



“PROTECTING CRITICAL INFRASTRUCTURE: KEEPING PENNSYLVANIANS SAFE”

**CONFIDENTIAL RESPONSE OF THE
PENNSYLVANIA PUBLIC UTILITY COMMISSION
AND THE
PENNSYLVANIA EMERGENCY MANAGEMENT AGENCY
TO
HOUSE RESOLUTION 361**

CONFIDENTIALITY NOTICE

This report contains information that is confidential and is intended to be conveyed only to the designated recipient(s). Unauthorized use, dissemination, distribution, or reproduction of this report, therefore, is strictly prohibited and is unlawful. In addition, House Resolution 361 expressly provides that proprietary, security and competitively sensitive information and trade secrets of regulated public utilities, operative and nonoperative nuclear power plants, electric generating companies, natural gas producers, independent electric system operators, cooperative associations, municipal corporations and municipal authorities shall not be public records for purposes of the Act of June 21, 1957 (P.L. 390, No. 212), referred to as the Right-to-Know Law, and shall not be subject to mandatory public disclosure which would compromise the security and integrity of critical utility infrastructures.

CONFIDENTIAL HR 361 REPORT

TABLE OF CONTENTS

	<u>Page</u>
Confidentiality Notice	
Executive Summary	I
I. Introduction to the Resolution.....	1
II. Procedures Employed.....	2
III. Assessment Approach.....	4
IV. Overall Findings	
1.1 Emergency Response/Contingency Plans.....	6
1.2 Vulnerability/Risk Assessments.....	7
1.3 Business Continuity Plans.....	8
1.4 Cyber Security and Disaster Recovery.....	10
1.5 Policy for Financial Protection and Insurance Liability.....	12
V. Company/Industry Participation in Community.....	14
VI. Industries Examined.....	16
VII. Report on the Investigation by Industry	
2.1 Electric Generation and Suppliers.....	17
2.2 Electric Transmission and Distribution.....	19
2.3 Nuclear Generation.....	25
2.4 Natural Gas.....	30
2.5 Telecommunications.....	35
2.6 Water and Wastewater.....	39
2.7 Steam Heat.....	42
2.8 Rail.....	44
2.9 Motor Carrier.....	47
VIII. Issues Identified and Resolved.....	49
IX. Conclusions from the Review and Analysis Performed.....	51
X. Recommendations for Legislative Attention	
3.1 Protection of Assets through Sharing Best Practices.....	53
3.2 Education and Training	54
3.3 Employer/Employee Liability and Background Checks.....	56
3.4 Access Control and Zoning.....	57
3.5 Incident Command System/Unified Command, Emergency Response Teams and Color Code	58
3.6 Public Information/Privacy - Media, Maps, and Unions; Legal Review of Regulations.....	58
3.7 Security Costs and Insurance.....	59
3.8 Bridges, Mutual Aid, and Waivers.....	61

XI. Appendices

- A. House Resolution 361
- B. Workplace Security Survey
- C. PUC/PEMA letter to Industries recommending participation in the Regional Counter-Terrorism Task Force; and
Regional Counter-Terrorism Task Force Map
- D. Nuclear Regulatory Commission Advisories
- E. 911 Section from the Governor's Task Force on Security-10/26/02
- F. Acronyms

EXECUTIVE SUMMARY

The Pennsylvania House of Representatives introduced House Resolution (HR) 361 on November 20, 2001, and issued it on December 3, 2001. The Resolution tasked the Pennsylvania Public Utility Commission (PUC) and the Pennsylvania Emergency Management Agency (PEMA) to review, analyze, and evaluate utility infrastructure security protection and risk mitigation policies and other related security issues. Further the resolution requested the agencies to recommend prudent strategies to enhance the standards for the physical security and integrity of this infrastructure. The PUC and PEMA were required to submit a comprehensive report to the House of Representatives addressing utility infrastructure security issues on or before September 1, 2002. This report is the PUC/PEMA response to the requirements of the Resolution.

The PUC assembled a security task force to review security issues of utility infrastructure in Pennsylvania. PEMA acted in an advisory capacity to this task. Seventy-two companies, spanning nine industries, were profiled during this assessment and include the fixed utilities of electric, natural gas, water and wastewater, telecommunications, steam heat, and the transportation utilities of rail, motor carrier (trucking), taxi and limousine, and buses.

Prior to the events of September 11, 2001, the Commonwealth and the PUC took steps to ensure the safe, secure and reliable delivery of utility services. In July 1998, the PUC instituted a formal investigation to determine the Year 2000 technology problem (Y2K) readiness of approximately 750 public utilities which lasted eighteen months and included the testing and verification of mission critical components, emergency response and contingency plans, and business continuity plans at twenty-four companies.

When the events occurred on September 11th, Pennsylvania utility companies were prepared to respond to those events by implementing their emergency plans where appropriate and operating at a "heightened state of awareness." Plans have since been reviewed by the companies and modified or updated where necessary.

The PUC and PEMA, as well as the infrastructure industries, recognize that it is impossible to completely protect all utility infrastructures in Pennsylvania. Nevertheless, all parties want a foundation to organize efforts to protect the Commonwealth, its critical facilities, and its citizens from any type of event -- man-made or natural. The parties involved recognize that as security risks and vulnerabilities change, and information becomes available, plans will need to be adjusted and amended over time to reassess priorities and realign resources. The initiatives are recognized as permanent additions to our society and will need to be addressed for years and decades, not just weeks or months.

A "Workplace Security Survey" was developed and distributed to the utilities as the first step in the assessment process. Once completed and returned by the companies, the PUC established site visits to further discuss the results of the survey. This report will cover the findings of the survey, the site visits and additional information relating to the security of critical infrastructure in the Commonwealth. Five main areas were addressed with the companies during the assessment: Emergency Operations Plans, Contingency Planning, Business Continuity, Cyber Security, and Insurance and Security-related Costs. Finally, the companies were asked to identify any potential or actual legal or regulatory barriers to implement their security processes. Where appropriate, Emergency Operations Plans, Contingency Plans, Cyber Security Plans, and Business Continuity Plans were reviewed.

The Overall Findings consistent within all industries are fully profiled. The industry specific findings with differences within or between industry groups are also described in further detail in the report. The companies' and industries' participation in community security related activities is also presented. Several issues were initially identified as potential recommendations, but were resolved during the assessment process, and are offered as reference (Section VIII). Conclusions regarding the process employed and areas for further attention are explained. Finally, the following areas for legislative attention are designed to provide information to the House of Representatives as they deliberate the development of legislation for homeland security, consult with other agencies, and review issues with constituents. Based upon the findings, conclusions and recommendations from all participants, the PUC and PEMA find the following areas have some degree of merit and recommend further review by the Legislature.

Protection of Assets through Sharing Best Practices

- ◆ Government bodies or specific industry groups should distribute consistent physical and cyber security-related information to each industry.
- ◆ Clarify when utility-related events should be reported to state and local agencies and the expected response of state and local officials.
- ◆ Continue to enhance information flowed through the FBI's InfraGard Program, National Infrastructure Protection Center (NIPC), the CERT Coordination Center at Carnegie Mellon University and other programs available to utility companies.
- ◆ Expand the Pennsylvania State Police (PSP) Cyber Crimes Enforcement programs to allow more interactions with critical infrastructure companies and to assist them in tracking and prosecuting cyber crimes.
- ◆ Develop FBI levels for reporting cyber crimes specific to utilities and critical infrastructure.
- ◆ Define the roles of state agencies when reacting to an actual or suspected contamination event.

- ◆ Create a unified technical assistance database or communication procedure that can track unusual occurrences and link with local and state public health, law enforcement, state agencies and utilities.
- ◆ Amend the PA One Call Act to limit notification exceptions when excavating.
- ◆ Mandate the filing of a utility damages report with the Department of Labor and Industry.

Education and Training

- ◆ Develop an education process for company awareness through utility industry trade associations. The associations should include non-members, and invite smaller companies to participate in their planning and discussions relating to current trends, threats and best practices.
- ◆ Accept a "Train the Trainer" concept for first responders that could filter down to state, regional and local communities as described in *The National Strategy for Homeland Security (The Strategy)*.
- ◆ Train and network hospitals and health care facilities with a centralized analysis point to recognize indicators of sickness from water contamination and waterborne disease.
- ◆ Coordinate uniform security standards with other states.
- ◆ Create a training and support program similar to the air marshal program, to include the hiring, training, and use of rail or bus marshals to recognize terrorist activity or weapons of mass destruction, and to utilize bomb dogs. Allow passenger rail and bus personnel to perform random search of luggage.
- ◆ Institute a defined set of protocols for responsibilities of supplemental nuclear site security personnel (i.e. PSP and National Guard), particularly in the areas of detaining and arresting intruders and the use of deadly force.
- ◆ Define the level of credible threat against which NRC licensees are expected to secure their facilities.
- ◆ Provide education and assistance to the public with regard to training for safety and security around utility sites and critical infrastructure. Discuss areas of law such as trespass and vandalism, as well as "critical area" designations.
- ◆ Utilize the Operation TIPS (Terrorism Information and Prevention System) as proposed in *The Strategy* to help thousands of American truck drivers, letter carriers, train conductors, ship captains, and utility workers report potential terrorist activity.

Employer/Employee Liability and Background Checks

- ◆ Provide protection for prospective and previous employers against legal repercussions when providing a character or work reference for an employee.
- ◆ Protect new and former employers from liability when asking whether a prospective employee in a required "drug test position" previously failed a test.

- ◆ Establish a law enforcement service to perform a consistent statewide and nationwide criminal background check on prospective utility employees in PA.
- ◆ Use the FBI's NCIC (National Crime Information Center) to assist in a national criminal background check for prospective utility employees.
- ◆ Support *The Strategy* where the Director of Homeland Security and the Attorney General are to convene and participate with them in a panel with representatives from federal, state and local government, and the private sector, to examine whether employer liability statutes and privacy concerns hinder necessary background checks of personnel with access to critical infrastructure facilities or systems.

Access Control and Zoning

- ◆ Undertake a comprehensive review of other protection measures necessary to deny terrorist access to critical infrastructure in a similar manner as we control access at airports.
- ◆ Allow companies to secure facilities regardless of local, county or state zoning or ordinance issues. Local ordinances and state regulations should allow for expedited variances where the ordinance or regulation impedes the implementation of critical infrastructure security measures.
- ◆ Assess the use of co-located facilities or other equipment with respect to security issues.
- ◆ Consider the security of public access to waterways near critical facilities such as rights-of-ways, walkways, dams, reservoirs, and green ways that are part of a company's "secure" area. Strengthen the ability to prosecute or deter violations.

Incident Command System/Unified Command, Emergency Response Teams, and Color Code

- ◆ Require state and local first responder organizations to adopt the already widespread Incident Command System by making it a federal and/or state requirement.
- ◆ Assure a single point of contact for utility emergency response teams to access disaster areas. Employee photo-I.D. cards do not assure that law enforcement, federal agencies, and National Guard personnel who secure the area will permit passage to utility workers and supervisors.
- ◆ Maintain consistent use of the color codes developed by the Homeland Security Office in all utility industries.

Public Information/Privacy - Media, Maps, and Unions; Legal Review of Regulations

- ◆ Limit public disclosure of physical and cyber critical infrastructure information without compromising the principles of openness that ensure government accountability.
- ◆ Review public right to know laws, which allow access to critical security information about utility companies. These laws should be assessed to ascertain if exclusions are necessary to protect against exposure to terrorist activities.
- ◆ Examine public right to know laws for exclusion during times of crisis to allow access to police, law enforcement, and emergency management without allowing media access to facilities or records.
- ◆ Review regulations and policies that restrict the release of information and will provide a quick response on criminal profiles, when crimes are related to utilities, and infrastructure. Pennsylvania should conduct reviews on criminal statutes for prosecution of conspiracy or attempts to damage facilities.
- ◆ Obtain an appropriate level of federal security clearance for nuclear plant licensees in order to provide them with access to information considered classified which describes threats to licensed facilities.
- ◆ Monitor the challenges by utility labor unions regarding security issues such as surveillance cameras and other union challenges that, if allowed, could possibly increase vulnerability of the utility systems.

Security Costs and Insurance

- ◆ Prohibit exclusions of terrorism events from insurance coverage, as implemented in other states. Insurance companies should be required to work with state insurance commissions to write terrorism policies for corporations at reasonable rates.
- ◆ Explore options for potential recovery of prudent expense and capital investment for security related items.
- ◆ Balance the costs and benefits of increased security according to the threat level. Federal grant programs may be used to assist state and local infrastructure protection efforts.
- ◆ Analyze actual and potential insurance increases in the areas of liability, property, and worker compensation. Address terrorism coverage being dropped from utilities' primary coverage and review availability and cost of supplemental terrorism coverage.
- ◆ Conduct on-site inspections of physical assets with the PSP, local police, and insurance carriers, to provide an assessment of a company's present security, with recommendations for improvement.
- ◆ Clarify the issue of public safety and ratepayer recovery. Consider adopting the FERC process to expedite recovery of security costs for the energy

industries and modify to include telecommunications, water/wastewater and transportation industries.

- ◆ Mandated rules and legislation should be uniformly enforced, with appropriate opportunities for cost recovery, for all regulated and non-regulated companies in an industry group.
- ◆ Consider issues of tax incentives and/or tax credits to help transportation, energy, water, and telecommunications companies to encourage security investments.
- ◆ Monitor potential insurance liability increases related to the extension of the protected and/or owner controlled areas and the use of deadly force for NRC licensees.

Bridges, Mutual Aid, and Waivers

- ◆ Implement waiver process for utility repair vehicles regarding weight restrictions on small bridges in Northern and some Central counties during times of storms or other emergencies. Identify bridges and place on a priority list for upgrades or replacement.
- ◆ Continue and expand regional mutual assistance programs in all industry groups that currently share personnel and equipment during emergencies.
- ◆ Coordinate the state waiver process used to move utility crews and equipment between states during an emergency with multi-state serving companies and all states that routinely receive and provide assistance to/from Pennsylvania. This process is already in place and streamlined in Pennsylvania.

The PUC and PEMA have concluded that the foundation created in preparation for Y2K served as an excellent stepping stone for responding to events of September 11th. From our analysis, it is quite apparent that the companies have used their response to the events as “lessons learned” for enhancing and improving their security profile. Given continued legislative support and direction, we expect that security at our critical infrastructure will continue to evolve and improve.

I. INTRODUCTION TO THE RESOLUTION

House Resolution (HR) 361 was introduced on November 20, 2001, and issued on December 3, 2001. The Pennsylvania House of Representatives tasked the Pennsylvania Public Utility Commission (PUC) and the Pennsylvania Emergency Management Agency (PEMA) with the following:

- ◆ To review, analyze, and evaluate utility infrastructure security protection and risk mitigation policies and other related security issues;
- ◆ To recommend prudent strategies to enhance the standards for the physical security and integrity of this infrastructure; and
- ◆ To recommend statutory changes to enable cost recovery mechanisms for any security modifications to utility infrastructure.

This resolution also directed the PUC and PEMA to submit a comprehensive report to the House of Representatives addressing utility infrastructure security issues on or before September 1, 2002. A copy of House Resolution 361 is attached at Appendix A.

Invitations were extended to representatives of: the Pennsylvania State Police (PSP), the Department of Military and Veterans Affairs (DMVA), the Nuclear Regulatory Commission (NRC), the Department of Environmental Protection (DEP), and County Health Departments where applicable, to participate in meetings in order to both offer input and apprise the various agencies of the scope and specifics of the PUC and PEMA taskings. The cooperation received from these agencies was greatly appreciated. In addition, we would like to acknowledge the Energy Association of Pennsylvania, the Pennsylvania Jersey Maryland Interconnection (PJM), the Pennsylvania Rural Electric Association (PREA), the National Association of Water Companies - Pennsylvania Chapter, the Pennsylvania Telephone Association, and the Transportation Associations for their assistance in completing this assessment.

Coordinated tasks were addressed in the areas of energy, water, transportation, telecommunications, and emergency preparedness and response to ensure a priority on this project. Each area is interdependent upon one another to some degree. Increased collaboration and coordination in policy development and implementation better aligns public and private resources. During a security event or natural disaster, these groups work together to address common goals and purposes: to prepare, prevent and minimize the impact of an event through coordination, development, prior planning and training.

Shortly after the events of September 11th, President George W. Bush signed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA Patriot Act or USAPA) on October 26, 2001. The USA Patriot Act defines critical infrastructure as: those "systems and assets, whether physical or virtual, so vital to the United States 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."

The PUC and PEMA, as well as the infrastructure industries, recognize that it is impossible to completely protect all utility infrastructures in Pennsylvania. Nevertheless, all parties want a foundation to organize efforts to protect the Commonwealth, its critical facilities, and its citizens from any type of event, man-made or natural. The parties involved recognize that actions and plans will need to be adjusted and amended over time to reassess priorities and realign resources. The initiatives are recognized as permanent additions to our society and will need to be addressed for years and decades, not just weeks or months.

II. PROCEDURES EMPLOYED

In July 1998, the PUC instituted a formal investigation to determine the Year 2000 technology (Y2K) readiness of approximately 750 public utilities. The investigation lasted eighteen months. As part of the investigation, the PUC directed the utilities to be Y2K compliant on or before March 31, 1999, have acceptable contingency plans in place, or demonstrate why they should be granted an extension of time.

