (V) and the resulting degree of consequences (C) on an asset. A risk assessment provides the basis for the rank ordering of risks and thus establishing priorities for the application of countermeasures.


Risk Reduction: The practice of reducing criminal opportunity by reducing the exposure of an asset to the possibility of criminal attack.


Rotary Interlocking Dead Bolt Lock: A type of a rim lock in which the extended dead bolt is rotated to engage with the strike.


Salami Techniques: Involve the execution of unauthorized programs used to steal small amounts of assets from a large number of sources without noticeable reducing the whole.

2005 Fraud Examiners Manual (Canada).

Sally Port: Similar to a mantrap except it is large enough for a truck to drive into. At military posts, they are built of heavy reinforced chain link fencing or masonry. At a federal reserve bank, they are interior and are built to withstand a bomb.


Section 871 of the Homeland Security Act of 2002 (Sec. 871): Section 871 of the Homeland Security Act of 2002 provides the Homeland Security Secretary the ability to establish an advisory committee and exempt it from the Federal
Advisory Committee Act (FACA). Secretary Chertoff utilized his Section 871 authority in establishing the Critical Infrastructure Partnership Advisory Council.

Sector Coordinating Council (SCC): The counterpart to a CI/KR sector’s Government Coordinating Council (GCC), these councils are self-organized, self-led, broadly representative of owners and operators (and their associations) within the sector, and are focused on homeland security and critical infrastructure protection. SCCs serve as the government’s principal point of entry into each sector for developing and coordinating a wide range of CI/KR protection activities and issues.

Sector-Specific Agency (SSA): SSA refers to those Federal Departments and Agencies identified under HSPD-7 as responsible for the protection activities in specified CI/KR sectors. SSAs provide the subject matter and industry-specific expertise and relationships to help ensure infrastructure protection within the specific sectors.

Sector-Specific Plan (SSP): SSPs complement and extend the NIPP Base Plan and detail the application of the NIPP framework specific to each CI/KR sector. SSAs develop the SSPs in close collaboration with other public and private sector security partners.

Security Audit: The examination of a facility, a process, or the security program itself. A financial audit is an examination of those accounting records and practices which have material impact upon the financial condition of the enterprise. Also called security survey. www.asisonline.org, 2006.

Security Incident: A security-related occurrence or action likely to lead to death, injury, or monetary loss. An assault against an employee, customer, or supplier or company property would be one example of a security incident. General Security Risk Assessment Guideline, ASIS International, 2003.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Security Risk:</strong></td>
<td>A function of the consequences of a successful attack against an asset; coupled with the likelihood of a successful attack against that asset. <em>Security Vulnerability Assessment Workshop, AcuTech Consulting Group, 2006.</em></td>
</tr>
<tr>
<td><strong>Security Survey:</strong></td>
<td>Any of several methodological approaches for assessing a system’s vulnerability to loss or disruption by examining the separate criticalities of its components. A system is typically organization, facility, or process. Also called security audit. <em><a href="http://www.asisonline.org">www.asisonline.org</a>, 2006.</em></td>
</tr>
<tr>
<td><strong>Security Vulnerability:</strong></td>
<td>An exploitable capability; an exploitable security weakness or deficiency at a facility, entity, venue, or of a person. <em>General Security Risk Assessment Guideline, ASIS International, 2003.</em></td>
</tr>
<tr>
<td><strong>Security Vulnerability Assessment (SVA):</strong></td>
<td>A SVA is the process of determining the likelihood of an adversary successfully exploiting vulnerability, and the resulting degree of damage or impact. SVAs are not a quantitative risk analysis, but are performed qualitatively using the best judgment of security and safety professionals. The determination of risk (qualitatively) is the desired outcome of the SVA, so that it provides the basis for rank ordering of the security-related risks and thus establishing priorities for the application of countermeasures. <em>Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries, Second Edition, American Petroleum Institute (API), October 2004.</em></td>
</tr>
<tr>
<td><strong>Self-report Study:</strong></td>
<td>An investigation by means of a questionnaire or similar device in which the respondent is asked to indicate the nature, extent, and frequency of personal illegal behavior. <em><a href="http://www.asisonline.org">www.asisonline.org</a>, 2006.</em></td>
</tr>
<tr>
<td><strong>Sensitive Security Information (SSI)</strong></td>
<td>Federal regulations exist protecting certain transportation-related information records. Refer to 49 CFR Part 1520. SSI is a protection frequently used by DHS / TSA. <em><a href="http://www.tsa.gov/research/laws/regs/editorial_multi_image_with_table_0202.shtm">www.tsa.gov/research/laws/regs/editorial_multi_image_with_table_0202.shtm</a>.</em></td>
</tr>
<tr>
<td><strong>Sequential Card Reader:</strong></td>
<td>A reader that requires the use of a card plus the input of a sequential code at a keypad.</td>
</tr>
</tbody>
</table>
Sequential Switcher: A CCTV system feature that displays camera views in a predetermined order on a single monitor. The order and time of camera views may be programmed for automatic operation.

