



Physical Security Plan

CONFIDENTIAL AND PROPRIETARY

This document is the property of Peoples Natural Gas (PNG). It contains information that requires protection against unauthorized disclosure. The information contained herein shall not be released to the public or other personnel who do not have a valid need to know without the prior approval of an authorized representative of PNG. At a minimum, this document shall be disseminated only on a need to know basis and, when unattended, will be stored in a locked cabinet or area offering sufficient protection against inadvertent access and unauthorized disclosure.

December 2021

Table of Contents

Purpose of plan	2
Promulgation of plan	2
Physical Security Team organization chart and team roster	4
Plan Process – Triggers and event assessment.....	5
Plan Process – Physical Security alert levels and team conference calls.....	6
Plan Process – Incident Management Plans – Manager activation process.....	8
Plan Process – Using ARCOS to activate Incident Management Plans	10
Plan Process – Decision making and communication.....	11
Plan Process – Team position descriptions and typical task lists.....	12
Physical Security Manager.....	12
General Counsel.....	13
Safety Officer.....	14
Communications Officer.....	15
Regulatory Officer	17
System Operations Coordinator	18
Operations Services Coordinator	19
Operations Coordinator.....	20
Customer Services Coordinator	21
Information Technology Coordinator	22
Human Resources Coordinator	23
Administration and Finance Coordinator.....	24
Appendices	25
PSP-1 – Existing Physical Security procedures	26
PSP-2 – Normal Security Level procedures.....	32
PSP-3 – Elevated Security Alert procedures.....	33
PSP-4 – Imminent Security Alert procedures	34
PSP-5 –Conference Call/Meeting Initiation Protocol	35
PSP-6 – Physical Security Team Conference Call agenda.....	36
PSP-7 – Elevated and Imminent Security Alert tasks check list.....	41
PSP-8 – Responding to the media	42
PSP-9 – Media activity log.....	43
PSP-10 – Communications Officer Hotwash.....	44
PSP-11 – Bomb threat procedures and call form	45
PSP-12 – Intruder on property procedures	47
PSP-13 – Facility and corresponding law enforcement contacts	49
PSP-14 – Facility internal contact list	53
PSP-15 – Physical Security Team contact list.....	55
PSP-16 – Physical Security Plan Testing Certification.....	57

Purpose of the Physical Security Plan

Peoples Natural Gas (PNG) Security Plan is intended to be a guide for all employees in reference to security measures for facilities and employees, as well as designating a Security Team that will be responsible for all aspects of the plan. For the purpose of this plan, security encompasses:

- Physical security of all areas, buildings and other structures.
- Identification of critical company facilities
- Specific triggers to activate a higher level of the security plan
- Proactive actions to be taken during Elevated and Imminent security situations
- Team member descriptions, typical tasks, and team conference call agenda

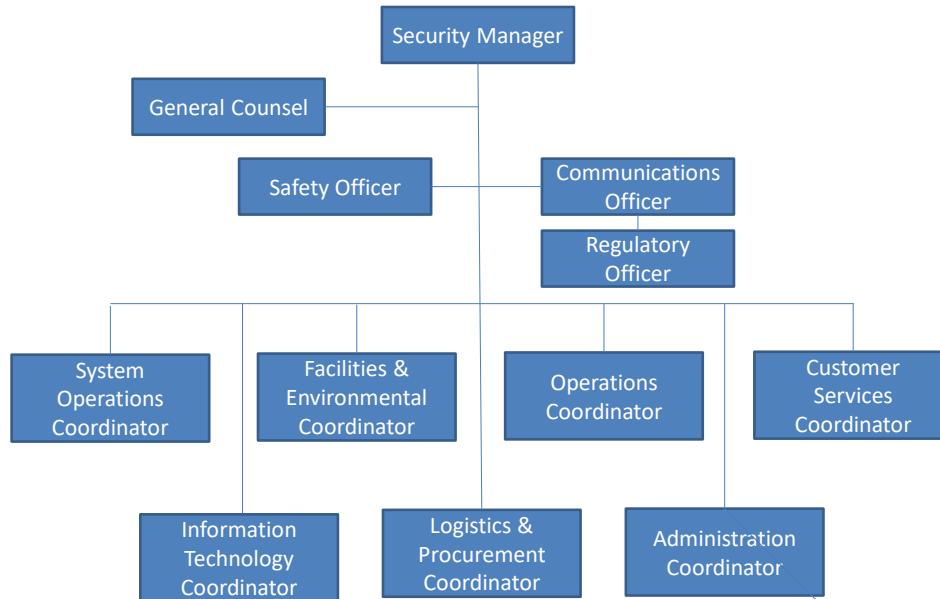
Promulgation for Physical Security Plan

- The Physical Security Plan was last updated November 2019.
- The Physical Security Plan should be exercised once a year no later than Dec. 15
- Changes to the plan should be tracked using the chart below

Document Revision History		
Date	Approved by:	Description
5-04-2016	Nagy Nagiub	Updated Plan Owner and Team Roster
7-15-2016	Nagy Nagiub	Updated plan due to reflect new organization structure, employee retirements, and shop consolidation
2-17-2017	Nagy Nagiub	Updated plan to include items as recommended by external counsel. These is include addition of General Counsel and Regulatory Officer positions
7-27-2017	Nagy Nagiub	Updated Plan to reflect organizational changes and PNG personnel and facility information
1/23/2018	Nagy Nagiub	Miscellaneous updates
12/7/2018	Nagy Nagiub	Updated plan to include plan manager activation process, GETS/WPS process, organizational changes and miscellaneous updates
11/4/2019	Nagy Nagiub	Miscellaneous updates, add ARCO activation process
4-1-20	Mark Pietrone	Update Physical Security Plan organization and miscellaneous updates
12-6-21	Mark Pietrone	Miscellaneous updates

Plan Owner: Mark Pietrone

Physical Security Team Organization Chart



Physical Security Team Roster

Position	Representative	Representative	Representative
Physical Security Manager	Mark Pietrone	Andy Rockwell	William Schade
General Counsel	Mike Turzai	Bill Roberts	Jennifer Petrisek
Safety Officer	Chad Ravotti	Jared Long	Paul Pantages
Communications Officer	Barry Kukovich	Erin O'Donnell	Jackie Ziemianski
Regulatory Officer	Bill Roland		
System Operations Coordinator	Ron Ferrere	Johnetta Ryan	TBD
Facilities & Environmental Coordinator	William Schade	Andy Rockwell	TBD
Operations Coordinator	Paul Becker	Randy Ciotola	Ralph Comito
Customer Services Coordinator	Heather Doyle-Conley	Michelle Parks	Lisa Reilly
IT Coordinator	Kevin Turkovich	Nagy Nagiub	Joe Brado
Logistics & Procurement Coordinator	Andy Rockwell	Katie Saulsbery	Ryan Milko
Administration Coordinator	Karen Worcester	Dave Hershberger	John Oravec

Plan Process – Triggers, Event Levels, and Position Task Lists

Specific Triggers for Activation of Plan

- Bomb threat (See Appendix PSP-11)
- Unauthorized access to PNG facilities (buildings, compressor stations, regulator stations, city gate stations, mainline valves and pipeline junctions, and SCADA sites)
- Terrorist threat or attack/sabotage
 - Utilize the **National Terrorism Advisory System (NTAS)** to trigger. The NTAS has two levels, *Elevated Threat Alert* and *Imminent Threat Alert*.
 - An *Elevated Threat Alert* warns of a credible terrorist threat
 - An *Imminent Threat Alert* warns of a credible, specific and impending terrorist threat

Physical Security Event Assessment

The nature and severity of the security event must be evaluated to determine the required response, coordination and resources required. Assessment of a security event is based upon:

- Employee and public safety
- Operational impact
- Geographic areas involved
- Facilities affected
- Critical infrastructure affected

Plan Process – Triggers, Event Levels, and Position Task Lists

Physical Security Alert Levels

Security events are classified into three levels – Normal, Elevated and Imminent – and should be classified based on the security event assessment below.