Beginning in February 1999, the PUC contracted with an information technology consultant to conduct an assessment of Y2K readiness for the fourteen largest jurisdictional public utilities. This included seven electric companies, three natural gas companies, two telephone local exchange carriers, and two water companies. As follow up to this assessment, the PUC emergency management staff also observed and verified actual testing of date sensitive, mission critical components at the above referenced fourteen utilities between April and July 1999.

The PUC continued to observe and verify Y2K testing of mission critical components and systems at ten additional utilities, and the PREA during September 1999 through November 30, 1999. These companies represented the largest potential impact to Commonwealth citizens. The twenty-four profiled companies also provided emergency response plans, business continuity plans and contingency plans for review. At that time, it was unknown what type of events (terroristic, physical, cyber threats, or other actions) could potentially trigger an emergency. The companies were prepared for what were then perceived as the "worst case scenarios."

The PUC was secure in its findings going into the Millenium. As then PUC Chairman John M. Quain stated in his testimony to the Senate on October 13, 1999: "The PUC has confidence that the lights will stay on, that natural gas and water will flow, and that the telecommunications system will work through Y2K and beyond." As the roll-over to the Year 2000 occurred, it was considered a

"non-event" throughout the U.S., but nevertheless, the Pennsylvania companies had staff at key facilities and were adequately prepared to mitigate, react, and restore service if necessary. PUC, PEMA and other state agencies staffed the State Emergency Operations Center (SEOC) during the "roll-over" to Y2K and were prepared to respond to any problems.

When the events of September 11th occurred, PEMA activated their emergency plans and directed state agencies to report to the SEOC. The PUC immediately surveyed its jurisdictional companies, PJM and PREA to determine what actions were being taken. Rail safety inspectors, gas safety inspectors and telecommunications staff were also contacted to assess their industry groups. All companies responded that they were at a "heightened state of awareness," had implemented emergency procedures as developed during Y2K, and took additional steps in preparation for responding to a potential event in their service territories within the Commonwealth. The DEP offered recommendations to public water suppliers and dam owners to take reasonable precautions to protect raw and finished water supplies and dams from external threats.

Additionally, four Pennsylvania-serving companies were directly affected by the events of September 11th. Two telecommunications companies were severely impacted in New York City, one of which was also involved in the events of Somerset County, PA. Two electric companies, a PUC jurisdictional and a PREA member, were impacted in the Somerset County disaster. The four companies had established emergency operation plans (during Y2K) prior to September 11th and were able to respond and handle the situation. For example, the loss of both World Trade Center Towers in New York required the recovery of local telecommunications services and to provide emergency communications for the relief effort in lower Manhattan. The response to Somerset County included emergency disconnection of electric service to downed power lines, restoration of electric service, the installation of additional phone and electric lines to support relief efforts of federal, state, and local agencies on the scene, and the loan of a self-contained "command center vehicle." The resulting activities in those urban and rural areas were both "lessons learned" and "lessons of success." Overall, the companies were well prepared to handle the scope and magnitude of those events with minimal work-around for the minor difficulties encountered.

Post September 11th PUC and PEMA personnel also assisted in the review and analysis process for Executive Order 2001-6, the Governor's Task Force on Security, with PUC staff participating in all eleven subcommittee meetings. The subcommittees were:

- ◆ State and Local Planning
- ◆ Mutual Aid
- ◆ Critical Infrastructure
- ◆ Nuclear and Radiological
- ◆ Cyber

- ◆ Biological
- ◆ Chemical
- ◆ Domestic Attacks
- ◆ Radio/Radio Frequency Systems
- ◆ Public Outreach/Communications
- ◆ Control/Monitoring of Land/Air Borders

III. ASSESSMENT APPROACH

Upon the passage of HR 361, the PUC again assembled a security task force to determine how to proceed in the assessment of utility infrastructure in the Commonwealth. PEMA acted in an advisory capacity for this task force. Due to the sensitive and confidential nature of the material to be reviewed, procedures were instituted, consistent with the PUC's Y2K investigation, to protect information. A "Workplace Security Survey" was developed to ensure a consistent and comprehensive evaluation of all nine industry groups. The nine industries included the fixed utilities of electric, natural gas, water and wastewater, telecommunications, steam heat, and the transportation utilities of rail, motor carrier (trucking), taxi and limousine, and busing.

An analysis was conducted to determine the best scope of evaluation within each industry group. The evaluations included small, medium, and large-scale companies, as well as non-jurisdictional entities, such as electric generators, natural gas suppliers, municipal authorities, etc. The jurisdictional and non-jurisdictional companies were profiled to address the industry as a whole, and also to identify any trends within an industry. Seventy-two companies were provided the attached "Workplace Security Survey" in Appendix B, and were asked to complete the survey and return it to the PUC.

As described in HR 361, the companies were assured of the proprietary and confidential nature of their responses, and that their responses would be protected from disclosure pursuant to the Public Utility Code, 66 Pa. C.S. §335(d). In addition, HR 361 mandated that:

"Proprietary, security and competitively sensitive information and trade secrets of regulated public utilities, operative and non-operative nuclear power plants, electric generating companies, natural gas producers, independent system operators, cooperative associations, municipal corporations and municipal authorities shall not be public records for purposes of...the Right-To-Know Law, and shall not be subject to mandatory public disclosure which would compromise the security and integrity of critical utility infrastructures..."

Upon the receipt of the completed surveys, the PUC was able to further analyze the results and to determine the similarities and differences in industry groups.

An on-site visit was conducted with all companies to obtain any supporting documentation or information and to coordinate employee interviews necessary to complete the review.

For the most part, security features are inherent in the utility business such as redundant or tandem systems, underground or remote locations that are not obvious and integrated into the companies' overall business practices. During the site visits, the PUC security task force explained the scope and purpose of HR 361, reiterated the confidential and proprietary nature of this review, and expressed concern that security and safety encompasses more than just terroristic threats and actions. From the PUC perspective, a security event might include all levels of threat ranging from a disgruntled employee, a terminated customer, mischievous individuals who vandalize a field location, domestic terrorism, or even a "copycat" event unrelated to another deliberate event.

Generally speaking, it would not matter if service were disrupted by a routine occurrence, a summer or winter storm, or by a security-related event. The responding utility's actions in restoring service, mitigating risks, and reacting to the situation would be almost identical in terms of procedures and processes. The main difference would be in regard to securing the area and restoring the service within a "crime scene" or incident command situation. These designations could severely restrict access to infrastructure facilities and delay restoration and reconstruction of facilities.

Five main topics were addressed with the companies: Emergency Operations Plans, Contingency Planning, Business Continuity, Cyber Security, and Insurance and Security-related Costs. Finally, the companies were asked to identify any potential or actual legal or regulatory barriers in implementing their security process. Where appropriate, Emergency Operations Plans, Contingency Plans, Cyber Security Plans, and Business Continuity Plans were reviewed.

Specifically, the PUC confirmed:

- ◆ Comprehensive detail of programs and policies;
- ◆ Corporate knowledge of plans and procedures for security incidents and threats;
- ◆ Changes in plans and procedures since September 11th;
- ◆ Training and screening of personnel regarding security practices of the corporation;
- ◆ Perception of regulatory response and participation within corporate programs;
- ◆ Acknowledged limitations or barriers to regulatory discussion of practices;
- ◆ Regulatory barriers to the implementation of their plans; and
- ◆ Current contact names and numbers for law enforcement and emergency management.

In most instances, the PUC jurisdictional companies who participated in the Y2K reviews had current plans in place. In some instances, industries and/or companies who were not computer dependent, who have operations that affect limited customers, or who were not profiled during Y2K did not have these types of plans available. However, others were able to provide such plans.

IV. OVERALL FINDINGS

1.1 Emergency Response/Contingency Plans

General findings during this review showed company responses on September 11th were directly related to the availability of their plans. Companies who had plans in place executed the previously implemented procedures. Companies who did not have plans in place recognized their shortcomings, and immediately began an assessment to develop plans in the days following September 11th. The industry groups all regard their emergency plans, business plans, contingency plans and disaster recovery plans as living documents that must be continually updated and reviewed. All companies recognize the need for these plans to be routinely updated with the latest contingencies, procedures and emergency contacts. The contents of the plans, industry-wide, were similar, but it was found that some companies put a great effort into the content of the plans, but disregarded the availability of the physical plans in an emergency situation. These companies relied heavily on electronic copies that may not be available, depending upon the emergency or event. Specific contingencies were reviewed including, but not limited to, bomb threats, chemical storage, local police and fire contacts, emergency notification procedures, media policy and statements, weather-related emergencies, power outages, communication loss, corporate contacts, contacts of high priority customers, and contacts at state agencies. Staff made recommendations to address any deficiencies. It was discovered that some companies rely extensively on the 911 emergency communication system to access outside response personnel, while skilled employees, guards or emergency personnel are able to respond to situations in-house, for the other companies.

All companies were queried as to their involvement and networking with local and state law enforcement, and local and state emergency management agencies. Companies were provided with an updated contact list for PUC emergency management personnel and their specific areas of expertise. Companies test effectiveness and efficiency of implementing these plans by different means, including tabletop and real-time exercises. If not already doing so, companies were urged to include law enforcement and emergency responders in any drills, testing and training. Most companies conduct drills, training and testing regularly, but the scope of training or drills expanded with the increased possibility of a terrorist event. Almost all companies have added additional training for terrorism events. Utilities in large metropolitan areas put such plans into use almost daily due to the vast number of emergency situations created by

their geographic location and sheer volume of population. All companies responded in a positive manner as to their involvement with community contacts who were familiar with company procedures, locations, and what would be expected of them in the event of an emergency or security event. Conversely, the companies knew who to notify in such an event, have been in recent contact with appropriate personnel and have updated names, numbers and prospects of what the organization can offer.

1.2 Vulnerability/Risk Assessments

Vulnerability and Risk Assessments are reviews that allow the utilities to look at system components and locations based on a ranked threat of a physical attack or other event. Such assessments can be completed using company personnel that have a vast knowledge of the working of the system, through a hired security consultant, or utilizing both resources. Every company reinforced the need for developing a "vulnerability or risk assessment" post September 11th. These assessments allow the utilities to re-evaluate their "critical" areas and look at system components, specific locations and vital operational needs based on a ranked threat of an event. Each industry group, though providing a comparable end product using similar components, assesses risk and vulnerability on an individual basis. The assessment determines which components, or areas, are the most critical for a particular company or facility and indicates where security infrastructure and personnel should be focused. The Vulnerability and Risk Assessments also address any deficiencies in response and contingency planning.

Some companies completed, or were in the process of completing, such a study prior to September 11th, while other companies decided to conduct the assessment as a result of September 11th. All companies established internal security task forces and have implemented security-related upgrades to varying degrees for plant emergency and operating procedures. Companies with existing plans reviewed their risks and vulnerabilities due to the events of September 11th and a new approach to "worst case scenarios." Companies without plans made the Vulnerability and Risk Assessments a top priority. This assessment process, although somewhat generic by industry type, requires a utility to focus on its own company or facilities to indicate where security and personnel should be vigilant.

Some companies conducted this assessment utilizing "in-house" talent and personnel, while others hired outside, independent consultants to provide assistance, or a combination of both. Company personnel have a vast, intimate knowledge of the workings of their systems, while an outsider may provide a "fresh" perspective. Overall, each company recognized the seriousness and magnitude of the events and the potential for future actions. Each wished to prepare their company and their locations for minimal disruption, mitigate risks or vulnerabilities, and be prepared to react, respond and restore service in a safe

and timely manner. However, all companies recognize their limitations, where preventing and stopping any and all terrorism events may not be feasible for many reasons. Efforts of the companies are now directed toward detecting, delaying impact, and responding to such events.

The recently adopted national legislation on bio-terrorism (HR 3448), Title IV deals with Drinking Water Security and Safety. Title IV requires water utilities to conduct vulnerability assessments and submit them to the Administrator of the Environmental Protection Agency (EPA). This requirement is explained in further detail in the Water Industry section.

At this time, other industries have not been mandated to perform a Vulnerability and Risk Assessment. However, the *National Strategy for Homeland Security* dated July 16, 2002 (The *Strategy*) stresses that the private sector should conduct risk assessments on their critical infrastructure holdings and invest in systems to protect key assets. The *Strategy* expresses that this is "not only a matter of sound corporate governance and good corporate citizenship but also an essential safeguard of economic assets for shareholders, employees, and the Nation." To continue, *The Strategy* stresses vulnerability assessments are important from a planning perspective by enabling authorities to evaluate the potential effects of an attack on a given facility or sector, and then to invest accordingly in order to protect such facilities and sectors. The vulnerability assessments are building blocks for threat-vulnerability integration.

1.3 Business Continuity Plans

Business continuity is the next concern after responding to and controlling the emergency situation. This plan dictates what personnel are to replace key personnel in the situation when they can no longer carry out duties. It also addresses the availability of back-up facilities, and the procedures to restore service. Since it is not cost effective to have back-ups for each component, the companies examine the operational redundancies and capacities of the systems. Most plans contain sections for availability of back-up facilities, vendor contacts, and equipment. Most companies have redundancy in their systems if one component fails, while recognizing that the loss of several major components may cripple the system. Some companies serving large geographic regions (within the state, or having out-of-state locations) are able to re-establish headquarters or operating areas in distant locations if a specific geographic region is impacted.

Natural gas, electric, telecommunications and transportation systems are somewhat interconnected with intrastate and interstate systems, which can escalate the impact of the loss of a facility and yet also provide necessary redundancy to mitigate the impact of an event and aid in recovery. At the same time, the fact that water, wastewater, steam and some transportation facilities are

not interconnected can isolate and contain an event, but may devastate a system that is totally self-sufficient and not interconnected.

For a number of years, most energy companies have had mutual aid agreements in place with neighboring utilities for replacing major equipment or components, and have initiated processes for sharing personnel. This process, which has been in place in the electric industry and on a limited basis in the natural gas industry, could serve as a model for other industries. The cooperation of mutual aid programs, in general, has been well served during times of need. This helps to provide a timely restoration of service and reliable delivery of energy while minimizing costs for excess supplies and personnel that might only be used during an emergency. This same type of agreement does not seem to be utilized in other industries. The PUC suggests that mutual aid agreements should be considered by all industries to better serve the public in times of emergency.

At all larger and most mid-sized companies, there is a detailed succession plan for a scenario involving loss of key personnel. These plans may or may not be formalized, legal agreements, but often are written corporate policies. Smaller companies did not initially consider succession plans, but post-September 2001, are developing the plans. Some companies have limited the means of travel for corporate officials and the number of corporate officials traveling together. Others are in the process of reviewing the need for such a procedure. Following September 11th, some companies updated plans and procedures while others gave less attention to them. PUC visits prompted a closer review of the business continuity plans.

In general, natural gas, water, telecommunications, and electric companies have a very low turnover rate of employees in management and labor related or technical positions, with most employees working their entire career for just one company, or hired from another company in the industry. The majority of workforce reductions in recent years have occurred through the combination of an early retirement option, normal attrition, and other selected staff reductions. Customer service (bills, complaints, terminations, etc.) areas tend to have higher turnover rates, but are average for service employees in any industry. In the motor carrier and rail industries, there is generally a low turnover in employees; the exception is in the small (taxi and limousine) motor carriers. Rail conductors and engineers who are often away from home and have on-call schedules are also high turnover positions due to the nature of the job.

New employees receive some degree of background check at all companies, but the extent of a background check varies company to company. There is a cost associated with each background check and there seems to be industry-wide confusion about the types of information available from state and local police. Early assessments conducted with companies described a void in receiving centralized, extensive data from any one source. Companies stated that no matter what the cost, the means did not exist to request a detailed statewide or

nationwide criminal and driver license background investigation. However, other companies stated that the means do exist, but often at high expense to perform a detailed background check. This is usually available from an independent firm, not a law enforcement entity.

For the most part, the Human Resources Departments of the companies conduct pre-employment security checks through the use of third party, independent firms, or the PSP. Costs can vary from \$10/applicant to \$150/applicant, depending on the level of background check requested by the company, and additional features such as pre-employment physical exam and/or drug testing. Most background checks take from ten days to four weeks for the company to receive the results. Contractors and vendors to the utilities are usually verified by their own firm's employment screening which may or may not include extensive background information. Additional security checks may be necessary for select employees who work closely with other companies, and is based upon the other's requirements, such as some 911 centers, military operations, or nuclear plants.

Contracted security guards were hired at some companies while others prefer to utilize a corporate security staff. Union agreements at some companies restrict the hiring of outside, or contracted, security guards. A large number of companies hired off-duty law enforcement employees on September 11th and the days following to serve as additional security for their facilities.

1.4 Cyber Security and Disaster Recovery

Almost all companies surveyed have addressed Cyber Security. To some degree, each company addressed network access restrictions, physical security of computer operation areas, back-up capabilities, restoration efficiencies, recovery plans, firewall installations, email, internet usage and all computer-related security issues. Some companies feel that security and back-up facilities are best operated with company personnel while other companies found it necessary to hire a provider, or vendor, for information technology services. Many have hired consultants to determine cyber security effectiveness and resilience to hacking. One area of staff concern was the number of companies, utility or non-utility, relying on the same provider or vendor for emergency system restoration service.

Currently, the physical and cyber infrastructures are connected, while the security for physical and cyber infrastructures are not coordinated. Cyber Security was addressed during Y2K readiness. Companies that prepared for Y2K are able to build from a solid foundation. The companies recognize that with ever changing technology, security of a cyber network is a continuing battle and efforts can not be handled complacently. Other companies who did not prepare for Y2K have strengthened their cyber security in recent years. Attacks on electronic and computer networks, which are linked to critical infrastructure,

present an almost infinite range of potential targets. Cyber incidents remain an increasingly significant threat and should be addressed over immediate and long-term periods.