Shear Lock: An adaptation of the electromagnetic lock. The electromagnet is concealed in the header of the door frame and the armature is mounted in a channel in the top of the door.

Silent Alarm: A noiseless alarm transmitted from the scene of a hold-up, intrusion, or other emergency for the purpose of summoning help.

Single Entry System: An access control system that has anti-passback protection. It requires that a card used to enter an area be used to exit that area before it can be reused for entry. This prevents the “passing back” of an access card from an individual who has gained entry to one who has not.

Site Assistance Visits (SAV): Information derived from SAVs are used to create three series of Sector-specific reports that are disseminated to owners, operators, security planners and local law enforcement officials to integrate into their respective risk management processes. The Common Characteristics and Vulnerabilities reports highlight common issues so relevant stakeholders can address possible vulnerabilities and improve overall site security. Potential Indicators of Terrorist Attack reports give further insight to owners, operators, and law enforcement officials on how to better protect facilities and, in turn, thousands of Americans in surrounding communities. Protective Measure reports further identify categories of generally applicable protective measures, and recommend protective measures for implementation based on the Homeland Security Advisory System threat level.

Smart Card: Personal identification device. It is similar to a credit card or conventional ID card in that it contains an integrated circuit (IC). The card stores all the information needed to identify and permit access to the card bearer in its chip memory. The advantage of using
a smart card is the device validates itself when used in conjunction with the security system as a whole. *Protection of Assets Manual, Volume I, 2000.*

**Smurfing:**

The process of breaking transactions up into smaller amounts to **off Target:** A (normally civilian) target with limited or no physical protective security and therefore more vulnerable to a terrorist attack. *JTAC Terrorism Report, June, 2007.*

**Straight Bomb:**

See “Open Bomb”.

**Strike:**

A metal plate attached to or mortised into a door jamb to receive and hold a projected latch bolt and/or dead bolt in order to secure the door to the jamb. [www.asisonline.org](http://www.asisonline.org), 2006.

**Support Network:**

A network currently undertaking fundraising and logistics activity for other terrorist networks or cells (also known as a facilitation network). *JTAC Terrorism Report, June, 2007.*

**Surveillance:**

The observation of a location, activity or person(s), usually done secretly. [www.asisonline.org](http://www.asisonline.org), 2006.

**Systems Approach:**

A logical method for problem solving in which a comprehensive solution is developed in relation to a problem having several dimensions. A type of systems approach follows three general steps: assessment of vulnerability, implementation of countermeasures, and evaluation of effectiveness. [www.asisonline.org](http://www.asisonline.org), 2006.

**Tabletop Exercise:**

A test method that presents a limited simulation of a crisis scenario in a narrative format in which participants review and discuss, not perform, the policy, methods, procedures, coordination, and resource assignments associated with plan activation. *Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery, ASIS International, 2005.*

**Target of Opportunity:**

An entity that becomes available by chance. [www.asisonline.org](http://www.asisonline.org), 2006.