Security Event Level	Description Examples
Level I – Normal – Usual daily activities continue with no extraordinary measures taken. (Appendix PSP-2)	Report of vandalism to the security fencing that surrounds a compressor station.
Level II – Elevated – Physical Security Team activated; procedures for Elevated level implemented (Appendix PSP-3) as necessary.	Dept. of Homeland Security threat level is raised to the <i>Elevated Threat Alert</i> . Reports of multiple bomb threats to company facilities received.
Level III – Imminent – Physical Security Team activated; procedures for Imminent level implemented (Appendix PSP-4) as necessary. Incident Command and/or Business Continuity Teams also activated.	Dept. of Homeland Security threat level is raised to the <i>Imminent Threat Alert</i> . Multiple compressor stations / facilities have been compromised.
Return to Normal – Once the Physical Security event has been rectified, or the Department of Homeland Security has lowered its threat level to normal, the Physical Security Manager should hold a final conference call to wrap up the event and return the company’s security event level to normal.	

Physical Security Team Conference Calls and Agenda

Once the Physical Security Team has been activated, the Physical Security Team Manager should schedule a conference call with all team members. The number for the conference call is x7950 (internal) or 1-800-499-1133 (external) with the passcode 418005. Each team member should be alerted to this call via telephone and email. The Physical Security Team Manager should use the agenda (Appendix PSP-6) of this plan as a guideline for leading the calls, and use the gathered information as a resource to manage and memorialize the event.

Employee Alerts and Updates

When necessary, employees will receive a text message alerting them an event has occurred and providing notification where to go for more information. Also, the employee hotline (800-499-1188) will be updated as necessary during an event.

Government Emergency Telecommunications Service (GETS) and Wireless Priority Service (WPS) Access

GETS provides priority land line access, and WPS provides priority cellular service to our organization. Utilities, such as PNG can use this access in emergency situations where cellular and land line communication is congested, particularly the first 24-72 hours following an event.

GETS and WPS are companion services for priority calling offered by the Office of Emergency Communications (OEC). Key Incident Management Team Members in the PNG organization hold GETS/WPS cards and are authorized to use them in an emergency. A GETS/WPS service card is a single card that contains all the information and instructions needed for making a call during an emergency situation. Mark Steve is our point of contact person (POC) for this program.

Incident Management Plans - Manager Activation Process

Incident Manager Activation:

When an event occurs, the Incident Manager will be notified by either the Operations Center, or one of the plan managers.

Operations Center Notification:

When a call is received by control room personnel, the person taking the call/report will record the information on Incident Management Event Initial Report Form. They will then notify the Incident Manager (Using the call information on the form). The Incident Manager will then decide if a plan needs to be activated, and will contact the appropriate plan manager who will then activate their plan.

Incident Manager Notification from a Plan Manager:

When an event occurs and a plan manager is aware of the situation and feels it is necessary to immediately activate their plan, they may self-activate, and then notify the Incident Manager.

Business Continuity, Cyber Security, Physical Security and Emergency Plan Manager Activation:

Plan managers and their plans can either be activated by the Incident Manager, or can self-activate if the situation warrants. In the event of a plan manager self-activation, he or she must notify the Incident Manager that their plan has been activated.

Separation of Manager Roles When More Than One Plan is Activated:

When an individual plan has been activated and the need arises to then activate the Incident Manager, the following procedure will be used to ensure effective separation of duties.

If the current activated plan manager is also the primary or first to be contacted Incident Manager, he or she should assume the Incident Manager role and then transfer the current plan manager responsibilities to the next in line person for the currently activated plan. Alternatively, the Incident Managers can also discuss, and then decide the best course of action for filling the roles.

Incident Manager/Plan Manager Activation Scenarios

Incident Manager Activates Plan Manager



Plan Manager Self Activation



Using ARCOS to Activate Incident Management Teams

When a plan manager needs to activate a specific Incident Management team (Incident Management, Business Continuity, Cyber Security, Physical Security or Emergency Response), the plan manager has the option of using the ARCOS callout system to quickly call all team members at once. The plan manager will call the Operations Center at **1-800-764-0686** and:

- Tell them which team(s) needs to be mobilized
- Provide the message to be delivered
- Instruct the agent to send the message to all recipients via automated phone call AND email
- If scheduling a meeting or conference call, instruct the agent to send an email to the plan manager with a Response Report indicating which team members plan to participate

Please note, the Business Continuity team has two rosters in ARCOS:

- Business Continuity Core Team
- Business Recovery Leads

Decision Making and Communication

When directing incident response activities, the Managers of the Emergency Response, Business Continuity, Cybersecurity, and Physical Security plans must escalate any decisions beyond their authority to the Incident Manager, who will consult with the executive team. The executive team consists of the CEO and his/her direct reports, and should be consulted with on the following types of matters:

- Life safety of employees, customers, and suppliers
- Financial loss in excess of \$250,000
- Loss of sensitive data
- Extended service outage
- Legal liability
- Regulatory violation
- Harm to the Peoples brand image
- Public announcements
- Incidents deemed reportable to federal, state, or local authorities

Decisions will be made by the CEO in consultation with his/her direct reports. All decisions, directives, communications to employees will flow from the CEO to the Incident Manager and then to the relevant plan Managers. The Managers will inform their teams. In situations where actions need to be taken by employees who are not members of one of the response teams, the appropriate Coordinator will communicate the directive to the relevant functional manager within the organization. This information flow can take the form of face-to-face discussions, phone calls, conference calls, emails, recorded messages on the Employee Emergency Hotline and PeoplesPlace, depending on the nature and urgency of the message.

Physical Security Manager Position Description and Typical Tasks List

The Physical Security Manager is responsible the overall management of the Physical Security Plan during a security incident, which includes activation of the plan, assignment of tasks to team members, communication with the Incident Manager and company senior management, and coordination of all recovery efforts.

Tasks:

- Activation of the Physical Security Plan and as-required team members based on security event levels
- Assignment of recovery activities and efforts for all team members
- Coordination of security measures as needed
- Communication with Incident Manager and senior management on event status and any unusual events
- Communication with all pertinent outside agencies (Department of Homeland Security, state and local law enforcement, PEMA) as to event status within the company
- Schedules and facilitates all conference calls (or in-person meetings) with Physical Security Team members
- Maintain an event log of each event
- Conduct a post-event Hotwash with team members leading to a “Lessons Learned” review.

General Counsel

Position Description and Typical Tasks List

The General Counsel, reporting to the Incident Manager, is responsible for working with the entire team to understand the nature of the event, monitoring and evaluating all activities for legal implications, and advising the Incident Manager on actions to be taken to ensure the Company's legal interests are protected.

Note: In events where more than one emergency plan is activated, and the Incident Manager is actively prioritizing and coordinating the activities of resources across multiple plans, the General Counsel reports to the Incident Manager so they can advise on legal-related matters across all active plans.

Typical Tasks:

- Act as an advisor to the Incident Manager during an event
- Ensure appropriate use of the attorney-client privilege to protect PNG's interests during investigation and remediation efforts in response to an incident, including the ability to protect communications with and the deliberations of the executive team
- Advise when to interact with law enforcement, and manage the interaction with law enforcement to avoid unintentionally exposing PNC to liability
- Advise of any federal, state and regulatory notification laws that may be implicated by a breach
- Advise of any regulatory reporting obligations
- Ensure availability of insurance coverage and advise of steps necessary to preserve coverage
- Advise of contractual obligations PNG may owe third parties as a result of an incident
- Assess PNG's various legal and contractual obligations to its employees
- Assess whether third parties may be legally obligated to PNG as a result of an incident

Safety Officer

Position Description and Typical Tasks List

The Safety Officer is responsible for monitoring and evaluating all operations for hazards and unsafe conditions, and developing measures for assuring all personnel and the public are safe during the event.

Note: In events where more than one emergency plan is activated, and the Incident Manager is actively prioritizing and coordinating the activities of resources across multiple plans, the Safety Officer reports to the Incident Manager so they can advise on safety-related matters across all active plans.

Tasks:

- Acts as an advisor to the Physical Security Manager and employees on all safety related matters during a physical security incident
- Conducts in-house and field safety inspections during an event, as necessary
- Monitors any hazardous materials clean-up, and assists the Process Manager, Environmental in compiling the necessary forms related to the spill/clean-up
- Records and reports on any injuries to or deaths of employees or the general public that are related to the Physical Security event
- Maintains logs of any safety incidents and hazardous material events

Communications Officer Position Description and Typical Tasks List

The Communications Officer is responsible for communicating event status as the primary corporate spokesperson – both internally and externally – to necessary stakeholders, which might include:

- Local, regional and national media outlets (radio, TV, newspaper)
- Statewide emergency management agencies (PEMA, PUC)
- PNG’s call center representatives
- Other internal stakeholders (Government Relations, large customer representatives, etc.)