Most companies maintain separate networks for their customer service and billing operations that are distinct from the overall corporate network, and would not affect control operations if a problem existed on either system. Supervisory Control And Data Acquisition (SCADA) is commonly used in the natural gas, water, wastewater and electric industries to operate and monitor system operational parameters. The security of such operating systems was addressed. The common response was that the systems operate independently of the network and if, for some reason, the SCADA is inoperable, operations can be completed manually. Access to the SCADA system is based on various levels of protection, with only a few employees having access to each level as appropriate to their job description. Operators are immediately able to change passwords upon attempted breach of security or switch to manual operations.

Disaster Recovery Plans were reviewed. A Disaster Recovery Plan establishes the process to recover a cyber system in the case of a major loss of infrastructure or access capabilities. Several companies test these regularly and have elaborate plans in place. Most companies are maintaining back-up facilities off-site and are able to replicate/operate their business upon a moment's notice. A few companies have contracted services with an outside vendor and would require assistance in maintaining or restoring their normal operations. This would help to minimize the downtime of business practices. Computer back-ups and contingency plans are implemented and have been reexamined since September 11th.

One company noted their use of "cyber insurance" to protect themselves from liability if a customer's information is transferred or an identity is stolen during a "hack." This appears to be a relatively new and seldom used measure of protection for companies.

A draft proposal for the Federal Energy Regulatory Commission (FERC) security standards was issued on July 18, 2002, as a joint effort of FERC and the North American Electric Reliability Council (NERC) to identify minimum daily security requirements to be included in a proposed Notice of Proposed Rulemaking (NOPR) for Standard Market Design, which was issued on July 31, 2002. This draft proposes to ensure that electric market participants have a basic security program protecting the electric grid and market from accidental or malicious acts that could cause wide ranging, harmful impacts on grid operations. This security program will cover governance, planning, prevention, operations, incident response, business continuity for cyber and physical security, and will apply to the ISO, marketers, transmission owners, power producers, load serving entities, and NERC members. Effective January 1, 2004, and January 1st each year thereafter, participants must file self-certificates signed by an officer of the

company indicating compliance and identifying non-compliance. Failure to comply will result in loss of direct access privileges to the electric market. This minimum set of measures will incorporate NERC standards by reference.

1.5 Policy for Financial Protection and Insurance Liability

Cost recovery is generally not as high of a concern to natural gas, electric and telecommunications companies as to other industries. Most consider the security upgrades a "cost of doing business" and have been implementing such physical changes and enhanced security measures for many years. Some companies are very advanced and have employed the latest technology. However, these industry groups are very concerned about other measures that might be available for cost recovery. Water, wastewater, steam heat and transportation companies are heavily dependent upon cost recovery to assist in completing upgrades and enhancements, or to undertake additional projects. Most companies in these industries are operating with the basic equipment or supplies in place and their security programs should be enhanced. The respondents predict significant increases in security-related capital and operating costs that will not be recoverable through their rate base.

Many utilities have concerns with regard to neighboring, competitive states and how they will recognize security costs -- i.e., offering such tax incentives or enhancements that would leave Pennsylvania at a competitive business disadvantage and undermine the impact on utility markets. In Pennsylvania, the price of electric generation and natural gas production has been deregulated and Pennsylvania-based generation/production companies no longer have the ability to recover costs through traditional rate cases at the PUC. As a result, the industry respondents have put forth suggestions on potential ways to recognize the costs associated with security such as:

- ◆ General security surcharges on utility bills with funds appropriately divided among generator/providers, where applicable;
- ◆ Tax breaks for security-related capital and operating costs;
- ◆ Critical infrastructure security grants and low interest loans; and
- ◆ Other financial incentives.

Another cost of concern is insurance coverage. Insurance costs and coverage needs vary company to company, but most companies expect, and some have incurred, increases in their property, liability and workers compensation premiums. Some have received quotes of increases from 10% to over 55% of their previous policy. Another great concern, in addition to the increased premiums, is the exclusion of terrorist acts from the insurance policies and dilution of existing coverage. Most respondents stated that while supplemental terrorism coverage is becoming available, it is still cost prohibitive, only low limits of coverage are being offered, and to some extent forcing companies to self-insure such risks. Some insurance companies adhere to the federal definition of

"terrorism" while others include almost all types of events, even civil disobedience, under the umbrella of "terrorism." One company that serves in other states said some states have laws in place that would not allow terrorism restrictions. Property insurance and workers compensation increases are currently expected to be higher than other insurance types. Workers compensation issues only began to be realized by the industries in late May 2002, toward the end of the assessments due to the long time processing property and liability claims post September 11th. Some companies did not renew their insurance policies prior to the assessment being conducted. Thus, a complete explanation of increases are unknown by many companies at this time. However, all industries are anticipating an increase and potential for problem areas. Even the underwriters for utility-owned consortiums for self-insurance are anticipating higher costs.

Page 49 of The *Strategy* describes one initiative in the proposed Department of Homeland Security for states to address in order to enhance market capacity for terrorism insurance:

"The need for insurance coverage for terrorist events has increased dramatically. Federal support is clearly critical to a properly functioning market for terrorism insurance; nonetheless, state regulation will play an integral role in ensuring the adequate provision of terrorism insurance. To establish a regulatory approach which enables American businesses to spread and pool risk efficiently, states should work together and with the federal government to find a mutually acceptable approach to enhance market capacity to cover terrorist risk."

The Commission believes that it has adequate statutory authority to provide current and timely recovery to companies for security expenditures under 66 PA C.S. § 1307. However, the current statute prohibits its applicability to natural gas distribution companies over \$40 million in revenues and to all common carriers. Conventional timeframes for recovery are available to those entities under §1308. In addition, most electric distribution companies are subject to restructuring settlements implemented under Chapter 28, which extended their transmission, distribution and generation rate caps. In order to provide timely recovery, rather than deferred recovery, for the electric companies, the Commission would need to conduct a review and direct specific upgrades pursuant to 2804 (4) (iii) (E) as an exception to the rate cap. For non-regulated entities, such as municipalities, authorities and gas/electric suppliers, legislative solution to their recovery can only be fostered by grant or tax relief measures. Such measures would also provide cost benefits to regulated companies, lessening the need for rate relief.

On September 14, 2001, the FERC issued a statement of policy and assured its regulated companies that it will "approve applications proposing the recovery of

prudently incurred costs necessary to further safeguard the nation's energy systems and infrastructure made in response to the heightened state of alert the country is now experiencing." The FERC encourages the regulated electric, natural gas and oil companies to take all precautionary steps needed to secure the facilities. The FERC committed to expedite the priority processing of applications to recover costs from wholesale customers. Companies may propose a separate rate recovery mechanism, such as a surcharge over currently existing rates or some other cost recovery method. Safety and reliability of the energy supply and infrastructure are viewed by the FERC as critical to the nation's economic well being. To date, two companies filed applications in order to recover costs incurred resulting from increased security measures. One company was granted the recovery and one company was approved to defer accounting of its incremental costs for security, insurance, and disaster recovery.

Industries are spending money or planning to spend money on defending and protecting their facilities and the critical infrastructure operations of their businesses. States and the federal government can offer these industries economic incentives to mitigate their risks through cost recovery, cost minimization, or proper insurance coverage.

V. COMPANY/INDUSTRY PARTICIPATION IN COMMUNITY

Some companies are participating in the Federal Bureau of Investigation's (FBI) InfraGard program. InfraGard is a cooperative undertaking between the U.S. Government led by the FBI and the National Infrastructure Protection Center (NIPC) and an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to increasing the security of United States' critical infrastructures. The InfraGard initiative was developed to encourage the exchange of information by the government and the private sector members. Private sector members and a FBI field representative form local area chapters. These chapters set up their own boards to govern and share information within the membership.

The NIPC and the FBI play the part of facilitator by:

- ◆ Gathering information and distributing it to members;
- ◆ Educating the public and members on infrastructure protection;
- ◆ Disseminating information through the InfraGard network;
- ◆ Producing valuable analytical products on information received through the InfraGard network; and
- ◆ Opening the doors of communication between government and private sector members.

Feedback from participating companies has shown that some of the InfraGard chapters (based on geographic areas of the state) are more active than other

chapters. There does not appear to be consistency among chapters or activities by members. Some companies are considered members because they "show up for meetings" and receive daily alerts. Other chapters have advisory positions and very organized meetings with specific rules and actions and heavy participation.

Utility companies serving Western Pennsylvania participated actively in the City of Pittsburgh's Emergency Operations Working Groups. Pittsburgh Mayor Tom Murphy formed the Emergency Operations Working Groups in October of 2001 to thoroughly review the City's emergency preparedness in the wake of September 11th.

Each of the seven Working Groups reported their findings to the Mayor's Pittsburgh Security Council. Each working group was led by an individual recognized as an expert in their field and was supported by the appropriate staff from the City of Pittsburgh. The mission of each working group addressed the following issues:

- ◆ Assess the risk to each designated area;
- ◆ Assess response procedures and capabilities;
- ◆ Identify where gaps exist in these response procedures and capabilities; and
- ◆ Develop recommendations to remedy those gaps.

On May 21, 2002, Mayor Murphy announced the creation of a permanent new agency, the Emergency Management Advisory Council (EMAC), that will continue to advise him as he implements the findings of the Emergency Operations Working Groups. The EMAC continues to meet on a regular basis in an effort to constantly improve the City's blueprint for emergency management.

Regional Counter-Terrorism Task Forces (RCTTF) were established in 1998, by PEMA, in response to the growing threat of the use of Weapons of Mass Destruction against the United States. The RCTTFs are aggregated county groups augmented by the various state and federal officials having responsibility in the area. Pennsylvania developed nine RCTTF groups to primarily integrate federal, state and county responses, institutionalize mutual aid in the region, establish regional response groups and encourage regional networking. Each RCTTF group is comprised of emergency managers, law enforcement, fire service, emergency medical services, hazardous material experts, health officials, postal inspectors, public works, and other county and local elected and appointed officials.

On June 4, 2002, the PUC and PEMA contacted all survey participants to encourage their participation with the nine Regional Counter Terrorism Task Forces in Pennsylvania. Both agencies believe that utility participation on the Task Forces will help the utilities to better respond to terrorist threats and provide the Counter-Terrorism Task Forces with a utility perspective. Companies were

encouraged to contact the Task Forces and provide written notification to the PUC prior to June 21, 2002, of their participation. A map of the nine regions is attached as Appendix C.

VI. INDUSTRIES EXAMINED

The PUC regulates more than 7,100 public utility entities furnishing the following in-state services for compensation: electricity, natural gas, telephone, water, wastewater collection and disposal, steam heat, transportation of passengers and property by train, bus, truck, taxicab, aircraft, boat, and pipeline transmission of natural gas and oil. Municipal utility service is exempt from PUC regulation, with the exception of that part furnished beyond a municipality's corporate boundaries. Rural electric cooperatives also are exempt from PUC regulation. However, some municipal utilities and the PREA were included in this survey.

Over the last four years, the PUC has worked diligently to ensure an effective transition to competitive markets in the electric and natural gas industries. Customers may now choose from a number of suppliers that generate their electricity or supply their natural gas. The number of telecommunications companies offering local phone service in competition with the incumbent phone companies is also steadily increasing. Although parts of the natural gas, electric and telecommunications markets are deregulated, customers still receive transmission and distribution services, the "lines and wires" from their local utilities, which also maintain the electric and telecommunication lines or natural gas pipelines. While some of these areas are not "typical" utility services in a deregulated world, they are considered integral parts of service to the regulated customers, and were included in this assessment.

The following industries and company types were the subject of the survey:

Electric

- ◆ Electric Generation (6)
- ◆ Electric Distribution (8)
- ◆ Electric Suppliers (3)
- ◆ Nuclear Generators (3)
- ◆ Electric Power Pool (1)

Natural Gas

- ◆ Natural Gas Distribution (11)
- ◆ Natural Gas Suppliers (2)
- ◆ Natural Gas Interstate Pipelines (5)
- ◆ Natural Gas Storage (3)
- ◆ Natural Gas Production (1)

Telecommunications

- ◆ Incumbent local exchange carriers or "ILEC" (5)
- ◆ Competitive local exchange carriers or "CLEC" (1)
- ◆ Inter exchange carriers or "IXC" (1)

Water/Wastewater (8)

Steam Heat (2)

Transportation

- ◆ Rail (3)
- ◆ Motor Carrier (3)
- ◆ Taxi and Limousine (3)
- ◆ Buses (3)

VII. REPORT ON THE INVESTIGATION BY INDUSTRY

2.1 Electric Generation and Suppliers

Currently, there are sixty-seven licensed electric generation suppliers (EGS) able to supply electricity to consumers in Pennsylvania. However, only thirty-one suppliers are providing competitive services at this time. Pennsylvania Generators produced 195,645,000-MegaWatt hours (MWh) in 1999, with 96,023,000 MWh of that production consumed in the Commonwealth. Pennsylvania had net exports to other states of 99,622,000 MWh during 1999.

Six owners/operators of electric generation in Pennsylvania were surveyed and interviewed to address the industry as a whole and identify any trends within the industry. Respondents represent the non-nuclear (i.e., coal, oil, natural gas and hydro powered) portion of the generation industry. The nuclear industry is addressed in a separate section. Additionally, three licensed electric generation suppliers who serve as supplier/marketers to buy and resell generation supply, but do not own or operate the generation they provide were also profiled.

There is a distinct business practice for both of these groups. While similarly providing a generation product into the Power Pool, the security aspect is obviously of larger concern to the owner/operator than to the supplier/marketer. The owners/operators' concerns for security are consistent with the transmission and distribution companies' concerns as both have physical equipment, facilities and operations at risk. The concern for a supplier/marketer is not as great as they do not physically possess any tangible production means.

In the absence of a supplier/marketer serving in Pennsylvania or the Independent System Operator (ISO), the responsibility for providing electricity would ultimately fall upon the Provider of Last Resort (POLR) who is often the traditional

distribution company. The POLR provides generation services to those customers that do not choose another supplier, are unable to find a supplier willing to serve them, or for some reason no longer receive generation services from another supplier.

The ultimate security objective of the electric generation owners and operators is to maintain the physical and cyber security of their facilities in order to ensure the adequacy of supply to the electric grid system. To reach this goal, the industry must protect its most critical assets. Some of the electric generation industry's key assets include the generation facility and equipment, fuel supply, transmission lines, substations and switchyards directly connected to the generation site and the facility control systems.

Owner/operator companies are participating in task forces and working groups sponsored by various industry trade associations, such as the Energy Association of Pennsylvania (EAP), the Edison Electric Institute (EEI), and the NERC, to name a few.

The owner/operator companies currently have emergency response plans and have had such plans in place for years to deal with weather and security-related emergencies. In 1999, all companies initiated a review and update of their emergency response and contingency plans due to Y2K. All of the companies surveyed are again in the process of reviewing and updating their emergency response and contingency plans due to recent events.

All owner/operators are in the process of completing or have completed vulnerability assessments.

All of the respondents had succession plans for key personnel, as a corporate policy, but some are now in the process of placing those plans into legal format. Companies do not have back-up facilities for the actual generation plants, but would have back-up facilities for control room operations.

All owner/operator companies involved in the assessment have addressed cyber security. All respondents have Cyber Disaster Recovery Plans in place. In all cases, back-up data is stored at a remote location. Generation facilities profiled during Y2K responded to staff inquiries about computerization of their operations at that time. Many plant operations are performed by computer function, but some are also controlled via manual actions. Even the computer dependent controls may be operated on manual override. In the event an intruder penetrates a SCADA system or communication through telephone lines is lost, the respondents state that they have the ability to continue operations manually and the ability to employ radios and satellite phones for communications. Such plans were tested and implemented during the Y2K rollover to avoid any generation plant outages or energy shortages due to potential computer component malfunctions.

Most companies expect, and some have addressed, increases in security-related capital and operating costs and their property, liability and workers compensation premiums. The exclusion of terrorist acts from insurance policies is of great a concern as the increase in premiums.

As discussed above, in Pennsylvania, the price of electric generation has been deregulated and Pennsylvania-based generation owner/operator companies no longer have the ability to recover costs through traditional rate cases at the PUC. In addition, there must be special attention to how surrounding states are recognizing security costs related to electric generation such that Pennsylvania companies are not left at a competitive disadvantage.

Specific to the supplier/marketer respondents, only one company is participating in the FBI InfraGard program, whereas almost all generation owner/operations are members. One of the supplier/marketers profiled has a Y2K plan in place for cyber operations, but did not include emergency response, business continuity, or contingency planning. Emergency personnel listings and contact with local law enforcement or emergency management agencies was not perceived as necessary by the supplier since it does not have any key assets or risks. Plans for cyber disaster recovery are in place and have been updated and tested since September 11th. The company states its insurance cost varies by type and could not provide any information on whether it has experienced increased rates; however, "sabotage and terrorism" have been excluded from coverage. The supplier/marketer does have a third party independently verify employee background information on behalf of their Human Resources Department.

The other supplier/marketer company responded that they reside in a leased office space, have no key assets or personnel, did not participate in any Y2K reviews, and have no plans involving emergency response, business continuity, contingency planning or cyber disaster recovery. The supplier/marketer has not experienced any changes in insurance policies to date. The company does protect their cyber system with encryption, virus protection, firewalls and off-site backup of records. They do not drill for any type of incidents, nor do they have a formal, written disaster recovery plan. A Human Resource Department provides the services for a background check of employees.