**Technical Security:**

Electronic systems for increased protection or for other security purposes including access control systems, card

**Tempered Glass:** Glass treated to resist breakage. It can be utilized for both safety and security purposes. Protection of Assets Manual, Volume I, 2002.

**Terrorism:** The unlawful use of force or violence against persons or property to intimidate or coerce a Government, the civilian population, or any segment thereof, in furtherance of political or social objectives. There are numerous types of terrorists groups including: separatists, nationalistic, eco, revolutionary, political, religious, social, domestic, and international. Federal Bureau of Investigation. http://www.fbi.gov/

**Testing:** Activities performed to evaluate the effectiveness or capabilities of a plan relative to specified objectives or measurement criteria. Testing usually involves exercises designed to keep teams and employees effective in their duties and to reveal weaknesses in the Business Continuity Plan. Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery, ASIS International, 2005.

**Threat:** Any indication, circumstance, or event with the potential to cause the loss of, or damage to an asset. Threat can also be defined as the intention and capability of an adversary to undertake actions that would be detrimental to critical assets. Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries, Second Edition, American Petroleum Institute (API), October 2004.

**Threat Assessment:** See ‘Violence Risk Assessment’

**Threat Management Team:** Also termed Incident Management Team. A Threat Management Team refers to the personnel designated within an organization to receive, respond to, and

**Top Officials Exercise Series (TOPOFFS)**

TOPOFF is a national-level, multi-agency, multi-jurisdictional, “real-time,” limited-notice WMD response exercise, designed to better prepare senior government officials to respond effectively to an actual terrorist attack involving WMD. Additionally, TOPOFF 4 involves law enforcement, emergency management first responders, and other non-governmental officials.

**Top Secret:**

A designation applied to information or materials the unauthorized disclosure of which reasonable could be expected to cause exceptionally grave danger to the national security. *www.asisonline.org, 2006.*

**Transportation Security Administration (TSA)**

Formed immediately following the tragedies of September 11, the TSA is a component of the Department of Homeland Security and is responsible for security of the nation’s transportation systems. With state, local and regional partners, the TSA oversees security for highways, railroads, buses, mass transit systems, pipelines, ports and the 450 U.S. airports. *www.tsa.gov, 2006.*

**Transportation Worker Identification Credentials (TWIC)**

Existing regulatory standards relating to Coast Guard requirements for natural gas facilities in their jurisdiction. Refer to 33 CFR Parts 101, 103, 104, 105, 106, & 125; 46 CFR Parts 10, 12, & 15.

**Trinitrotoluene (TNT):**

Highly explosive compound usually stable in its cast form. In colour it is cream or yellow and is commonly produced in half pound or one pound blocks. *www.asisonline.org, 2006.*