Further, the Communications Officer is responsible for the oversight of updating the company’s digital platforms, including Twitter, Facebook, email as well as the external company website. Regardless of the outlet, care should be taken to make sure the company – via the Communications Officer – is following a “one message, one voice” system, to ensure incident updates are consistent across all mediums, balancing the need to provide information to internal and external stakeholders, while also protecting the integrity and reputation of the company.

Note: In events where more than one emergency plan is activated, and the Incident Manager is actively prioritizing and coordinating the activities of resources across multiple plans, the Communications Officer reports to the Incident Manager so they can advise on communications-related matters across all active plans.

Typical Tasks:

- Gather necessary information from the Physical Security Manager
- Coordinate regulatory activity (With the Regulatory Officer)
- Coordinate responses to media inquiries. Prepare press releases, email updates, Social media, internal communication updates in a timely manner (Appendix PSP-8)
- Act as the primary company spokesperson
- Coordinate all internal communications, including sending company-wide text messages and updating the employee hotline when necessary.
- Establish a presence at the site of incident as necessary
- Establish a media briefing area as necessary. If multiple agencies are involved in the incident, the Communications Manager should work with peers to develop messaging
- Receive approval of all internal and external communications from the Physical Security Manager
- Monitor and report media activities to the Physical Security Manager

- Attend all update meetings/calls held during the incident
- Create and manage a media contact list
- Maintain a media activity log (Appendix PSP-9) and perform a hotwash after the event (Appendix PSP-10)
- Monitor and report digital/social media conversations to the Physical Security Manager

Regulatory Officer

Position Description and Typical Tasks List

The Regulatory Officer is responsible for working with the entire team to understand the nature of the event, communicating with Federal, State and Local Officials and Regulators during an event, including:

- State Governors' offices
- State Representatives and Senators and their staffs
- City and county officials and their staffs
- State Public Utility Commissioners and their staffs
- Local municipalities

To ensure consistent messaging during and after an event, the Regulatory Officer reports to the Communications Officer.

Note: In events where more than one emergency plan is activated, and the Incident Manager is actively prioritizing and coordinating the activities of resources across multiple plans, the Regulatory Officer reports to the Incident Manager so they can advise on regulatory-related matters across all active plans.

Typical Tasks:

- Provides updates to State Public Utility Commissions
- Responsible for real time communication with elected officials
- Coordinates regulatory messaging with the General Counsel when necessary
- Keeps PNG regulatory staff updated with all pertinent event information and activities

During and after an event, provides assistance as needed in the filing of regulatory reports

System Operations Coordinator Position Description and Typical Tasks List

The System Operations Coordinator is responsible for oversight of all operations control room and field dispatch activities as they relate to a physical security event. This position is the main liaison between the Physical Security Manager and the control rooms, providing information on the status of the gas system as it relates to the physical security event.

Tasks:

- Monitors all gas system activities and reports information to the Physical Security Manager
- Advises Physical Security Manager on remediation options if critical gas nodes have been affected by a physical security event
- Works closely with IT Coordinator in monitoring SCADA and other operations related technology systems
- Liaison to the Customer Operations Center
- Maintain an activity log

Facilities & Environmental Coordinator Position Description and Typical Tasks List

The Facilities & Environmental Coordinator is responsible for all facilities and environmental activities during a physical security event, which could include repair and/or replacement of existing security measures (card readers, fencing, etc.), acquisition and/or placement of physical barriers, security related needs and any other facilities needs that arise during a physical security event.

Tasks:

- Monitor and facilitate any repairs/replacements to existing security measures (fencing, card readers, etc.)
- Purchase and/or facilitate placement of physical barriers at site as necessary
- Ensures that all mail, package delivery and materials delivery are appropriately monitored during a physical security event
- Coordinates all environmental issues during a security event
- Coordinate any security contractor activities

Operations Coordinator

Position Description and Typical Tasks List

The Operations Coordinator is responsible for leading the direction of all field employees and offices during a physical security event. Based upon the security threat level, and the location of the event, the Operations Coordinator may be responsible for assignment of field workers to patrol critical sites and report any suspicious activities/damage.

Tasks:

- Work with Operations' senior management to direct activities of field offices/personnel during a physical security event
- Coordinate communication with field offices/personnel during a physical security event
- Direct field personnel to patrol critical sites and report suspicious activities or damage
- During an event, coordinates all construction, engineering, compression and reliability issues and communication

Customer Services Coordinator Position Description and Typical Tasks List

The Customer Services Coordinator is responsible for the oversight of the company's call center and call center representatives during a physical security event. Working in close conjunction with the Communications Officer, the Customer Services Coordinator will assist in the dissemination of incident updates that are to be used by the CSRs when customers call with questions related to a physical security event.

Tasks:

- Work closely with Communications Officer in designing verbiage for the CSRs to disseminate to customers during a physical security event
- Assure that CSRs follow the developed script for answering calls related to the physical security event
- Notify Physical Security Manager and Communications Manager of any pertinent information that is received from customers

Information Technology Coordinator Position Description and Typical Tasks List

The Information Technology (IT) Coordinator is responsible for leading all information technology activities during a physical security event, as well as activation of the IT Cyber Security Plan as needed.

Tasks:

- Support all departments with IT needs during a physical security event
- Activate the company's IT Cyber Security Plan as needed

Logistics and Procurement Coordinator Position Description and Typical Tasks List

The Logistics and Procurement Coordinator is responsible for all HR and benefit activities during a physical security event.

Tasks:

- Monitor and facilitate any transportation needs during an event
- Monitors and orders materials for field crews as needed
- Contact any appropriate vendors to advise them of the situation
- Facilitate any lodging needs

Administration Coordinator Position Description and Typical Tasks List

The Administration Coordinator is responsible for all financial, legal, human resource and other administrative support related activities during a physical security event.

Tasks:

- Work with accounting and finance departments to assure availability of funds for emergency purposes
- Work with accounting and finance departments to track all expenditures during event
- Track and report on all insurance related activities
- Work with legal and regulatory departments to collect necessary information on the event for regulatory reporting requirements
- Manage all injury/fatality notifications to employee families
- Oversee all temporary hiring as needed during event
- Oversee the implementation of employee counseling services as needed
- Other human resources activities as needed

Appendices

Appendix PSP-1 –Existing Physical Security Procedures

The company has implemented the following security measures organized by the categories of personnel, materials, and vehicles for its critical sites. Additional security measures are also discussed.

North Shore Headquarters (All Buildings)

1. Personnel Access – Employees that work in either of the North Shore Headquarters (HQ) gain access through swipe cards that activate electric door switches at all entrances to the buildings. The Facilities and Security group issues the swipe cards and control the days and hours that access is permitted for each employee. Access is further restricted within the HQ buildings to the Computer Rooms. Only those employees responsible for the operations of these functions have access to these rooms. The same key card is used and controlled by the Facilities and Security group.

All field (non HQ) employees, some contractors and delivery personnel are permitted access to the buildings by the guard during normal business hours. All vendor and contractor personnel and other visitors are required to show photo identification and sign the guest register at the security desk.

2. Material Control – Mail from the post office, deliveries from overnight mail services, and office supplies are the primary materials coming into the building. Any package that looks suspicious is brought to the attention of the guard in the building lobby and if necessary referred to law enforcement personnel.
3. Vehicle Control – Parking is available in public lots near the buildings. Access to the parking lots is by pass or by daily payment. The company does not control these lots.
4. Additional Safety Measures
 - a. Protective lighting illuminates the parking lots and the exterior of the buildings. If any employee sees a safety risk at any time the guard in the building lobby should be alerted to take action.
 - b. An emergency generator is located in each office building. The generator automatically starts and provides electrical service for the Data Room if the commercial power fails. The generator is driven by a natural gas engine with unlimited fuel supply. Emergency lighting is provided by building management.
 - c. Smoke detectors are located through-out the building. If one of these devices activates, fire alarm bells located on each floor send an alarm to the employees to evacuate the building. The alarms are also connected directly to fire department.
 - d. Emergency battery lighting is installed in each building and activates whenever the commercial power is interrupted.

District Offices/Shops

1. Personnel Access – Access to most locations requires a company swipe card that will unlock the building doors and unlock the fence gates. The building doors are locked at all times when company personnel are not present. The fences are also to be locked during the day and locked after normal working hours.