2.2 Electric Transmission and Distribution

In 2000, there were sixteen electric distribution companies (EDC) serving Pennsylvania consumers. Eleven of these are traditional utilities and five are municipal power companies serving outside their corporate boundaries. There are more than 4.7 million residential customers in Pennsylvania, and over 632,000 commercial, industrial and other customers dependent upon the delivery of electricity to their homes and workplaces. Security surveys were conducted with the seven largest PUC jurisdictional electric distribution companies, the PREA member companies, and PJM Interconnection, the ISO.

Throughout the States of Pennsylvania, New Jersey, Maryland, Delaware, Virginia and the District of Columbia, electric energy that is bought and sold, along with the energy imported and exported through this region, is exchanged through the ISO. The ISO performs two key functions: (1) the coordination of the power grid and reliability of that system in the region and (2) the operation of multiple markets including the wholesale energy market. Pennsylvania is dependent upon the activities of the ISO to ensure reliability of the overall electric system within this state.

Participants (ISO members) are entitled to trade electricity through the ISO. They include power producers, power marketers, distributors, cooperatives, and municipalities. Buyers and sellers trade electricity and arrange for transmission of that electricity through the ISO, which manages the region-wide transmission grid.

To follow the actual increases and decreases of demand on the system, the ISO dispatches (call on and off) the required generation to meet the actual system demand.

The ISO is also responsible for the safe and reliable operation of the Mid-Atlantic electric system. As demand for electricity shifts up or down throughout the day, the ISO keeps supply and demand in balance by giving instructions to power suppliers and purchasers regarding the amount of energy that is to be supplied to or taken off the system. Operating from the Control Room, the system operators and staff perform this control function twenty-four hours per day, seven days per week (24/7).

Once electricity is generated, the ISO dispatches the electricity over transmission lines, which carry it to load centers (heavy usage areas) and through distribution lines, which carry the electricity to where it will be used in homes and businesses. Electricity by its nature cannot be stored easily or economically. As a result, it must be generated, transmitted and distributed almost at the moment it is needed. Electricity flows over the path of least resistance and is difficult to direct to a specific path like water or gas in a pipeline. Due to this reason, substations perform "step-up" and "step-down" operations to increase or decrease the voltage where it is needed. Higher voltage will travel farther with minimal resistance, while lower voltage is necessary to power our homes and businesses.

The ultimate security objective of the electric Transmission and Distribution (T & D) operators is to protect and maintain the integrity of the electric distribution and transmission systems. To reach this goal, the industry must protect its most critical assets. Some of the electric distribution and transmission industry's key assets include the transmission and distribution lines, the transmission substations and switchyards, SCADA systems and the ISO dispatch centers.

The companies that comprise the electric distribution and transmission industry have emergency response plans in place and have had such plans in place for years to deal with weather and security-related emergencies. In 1999, in response to cyber and terrorist threat concerns associated with Y2K, all companies including the ISO, initiated a review and update of their emergency response and contingency plans. Now, as a result of the various threats that have presented themselves since September 11th, all of the companies surveyed are again in the process of reviewing and updating their emergency response and contingency plans.

During site visits, emergency response and contingency plan topics were reviewed with survey respondents including, but not limited to:

- ◆ Response to direct and specific bomb threats;
- ◆ Response to general security threat levels;
- ◆ Security incident response procedures and drills;
- ◆ Initiation and/or familiarization of law enforcement and fire department contacts; and
- ◆ Verification of updated contacts for the company personnel, high priority customers, and state agencies.

Some specific responses are provided below and were received from the ISO, T & D companies, and PREA as to their activities on September 11, 2001:

- ◆ Staffed critical facilities and coordinated enhanced physical security;
- ◆ Reviewed system limits and increased reserves;
- ◆ Reviewed/canceled maintenance outages;
- ◆ Staffed redundant control sites; and
- ◆ Emergency plans in place (Y2K model).

All respondents are in the process of completing or have completed vulnerability assessments by either utilizing internal expertise or hiring consultants. Companies are participating in task forces and working groups sponsored by various industry trade associations, such as the EAP, the EEI, NERC and the Electric Power Research Institute (EPRI), to name a few. In addition, the industry participates with law enforcement and security liaisons, including:

- ◆ National Infrastructure Protection Center (NIPC);
- ◆ FBI InfraGard Program;
- ◆ FBI Awareness of National Security Issues & Response (ANSIR);
- ◆ Department of Energy (DOE);
- ◆ NERC Critical Infrastructure Protection Working Group;
- ◆ EEI Security Committee;
- ◆ Township Police, Fire and Emergency Management Agency(EMA) Departments;

- ◆ County Regional Tactical Team and Bomb Squad; and
- ◆ Contracted Private Security Firms provide specialized services (e.g., armed officers, electronic countermeasure sweeps and bomb sniffing dogs).

Since September 11th, changes to the ISO, T & D companies, and the PREA include: developing a new crisis section to the Emergency Procedures Manual Security Levels, adding these procedures to the operator training and emergency procedure drills, and creating a National Reporting.

Business continuity is the next concern after responding to and controlling the emergency situation. All of the respondents had succession plans for key personnel; however, some are just now in the process of placing those plans in writing. In addition, each respondent had a Business Continuity Plan for continuing business following the loss of a corporate headquarters or a dispatch center. For example, a key facility to all electric distribution and transmission companies is the building that houses the SCADA system. Each respondent had a back-up SCADA facility from which electricity could continue to be dispatched, should the primary location become inoperable or inaccessible.

Examples of new business continuity planning were offered by the industry:

- ◆ Enhanced physical security supplements ongoing processes to prevent interruption of operations and business functions;
- ◆ Expanded and upgraded external facilities to assure continuity of bulk power system operations and expeditious resumption of energy markets in the event of a site emergency;
- ◆ Comprehensive plans for resumption of support processes are in place for all business units;
- ◆ Priority placed on maintaining continuity of the transmission system and dispatch operations, where a disruption would have the most serious consequences. Alternate site functionality has been provided for this service;
- ◆ The approach has been to protect operations from potential risks. High levels of physical security and system redundancy reduce the probability of service interruption; and
- ◆ Efforts to further reduce the probability of business interruption and expand the functions that can be resumed at a remote site.

The hiring of quality personnel is key to implementation of each respondent's Business Continuity Plan. Each respondent stated that new employees receive some degree of background checks, but the extent of background checks varies from company to company. The time and cost associated with background checks varied by respondent, with many respondents concerned that they were unable to timely and cost effectively perform statewide or nationwide criminal background checks. Another area of concern to the respondents was that, because of apprehension over liability issues, previous employers do not give

information about employee character or work habits, but only provide the dates of employment.

Additionally, companies offered summaries of their physical security improvements after September 11th:

- ◆ Heightened security;
- ◆ Central monitoring station;
- ◆ 24/7 security coverage;
- ◆ Expanded access control and video surveillance;
- ◆ Systems/coverage/motion detection ;
- ◆ Perimeter protection;
- ◆ Perimeter wall and boulders;
- ◆ Vehicle access barriers at entrances and strategic locations;
- ◆ Constructed central receiving building;
- ◆ Incoming mail, packages and deliveries will be scanned through x-ray security scanning system;
- ◆ Additional security doors added to strategic locations;
- ◆ Expanded and enhanced physical access control systems;
- ◆ Reviewed and re-authorized access to critical infrastructure areas;
- ◆ On-going auditing of physical security program;
- ◆ Reviewed and revised current security policies and procedures;
- ◆ Enhanced emergency operations plans;
- ◆ Enhanced security awareness program;
- ◆ Provided travel advice to travel coordinator;
- ◆ Expanded local law enforcement patrols.

All electric distribution and transmission companies involved in the survey have addressed cyber security. Some companies utilized in-house expertise, while a provider or vendor, supplements other companies. Many have hired consultants to determine cyber security effectiveness and resistance to hacking.

SCADA systems are critical to the operations of the electric T & D industry to operate equipment and monitor system parameters. Most respondents' SCADA systems can be operated remotely via a laptop. However, remote access is often limited to only two or three company persons. In the event the SCADA system is penetrated by an intruder, the respondents state that they have the ability to remove the remote access operation function from any piece of equipment that is being manipulated in an unwanted fashion and control the equipment manually in the field. Such plans were tested and implemented during the Y2K rollover to avoid any electrical outages due to potential computer component malfunctions.

All respondents have Cyber Disaster Recovery Plans in place. These recovery plans are designed to bring critical computer systems back on-line following

some type of catastrophic failure. In all cases, back-up data is stored at a remote location and, in many cases, the applications themselves are available for use at alternate worksites. Many of the respondents have "hot sites" available where operations can be performed almost instantaneously. By this description, these sites have readily available phone, fax, and computer access lines and equipment for key personnel or operations. Companies without "hot sites" have "cold sites" available where operations can be performed in a timeframe of an hour or two, or more quickly for a very limited number of employees. Respondents test these locations during drill exercises, often performing their daily operations from the other sites transparent to end-users or their overall operations.

After September 11th, cyber security was addressed by the review of standards and additional standards being developed along with the refinement of procedures for operating systems. Hardware/Software, networks and connectivity, applications and data, practices under external audit, periodic internal audit review with recommendations and follow-up, compliance monitoring, periodic internal vulnerability testing, and penetration testing by external party.

Methods for cyber security include hardening of the cyber environment by use of: additional firewalls, stricter authentication for remote access, two factor authentication, more detailed internal standards and additional project reviews. Companies implemented additional intrusion detection points, development of incident response team, correlation of events analysis, monitoring centers operational 24/7, and expansion of website encryption.

Security awareness is becoming mandatory for all employees and contractors, with updates annually. Sharing of data and information occurs through community and industry groups such as the FBI InfraGard, the NERC - Critical Infrastructure Protection Group, EPRI - Enterprise Infrastructure Security Program, and a communications loop back to ISO members.

The recovery of costs incurred for security measures implemented in response to September 11th is a concern of each company. Some respondents predict significant increases in security-related capital and operating costs, while others believe that the additional costs will not be burdensome on rates at this point. In Pennsylvania, the PUC jurisdictional electric distribution companies are subject to capped rates for varying amounts of time. As a result, the industry respondents have put forth suggestions on potential ways to recognize the costs associated with security such as:

- ◆ Security surcharges on utility bills, where applicable;
- ◆ Tax breaks for security-related capital and operating costs;
- ◆ Critical infrastructure security grants and low interest loans; and
- ◆ Deferral of recovery of security costs through recognition of regulatory assets.

Another cost that respondents have concerns about is insurance coverage. Insurance costs vary company to company, but most companies expect, and some have incurred, increases in their property, liability and workers compensation premiums. An equally great concern is the exclusion of terrorist acts from the insurance policies. Most respondents stated that while supplemental terrorism coverage is becoming available, it is still cost prohibitive and to some extent is forcing companies to self-insure such risks. This is becoming a burden to security practices.

2.3 Nuclear Generation

Nuclear power plants in Pennsylvania are: Limerick Generating Station Unit 1 and Unit 2; Peach Bottom Atomic Power Station Unit 2 and Unit 3; Three Mile Island Nuclear Station Unit 1 and Unit 2; Susquehanna Steam Electric Station Unit 1 and Unit 2; and Beaver Valley Power Station Unit 1 and Unit 2.

As an overview, the security systems at nuclear power plants include measures that provide deterrence, detection, delay, assessment, and armed response. All these security features are designed to collectively prevent radiological sabotage at nuclear power plants.

Security Areas

In order to understand the security at nuclear power plants, it is important to note that several different kinds of security areas exist:

1. **Owner Controlled Area** – The largest part of the plant site, usually several hundred acres. This typically includes all the property owned by the utility. In this area are buildings typical of any industrial site, such as warehouses, office buildings and large electrical distribution centers. Prior to September 11th, there were no security checkpoints controlling entry into the Owner Controlled Area. Since September 11th, an Owner Controlled Area vehicle checkpoint has been implemented at sufficient distance to stop an explosive device.
2. **Protected Area** – Within the Owner Controlled Area is a security area called the Protected Area. The Protected Area is fenced and gated and incorporates sophisticated intrusion detection devices. Following events at Three Mile Island (TMI) in 1993, Protected Area fences have been increased by the addition of concrete barriers that prevent vehicle intrusion and removable barricades at vehicle entry points. Normal

entry into this area is through guarded access points with security measures that include passage through a metal detector and an explosive detector. In addition, all hand-carried items are x-rayed. Vehicle entry is through a set of double gates and involves detailed search procedures in, under and around vehicles before they are allowed into the Protected Area. The Protected Areas contain much of the non-nuclear side of the plant such as the Turbine Building, which contains equipment similar to that at a non-nuclear power plant. Armed security guards routinely patrol the Protected Area.

3. **Vital Area** – Inside the Protected Areas are the Vital Areas of the plant. The Vital Areas contain equipment, systems, devices, and nuclear material that the failure, destruction, or release of which could directly or indirectly endanger the public health and safety by exposure to radiation or radioactive materials. The Vital Areas have an added level of intrusion prevention. These areas are within heavily reinforced concrete walls and bulletproof doors that are accessed by specially designed key cards or by special keys and are alarmed.

Nuclear Regulatory Commission's (NRC) Role in Regulating Security at Nuclear Power Plants

The security and safeguard regulations of the commercial nuclear power plants are the exclusive authority of the NRC. States have no jurisdiction over the security regulations of these facilities, nor do we normally have access to safeguards (security) information since this is limited to a "need to know" basis.

According to NRC regulations, the nuclear power plants are designed to meet a certain Design Basis Threat. The Design Basis Threat is a hypothetical threat (the details of which are safeguarded) that was developed by the NRC based on technical studies and information received from experts on crime and terrorism in the intelligence community and federal law enforcement agencies. The Design Basis Threat is continually compared with actual events and formally revalidated by the NRC. The installation of concrete barriers after the 1993 TMI intrusion is an example of upgrades required by the NRC.

Note that an attack utilizing an aircraft is not part of the NRC's Design Basis Threat against which nuclear power plants have to defend. The NRC is continuing to coordinate with law enforcement and intelligence agencies to assess the implications of this new manifestation of terrorism. If the NRC determines that the Design Basis Threat warrants revision, such changes would occur through a public rulemaking.

Nuclear Power Plants and Aircraft Crashes

Nuclear power plants have inherent capability to protect public health and safety through such features as robust containment buildings, redundant safety systems, and highly trained operators. They are among the most hardened structures in the country and are designed to withstand extreme events such as hurricanes, tornadoes and earthquakes. In addition, all NRC licensees with significant radiological material have emergency response plans to enable the mitigation of impacts on the public in the event of a release.

However, the NRC did not specifically contemplate attacks by aircraft such as a Boeing 757 or 767 and nuclear power plants were not designed to withstand such crashes. Pressurized water reactors (PWRs) were designed to withstand the impact of some older commercial jet airliners. Boiling water reactors (BWRs) were designed for the impact of small single engine aircraft.

World Trade Center Event and Recent Security Measures at Nuclear Power Plants

In light of the recent terrorist attacks, the NRC officials and staff have been working around the clock to ensure adequate protection of nuclear power plants and nuclear fuel facilities. This has involved close cooperation with the FBI, other intelligence and law enforcement agencies, NRC licensees, military, and state and local authorities.

Immediately after the attacks, the NRC advised nuclear power plants to go to the highest level of security (Level III), which they promptly did. The NRC has advised its licensees to maintain heightened security. The agency continues to monitor the situation, and is prepared to make any adjustments to security measures as may be deemed appropriate.

The highest level of security (Level III) involves specific actions including:

- ◆ Increased security patrols;
- ◆ Augmented security forces and capabilities;
- ◆ Additional security posts;
- ◆ Heightened coordination with law enforcement and military authorities; and
- ◆ Limited access of personnel and vehicles to the sites.

In response to the Acts of Terrorism on September 11th in Pennsylvania, New York City, and Washington, DC, the Governor of Pennsylvania issued a Proclamation of Disaster Emergency for Somerset County, PA. The Proclamation provided supplementary personnel and other resources at critical facilities in Pennsylvania, including the five nuclear power plant sites in the state. This was done to provide additional security, monitoring and other measures to protect the safety and well being of the citizens of the Commonwealth. The

Governor directed the PSP and the National Guard to provide sufficient personnel at all five nuclear power plant sites, in order to provide additional emergency response, security and law enforcement resources in the ongoing fight against terrorism. The Proclamation was amended and extended several times due to the uncertainty of credible or probable security threats, and will remain in effect until September 5, 2002, unless extended further.

In 1998, the NRC issued an Information Notice (IN-98-35) to all licensed nuclear power plants that identifies security level classifications. The information is considered "Safeguards Information" and cannot be discussed in this report. However, the Pennsylvania Department of Environmental Protection's Bureau of Radiation Protection (DEP's BRP) has access to this document.

On February 25, 2002, the NRC issued an Order Modifying Licenses to each nuclear power plant which required such licensees to implement certain interim compensatory measures to address the generalized high-level threat environment in a consistent manner throughout the nuclear reactor community. These requirements will remain in effect pending notification from the NRC that a significant change in the threat environment occurs, or until the NRC determines that other changes are needed following a comprehensive re-evaluation of the current safeguards and security programs. Complete implementation of the requirements of the Order is required by no later than August 31, 2002. Again, the information is considered "Safeguards Information" and cannot be discussed in this report. Nevertheless, the BRP has access to this document.