**Trouble Signal:**

In some building security systems, a differentiation is made between a break alarm and a cross alarm. Generally, the cross alarm is used to indicate intrusion or a dangerous condition; the break alarm indicates trouble, such as a broken line – more often found in fire alarm systems. Generally used to describe internal problems with the system, not a security alarm event. *Protection of Assets Manual, Volume I, 2001.*
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>U.S. Department of Homeland Security Operations Center</td>
<td>Serves as critical national centre for homeland security information sharing and domestic incident reporting. HSOC represents over 35 agencies and is staffed 24/7. The HSOC also includes the National Infrastructure Coordinating Center (NICC), which has primary responsibility for coordinating communications with the Nation’s critical infrastructure during an incident. <a href="http://www.dhs.gov/xnews/releases/press_release_0456.shtml">www.dhs.gov/xnews/releases/press_release_0456.shtml</a></td>
</tr>
<tr>
<td>United States Coast Guard (USCG):</td>
<td>The USCG is a military branch of the United States involved in maritime law, mariner assistance and search and rescue, among other duties of coast guards elsewhere. Its stated mission is to protect the public, the environment, and the United States economic and security interests in any maritime region in which those interests may be at risk, including international waters and America’s coasts, ports, and inland waterways.</td>
</tr>
</tbody>
</table>
| **United States Computer Emergency Readiness Team** | Established to protect the nation’s Internet infrastructure, US-CERT coordinated defense against and responses to cyber attacks across the nation.  
*www.us-cert.gov.* |
|---|---|
| **Vehicle Checkpoint:** | A location at which the identity and contents of inbound and outbound vehicles can be determined before they are permitted to proceed.  
| **Vibration Sensor:** | A sensor pre-set for a degree of vibration which if exceeded will cause an alarm to be given. It is commonly used for door and window protection.  
*www.asisonline.org, 2006.* |
| **Video Motion Detector:** | A sensor that sends an alarm signal when the electrons on the face of a closed circuit television camera tube are excited by an object moving into the field of view or a designated portion of the field of view. This system allows the operator immediate viewing of the act causing the alarm.  
*www.asisonline.org, 2006.* |
| **Vindictive Vandalism:** | Results from the actions of an individual or group that was motivated to express antagonism or hatred toward an individual, group, or institution.  
| **Violence Risk Assessment:** | Also termed a “Threat Assessment.” A Violence Risk Assessment refers to the investigative and analytical process followed by a specifically qualified professional to determine the nature of the threat and level of risk of violence presented by an individual and the steps to be taken to mitigate the risk.  
| **Vulnerabilities:** | Any weakness that can be exploited by an adversary to gain access to an asset. Vulnerabilities can include but are not limited to building characteristics, equipment properties, personnel behavior, locations of people, equipment and buildings, or operational and personnel practices.  
Vulnerability Analysis: A method of identifying the weak points of a facility, entity, venue, or person. [www.asisonline.org], 2006.

Wafer Tumbler Lock: A lock that utilizes flat tumblers fashioned of metal or other material to bind the plug to the shell. A properly designed key raises the wafers out of the lower portion of the shell until they are all contained within the plug, thus creating a shear line, with the plug free to turn inside the shell. *Protection of Assets Manual, Volume I, 2002.*

Walk Test: Walking through an intrusion detection sensor’s expected detection zone to determine if it is functioning properly. [www.asisonline.org], 2006.

Wanton Vandalism: This type of vandalism can range from damage resulting from the simple play of children to the spontaneous destruction by individuals or groups. Excitement and fun are the main motivating factors. *Protection of Assets Manual, Volume IV, 2006.*

Warded Lock: A lock exemplified by the see-through keyway and the long, barrel-like key. The greatest weaknesses of this type of lock are its vulnerability to spring manipulation by any key that is not stopped by the wards and corrosion due to weathering and age. *Protection of Assets Manual, Volume I, 2002.*

Weapons of Mass Destruction (WMD): Any destructive device that is intended or capable of causing death or serious injury to a large number of people through the release, dissemination, or impact of toxic or poisonous chemicals or their precursors, disease-causing organisms, radiation or radioactivity, or conventional explosives sufficient for widespread lethality. [www.asisonline.org], 2006.

Workplace Violence: A broad range of behaviors falling along a spectrum that, due to their nature and/or severity, significantly affect the workplace, generate a concern for personal safety, or result in physical injury or death. *Workplace Violence Prevention and Response Guideline, ASIS International, 2005.*

Worm: Self-replicating program which resides as a file on a system, executes an autonomous process, and deliberately moves from system to system. It looks for
other nodes on the networks, copies itself to them, and causes the self-copy to execute on other nodes. 
*2005 Fraud Examiners Manual (Canada).*

**X-ray Bomb:**

A bomb triggered to explode when exposed to x-rays. 

**Zoning:**

The process by which a protected building is divided into areas or zones. Any alarm-initiating device in a given zone can be arranged to sound an identifying code and/or indicator on an annunciator, the area of the emergency. 