All field employees, vendors, contractors, delivery service personnel and customers are permitted access to the building by office employees during normal business hours. All vendor and contractor personnel and other visitors are required to show photo identification. These visitors are escorted through the building by Peoples employees.

2. Material Control – Materials and equipment related to maintaining the gas pipelines and associated facilities are delivered from outside vendors. Overnight delivery services bring packages to the facility and US mail is delivered by a post office employee or picked up at a post office box.

Materials leaving the shops include those used to maintain the gas facilities on company work trucks, meters sent for testing and repair and intercompany mail. These items are transported by company or vendor vehicles.

Trash and paper wastes are put in dumpsters that are picked up by a waste disposal contractor.

US mail is generally taken to the post office.

Scrap metal is placed in a waste bin and pick-up is contracted through a local scrap dealer.

Occasionally, plastic pipe is delivered to the Regional offices by a third party carrier.

This pipe is inspected and unloaded by company employees.

3. Vehicle Control – Company vehicles are parked after hours within fenced enclosures and the keys are stored in locked steel cabinets in district offices.
4. Additional Security Aids
 - a. All of the districts have at least one “dusk-to-dawn” light and most have multiple lights that illuminate the office and shop buildings and equipment parking areas.
 - b. Emergency generators are located at most regional offices. These generators start automatically if the commercial power is interrupted and they provide electrical service for the offices and shops. The generators are driven by natural gas engines. Fuel supply is unlimited unless interrupted by outage.
 - c. Smoke detectors are located in some of the regional offices. If one of these devices activates, it alerts employees to evacuate the building.

Compressor Stations

1. Personnel Access – Access to the compressor stations is through gated fences and building doors that are locked with the company’s master pad locks. The doors and fences are locked at all times unless an employee is working at the station.
2. Material Control – Materials delivered to compressor stations includes oils, antifreeze, and parts to maintain the electric motors, gas engines, and compressors. All materials are delivered by company employees, or company employees are present during such deliveries. Materials leaving the compressor stations are used oil and parts which are carried out by company employees or hauled by third parties under the direction of company employees.
3. Vehicle Control – In general, only company vehicles are permitted at the compressor stations or personal vehicles of company personnel working at the Stations. Approved vendor and contractor vehicles are also permitted in the presence of company employees.
4. Additional Security Aids
 - a. Dusk-to-dawn lights are installed at each compressor station for security purposes and to assist employees for after-dark emergency work at the station.
 - b. Signs are posted at all compressor stations advising the public of the station owner with a telephone number to call in case of an emergency.
 - c. All compressor stations have alarms for the loss of commercial power that are sent to the Gas Control Center.
 - d. Each compressor building has a gas detection device that monitors the percentage of gas-in-air. When the gas level reaches 20% of the lower explosive limit (LEL) the vent fan(s) start, an alarm is sent to the Gas Control Center, and an external red light starts blinking to warn employees of a potential explosive atmosphere. When the gas level reaches 65% of the lower explosive limit (LEL) the compressor(s) shut down, an alarm is sent to the Gas Control Center, and an external red light blinks to warn employees of a potential explosive atmosphere.

Regulator Stations

1. Personnel Access – The majority of the regulator stations are enclosed in fences or installed in wooden or metal “houses.” The fence gates and houses are locked with the company’s master pad locks. The fence gates and houses are locked at all times unless an employee is working at the station.

If there is no fence or house, the key valves at the regulator stations are individually locked with a master pad lock.

2. Material Control – Regulator parts to maintain the regulators and cleaning fluids are the primary materials taken to regulator stations. Weed killer may also be applied by contractors to maintain the ground cover within the fence or perimeter of the stations.
3. Vehicle Control – Only company vehicles are permitted at the regulator stations. However, during the summer months, a contractor mows the grass at a few regulator sites. He gains access through his padlock that is interlocked with the company’s padlock.
4. Additional Security Aids
 - a. Signs are posted at all regulator stations stating “DANGER, Natural Gas”, and provide the Company name, address, and emergency telephone number.
 - b. Pressures are monitored at key regulator stations and alarms are sent to the Gas Control Center if the pressure exceeds pre-determined limits.

City Gate Stations

1. Personnel Access –The city gate stations are fenced and locked with pad locks from the various companies that own and operate the facilities at the stations (Peoples and Interstate Suppliers). The locks are interlocked so that each of the operators can gain access without the other operator(s) being present. These locks are always locked unless an operator is working at the station. PNG also operates a small number of supply points in a bubble distribution system located in and around the Grove City, PA area. Some of the supply points are enclosed in fences or installed in wooden or metal “houses.” The fence gates and houses are locked with the company’s master pad locks. The fence gates and houses are locked at all times unless an employee is working. If there is no fence or house, the key valves at supply points are individually locked with a master pad lock.
2. Material Control – Replacement parts for regulators, meters, etc. and odorant are the primary items delivered to a city gate station. These parts are brought to the stations by company and the interstate pipeline employees. Odorant is delivered and filled by contractors one time per calendar year.
3. Vehicle Control – Only company vehicles and those of the interstate pipelines or a contractor hired by the company or interstate pipeline are permitted within the city gate stations.
4. Additional Security Aids
 - a. Signs are posted at all city gate stations advising the public of the station owner with a telephone number to call in case of an emergency. The signs say DANGER, Natural Gas, and NO TRESPASSING.

SCADA Sites

1. Personnel Access – For SCADA locations including compressor stations, regulator stations, city gate stations, valve junctions, delivery points to other companies, and repeaters all electronic equipment is installed in locked cabinets, which are located inside of a building or fence or both. The fences and buildings are locked with the company master key and the cabinets are locked with a master pad lock issued only to the personnel requiring access.
2. Material Control – No materials are taken into or out of these sites except for part replacements which are handled by company employees
3. Vehicle Control – Only Company vehicles are permitted at the SCADA sites.
4. Additional Security Aids - Signs are posted at all SCADA sites with the notice “NO TRESPASSING” and the company’s name, address, and emergency telephone number.

Main Line Valves and Pipeline Junctions

1. Personnel Access – The majority of the main line valves and pipeline junctions are buried below ground. The only indication of a buried valve is a valve box at the surface and the only means of operating a buried valve is through the use of a special valve key. (The valve key is a tee handle with an extension of approximately five feet of solid steel stock and a fitting on the end that will operate the valve.) Some of the above ground main line valves and pipeline junctions are fenced. Those that are not fenced have their valves locked with locking devices or chains and master pad locks.
2. Material Control – The only materials that would be used at a mainline valve or junction would be weed killer and valve grease, which would be supplied and used by company employees. No materials would be taken from these sites.
3. Vehicle Control – Only company vehicles are permitted at the valve and junction sites.
4. Additional Security Aids – Signs are posted at all pipeline junctions that are located above ground and are fenced. The signs state “DANGER, Natural Gas”, and provide the company name, address, station identification number and emergency telephone number.

Appendix PSP-2 – Normal Security Level Procedures

The Normal Security Level is a normal day level, with no extraordinary security measures being taken, following the guidelines identified in Appendix PSP 1 – Existing Physical Security Procedures.

- Physical Security Manager should keep abreast of any changes in the National Terrorism Advisory System (NTAS)
- All employees should follow the normal security procedures
- All employees should continue to be aware of any potential security incidents, and report any unusual activity to their immediate supervisor
- Field crews, as they are working at sites, should keep an eye out for any potential security problems (broken locks, non-working card readers, etc.) and report immediately to their supervisors for remediation

Appendix PSP-3 –Elevated Security Alert Procedures

During an Elevated Security Alert, there exists credible security threats to company facilities or employees, or the Department of Homeland Security has raised the National Terrorism Advisory System level to **Elevated**, which is defined as a credible terrorist threat.