A comprehensive list of all NRC Advisories issued since September 11th is attached to this report as Appendix D.

NRC Security Inspection Findings

The NRC Region 1 conducts security inspections at Pennsylvania nuclear power plants. The NRC resident inspectors also conduct routine security inspections at their respective power plants. Based on the most recent NRC Region 1 inspections, all nuclear power plants in Pennsylvania have received inspection ratings of "No findings were identified." Under the NRC's new Reactor Oversight Process, inspections do not state that the plant was Poor, Average, Excellent, etc.; in fact, no positive information is contained in the reports. Hence, "no findings" means that the plants meet or exceed the NRC requirements in that area.

Role of the Commonwealth during a Security Event

States and localities have authority for emergency response planning for accidents at nuclear power stations, and business owners are responsible for security within the Owner Controlled Area. Federal guidance (NUREG-0654) does not address facility security issues. The reason for this silence is that any plant damage done by intruders may change the probabilities of accident sequences but it does not change the outcome. The purpose of these plans is to limit radiation doses; that is, to deal with the outcome regardless of the initiating event.

The Commonwealth has expertise in the areas of radiation protection and nuclear safety. However, we have no authority or expertise in the area of nuclear power plant security and safeguards, as that is the jurisdiction of the NRC.

The PSP and local police (where applicable) are the law enforcement response agencies. The PSP is capable of providing the following in addition to the post-September 11th increased presence:

- ◆ Routine Vehicular PSP Patrol Units – Receives the initial report of an emergency situation and responds;
- ◆ Intelligence Unit – Gathers criminal intelligence and coordinates intelligence operations and information;
- ◆ Criminal Unit – Conducts the criminal investigation of an incident to identify, apprehend, and prosecute a perpetrator; and
- ◆ Special Emergency Response Team (SERT) – Responds to suspected acts of sabotage, terrorism, hostage situations, and other events. The SERT is a rapid deployment team trained and equipped for such incidents.

PEMA is the designated lead agency for planning off-site radiological emergency responses in incidents/events, which are officially designated under the NRC Emergency Classification System and the agency through which the Governor exercises control and coordination during an emergency.

BRP has little expertise and no authority in the area of nuclear power plant security and safeguards. One of BRP's major responsibilities is to provide technical support and assistance to PEMA during a nuclear event or emergency. Therefore, the BRP will continue to monitor the NRC's response to these terrorist attacks with the utilities, coordinate any emergency response and plan revisions with PEMA, and advise management of this work.

Prior to 1996 and the deregulation of electricity generation, the PUC would have been concerned with the physical assets of the facility and the financial impacts of a nuclear event on the company. However, since deregulation, the PUC's primary concern rests with the impact of an event on the remainder of the electric power pool system. Examples would be the continuity of service in non-affected

areas and measuring the potential impact or loss on the remaining population. The PUC's role is consistent with BRP in monitoring the NRC's response, as well as participating in security tasks with other agencies or the utilities. The difference remains in how the PUC monitors the impact of the event and its response to operations on the electric grid. Other agencies respond to the actual event.

DEP's Nuclear Safety Oversight Review Program

In compliance with the Pennsylvania Radiation Protection Act of 1984, the DEP's BRP has implemented a comprehensive statewide Nuclear Safety Oversight Review Program. The Act has established a fee system that requires the nuclear utilities in Pennsylvania to pay for the costs associated with the implementation of this program.

The DEP's BRP Nuclear Safety Oversight consists of an experienced nuclear plant safety specialist assigned to each of the five nuclear power plant sites. The Nuclear Safety program staff conducts nuclear power plant evaluations and participates in inspections with the NRC inspectors at these facilities. The BRP nuclear power plant specialists also act as on-site representatives for the Commonwealth during emergencies. A major lesson learned from the 1979 accident at TMI-2 and the 1993 security event at TMI-1 was that independently obtained information by the BRP technical staff and their independent assessment were vital to the Commonwealth's decision-making process.

2.4 Natural Gas

The PUC's Bureau of Transportation and Safety, Division of Gas Safety acts as an agent for the Office of Pipeline Safety, U.S. Department of Transportation. The division inspects facilities and records of regulated gas companies to ensure compliance with state and federal requirements. It also investigates gas explosions. In addition, the Gas Safety Division receives meter certifications from all fixed utilities, i.e. gas, water and electric in Pennsylvania. As of 1999, there were 39,288 miles of installed natural gas mains subject to the Commission's jurisdiction. Thirty-four natural gas distribution companies and seven pipeline companies were servicing Pennsylvania consumers in 2000.

This section discusses the production, transmission, distribution and storage of natural gas within and through Pennsylvania, noting that distribution is the only utility service coming under PUC jurisdiction. Produced natural gas is fed through gathering lines, which link production areas to central collection points. Some natural gas gathering systems include a processing facility, which removes impurities that might corrode a pipeline, or inert gases that could reduce the energy value of the gas. The pipeline transmission system, is the "interstate highway" for natural gas. It moves huge amounts of natural gas thousands of miles from producing regions to local natural gas utilities. Compressor stations

every fifty miles boost the pressure that is lost through the friction of gas moving through steel pipe. These two areas are not PUC jurisdictional, but are essential services for the other two areas.

Pennsylvania Natural Gas Producers: Currently under the new marketing concept, gas suppliers purchase gas from a series of independent producers and sell to the gas distribution companies or directly to end users. The distribution companies sell it to the consumer, at a rate set by the PUC. Each of these transactions contain operating cost and profit margins that result in the current "burner tip" costs.

Intrastate and Interstate Gas Pipelines: The PUC retains jurisdiction over Intrastate pipelines and the FERC is charged with providing oversight to Interstate pipelines. Interstate pipelines are used to move natural gas in, out and through the state, and the intrastate pipelines (transmission lines) are interconnected into the distribution systems and then to the consumer.

Local Distribution Companies (LDC's): Distribution pipes are used (known as mains), to bring natural gas service to homes and businesses. To help ensure reliable service, local natural gas companies can store natural gas underground for use during peak demand, such as cold days. As relating to the operations described above, both PUC jurisdictional and non-jurisdictional companies were surveyed and interviewed in order to address the natural gas industry as a whole and identify any trends within the industry and potential impact on the Commonwealth. Two Liquefied Natural Gas (LNG) companies were also profiled for this assessment. Liquefied Petroleum Gas (LPG) companies were not included due to time considerations. Propane and butane are the principal examples of the type of gas provided by LPG companies.

The PUC Gas Safety Inspectors participated in the interviews held with the companies in order to provide their expertise and technical assistance into the scope and specifics of the security process in the natural gas industry. The Gas Safety Inspectors also presented an understanding of other matters in their jurisdictional requirements regarding federal issues, such as federal Department of Transportation (DOT), Federal Pipeline Authority and FERC jurisdictional issues.

The threat of an event or physical destruction of a natural gas system is not a new concern to the industry. On a daily basis, natural gas systems may be compromised or breached accidentally by every day occurrences such as heavy equipment or a homeowner digging into an area where gas lines are located. Pipeline companies are accustomed to preparing for catastrophic events, such as hurricanes and earthquakes, and companies continue to work extensively on preparing for and mitigating any disruption to the service provided.

The events of September 11th caused the industry to reassess the risks and vulnerabilities of potential and deliberate attacks. Natural gas suppliers need to supply adequate quantities of gas, at a sufficient pressure, and many areas of the Commonwealth are directly linked to other states' dependence on gas being transported reliably and safely through Pennsylvania. Immediately following the attacks on September 11th, pipelines and storage facilities across America instituted heightened security measures. They continue to monitor and patrol the pipelines and storage facilities regularly via aircraft, vehicles, and/or on foot. Pipeline companies across the country have been working with the appropriate law enforcement authorities to ensure the continued safe operation of facilities. The natural gas industry appears consistent with other industry groups by regarding the emergency plans, business plans, contingency plans and disaster recovery plans as living documents that must be continually updated and reviewed.

The natural gas industry has emergency response plans in place which address various levels of emergency situations. Updates are based on standards or best practices from industry specific trade association working groups. Such groups are the Interstate Natural Gas Association of America (INGAA), the Interstate Oil and Gas Compact Commission (IOGCC), the American Gas Association (AGA), and the Energy Association of Pennsylvania (EAP) to name a few. In general, concerns associated with Y2K initiated review and updates to the emergency response plans and contingencies. The companies recognized post September 11th that these plans need to be routinely updated with the latest contingencies, procedures and emergency contacts. Recommendations were made to address any deficiencies.

Each natural gas facility completed or was in the process of completing a Vulnerability and Risk Assessment study prior to September 11th. All companies have implemented security-related upgrades to varying degrees for plant emergency and operating procedures.

Companies test the implementation of these plans by different means. If not already doing so, companies were urged to include law enforcement and emergency responders to participate in any drills, testing and training. Most conduct drills, training and testing regularly. Almost all companies have added additional training for terrorism events. Natural gas systems in large metropolitan areas put such plans in use almost daily due to the vast number of emergency situations created by such an atmosphere.

The companies examined the operational redundancies and capacities of the natural gas supplies, and natural gas collection and pumping systems with regard to their Business Continuity Plans. Most plans contain sections for availability of back-up facilities, vendor contacts, and emergency connection capabilities. Most have some degree of redundancy for natural gas supplies, while recognizing that loss of a major natural gas supply may cripple the system.

Natural gas systems are somewhat interconnected with intra-state and interstate systems and this can escalate the impact of the loss of a facility. At the same time, the fact that they are not fully interconnected can isolate and contain an event. Most companies have mutual aid agreements with neighboring utilities for replacing major equipment or components in place for many years, and have initiated processes for sharing personnel only in recent years. This is an extremely positive approach and the PUC/PEMA support the expansion of these programs.

In general, natural gas companies have a very low turnover rate of employees. Most employees work their way from entry level jobs to management positions, so cross training has occurred.

Almost all natural gas companies involved in the survey have addressed cyber security to a sophisticated level. Almost all companies feel that security and back-up facilities are best operated with company personnel while a few companies found it necessary to hire a provider, or vendor, for information technology services. Many have hired consultants to determine cyber security effectiveness and resilience to hacking.

Cyber security was a major aspect of Y2K readiness; however, some of the companies addressed in this assessment were not part of the Y2K investigation and have only focused on cyber issues in recent years. One company had little to no computer operations, aside from a billing system and did not seem concerned with cyber security. The company did state it would make efforts to address this issue after staff noted its importance.

SCADA is commonly used in the natural gas industry to operate and monitor system operational parameters. Security of such operating systems was addressed. A few companies did not have SCADA, or used it strictly for data collection and not operations. The common response from companies employing SCADA was that the systems operate independently of the network and, if for some reason, it were inoperable, operations would be completed manually.

Disaster Recovery Plans were reviewed. Several companies test these regularly and have elaborate plans in place. Most natural gas companies are maintaining back-up facilities off-site and are able to operate their business upon a moment's notice. A few companies have contracted services with an outside vendor and would require assistance in maintaining or restoring their normal operations and would result in a minimal (few hours) delay in their business practices. Computer backups and contingency plans are implemented and have been reexamined since September 11th.

Most companies consider the security upgrades a "cost of doing business" and have been implementing such physical changes and enhanced security

measures for many years. Some companies are highly advanced and technologically progressive with their security devices.

In Pennsylvania, the price of natural gas has been deregulated and the local distribution companies are no longer the exclusive providers of the product. Pennsylvania-serving production companies no longer have the ability to recover costs through traditional utility rate cases at the PUC.

Insurance coverage and costs vary company to company. Most companies expect, and some have already incurred, increases. One area of concern addressed by the gas industry relates to a "fine line" of ownership when it comes to jointly operated locations that are owned by one party. A pipeline company's delivery point to a LDC, where one company may own the location, but the other is dependent upon its operations. Who would suggest, implement, and/or pay for security-related enhancements or upgrades? What if the "tenant" wanted an improvement beyond what the "owner" was willing to provide? Industry working groups are meeting to resolve these issues. Nevertheless, the LDCs have stated that more cooperation is being shown by the pipeline companies in sharing access and information than during Y2K preparation.

On December 15, 2001, final regulations for Natural Gas Emergency Plans and Emergency Actions were adopted by the PUC. These regulations established procedures to follow in managing natural gas emergencies in order to maintain gas service and minimize service disruptions. The PUC began this process on July 20, 2000, in response to the passage of Pennsylvania's Natural Gas Choice and Competition Act in 1999, 66 Pa. C.S. §2201 et seq., which restructured the natural gas utility industry. A collaborative working group was established to address a number of issues, including:

- ◆ Emergency load shedding;
- ◆ A call for voluntary usage reduction;
- ◆ A call for mandatory load and usage reduction;
- ◆ Issuance of periodic reports to the media on emergency situations;
- ◆ Notice to affected customers and natural gas suppliers (NGS);
- ◆ Customer and NGS delivery requirements that apply to emergency actions;
- ◆ A procedure for focusing emergency measures to confined geographic areas; and
- ◆ Procedures for establishing communications.

Although not originally intended to deal with security and terrorist type incidents, these regulations are referenced as additional measures familiar to, and available to, companies during an emergency situation.

2.5 Telecommunications

The telecommunications infrastructure in Pennsylvania can be divided into four areas: Local Service, Long Distance Service, Wireless/Cellular Service, and Public Safety Answering Points (PSAPs) - - 911 services. There are thirty-four incumbent local exchange carriers (ILECs), ninety-eight competitive local exchange carriers (facility based), sixty-seven competitive local exchange carriers (resellers) both known as CLECs, 105 access/interexchange carriers (IXCs), 511 toll resellers and one telegraph company offering services to consumers in Pennsylvania.

Seven telecommunications companies were profiled for this assessment: five ILECs, one CLEC, and one IXC. With respect to security considerations, neither cellular service nor 911 emergency services are part of this report due to time considerations. 911 services were previously profiled in the Governor's Security Task Force Report, (attached as Appendix E). Wireless services are under the jurisdiction of the Federal Communications Commission (FCC).

There are approximately 850 local telephone exchanges in Pennsylvania. The thirty-four ILECs have at least one building that serves as the central office (CO) in each exchange and has switching equipment, transmission equipment, power equipment, environmental equipment, and emergency power equipment located at the CO. The CO controls all of the local telephone traffic within its particular exchange area and also controls all long distance traffic to and from the exchange.

All companies have a Network Operation Center (NOC) which is staffed around the clock, every day of the year. Every building and location in a company's serving area is typically monitored from the NOC for building entry (intrusion detection), building temperature, water presence, fire alarms, and equipment operation and condition. Each NOC monitors many COs within their area of responsibility. Personnel can switch both working and spare equipment on or off in the remote locations. If anyone enters a remote building or enclosure, the NOC staff/employees are aware of it. All CO alarms are monitored from the NOCs and repair personnel are dispatched when necessary.

Each local exchange is interconnected to other local exchanges in the immediate area by local trunks. Each local exchange is connected to its serving tandem office by tandem trunks. Each local exchange is also connected to all exchanges serving long distance carriers' points of presence ("POPs") by transport trunks. Radio is not used for Intraexchange connections in Pennsylvania, as in other states.

Any disruption to local telephone service in a single exchange will, at most, be limited to the customers served within that exchange. Depending on the nature and location of the disruption, either some or all customers within an affected

exchange may experience service disruptions. The disruptions may permit affected customers to make calls within, but not outside of their exchange area, or the disruption may prohibit affected customers from making any calls at all. Service for customers in all adjacent exchanges will continue, uninterrupted. Adjacent exchange customers will, of course, not be able to place calls to, or receive calls from, the affected exchange.

The long distance switching centers, owned by the IXCs, are interconnected by fiber optic cables and microwave radio links. The microwave radio links run from an IXC switching center to another switching center. There are sometimes microwave relay towers along the microwave radio route (every fifty miles or less) to regenerate the signal.

Any disruption to long distance service will affect customers over a wide area. The area affected depends upon how high the affected node is in the long distance switching hierarchy. An IXC's POP, if disabled, will affect long distance service to and from all ILEC COs which are subtended by the POP. A disabled large regional switching center would limit long distance calling over several states. All subtended POPs would be affected.

Key assets include:

- ◆ Local Switching Center Systems, which are used to switch and route local calls as well as originate and terminate long distance calls. This includes calls to PSAPs or 911 centers.
- ◆ Long Distance Switching Center Systems, which are used to switch and route long distance calls.

Local & Long Distance Carriers both have:

- ◆ NOC Systems used to control the routing of interoffice local calls and long distance calls.
- ◆ Repair and Maintenance Systems.
- ◆ Customer Record Information Systems that contain information on customer accounts.
- ◆ Customer Billing Systems that accumulate local and long distance call data for one-month intervals. The billing is for other telephone companies as well as end users.

There is a regional switch located in Pennsylvania (one of ten in the U.S.). This regional switch carries much of the long-distance traffic for the Mid-Atlantic States.

Many of the switching centers are redundant so if one becomes inoperative, calls may be rerouted around the inoperative switching center to other centers for completion. Long distance calls may be completed but over a more circuitous

route than under normal circumstances. In fact, this occasionally happens with callers not noticing anything unusual or, at most, noticing slight delays.

All telecommunications companies assessed are participating in security task forces and working groups sponsored by various industry trade associations, such as the Pennsylvania Telephone Association (PTA) and the United States Telephone Association (USTA), to name a few.