Once the Physical Security Manager has received notification of a threat against the company, or the raising of the DHS's level, the following procedures should be considered as the event warrants:

- Alert the company's Physical Security Manager to the situation
- The Physical Security Manager will activate the Physical Security Team and alert all team members as to the situation
- Schedule a conference call with the Physical Security Team and consider implementing the Elevated Security Alert tasks of the Physical Security Plan (see Appendix PSP 6 – Elevated and Imminent Security Alert Task Lists)
- Assure all existing security measures are in place and being utilized
- Establish communication with local, state and federal law enforcement officials, as necessary, and advise of company security status
- Consider utilizing guards at specific sites and/or critical facilities for restricting access and checking company ID cards
- Schedule patrols of operations facilities
- Communicate incident to all employees, remind them of company security policies, and ask for increased vigilance

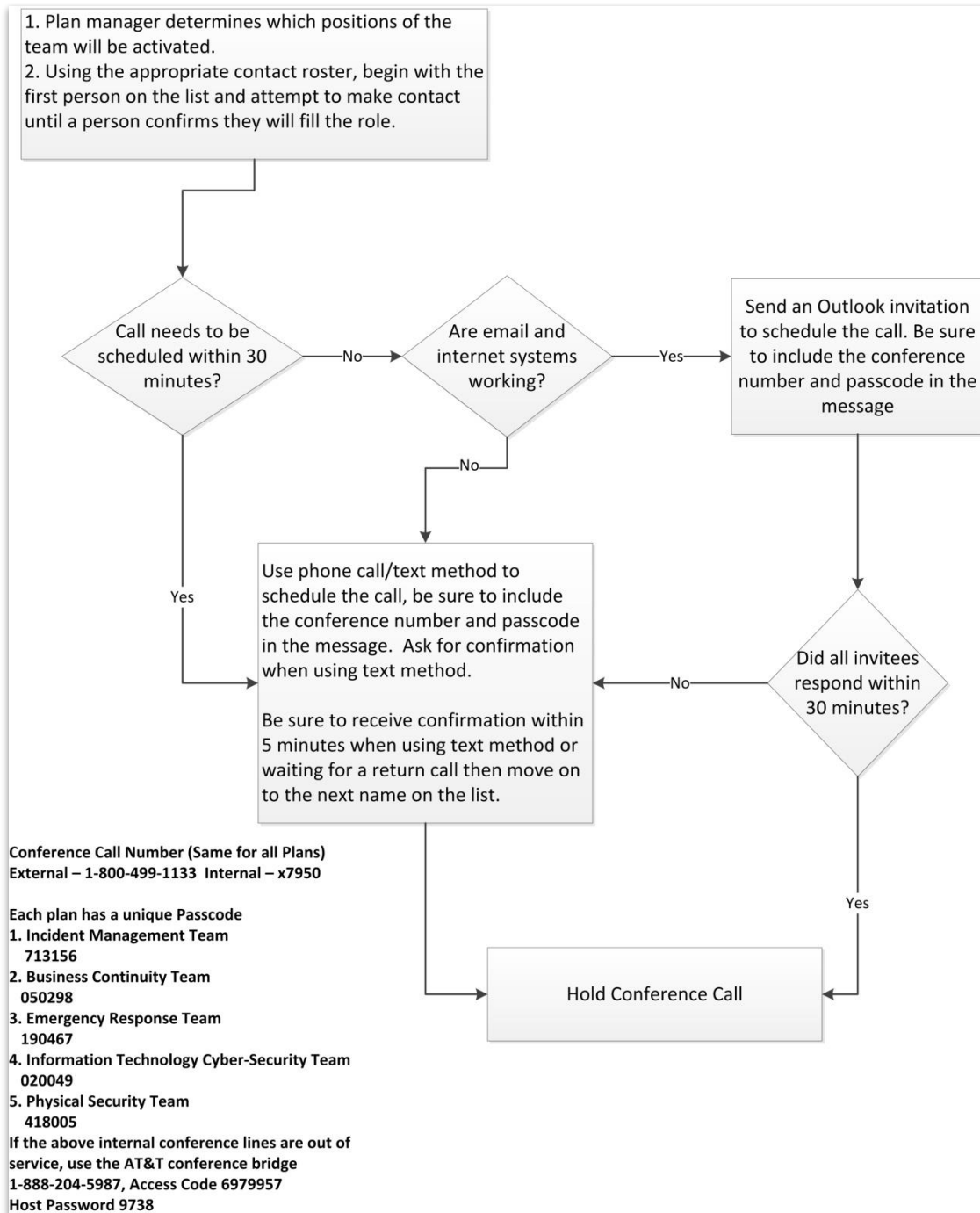
Appendix PSP-4 – Imminent Security Alert Procedures

During an Imminent Security Alert, there exists multiple security issues to company facilities or employees, or the Department of Homeland Security has raised the National Terrorism Advisory System (NTAS) level to **Imminent**, which is defined as a credible, specific and impending terrorist threat.

Once the Physical Security Manager has received notification of multiple security issues to company facilities or employees, or the raising of the DHS's level, the following procedures should be considered as the event warrants:

- Ensure all procedures from Appendix PSP 3 – Elevated Security Alert Procedures are implemented
- Consider implementing the Imminent Security Alert tasks (see Appendix PSP 7 – Elevated and Imminent Security Alert Task Lists)
- Access to all company facilities should be restricted to employees only with valid IDs
- 24 hour guards should be posted at all company offices and critical operations' facilities as necessary
- Erect barriers as necessary
- Visually inspect all vehicles entering company facilities as necessary
- Request assistance from local, state or national law enforcement for protection of critical facilities as needed
- Inspect all employee bags, briefcases, etc., as they are brought into company facilities as necessary
- Maintain contact with all law enforcement, emergency management agencies, PEMA and FEMA with the company's status and actions as necessary

Appendix PSP-5 – Conference Call/Meeting Initiation Protocol



Appendix PSP-6 - Physical Security Team Conference Call/Meeting Agenda

Date: _____

Time: _____

Team members in attendance (perform roll call)

Position	In attendance?	Representative Name?
Physical Security Manager		
General Counsel		
Safety Officer		
Communications Officer		
Regulatory Officer		
System Operations Coordinator		
Facilities & Environmental Coordinator		
Operations Coordinator		
Customer Services Coordinator		
IT Coordinator		
Logistics and Procurement Coordinator		
Administration Coordinator		

Current Alert Level: Normal Elevated Imminent

Review current security issues:

Review current remediation activities as required - (1) Elevated tasks (2) Imminent tasks:

General Counsel Report:

Safety Officer Report:

Communications Officer Report:

Regulatory Officer Report:

System Operations Coordinator Report:

Facilities and Environmental Coordinator Report:

Operations Coordinator Report:

Customer Services Coordinator Report:

IT Coordinator Report:

Logistics and Procurement Coordinator Report:

Administration Coordinator Report:

Outstanding needs and issues:

Next conference call: _____

Appendix PSP-7 - Elevated and Imminent Security Alert Tasks Check List

Elevated Security Alert Task List

- Alert the company's Physical Security Manager to the situation. The Physical Security Manager will then alert the Incident Manager.
- The Physical Security Manager will activate the Physical Security Team and alert all team members as to the situation
- Schedule a conference call with the Physical Security Team
- Assure all existing security measures are in place and being utilized
- Establish communication with local, state and federal law enforcement officials, as necessary, and advise of company security status
- Consider utilizing guards at specific sites and/or critical facilities for restricting access and checking company ID cards
- Schedule patrols of operations facilities as necessary
- Communicate incident to all employees, remind them of company security policies, and ask for increased vigilance

Imminent Security Alert Task List

- Ensure all procedures from Appendix PSP 3 – Elevated Security Alert Procedures are implemented
- Access to all company facilities should be restricted to employees only with valid IDs
- 24 hour guards should be posted at all company offices and critical operations' facilities as necessary
- Erect barriers as necessary
- Visually inspect all vehicles entering company facilities as necessary
- Request assistance from local, state or national law enforcement for protection of critical facilities as needed
- Inspect all employee bags, briefcases, etc., as they are brought into company facilities as necessary
- Maintain contact with all law enforcement, emergency management agencies, PEMA and FEMA with the company's status and actions as needed

Appendix PSP-8 - Responding To and Updating the Media

Proactively updating the media, as well as responding promptly to media inquiries is a key component of the Communications Officer's responsibilities during an event. The proactive approach many times will help to dispel rumors, cut down on the number of questions, and help to create a positive relationship between the company and the media.

The Communications Officer should take great care in assuring that information that is provided to the media is the same that is provided to all internal audiences, as well as what is posted on the company's website and Social Media outlets.

A good methodology to follow when updating the media includes:

- The update should follow the 5 Ws – Who, What, When, Where, Why and How
- Updates should be short and to the point, as much as possible. Copy and paste the body of the press release into an email, which is a preferred method for media outlets. Be sure to save copies of the press releases in specific incident folders.
- It is helpful to follow the news cycles when updating the media, sending the updates 15-30 minutes prior. It is also preferable to note in the update when the next update will be available.
 - The news cycles normally are 5, 6 and 8 a.m.; Noon, 4, 5, 6, 10 and 11 p.m.

As stated above, the company's website, Social Media outlets, and internal constituents (Customer Service, Government Relations, Senior Management, etc.) should be updated at the same time with the same information.

In between scheduled updates, the Communications Officer should utilize the company's social media outlets to post other relevant messages, such as general safety tips, locations of warming centers, photos of crews working, etc.

The company should decide on a policy to respond/engage customers that post on the company's Social Media outlets. However, it is recommended that the Communications Manager does respond to any rumors that someone might post. Dispelling rumors immediately is of the utmost importance. Also, should reports of a specific incident come across a Social Media outlet, the Communications Manager should immediately bring it to the attention of the proper department.

Appendix PSP-9 – Media Activity Log

All media inquiries (incoming) should be logged during an event.

DATE: _____

<u>Media Outlet</u>	<u>Reporter name</u>	<u>Phone Number</u>	<u>Inquiry</u>	<u>Response</u>

Appendix PSP-10 – Communication Officer Hotwash

Post-event, a Communications Hotwash should be conducted, identifying a number of key successes and weaknesses.

1. What did we do right?
2. What can we do better?
3. What were the strong points of our media response?
4. What were the weak points of our media response?
5. What were we most prepared for?
6. What surprised us?
7. Did we use all resources available?
8. Were there any actions that we forgot to take?
9. How well did we communicate our core messages?
10. Did we protect the company and its reputation?
11. Did internal communication work, i.e., were we able to gather needed information from internal sources?
12. How well did our Social Media outlets work during the event?
13. How can we improve our Social Media usage?

Appendix PSP-11 – Bomb Threat Procedures and Call Form

Most bomb threats are received by phone, and should be considered real and serious until proven otherwise. If a bomb threat is received, act quickly, but attempt to stay as calm as possible and gather as much information as possible using the form on the next page. Always alert the company’s Security Manager after you have notified 911. The company’s Security Manager will make the evacuation determination at that point.

Physical Security Manager

Contact	Work Phone	Cell Phone
Mark Pietrone	412-244-4662	412-660-0969
Bill Schade	412-258-4476	412-302-9707

Once you receive a bomb threat:

1. DO NOT use two-way radios or cellular phones as radio signals have the potential to detonate a bomb
2. DO NOT evacuate the building until police arrive and evaluate the threat
3. DO NOT activate the fire alarm
4. DO NOT touch or remove a suspicious package

If a bomb threat is received by phone:

1. Remain calm, and keep the caller on the line as long as possible. Do not hang up, even if the caller does
2. Listen carefully and gather as much information as possible using the form below
3. If possible, alert a nearby co-worker to call 911 while you still have the caller on the phone. If this isn’t feasible, immediately notify 911 yourself after the caller hangs up
4. If your phone has caller ID, copy the number down

If a bomb threat is received by a handwritten note:

1. Call 911 immediately
2. Handle the note as minimally as possible

If a bomb threat is received by email:

1. Call 911 immediately
2. Do NOT delete the email

Signs of a suspicious package:

1. No return address
2. Excessive or foreign postage
3. Stains, strange odor or sounds
4. Unexpected delivery, incorrect titles, poorly handwritten address or misspelled words

Bomb Threat Data Collection Form

BOMB THREAT CALL PROCEDURES

Most bomb threats are received by phone. Bomb threats are serious until proven otherwise. Act quickly, but remain calm and obtain information with the checklist. Then give the completed form to your supervisor

1. Remain calm. Keep the caller on the line for as long as possible. DO NOT HANG UP, even if the caller does.
2. Listen carefully. Be polite and show interest.
3. Try to keep the caller talking to learn more information.
4. If possible, write a note to a colleague to call the authorities or, as soon as the caller hangs up, immediately notify them yourself.
5. If your phone has a display, copy the number and/or letters on the window display.
6. Complete the Bomb Threat Checklist (Next column) immediately. Write down as much detail as you can remember. Try to get exact words.
7. Immediately upon termination of the call, do not hang up, but from a different phone, contact your supervisor immediately

If a bomb threat is received by handwritten note:

- Call your supervisor and then give the note to them
- Handle note as minimally as possible

If a bomb threat is received by email:

- Call your supervisor and forward the email to them
- Do not delete the message.

Signs of a suspicious package:

- No return address
- Excessive postage
- Stains
- Strange odor
- Strange sounds
- Unexpected delivery
- Poorly Handwritten
- Misspelled words
- Incorrect titles
- Foreign postage
- Restrictive notes

DO NOT:

- Use two-way radios or cellular phone; radio signals have the potential to detonate a bomb.
- Evacuate the building until police arrive and evaluate the threat.
- Activate the fire alarm.
- Touch or move a suspicious package

Complete the form and submit to your Supervisor IMMEDIATELY!!
If your Supervisor is not accessible CALL 911!!

Bomb Threat Checklist

Date: _____ Time: _____

Time Caller Hung Up _____ Phone # Where Call Received _____

Ask Caller

- Where is the bomb located? (Building, Room Floor Etc.) _____
- When will it go off? _____
- What does it look like? _____
- What kind of bomb is it? _____
- What will make it explode? _____
- Did you place the bomb? Yes No
- Why? _____
- What is your name? _____

Exact Words of Threat

Information About Caller

- Where is the caller located? _____
- Estimated age _____
- Is voice familiar? If so, who does it sound like? _____
- Other points _____

Caller's Voice	Background Sounds	Threat Language
<input type="checkbox"/> Accent	<input type="checkbox"/> Animal Noises	<input type="checkbox"/> Incoherent
<input type="checkbox"/> Angry	<input type="checkbox"/> House Noises	<input type="checkbox"/> Message read
<input type="checkbox"/> Calm	<input type="checkbox"/> Kitchen Noises	<input type="checkbox"/> Taped
<input type="checkbox"/> Clearing throat	<input type="checkbox"/> Street Noises	<input type="checkbox"/> Irrational
<input type="checkbox"/> Coughing	<input type="checkbox"/> Booth	<input type="checkbox"/> Profane
<input type="checkbox"/> Cracking voice	<input type="checkbox"/> PA system	<input type="checkbox"/> Well-spoken
<input type="checkbox"/> Crying	<input type="checkbox"/> Conversation	
<input type="checkbox"/> Deep	<input type="checkbox"/> Music	
<input type="checkbox"/> Deep breathing	<input type="checkbox"/> Motor	
<input type="checkbox"/> Disguised	<input type="checkbox"/> Clear	
<input type="checkbox"/> Distinct	<input type="checkbox"/> Static	
<input type="checkbox"/> Excited	<input type="checkbox"/> Office machinery	
<input type="checkbox"/> Female	<input type="checkbox"/> Factory machinery	
<input type="checkbox"/> Laughter	<input type="checkbox"/> Local	
<input type="checkbox"/> Lisp	<input type="checkbox"/> Long distance	
<input type="checkbox"/> Loud		
<input type="checkbox"/> Male	Other Information:	
<input type="checkbox"/> Normal	_____	
<input type="checkbox"/> Ragged	_____	
<input type="checkbox"/> Rapid	_____	
<input type="checkbox"/> Raspy		
<input type="checkbox"/> Slow		
<input type="checkbox"/> Slurred		
<input type="checkbox"/> Soft		
<input type="checkbox"/> Stutter		

Call Taken By _____



Appendix PSP-12 – Intruder on Property Procedure

If an armed or threatening intruder comes on to the property it is very important that 911 is immediately notified and protective actions are taken.

If you see an armed intruder and you are in an office:

- Remain in the office and immediately lock all doors, if possible.
- Call 911 and alert emergency personnel. Try and remain calm so you can give an accurate description of the person or person(s). Note type of dress, height, weight, sex, and any other characteristics/physical items that are particular to the individual(s). Report the type of weapon (if known) and direction of travel or building entered.
- Call the company's Physical Security Manager at 412-926-6647 and report the above information.
- Lock the windows and close blinds or curtains.
- Turn off lights and all audio equipment.
- Stay out of the open areas and be as quiet as possible.
- Keep the office secure until police arrive and give directions.

If you are caught in an open or exposed area and you cannot get into an office you must decide upon a course of action:

Hiding

Look for a safe and secure hiding area. Once in place try and remain calm. Stay hidden until you can make contact with emergency personnel.