All companies surveyed maintain an Emergency Response Plan. For larger companies a separate plan is maintained for each district within the company and/or for each major location/building. In those cases, each building is assigned its own Emergency Coordinator. All reports of emergencies (fires, bomb threats, etc.) are directed to the appropriate Emergency Coordinator who assesses each report and determines the next action (building evacuation, call company security personnel, call outside authorities, etc.).

All of the larger companies surveyed conduct emergency drills on a routine, but unannounced, basis. Most of the larger companies conduct semi-annual building evacuation drills -- one building at a time. No one in the target buildings is aware, in advance, of the date and time of each drill. Someone in the Network Operations Center calls a designated person in each building to begin the drill.

Some companies still continue to maintain their documentation in large binders with copies kept at each location. Other companies now maintain their emergency plan documentation in an online database on a company-wide Intranet. Much more information can be stored and retrieved online than would ever be possible in binders. One company visited had the site profiles for all of its offices, company maps, cable maps, technical data, corporate policy statements, security procedures, and personnel lists in their online plan. A concern was noted with the trend toward keeping this information online in case of cyber or other problems and the possibility of networked information not being available during an emergency.

Some companies in the survey maintain a Business Continuity Plan. The typical plan has: a list of contacts, control locations, control processes, personnel lists, and legal and regulatory contact information during emergency situations. Each of the companies that do not have a Business Continuity Plan reported that it was under development. These companies appeared to have the essence of a Business Continuity Plan integrated into their Emergency Plan, but not identifiable as a separate document.

All important buildings and remote equipment locations are equipped with battery backup power for short duration power outages and generator backup power for long duration power outages -- as long as fuel supplies are available. All COs have a battery backup. These emergency power systems are tested periodically, depending on individual corporate policy.

Regarding cyber security, one company issues an annual employee letter. It covers personal computer security as well as virus protection procedures. Other companies cover these matters with employees periodically. Virus protection at most companies required no action from individual employees. Typically, anti-virus software updates are automatically downloaded to all users' workstations upon network login. All inbound mail is automatically scanned for viruses. Further, the virus software automatically scans files stored on removable storage devices to guard against the introduction of a virus from an "outside" floppy disk or CD-ROM.

Internal networks (Intranets) are protected in all cases by firewall. Firewall logs of all connections are maintained. Company Information Technology (IT) staff state that they are familiar with computer forensics and know what actions to take if attempts to breach the firewalls are detected. Sensitive information, such as billing data, is encrypted before it is transmitted over the Internet.

Many companies hired outside contractors to do audits of the computer systems. One company hired an outside contractor to attempt remote attacks to company networks. Most companies use their own employees to attempt to break into the networks. Security was increased to eliminate any weaknesses encountered during these tests.

Some insurance carriers have removed the provision for coverage of loss due to terrorist events. Now, terrorism loss is only available as a separate coverage, at high costs, and excluded in certain large cities. One company that was directly involved in the September 11th disaster reported that only about 65% of its losses would be recovered from insurance. Workers Compensation has increased where there are more than ten employees in a location.

Some companies have reported that insurance premiums are increasing by 200-250% for nationwide, corporate property and general liability coverage. A breakdown of just Pennsylvania insurance costs was not available. One company, however, has reported that upgrading its physical asset security has led to decreases in insurance premiums.

All companies have close contact with local and state police. One company reported that they had state police personnel conduct an on-site building security inspection and offer feedback and suggestions.

New employees normally have a criminal background check performed through a third party. In addition, a driver's license check is performed and educational history is verified. Social Security history, financial status, and prior employment are examined and personal references are contacted. Some companies also conduct drug screening on new applicants. Present employees who possess a Commercial Drivers License (CDL) and other employees who drive company vehicles usually have driver license checks performed on them on an annual

basis. Fingerprinting is not taken on either prospective or present employees at most companies. The exception is certain present employees who work with federal government or military circuits and equipment. In these cases, fingerprinting is required by the Federal agencies for mandatory FBI background checks.

The larger companies participate in the FBI InfraGard program. Smaller companies who were aware of this process, generally did not participate and felt that the program did not have much to provide to smaller companies.

2.6 Water and Wastewater

Consistent with other industry groups, the water and wastewater industry was surveyed and interviewed. In 2000, there were 186 water and 86 wastewater companies offering services in Pennsylvania under the jurisdiction of the PUC for rates and quality of service. However, there are over 10,500 public water suppliers, of which 2,200 are community drinking water systems, and over 6,200 wastewater facilities that fall under jurisdiction of DEP. DEP enforces the Safe Drinking Water Act (SDWA) which pertains to water quality, quantity and associated permitting. Wastewater treatment is also permitted and regulated under DEP. During the survey and interview process, an invitation to attend was extended to DEP and the County Health Departments, where applicable, and the cooperation received from both was appreciated.

Pennsylvania water suppliers can use ground water or surface water as sources. Wells pump ground water to a storage reservoir or directly to a treatment facility. Surface water is normally stored in an open reservoir or dam. The water then either flows by gravity or is pumped to the treatment facility. Water treatment can include many processes that involve chemical, biological or mechanical treatment, but all drinking water requires disinfection, normally accomplished with the addition of chlorine. After treatment, water is stored in a capacity to supply adequate pressure to the customers. Larger water systems have finished water storage tanks to provide adequate storage for every day use, to supply fire protection service, and to maintain system pressure. Networks of underground transmission and distribution mains transport the water to each customer. In some instances, booster pump stations are required to increase pressure and flow to sections of the distribution systems.

Following the events of September 11th, DEP contacted and had face-to-face meetings with all major water suppliers. Guidelines relating to security and vulnerabilities were mailed to high hazard dam owners. Additionally, DEP distributed a water sampling kit to each of its regional offices to be used in the case of a suspected contamination event. The American Water Works Association and its affiliates have been actively providing security related information to water systems throughout the country.

Large Pennsylvania PUC jurisdictional water facilities were visited during Y2K investigations. These companies are now well prepared to handle emergency events. They are continuously making improvements to the systems and their plans in order to safeguard the industry's infrastructure, water supplies and customers served. Some non-jurisdictional facilities were visited during the HR 361 assessments, which were not a part of the Y2K process. Some companies were very capable and prepared, while others seemed to give little attention to emergency plans or contingencies and did not realize their vulnerabilities. PUC emphasized the importance of planning and stressed the point by describing various scenarios.

The threat of a contamination event or physical destruction of a water or wastewater system is not a new concern to either industry. The events of September 11th caused both industries to reassess the risks and vulnerabilities of such attacks. Water suppliers need to supply adequate quantities of water at sufficient pressures and of a quality safe to use. The water industry, unlike other fixed utilities such as electric, gas, steam and telecommunications, has to ensure the water can be not only supplied, but also that supply must be maintained at a quality level safe for human consumption. Wastewater plant operations pose a serious threat to sanitary living conditions and other environmental concerns. The collection system can pose as a conduit for many purposes.

The water and wastewater industries remain consistent with other industry groups by regarding their emergency response plans, business continuity plans, contingency plans and disaster recovery plans as living documents.

The water and wastewater industries, in general, have emergency response plans in place or are in the process of creating or updating emergency response plans that address various levels of emergency situations. However, it was also found that the availability of the plans was not always addressed or that companies were not familiar with the information in the plans.

Some companies, as of the date of the PUC survey and visits, have spent little on capital expenditures due to the fact that they are awaiting completion of their Vulnerability and Risk Assessment. Others have done some obvious upgrades immediately following September 11th and are waiting for funding, or a mechanism to recover funding, before carrying out extensive upgrades. All companies have implemented security-related upgrades for plant emergency and operating procedures, but to varying degrees.

In the House of Representatives Bill 3448 from the 107th Congress, 1st Session, Title IV, Drinking Water Security and Safety, the Safe Drinking Water Act (SDWA) was amended. As a result of this federal legislation, each community water system serving a population of 3,300 people or greater is required to conduct a vulnerability assessment and certify completion. The completion dates are December 31, 2002, for those systems serving more than 100,000 people,

June 30, 2003, for those systems serving between 50,000 and 100,000 people, and December 31, 2003, for those systems serving between 3,300 and 50,000 people. Additionally, each community water system serving 3,300 people or greater is required to prepare and certify completion of an Emergency Response Plan that incorporates the results of the vulnerability study. The EPA is tasked with providing small water systems, serving under 3,300 customers guidance relating to conducting vulnerability assessments, preparing emergency response plans, and threats from terrorist attacks or similar events that can affect public health and safety. Some funding was made available through the House of Representatives Bill 3448.

Water systems are generally stand-alone entities. They are not interconnected with a statewide grid and this can escalate the impact of the loss of a facility. At the same time, the fact that they are not interconnected can isolate and contain a contamination event.

Responses relating to business succession plans varied. Many plans are prepared and maintained on a high corporate level. Other facilities did not see a need to maintain a plan, but had an idea of likely candidates should key personnel become unavailable. The water and wastewater industries have low turnover rates for employees. Each company conducted some type of screening or backgrounds checks for new employees but the consistency and degree of the check varied. Some non-jurisdictional companies commented that it was uneconomical to conduct background checks for each employee and local governmental structure did not promote conducting the background checks for all positions. Some companies are satisfied with a screening process through references. Company policies for the background checks of contractors varied. Some check references while others screen individual contracted employees.

All water and wastewater entities have addressed cyber security to some extent. Some prefer to handle cyber issues with internal personnel while others rely on contracted assistance. To some degree, each water and wastewater company involved in the survey relies on computerized control and record keeping. Larger, more sophisticated facilities rely heavily on the computerized network and have made significant efforts to ensure the security of these systems. The less advanced systems also utilize computerized operations and billing procedures. Some facilities test the cyber system security through a hired firm that attempts to hack into the system. Disaster Recovery Plans were present at all locations, although testing procedures for the effectiveness of the plans varied. SCADA is used by many water and wastewater facilities to operate plants, but manual operation is enabled when the SCADA is not operating.

Water and wastewater companies both realize that changing technology requires diligent efforts to maintain a safe and secure cyber system. In order to bring a crashed system online, most have contracted with a provider. One concern is

the number of entities, utility and non-utility, using the same provider who may not be capable of dealing with a large demand.

Cost recovery is a concern of each company. Publicly-owned water systems that serve a population over 100,000, had the opportunity to apply for a federal grant through the EPA for up to \$115,000 that is to be used for approved security training sessions, developing vulnerability assessments, and developing operation and response plans, among other approved security tasks. Privately-owned companies incurred costs for security upgrades and were inquiring about compensation for these expenses and capital expenses, but, at the time, were not eligible for the EPA grant. In late July of 2002, the availability of this grant was extended to private, investor-owned water facilities. The grants were distributed per qualifying facility and not per company, so one company may receive more than one grant. Companies stated high recurring costs for employing security guards at facilities.

Insurance coverage and costs vary company to company. Most companies expect, and some have incurred, increases. Some have received quotes of increases from 15% to well over 100%. Some quotes predict increases along with terrorism exclusions. In many cases, property insurance increases are currently expected to be higher than other types of insurance. Water and wastewater companies were profiled prior to significant Workers Compensation increases becoming known. One recommendation by a company was that the Commonwealth should create a law disallowing terrorism exclusions by insurance providers; similar laws exist in other states.

2.7 Steam Heat

Steam Heat, also known as District Heat, is a common source of heating for industrial, commercial, institutional and residential entities. Generally, steam heat is produced in main generation plants by heating water to its boiling point, usually in coal-gas-or oil-fired boilers. The resulting steam is distributed to customers through an underground supply pipe network. At the radiators in customers' heating systems, the steam gives up its heat by conduction to the air, condenses and the water is pumped back to the boiler for re-heating.

During 2000, there were three steam heat companies under the PUC's jurisdiction, and three heating/cooling companies. Industry-wide, steam heat is not consistent from a regulatory standpoint. Institutions, universities, and hospitals, to name a few, which provide their own steam heat are exempt from some regulations and perform their operations differently than the PUC jurisdictional steam companies profiled. This contributes to a disparity in the nature of the cost of doing business where operating costs and ultimately security budgets are affected. The obstacle arises with end-use customers who are paying an approved rate for their service, as opposed to a privately-owned

and operated steam plant where additional security/operating costs can be absorbed by other areas of the budget.

One of the best protections for the steam industry is the hundreds of miles of pipes that are underground and not easily accessible to security breaches. Most companies are concerned with actual plant conditions and primarily, the security "behind the fence." The steam heat industry has Emergency Response Plans that address various potential on-site emergency situations, traditionally based upon safety protocols, operating conditions, or weather-related emergencies. Additionally, the safe reputation and the long history of the industry operations provide confidence for a rather traditional and somewhat simplistic source of energy. Post September 11th, these plans are being revised and updated periodically to address changing security threats and to update emergency contacts.

The steam heat facilities visited do conduct Vulnerability and Risk Assessments in-house, utilizing company personnel as opposed to hiring a security consultant to do the job. Some companies have installed additional security devices since last September, while others have plans to upgrade their security policy. Overall, financial constraints have made it impossible for most companies to install all desired security measures planned. All companies examined have implemented security-related upgrades for plant emergency and operating procedures.

Generally, the industry has a very low turnover rate of employees. Formal business continuity plans do not exist at the profiled companies; however, they do have limited plans to replace key personnel in a situation where necessary. These companies are able to utilize personnel from other corporate locations in the event of a lengthy employee disruption. There are available off site back-up facilities for files and other operating data. There are procedures for restoration of services in situations where service is disrupted. There are alternative sources of water supply in place to ensure continuity of service if the usual source is disrupted or destroyed. Small-scale recovery of computer operations can be conducted in-house while the corporate staff, in other locations, performs large-scale recovery operations.

Companies have incurred additional costs for security upgrades since September 11th. Security devices have been installed, and additional security enhancements can occur with minimal increased funding. Due to budget limitations, some companies are unable to implement all security measures they planned. Companies would like to be compensated for the extra expenses being incurred to upgrade security. All companies examined did not indicate a problem regarding potential increases in insurance coverage as a result of September 11th. They have not received notices of premium increase or exclusion of terrorism coverage. Workers compensation issues were not prevalent at the time of this industry's assessment.

Companies that were assessed did not offer recommendations specific to the steam industry. However, one company did offer comments regarding a potential conflict with the Coast Guard and had requested additional patrols along a waterfront property, which was resolved.

2.8 Rail

The PUC's Bureau of Transportation & Safety, Rail Safety Division, is responsible for the administration and processing of formal and informal rail safety complaints and safety inspections for compliance with the Federal Railroad Administration's (FRA) track, operating practice, and freight car standards. In addition, the division is responsible for rail crossing and bridge safety. Currently, there are approximately 5,000 bridges and 7,500 grade crossings in the Commonwealth under PUC jurisdiction.

The PUC Rail Safety Inspectors participated in the interviews held with the companies in order to provide their expertise and technical assistance into the scope and specifics of the security process in the rail industry. The Rail Safety Inspectors also presented an understanding of other matters in their jurisdictional requirements regarding federal issues, such as federal Department of Transportation (DOT), Federal Railroad Authority and the American Association of Railroads.

In Pennsylvania, there are over seventy railroad companies operating within its boundaries along 9,000 miles of track. In order to provide an overall picture as to security issues that are faced by the railroad industry, the security survey and interviews were conducted with a wide range of operators including a Class 1 railroad, a regional railroad and a passenger railroad. A Class 1 railroad is defined by the National Surface Transportation Board as the large railroad companies with Year 2000 operating revenue of at least \$261.9 million. A regional rail is a non-Class 1, operating 350 miles of track or more, with revenue of at least \$40 million. A passenger train hauls passengers for revenue.

Due to the vast physical infrastructure of the railroad industry, it is impossible to secure the entire railroad system from a terrorist attack. In addition, the rail industry was not profiled during the Y2K assessments.

The railroad industry is accustomed to dealing with emergency situations (i.e., derailments and hazardous material spills) and has extensive emergency response plans with toll free emergency call numbers. Although the Class 1 railroads and passenger rail have their own police force, they still rely on a cooperative effort with local and state police to assist in policing and responding to emergency situations. In a situation where an incident would occur along the railroad tracks, the railroad companies are prepared to contact first responders, county HAZMAT teams and local police. The railroad companies have an active

database, which identifies key personnel along their system in emergency situations. The railroad emergency plans include:

- ◆ Assessing assets and vulnerabilities, threats, and risks;
- ◆ Determining countermeasures and actions;
- ◆ Setting up alert actions and railroad actions;
- ◆ Implementing, monitoring, and testing the plan;
- ◆ Railroad red alert actions;
- ◆ Security instructions;
- ◆ Tank car vulnerability tests; and
- ◆ Participation in STRACNET.

The STRACNET is a Department of Defense (DOD) designated track to haul military equipment, usually high and wide loads. The military would have preference in movement over general freight in a military emergency. The railroads will cooperate with all agencies including the FBI during emergency situations. If the FBI takes over control of the tracks for investigation, the trains would be rerouted as practical.

Since September 11th, the American Association of Railroads (AAR) has setup a Railway Alert Network that operates 24/7 to provide railroad companies notification of possible threats and indicates the level of threat. The railroads have established employee watch programs whereby employees report suspicious activity. With respect to train dispatch centers, the railroad companies have the capability of dispatching trains from more than one location. Unattended trains are disabled so that they can not be moved. During high threat level, Key Trains (HAZMAT and military trains) are directed to safe havens and are protected around the clock with railroad personnel. The AAR hired a consultant to perform vulnerability and threat assessments for the railroad industry. Other railroads either performed their own independent assessment of threat vulnerability or hired consultants to perform the task. Since railroads deal with incidents every day, ranging from vandalism to major derailments involving hazardous material, the railroad industry frequently updates their emergency plans, and conducts emergency drills with local responders, police and county emergency personnel.