Running

If you think you can safely make it out of the area, do so. If you decide to run, stay low and do not run in a straight line. Attempt to keep objects (trees, vehicles, trash cans, etc.) between you and the hostile person. When away from immediate area of danger, summon help and warn others.

Playing Dead

If the intruder is causing death or physical injury to others and you are un-able to run or hide you may choose to assume a prone position and lay as still as possible.

Fighting

Your last option if you are caught in the open and are in close proximity of the intruder is to fight back. This is dangerous, but depending on your situation this could be your last option.

If you are caught by the intruder and are not going to fight back, obey all commands and avoid eye contact.

Once emergency personnel have arrived and taken over the situation, obey all commands. Once the threat is over, render first aid to injured near you and summon emergency aid responders.

Appendix PSP-13 – Facility and corresponding law enforcement list

IN CASES OF EMERGENCY, ALWAYS CALL 911 FIRST
ALTERNATE NUMBERS ARE NON-EMERGENCY NUMBERS

Offices

Facility Name	Address	Emergency Services Contacts
North Shore Offices	375 North Shore Drive, Pittsburgh, PA 15212	Police Z1– 911 or 412-323-7201 Fire – 911 or 412-255-2860
Allegheny District Office	6085 Freeport Road Natrona Heights, PA 15065	Police – 911 or 724-224-3355 Fire – 911 or 724-224-1912
Altoona Field Office	100 E. Bellwood Avenue, Altoona, PA 16602	Police – 911 or 814-949-2489 Fire – 911 or 814-949-2225
Butler District Office	334 East Cunningham St., Butler, PA 16001	Police – 911 or 724-287-7743 Fire – 911 or 724-283-3100
Butler Warehouse	336 East Cunningham St., Butler, PA 16001	Police – 911 or 724-287-7743 Fire – 911 or 724-283-3100
Butler Main Office	205 N. Main Street, Butler, PA 16001	Police – 911 or 724-287-7743 Fire – 911 or 724-283-3100
Gibsonia Field Office	5600 Community Center Dr., Gibsonia, PA 15044	Police – 911 or 724-443-7848 Fire – 911 or 724-443-3306
Ginger Hill Field Office	65 Ginger Hill Road, Finleyville, PA 15332	Police – 911 Fire – 911
Greensburg Field Office	195 Donohoe Road, Greensburg, PA 15601	Police – 911 or 724-832-3288 Fire – 911 or 724-837-8408
Grove City Field Office	1871 Mercer Grove City Road, Mercer, PA 16137	Police – 911 or 724-662-6162 Fire – 911 or 724-662-3290
Hopewell Field Office	1315 Gringo Road, Aliquippa, PA 15001	Police – 911 or 724-378-0557 Fire – 911 or 724-378-9445
Indiana District Office	5999 Rte. 119, Highway North, Home, PA 15747	Police – 911 or 724-349-1428 Fire – 911 or 724-349-1428
Jefferson District Office	1489 North Elkin Road Smicksburg, PA 16256	Police – 911 Fire – 911
Johnstown Field Office	3115 Elton Road, Johnstown, PA 15904	Police – 911 or 814-266-8333 Fire – 911 or 814-266-4331
Kentucky Field Office	463 Hambley Blvd., Pikeville, KY, 41501	Police – 911 or 606-437-6236 Fire – 911 or 606-437-6234
Kiski Field Office	432 Hyde Park Road, Leechburg, PA 15656	Police – 911 or 724-836-1551 Fire – 911 or 724-600-7300
McKeesport Field Office	261 Center Street, McKeesport, PA 15132	Police – 911 or 412-675-5015 Fire – 911 or 412-675-5042

Facility Name	Address	Emergency Services Contacts
McKeesport Training Center	2022 Ripple Road, McKeesport, PA 15132	Police – 911 or 412-675-5015 Fire – 911 or 412-675-5042
Monongahela Field Office	1291 West Main Street Monongahela, PA 15063	Police – 911 or 724-258-5511 Fire – 911 or 724-258-6871
Valley Field Office	1140 Margaret Road, Kittanning, PA 16201	Police – 911 or 724-543-2011 Fire – 911 or 724-783-7333
Waynesburg Field Office	127 Woodside Road, Waynesburg, PA 15370	Police – 911 or 724-627-6151 Fire – 911 or 724-627-5426
West Virginia Field Office	1192 Hoult Road, Fairmont, WV, 26554	Police – 911 or 304-367-0195 Fire – 911 or 304-367-0195
Wilkinsburg Field Office	1201 Pitt Street, Pittsburgh, PA 15221	Police – 911 or 412-244-2913 Fire – 911 or 412-244-2930
Wilkinsburg B	600 Poplar Street Etna, PA 15233	Police – 911 or 412-781-6271 Fire – 911 or 412-782-1333

Stations

Facility Name	Address	Emergency Services Contacts
Alabran Station	1489 North Elkin Road, Smicksburg, PA 16256	Police – 911 or 814-938-0517 Fire – 911 or 724-286-9406
Armbrust Station	Waycross Road, Greensburg, PA 15601	Police – 911 or 724-925-9463 Fire – 911 or 724-834-5380
Arnold Station	Lowe Road, Lower Burrell, PA 15068	Police – 911 or 724-339-4287 Fire – 911 or 724-339-9611
Atwood Station	West Indiana Street, Rural Valley, PA 16249	Police – 911 or 724-543-2011 Fire – 911 or 724-354-2261
Belknap Station	355 Belknap Road, Dayton, PA 16222	Police – 911 or 724-543-2011 Fire – 911 or 814-257-8874
Creekside Station	St. Clair Road, Indiana, PA 15701	Police – 911 or 724-357-1960 Fire – 911 or 724-349-6681
Creighton Station	926 Front Street, Creighton, PA 15030	Police – 911 or 724-224-3434 Fire – 911 or 724-226-3830
Crooked Creek Station	123 Pump Station Road, Ford City, PA 16226	Police – 911 or 724 763-9677 Fire – 911 or 724-763-7319
Dice Station	2300 Route 286, Pittsburgh, PA 15239	Police – 911 or 412-793-7400 Fire – 911 or 724-327-3456
Egry Station	3410 Saltsburg Road, Clarksburg, PA 15725	Police – 911 or 724-357-1960 Fire – 911 or 724-459-5643
Fisher Station	320 Fisher Road, New Bethlehem, PA 16242	Police – 911 or 724-543-2011 Fire – 911 or 814-257-8874
Gibson Station	156 Redds Mill Road, Charleroi, PA 15022	Police – 911 or 724-929-6262 Fire – 911 or 724-483-8005
Girty Station	115 Falling Oaks Lane, Shelocta, PA 15774	Police – 911 or 724-543-2011 Fire – 911 or 724-354-2261
Hill Station	Pine Run Road, Apollo, PA 15613	Police – 911 or 724-727-3410 Fire – 911 or 724-727-3079
Hughes Station	2209 Garden Way, Freeport, PA 16229	Police – 911 or 724-295-9500 Fire – 911 or 724-353-2338
Kinter Station	2738 Musser Road, Indiana, PA 15701	Police – 911 or 724-357-1960 Fire – 911 or 724-388-6462
Latrobe Station	Box 810 Beatty Flats Rd., Latrobe, PA 15605	Police – 911 or 724-832-7977 Fire – 911 or 724-537-9872
Limestone Station	672 Limestone Road, Summerville, PA 15864	Police – 911 or 814-226-1710 Fire – 911 or 814-764-5415
Mendon Station	R.R. #1 Gressley Road, Ruffs Dale, PA 15679	Police – 911 or 724-832-3288 Fire – 911 or 724-640-7725