The freight railroads perform background checks on all new hires and check every employee through the FBI Watch List. Due to the lack of funds and manpower, passenger rail only conducts background checks on the railroad police. The ticket counters for the passenger railroad are tied into the FBI Watch List to identify possible threats and each ticket that is issued includes a toll free number and instructions to report any suspicious activity to train conductors. Some Class 1 railroads issue Photo ID's to all employees.

All operational personnel are cross-trained to handle all work shifts. Upper management is not crucial for running the railroad on a short-term basis. The

railroad police command center for the Class 1 railroad is very secure. Key policies are in place to handle emergency situations. If there would be key people who are lost during an incident, railroads can transfer employees from other areas as a temporary measure. Employees are also cross-trained to a certain degree to fill-in during emergency situations. Long-term business continuity does need to be addressed by the railroad companies.

Some railroads have dispatch systems that are isolated from their network system and other railroads have multiple firewalls to protect the system from viruses and other unauthorized entries. There is redundancy in the computer facilities and there are contingency plans in place to supply customers with the ability to reroute trains. Manual procedures are in place through tandem systems if a system fails. Some railroads have the capability to manually check computer logs to see if there is an intruder. However, not all railroads have intrusion detection software for their IT systems.

Some train dispatch centers are on the corporate firewall, but run on a dedicated workstation. Passenger tickets can be issued manually if a system crashes. Certain railroads have a Cyber Disaster Recovery Plan for their cyber networks and they anticipate a down time of only 2-4 hours for mission critical systems. Some railroads have mirror data at their recovery center and every piece of data that is generated is replicated at the recovery center for quick recovery.

The AAR, with the support of the Department of Transportation, has created a Surface Transportation Information Sharing and Analysis Center (ST-ISAC) that will compile and analyze data from the rail industry to enhance transportation security measures. Freight railroads have a large physical infrastructure that is heavily dependent on information technology in their daily operations. Some railroads dedicate significant funds to increase security at intermodal transportation systems. The ST-ISAC will help ensure that intrusion into the transportation industry's information technology will not disrupt the nation's transportation systems.

Freight railroads carry large insurance deductibles and they are increasing as the result of September 11th events. Prior to this, some railroad liability insurance deductibles were as high as \$10 million and now will be increased to \$25 million. The deductible for property and cargo is \$12.5 million. Many railroads buy their insurance from overseas companies, as they are unable to secure the type of insurance necessary in this country. Some existing policies do not cover incidents caused by military and outside government action against its facilities. Some other policies will cover threats by an individual agent operating in secrecy or alone and not connected to a government. Insurance companies are getting strict with renewals by checking the backgrounds of railroad employees.

Many railroads consider the high deductibles along with the cost of increasing security at certain locations, whether it is video surveillance or additional intrusion

detection software, as the cost of doing business. These costs are absorbed by the railroad companies and can not be recovered through shipping rate increases because these rates are set for years to remain competitive. Any increase in rates will cause the railroad to lose revenue. Passenger rail companies estimate that on their mainline corridor, a suspension of service for an eight-hour period will result in a \$1.5 million dollar loss.

With respect to passenger rail, terrorism insurance is cost prohibitive. On a specific property damage only policy, one insurer quoted a \$3 million premium for a \$50 million annual aggregate policy with a minimum earned premium of 25% in the event of cancellation.

2.9 Motor Carrier

The PUC oversees 1,100 passenger carriers, which includes: 254 buses, 145 taxicabs, 228 paratransits, 395 limousines and 79 airport transfers. Additionally, 5,024 property carriers are also under PUC jurisdiction (4,699 property and 325 household carriers).

The PUC's Bureau of Transportation & Safety, Motor Carrier Services and Enforcement Division, is involved in all areas of motor carrier transportation regulation. They are responsible for the regulation of commercial property and passenger carriers within the Commonwealth. The five district offices located in Harrisburg, Philadelphia, Scranton, Altoona, and Pittsburgh ensure compliance of trucks, buses, taxis, and limousines with the Public Utility Code and the PUC regulations through regular inspections and audits.

Employees from the PUC's Motor Carrier Division participated in the survey and assessment processes to provide a liaison with the companies and to offer technical expertise where necessary.

Motor Carrier security issues includes crime, crowd management, disruption of the transportation infrastructure and attacks against the system that involve terrorism or sabotage. Due to the overwhelmingly large numbers of transportation facilities within the Commonwealth, a representative sample was surveyed and interviewed to discuss the topics related to our tasking. Three property carriers, three motor coach (large passenger) carriers and three taxi (small passenger) carriers were visited at their sites. Each type of carrier review included a large, medium and small-sized company which are representative of the motor carrier industries of the Commonwealth.

The motor carrier industry remains consistent with other industry groups by regarding the emergency plans, business plans, contingency plans and disaster recovery plans as living documents that must be continually updated and reviewed.

The larger motor carriers visited have emergency response plans in place, or are in the process of creating or updating emergency response plans that address various levels of emergency situations. The contents of the plans, industry-wide were similar. The medium and small motor carriers visited have a range from minimal awareness and preparation to extremely aware and thoughtful preparation on security issues. PUC recommended the development of emergency plans to prevent a disruption of vital motor carrier services that could place communities at risk for significant economic losses.

Each motor carrier assesses risk and vulnerability on an individual basis. Some of the smaller motor carriers failed to recognize their vulnerability. PUC stressed the need for awareness in this area. The cost of additional components and upgrades became a limiting factor for implementing preventative measures. Some carriers spent little on capital expenditures. Others have done immediate upgrades following September 11th and are waiting for funding before continuing extensive upgrades.

Several carriers utilize local law enforcement to participate in drills, testing and training. Others were urged to include law enforcement to participate in their drills, testing and training. Most have increased their training due to the September 11th; however, some do not believe they are likely to be chosen for a terrorist event. The PUC explained the position that security could encompass many areas, not just terrorism, and carriers were encouraged to investigate those possibilities and scenarios.

Most companies have some degree of business contingency redundancy, while recognizing that loss of only a few major motor carrier companies may cripple the system in a particular geographical area.

With the exception of the small passenger carriers, motor carriers have a low turnover rate of employees. New employees receive some degree of background checks, but the extent of background check varies from company to company. Security guards were hired at some companies, while others hired off-duty police officers as their security force.

All motor carriers involved in the survey have addressed cyber security to some degree. Few have hired consultants to determine cyber security effectiveness and resilience to hacking. It should be noted that one small property carrier had no computerization at all, and one large passenger carrier had no cyber security in its network. Some Disaster Recovery Plans were reviewed. Most companies regularly test their plans. It was stressed to the carriers without much cyber security in place that computer back-ups and contingency plans should be implemented and regularly examined.

It should be noted that motor carriers were not included in the PUC's Y2K review of companies due to the limited, computer-driven, customer interruptions that

were anticipated during the Year 2000 rollover. However, it is now shown that motor carriers do rely on computerization for inventory control, delivery tracking, maintenance scheduling, equipment location, and drivers' hours of service availability, to name a few.

Cost recovery is a concern of each company. The entire motor carrier industry operates on a thin profit margin line. Any property carrier operating on-time delivery systems can suffer serious financial loss as a result of any major breakdown in the transportation system. All have requested compensation to improve security and develop plans for emergency situations. One large passenger carrier incurred costs for security upgrades and inquired about compensation for these expenses.

Insurance coverage and costs vary from carrier to carrier. Most carriers expect increases in costs. Some have received quotes of increases. Some quotes predict increases along with terrorism exclusions.

VIII. ISSUES IDENTIFIED AND RESOLVED

The Pennsylvania One Call System

The Pennsylvania One Call System is a non-profit corporation created to protect the underground utility facilities and to better ensure public and excavator safety by providing an efficient, cost effective communications network between excavators and underground facility operators. This communication network receives and processes line location requests from excavators, contractors, plumbers, builders, designers, and the general public. The company provides a toll free telephone number for anyone to call when digging and requesting location of underground lines. The service is available 24 hours per day, every day of the year.

Established in September 1972, the service originally covered Allegheny County in Western Pennsylvania. During 1975 and 1977 with additional counties as members, and establishing the "Call Before You Dig" concept in the state, the company then sought passage of legislation mandating participation by all underground facility owner/operators. Enactment of Act 172 (1986) brought major growth and clearly established the need for a full time staff. Today, Pennsylvania One Call System serves all 67 counties and employs over 70 people.

The utility companies expressed concern with the lack of a screening mechanism in the process, leaving the companies unable to verify the legitimacy of a request for identifying lines or providing prints of the company locations. This leaves a company in a vulnerable position with regard to security, or possibly in violation of the regulations, if they did not comply with a request. Concern rests not with the legitimate contractors or engineering/architecture firms who use this service

regularly, and are familiar names to the process. The concern is with a public citizen submitting a request to locate in order to use the information to destroy a particular location or as an accelerant for nearby destruction. Upon researching this issue, PUC determined that the Pennsylvania System (PA One Call) has authored a paper entitled "*Infrastructure Protection America: Exposure, Security and Response*" which appears to address this issue. The *Infrastructure Protection America* proposal addresses management of public and private Rights of Way, certification and coordination of excavation activities and incident management with First Responder communities. This paper offers a pilot program for Pennsylvania to develop a model for accountability and security, along with verification for project management, access certification and authentication, intrusion detection, uniform reporting of incidents as they occur, and a central capability to analyze incidents as reported.

Industry Use of Consistent Alert Designations

A concern was noted with respect to the industries' use of various designations of alert or response. Prior to the implementation of Homeland Security Director Ridge's designation of color-coded levels of alert, industry groups were developing their own categories, descriptive phrases and company actions for each level. The terms ranged from a three tiered system (low/medium/high) to a five-tiered arrangement (SeCon for security condition, ThreatCon for threat condition, etc.). Even the phrasing within the three or five tiers was not consistent, nor were the companies' actions. However, since the Office of Homeland Security offered direction, all companies have modified their labels to adopt the federal color code.

Regional Counter Terrorism Task Force

A critical infrastructure liaison to the incident commander in an emergency situation would be helpful to expedite the recovery process. Such a liaison would provide one point of contact between critical infrastructure companies and the incident commander, instead of many different companies and industry groups vying for time with a potentially overwhelmed incident commander. The PUC and PEMA identified the nine Pennsylvania Regional Counter-Terrorism Task Forces as a recommended venue and began this process in June 2002. This process was detailed in Section V. Company/Industry Participation in Community.

IX. CONCLUSIONS FROM THE REVIEW AND ANALYSIS PERFORMED

Due to the limited time and staff considerations, both during Y2K and this project, the companies who were profiled were often the larger companies in their industry group or companies affecting the greatest number of Commonwealth citizens. However, for this assignment, the transportation industries tried to profile a small, medium and large company to represent their industries. Many areas of critical utility infrastructure were not profiled and should be reviewed. Wireless telecommunications and 911 services, autonomous municipal authorities, cable television and internet providers, and propane, diesel and gasoline are industries that overlap with the utility services offered by PUC companies.

In the interest of a limited scope and purpose of this assignment, these industries were excluded, but the PUC recommends that they should be assessed at a later date. For example, radio and television broadcast information is important during times of crisis and essential to the Emergency Alert System (EAS). Cellular phones are as common as landline telephones and are often used extensively during emergencies due to portability and tower locations possibly located away from the affected site, and are under the jurisdiction of the FCC. Municipal water, sewer, and electric authorities are serving numerous citizens in both rural and urban areas with limited oversight or awareness of security issues. Propane and diesel supplies and delivery are critical to supplement auxiliary energy generation in businesses, industry and health care centers, and gasoline for use in transportation. The Pennsylvania 911 centers were profiled during the "Governor's Security Task Force Report," (Appendix E).

As shown during the assessment process, companies who have recognized the importance of these types of assignments are often more in tune with their own company's and trade association's efforts on these types of projects, and have initiated these activities prior to Commission visits. However, non-jurisdictional companies that have not previously been profiled, and smaller to midsize companies often are not proactive to these needs. Whether it is a matter of a budgetary, business decision or some other reason, these companies do not achieve the same types of results as the others. This is an area where focus needs to be developed.

The PUC feels strongly that the smaller and mid-sized companies, as well as non-jurisdictional companies and industries, need to become more comfortable with emergency operations plans, business continuity plans, along with cyber and security issues. These concepts are essential in order to maintain the safe and reliable delivery of utility services, and the protection of critical infrastructure for residents and businesses in the Commonwealth. Many of these companies are overlooking valuable information that is readily shared and available.

Many of the smaller companies do not anticipate any impact due to their size and/or geographic locations. As mentioned previously, a security event might include all levels of threats ranging from a disgruntled employee, a terminated customer, mischievous individuals who vandalize a field location, domestic terrorism, or even a "copycat" event unrelated to another deliberate event. Some companies appreciated this aspect when it was pointed out, and hopefully are re-evaluating their businesses to include this information.

The PUC would like to share the following examples of encouraging actions taken by individual companies. Many of these ideas may be adapted to be used by almost any industry and are positive "lessons learned".

A "Community Awareness Letter" was sent to all customers of a company with language stressing the importance of security and the company's commitment to reliable delivery of utility service. The letter further expressed that consumers should report any suspicious behavior around the company facilities to the company, with any dangerous or imminent activities to be reported to the local 911 center. Other companies included this as a "bill stuffer" or part of their regular newsletter, but the direct mail approach seemed to reach more citizens.

One company responded that the PSP provided assistance and training to all employees who use company vehicles. The training included information on securing their vehicles, managing and averting road rage, weather-related safe driving skills, avoiding potentials for accidents, as well as procedures for reporting any vehicle incidents or violations.

One company is considering, and six have already implemented, biometric devices for their most sensitive areas whereby a fingerprint or a retinal scan must be used in conjunction with a card reader or other security badge. These highly sophisticated devices also provide additional failsafe measures so that others may not use a lost, stolen or borrowed badge. Additionally, the admitted person also had to have the bioscanner used again before they could leave the secure area. This measure assured that if, in the remote event, an intruder "coat-tailed" someone into the room and hid themselves, the intruder would be trapped in the secure area and could not exit on their own at a later time.

As noted in the section 1.4, the FERC has included a security self-certification process in its recent Standard Market Design rulemaking. The PUC believes that it has adequate statutory authority to also implement such a program with its regulated companies and that such a self-certification could be included in a company's annual report and be subject to audit. The Commission would also work with DEP and Penn Dot to implement a similar requirement for operations not subject to PUC regulatory scrutiny, but subject to their permitting or licensing oversight.

X. RECOMMENDATION FOR LEGISLATIVE ATTENTION

The following areas for legislative attention are designed to provide information to the House of Representatives as they deliberate on the development of legislation for homeland security, consult with other agencies, and as they review issues with constituents. Based upon the findings, conclusions and recommendations from all participants, the PUC and PEMA find the following areas have some degree of merit and recommend further review by the Legislature.

3.1 Protection of Assets through Sharing Best Practices

Distribute consistent physical and cyber security-related information.

There is a need for the timely distribution of consistent security-related information to each industry, both physical and cyber, through governmental bodies or specific industry groups. Often, a potential action or credible threat in one industry may compromise the integrity of another industry, or relate to operations in another service territory.

Continue to enhance information flows. There is a need to continue to utilize and enhance information flowed through the FBI's InfraGard Program, National Infrastructure Protection Center (NIPC) and the CERT Coordination Center, located at the Software Engineering Institute, operated by Carnegie Mellon University and other programs available to utility companies.

Expand PSP cyber crime enforcement. The PSP Bureau of Criminal Investigation cyber crimes programs should be expanded to allow more interactions with critical infrastructure companies and to assist these companies to track and prosecute cyber crimes. Current staffing and abilities need to be enhanced to specifically serve critical infrastructure.

Develop levels of cyber reporting to the FBI. A need exists to modify FBI levels for reporting cyber crimes specific to utilities and critical infrastructure. The FBI has established criteria on what kind of "hits" to report, but are constrained by conditions such as financial limits, intent to harm, or actual harm, which should be waived for utility or critical infrastructure related "hits." At the present time, the FBI will accept reports but generally does not track such reports unless it falls into the above referenced criteria.

Clarify reporting and response. The roles of state and local agencies need to be centrally defined with respect to reporting and tracking utility security events. Additional clarification is necessary from state and local agencies as to when utility related events should be reported and what can be expected of responding state and local regulators. Non-regulated entities should also be included in this process.

Define assistance and response during contamination. Water companies are concerned with an actual or suspected contamination event and are looking to the state agencies to maintain a list of suspected contaminants, preliminary testing procedures prior to lab analysis, availability and capabilities of testing laboratories, health implications of contaminant and a timeframe for testing results.

Create unified technical database. The creation of a unified technical assistance database or communication procedure that can track unusual occurrences and link with local and state public health, law enforcement, state agencies and utilities is also necessary.

Amend the PA One Call Act. The Underground Utility Line Protection Act, Act 187 of 1996, should be amended to require all excavators to notify the PA One Call System prior to doing any excavation work. The current law provides exceptions, which have resulted in unmarked utility lines being hit with varying degrees of damage and threats to the public safety. Elimination of these exceptions could result in greater public safety by reducing the number of damaged lines and the accompanying interruption to essential services. Additionally, the possibility of explosions, water and air pollution would also be reduced.