Facility Name	Address	Emergency Services Contacts
Merwin Station	243 Shady Lane, Apollo, PA 15613	Police – 911 or 724-727-3410 Fire – 911 or 724-727-3079
Portman Station	58-252 Kittanning Street, Butler, PA 16002	Police – 911 or 724-284-8100 Fire – 911 or 724-283-4200
Redbank Station	5091 Truittsburg Road, Fairmount City, PA 16224	Police – 911 or 814-226-1710 Fire – 911 or 814-365-5770
Roaring Run Station	1136 Edmon Road, Apollo, PA 15613	Police – 911 or 724-478-3357 Fire – 911 or 724-478-4210
Rubright Station	810 Rubright Road, Apollo, PA 15613	Police – 911 or 724-727-3434 Fire – 911 or 724-882-1347
Schmidt Station	8092 Saltsburg Road, Saltsburg, PA 15681	Police – 911 or 724-357-1960 Fire – 911 or 724-433-0183
Shady Plain Station	Townsend Road, Spring Church, PA 15686	Police – 911 or 724-543-2011 Fire – 911 or 724-478-4210
Shoemaker Station	335 Logansport Road, Ford City, PA 16226	Police – 911 or 724 763-9677 Fire – 911 or 724-763-7319
Sprankle Mills Station	250 Mauk Hill Road, Sprankle Mills, PA 15776	Police – 911 or 814-938-0517 Fire – 911 or 814-856-2429
Valley Station	1140 Margaret Road, Kittanning, PA 16201	Police – 911 or 724-543-2011 Fire – 911 or 724-783-7333
Vardy Station	243 Center Drive, Chicora, PA 16025	Police – 911 or 724-284-8100 Fire – 911 or 724-496-5964
Village Station	1120 Kennerdell Lane, Rural Valley, PA 16249	Police – 911 or 724-543-2011 Fire – 911 or 724-783-7333

General Contacts-

FBI Pittsburgh – 412-432-4000	FBI West Virginia – See FBI Pittsburgh
Dept. of Homeland Security – 202-282-8000	FBI Kentucky - 606-432-1226
Local DHS – Bob Winters – 412-995-3750	
FEMA – 202-646-2500	
PEMA – 717-651-2001	
PEMA Western Office – 800-972-7362	

Appendix PSP-14 – Facility Internal Contact List

Facility Name	Address	Contact
North Shore HQ & Offices	375 North Shore Drive, Pittsburgh, PA 15212	Heather Doyle-Conley: 412-841-4476 Kevin Turkovich: 412-398-6558
Allegheny District Office	6085 Freeport Road Natrona Heights, PA 15065	Tim Collins: 724-355-9782 Fred Henry: 724-321-5174
Altoona Field Office	100 E. Bellwood Avenue, Altoona, PA 16602	Todd Renney: 814-525-1458 Paul Mears: 724-420-6397
Butler District Office	334 East Cunningham St., Butler, PA 16001	Mark Smith: 724-801-0352 Don Zombek: 412-906-1065
Butler Warehouse	336 East Cunningham St., Butler, PA 16001	Mark Smith: 724-801-0352 Don Zombek: 412-906-1065
Butler Main Office	205 N. Main Street, Butler, PA 16001	Mark Smith: 724-801-0352 Don Zombek: 412-906-1065
Gibsonia Field Office	5600 Community Center Dr., Gibsonia, PA 15044	Drew Leshner: 412-295-3738 Don Zombek: 412-906-1065
Ginger Hill Field Office	65 Ginger Hill Road, Finleyville, PA 15332	William Drane: 412-812-0895 Ralph Comito: 412-721-0159
Greensburg Field Office	195 Donohoe Road, Greensburg, PA 15601	Ken Loughner: 724-640-0156 Ralph Comito: 412-721-0159
Grove City Field Office	1871 Mercer Grove City Road, Mercer, PA 16137	Eugene Koebler: 724-991-0761 Don Zombek: 412-906-1065
Hopewell Field Office	1315 Gringo Road, Aliquippa, PA 15001	Don Zombek: 412-906-1065
Indiana District Office	5999 Rte. 119, Highway North, Home, PA 15747	Larry George: 724-355-8580 Paul Mears: 724-420-6397
Johnstown Field Office	3115 Elton Road, Johnstown, PA 15904	William Wright: 412-600-7178 Paul Mears: 724-420-6397
Kentucky Field Office	463 Hambley Blvd., Pikeville, KY, 41501	Ralph Comito: 412-721-0159
Kiski Field Office	432 Hyde Park Road, Leechburg, PA 15656	Lawrence Shane: 724-822-4929 Fred Henry: 724-321-5174
McKeesport Field Office	261 Center Street, McKeesport, PA 15132	Greg Stanley: 412-670-0733 Mike Kunz: 412-370-8707
McKeesport Training Center	2022 Ripple Road, McKeesport, PA 15132	Kevin Campbell: 724-689-6142 Chad Dochinez: 724-323-2625
Monongahela Field Office	1291 West Main Street Monongahela, PA 15063	Jason Lenart: 412-508-3796 Ralph Comito: 412-721-0159

Facility Name	Address	Contact
Valley Field Office	1140 Margaret Road, Kittanning, PA 16201	Bill Byerly: 724-664-3037 Fred Henry: 724-321-5174
Waynesburg Field Office	127 Woodside Road, Waynesburg, PA 15370	Jason Lenart: 412-508-3796 Ralph Comito: 412-721-0159
West Virginia Field Office	1192 Hault Road, Fairmont, WV, 26554	Tonya Perkins: 304-641-5990 Ralph Comito: 412-721-0159
Wilksburg Field Office	1201 Pitt Street, Pittsburgh, PA 15221	Michael Bocian: 412-670-2630 Mike Kunz: 412-370-8707
Wilksburg B Field Office	600 Poplar Street Etna, PA 15233	
All PNG / PTWP Compressor Stations	Various Addresses	Tim Love : 412-258-4595

Appendix PSP-15 – Physical Security Team Contact List

Contact Name	Work Phone	Cell Phone	Email
Bill Roberts	412-208-6527	412-496-8942	William.h.roberts@peoples-gas.com
Mike Turzai	412-258-4473	724-815-1349	Mike.turzai@peoples-gas.com
Paul Pantages	412-208-6802	412-952-3021	Paul.pantages@peoples-gas.com
Barry Kukovich	412-208-6568	412-389-0864	Barry.D.Kukovich@peoples-gas.com
Bill Roland	412-208-6537	412s-657-3377	William.Roland@peoples-gas.com
Ron Ferrere	412-473-3663	412-510-7894	Ronald.ferrere@peoples-gas.com
Mark Pietrone	412-244-4395	412-660-0969	mark.pietrone@peoples-gas.com
Paul Becker	412-258-4406	724-822-4728	paul.becker@peoples-gas.com
Heather Doyle-Conley	412-208-6603	724-612-4336	heather.a.doyle-conley@peoples-gas.com
Kevin Turkovich	412-208-6538	412-398-6558	Kevin.A.Turkovich@peoples-gas.com
Dave Hershberger	412-258-4422	412-477-4232	David.M.Hershberger@peoples-gas.com
Andy Rockwell	412-258-4461	412-432-8990	Andrew.A.Rockwell@peoples-gas.com
Katie Saulsbery	412-258-4538	412-431-9549	katie.saulsbery@peoples-gas.com
Ryan Milko	412-208-7151	412-295-1648	ryan.w.milko@peoples-gas.com
William Schade	412-302-9707	412-302-9707	william.schade@peoples-gas.com
Jennifer Petrisek	412-208-6834	412-552-0671	Jennifer.Petrisek@peoples-gas.com
Chad Ravotti	412-208-7247	412-335-4961	Chad.R.Ravotti@peoples-gas.com
Jared Long	814-269-6319	714-822-4729	Jared.Long@peoples-gas.com
Scott Orkis	412-258-4456	724-321-5135	scott.r.orkis@peoples-gas.com
Randy Ciotola	412-244-2535	412-906-1188	randy.r.ciotola@peoples-gas.com

Contact Name	Work Phone	Cell Phone	Email
Ralph Comito	412-258-4629	412-721-0159	Ralph.Comito@peoples-gas.com
Lisa Reilly	412-208-6552	412-716-3819	Lisa.A.Reilly@peoples-gas.com
Michelle Parks	412-208-6555	412-290-5397	MICHELLE.PARKS@peoples-gas.com
Joe Brado	412-208-6906	724-448-9201	Joseph.D.Brado@peoples-gas.com
Erin O'Donnell	412-208-6614	412-266-2446	erin.g.odonnell@peoples-gas.com
Jackie Ziemianski	412-208-6515	412-651-1324	jacqueline.m.ziemianski@peoples-gas.com
Johnetta Ryan	412-258-4528	412-335-3210	JOHNETTA.RYAN@peoples-gas.com
Karen Worcester	412-208-6594	412-512-5240	karen.r.worcester@peoples-gas.com
John Oravec	412-302-4621	412-302-4621	John.oravec@peoples-gas.com

Appendix PSP-16 – Physical Security Plan Testing Certification

Date of test	
Exercise Participants	
Date After Action Report completed	
Approved by:	
Name:	
Position :	