Mandate filing of utility damages. It should be mandated that the Department of Labor and Industry, as the enforcement agent for the Underground Utility Line Protection Act (187 of 1996), be notified of all damages to utility lines caused by excavation. A report would be required from each person who owns and/or causes damage to the lines. This, in turn, would lead not only to a more efficient enforcement of the Law, but also a greater awareness of the Law and an accompanying reduction in the number of hits and damage to the utility lines.

3.2 Education and Training

Develop education process. Utility industry and company awareness of current trends, threats and best practices should be accomplished through an education process, or possibly undertaken by the utility trade associations. The associations should include non-members, as well as inviting smaller companies to participate in their planning and discussions relating to these topics.

Accept first responder training. *The Strategy* has recommended building a national training and evaluation system for first responders. This is a "Train the Trainer" concept that could filter down to state, regional and local communities. Utility industries should be included in these efforts to become familiar with practices involving a crime scene, incident command, suspicious devices, secondary devices, and how to evaluate and respond to a security situation or event.

Train and network hospitals and health care. It was recommended that hospitals and health care facilities become trained and networked/connected to a centralized analysis point to recognize indicators of sickness from water contamination and waterborne disease. Hospitals and other health care facilities should ask standard questions to gather patient information that may assist to recognize trends of a possible health-related situation. Health care facilities can inform water systems of indications of a water-related contamination event.

Coordinate uniform security standards. Coordination with other states will ensure their security standards are at the same level as our state. This is especially important for neighboring states or other states that transport or provide utility services into Pennsylvania such as electricity, transportation carriers, telecommunications, and natural gas and can potentially diminish the quality of response, service and communications during a security event.

Explore the need for transportation marshals. Transportation industries have requested training and education on security events and threats. Employee interaction with the public, the handling of freight and passenger cargo, and the vast geographic areas covered, place these employees in the front line of a potential attack. The creation of a training and support program similar to the air marshal program complete with hiring, training, and use of rail or bus marshals will assist this process. Increased training is essential for railroad and bus personnel to recognize terrorist activity and weapons of mass destruction. Additional security personnel and bomb dogs are needed at passenger rail and bus stations, intermodal facilities and rail yards. A private or governmental transportation marshal program could provide this necessary support and direction. Federal enabling legislation should be changed to allow passenger rail and bus personnel to perform random searches of luggage.

Institute nuclear protocols. A defined set of protocols for responsibilities of supplemental nuclear site security personnel (i.e. PSP and National Guard) is necessary, particularly in the areas of detaining and arresting intruders and the use of deadly force. The NRC also needs to define the level of credible threat against which licensees are expected to secure their facilities and the protocol involved in securing these facilities.

Educate the public. A training program should be developed to provide education and assistance to the public with regard to safety and security around utility sites and critical infrastructure. Areas of law such as trespass and vandalism might be covered, as well as "critical area" designations. Often, the public is allowed access to green ways, waterfront property and other areas important to securing the utility's property. This issue is described in further detail in Section 3.4 Access Control and Zoning.

Utilize Operation TIPS. As proposed in *The Strategy*, the President's National Strategy for Homeland Security at 12, Operation TIPS (Terrorism Information and Prevention System) will be a nationwide program to help thousands of American truck drivers, letter carriers, train conductors, ship captains, and utility workers report potential terrorist activity. Pursuant to *The Strategy*, Operation TIPS was scheduled to begin a pilot program in ten cities in August 2002. By the nature of their job descriptions, many utility and transportation employees are placed into the view of the public on a daily basis. Through Operation TIPS, these employees are able to identify and report activities or situations that will assist in securing their communities.

3.3 Employer/Employee Liability and Background Checks

Provide employer protections. Legislation is necessary to provide protection for prospective and previous employers, against legal repercussions when providing a character or working reference for an employee. Employers are hesitant to provide a character or work reference, and commonly only provide dates of employment rather than a reference. The reluctance is due to the liability issues raised. Those employers with the most knowledge of a person's work habits and ethical standing will not disclose any information due to perceived and actual liabilities. One company requested protection for former employers regarding a new employer asking a former employer whether a prospective employee in a required "drug test position" previously failed a test.

Establish consistent background checks through law enforcement. The ability to do a consistent statewide and nationwide criminal background check on perspective utility employees does not exist from a law enforcement service in Pennsylvania. The PSP background check is only based on current address and does not develop a deeper check based by Social Security Number, previous employment or residence. General background checks, similar to the sex offenders' checks on teachers and health care workers, should be required for critical infrastructure employees. Banking lobby groups successfully petitioned that full disclosure notices, including financial information, be made available for their hired individuals. Inclusion of utilities in this information stream should be reviewed. Utilities and critical infrastructure should have the ability (through a third party or other means) to access the FBI's NCIC (National Crime Information Center) database for national background checks on prospective employees. This service might also be offered through the PSP background check or some other law enforcement agency process.

Support participation in *The Strategy for liability and privacy issues*. As noted in the President's National Strategy for Homeland Security at 34, "the Director of Homeland Security and the Attorney General will convene a panel with appropriate representatives from federal, state and local government, in consultation with the private sector, to examine whether employer liability statutes and privacy concerns hinder necessary background checks of personnel with access to critical infrastructure facilities or systems."

3.4 Access Control and Zoning

Undertake comprehensive review of protections. State agencies in coordination with utilities should also undertake a comprehensive review of other protection measures necessary to deny terrorist access to critical infrastructure -- for example, establishing "security zones" and controlling access around vulnerable facilities in a manner similar as access is controlled at airports. This might be best assigned to the Department of Homeland Security or a similar agency.

Allow security of facilities. There is a need to allow companies to secure facilities regardless of local, county or state zoning or ordinance issues. Some zoning ordinances are restricting security enhancements for many utility industries. Local ordinances and state regulations should allow for expedited variances where the ordinance or regulation impedes the implementation of critical infrastructure security measures.

Assess use of co-locations. A concern exists for the use of co-located facilities or other equipment and access control to these areas. Since September 11th, utility companies are hesitant to honor agreements or contracts to allow access to their facilities. For example, wireless companies use water towers to secure their antennas in some areas to avoid zoning disputes and utilize existing structures. Both of these companies need to regulate/monitor their equipment and require access to such areas. In some cases, one company may not be willing to distribute access keys to other entities.

Limit Public Access. The respondents have expressed concern over the amount of public access to waterways near critical facilities. Patrols and responses are expected from U.S. Coast Guard or the Pennsylvania Fish and Boat Commission where critical infrastructure is located on a patrolled waterway. Utility companies are concerned with access areas such as rights-of-ways, walkways, dams, reservoirs, green ways, etc., that are part of the company's "secure" areas. There is a need to strengthen the ability to prosecute or deter violations. The Pennsylvania railroads feel a need to develop specific legislation regarding railroad trespass legislation.

3.5 Incident Command System/Unified Command, Emergency Response Teams, and Color Code

Adopt Incident Command System. The federal government should encourage state and local first responder organizations to adopt the widespread Incident Command System by making it a requirement. In this manner, all parties involved in a security situation would be readily able to communicate, respond and resolve the situation since all are trained in the same procedures and protocols.

Assure utility access to emergency sites. Utility company emergency response teams need a single point of contact for permission to access disaster areas. Employee photo I.D. cards do not assure that police, federal agencies, and National Guard personnel securing the area will permit passage to utility workers and supervisors. The development of a utility sub-committee within the established Regional Counter-Terrorism Task Force process would alleviate many issues during a security incident. A single point of contact would be established prior to an event, which recognizes a single individual for all utility-related issues, thereby lessening the confusion in communications/response to a security event.

Adopt color code. It is also recommended that utilities be required to use the consistent color code designation developed by the Homeland Security Office in all utility industries, rather than using other designations.

3.6 Public Information/Privacy - Media, Maps, and Unions; Legal Review of Regulations

Limit information flow. Limiting public disclosure of physical and cyber critical infrastructure information without compromising the principles of openness that ensure government accountability is a key concern. Protecting the public's right to access information must be balanced with security interests. The benefits of certain information being made public must be weighed against the risk that freely available sensitive homeland security information may pose a threat to the interest of the company, state, or nation.

Review public right to know Laws. Most public right to know laws allow access to critical information concerning utility companies. These laws should be reviewed to ascertain if exclusions are necessary to protect exposure against terrorist activities. State agencies should develop a process to restrict availability of, or screen persons requesting to view utility maps and documents that contain design specifications and infrastructure locations. Currently much of this information is available to the public. Availability of information regarding utilities is a major concern in the industries, especially the information sent to and stored by state agencies. Industries have concerns about the PA One Call screening

process prior to providing locations of systems or providing maps of their systems.

Examine public right to know laws. A need exists for a review of state and federal right to know laws. This may be best accomplished during the creation of a state homeland security agency. A modification to include exclusions during times of crisis will allow access to police, law enforcement, and emergency management but without allowing media access to facilities or records. Companies perceive the media, as exploiting situations, exposing vulnerabilities, endangering the public and "planting" ideas into the minds of some individuals. Companies are hesitant to run actual drills with law enforcement or emergency management personnel due to media coverage and the possibility of creating poor public relations. Regulations and policies should be reviewed that restrict the release of information. The laws should provide a quick response on criminals, when it is related to utilities or infrastructure. Pennsylvania should also conduct reviews on establishing or reaffirming statewide criminal statutes for prosecution of conspiracy or attempts to damage utility facilities, as opposed to allowing statutes or ordinances to vary by municipality. One company feels the statutes do not currently contain strong enough language for judges to understand and impose large enough penalties in appropriate areas.

Obtain federal nuclear clearances. An appropriate level of federal security clearance for nuclear plant licensees should be obtained in order to provide them with access to information considered classified which describes threats to licensed facilities.

Monitor labor challenges. In some cases, the labor unions are challenging security issues such as surveillance cameras. Such devices are being perceived as an invasion of privacy and a tool to monitor employees. Companies also mentioned other union challenges that, if allowed, could possibly increase vulnerability of the utility systems.

3.7 Security Costs and Insurance

Prohibit terrorism exclusions from insurance coverage. It was recommended that the Commonwealth of Pennsylvania adopt regulations to prohibit the exclusions of terrorism events for insurance coverage, as previously enacted in other states. Insurance companies should be required to work with state insurance commissions (through legislation) to write terrorism policies for corporations at reasonable rates. The industries are concerned about actual and potential insurance increases in the areas of liability, property and workers' compensation, as well as terrorism coverage being dropped from their primary coverage, and the availability and cost of supplemental terrorism coverage. Additionally, to offset some of the related costs, companies can have the PSP, local police, and insurance carriers conduct on-site inspections of physical assets

and provide an assessment of present security, with recommendations for improvements.

Explore options for potential security cost recovery. Companies need a timely means to seek recovery of the prudent expenses and capital investment spent for security-related items. To date, no jurisdictional water, wastewater or steam utility has filed separately with the PUC to recover these costs. Non-jurisdictional companies can recover these costs by increasing rates, which does not require review by the PUC or other state regulators. As described in the above report findings, other industry groups are limited, or unable to recover security-related costs and investments. Industries need to balance the costs and benefits of increased security according to the threat level. Federal grant programs may be used to assist state and local infrastructure protection efforts, but many companies or industry groups are unable to recover their costs for reasonable or necessary security enhancements and upgrades.

Analyze insurance issues. Several companies stated that security and insurance costs are not a ratepayer issue, but a public safety issue since all citizens benefit by the safe and reliable nature of utility services. Respondents mentioned that there is a need for an acceptable level of risk to the Commonwealth that should not be borne solely by their business practices or by ratepayers. The FERC at Docket PL01-6-000 has a process to expedite recovery of security costs relating to prudently incurred costs necessary to further safeguard the nation's energy systems and infrastructure. To date no Pennsylvania companies have taken advantage of the process

Consider financial incentives. It has also been suggested that Pennsylvania consider issues of tax incentives and/or tax credits to help energy, water, telecommunications and transportation industries to encourage security investments. Suggestions included tax deferrals for passenger and baggage screening systems, the deferment of incremental costs until rate caps expire for the electric industry, and other recovery mechanisms for the natural gas and telecommunications industries.

Uniformly enforce mandated security directives. Mandated rules and legislation should be uniformly enforced, with appropriate opportunities for cost recovery, for all regulated and non-regulated companies in an industry group.

Monitor nuclear licensee liability. NRC licensees are concerned about potential insurance liability increases related to the extension of the protected and/or owner controlled areas and the use of deadly force.

3.8 Bridges, Mutual Aid, and Waivers

Implement waiver process. There is a need for weight restriction waivers for utility repair vehicles on small bridges in Northern and some Central counties during times of storms or other emergencies. For example, while lineman trucks are not permitted to pass over, fire trucks, and ambulances may use the bridge. Often the repair technician needs to detour through a non-direct route creating delays in restoration efforts. If waivers are not feasible options, these bridges should be identified and placed on a "priority list" for upgrade or replacement.

Expand mutual aid. A regional or statewide mutual assistance program that currently shares industry personnel and equipment during emergencies should be continued and expanded by all industry groups.

Coordinate with other states. The state waiver process used to move utility crews and equipment between states during an emergency already is in place and streamlined in Pennsylvania. Multi-state serving companies and all states that routinely receive and provide assistance to/from Pennsylvania need to become more familiar with this process.

XI. APPENDICES

- A. House Resolution 361
- B. Workplace Security Survey
- C. PUC/PEMA letter to Industries recommending participation in the Regional Counter-Terrorism Task Force; and
Regional Counter-Terrorism Task Force Map
- D. Nuclear Regulatory Commission Advisories
- E. 911 Section from the Governor's Task Force on Security-10/26/01
- F. Acronyms

THE GENERAL ASSEMBLY OF PENNSYLVANIA

HOUSE RESOLUTION

No. 361

Session of 2001

INTRODUCED BY WOGAN, NOVEMBER 20, 2001

AS AMENDED, HOUSE OF REPRESENTATIVES, DECEMBER 3, 2001

A RESOLUTION

1 Directing the Pennsylvania Public Utility Commission AND THE <—
2 PENNSYLVANIA EMERGENCY MANAGEMENT AGENCY to conduct a
3 comprehensive ~~study~~ ASSESSMENT of the ~~safety and security~~ <—
4 policies adopted by ~~utility service providers that protect~~ <—
5 ~~critical utility infrastructures, including operative and~~
6 ~~nonoperative nuclear power plant facilities, private electric~~
7 ~~and natural gas generating plants and independent electric~~
8 ~~system operators and to~~ REGULATED PUBLIC UTILITIES, OPERATIVE <—
9 AND NONOPERATIVE NUCLEAR POWER PLANTS, ELECTRIC GENERATING
10 COMPANIES, NATURAL GAS PRODUCERS, INDEPENDENT ELECTRIC SYSTEM
11 OPERATORS, COOPERATIVE ASSOCIATIONS, MUNICIPAL CORPORATIONS
12 AND MUNICIPAL AUTHORITIES THAT PROTECT CRITICAL UTILITY
13 INFRASTRUCTURES AND recommend prudent strategies to enhance
14 the standards for the physical security ~~of utility facilities~~ <—
15 ~~that create, possess, handle, store or transport energy in~~
16 ~~this Commonwealth.~~ AND INTEGRITY OF THESE FACILITIES. <—

17 WHEREAS, The September 11, 2001, terrorist attacks on the
18 World Trade Center in New York City, the Pentagon in Washington,
19 D.C., and the plane crash in Somerset County, Pennsylvania,
20 clearly demonstrate that neither the United States nor the
21 Commonwealth is immune from orchestrated acts of terrorism; and

22 WHEREAS, The threats of potential terrorist attacks against
23 the United States' CRITICAL utility infrastructures create civil <—
24 unrest and are occurring more frequently since the September 11,
25 2001, attack; and

1 WHEREAS, Maintaining the ~~safety~~ SECURITY and integrity of the <—
2 CRITICAL utility infrastructures of this Commonwealth remains a <—
3 high priority of the General Assembly; and

4 WHEREAS, Terrorist attacks that incapacitate or destroy
5 CRITICAL utility infrastructure systems and operating systems <—
6 compromise the health, safety and welfare of the citizens of
7 this Commonwealth; and

8 WHEREAS, The protection of the critical utility
9 infrastructures in this Commonwealth is necessarily a shared
10 responsibility and partnership between owners, operators and THE <—
11 FEDERAL AND State Government; and

12 WHEREAS, The Pennsylvania Public Utility Commission is
13 responsible for ~~developing energy forecasts, conducting audits,~~ <—
14 enforcing the Public Utility Code and inspecting utility
15 facilities to assure the safe, reliable and adequate delivery of
16 utility service to the citizens of this Commonwealth; and

17 WHEREAS, The Pennsylvania Public Utility Commission is
18 responsible for evaluating programs that ensure the stability of
19 complex and interdependent utility systems in this Commonwealth
20 and for developing policy recommendations that support the
21 ~~continuous~~ operation of interconnected CRITICAL utility <—
22 infrastructures; and

23 WHEREAS, ~~Any physical disruption of the operation of critical~~ <—
24 CRITICAL utility infrastructures in this Commonwealth must <—
25 REMAIN RELIABLE SUCH THAT ANY PHYSICAL DISRUPTION WILL be rare, <—
26 brief, geographically limited in effect, manageable and
27 minimally detrimental to the economy, human and government
28 services and the security of our State and nation; and

29 WHEREAS, THE PENNSYLVANIA EMERGENCY MANAGEMENT AGENCY IS <—
30 CHARGED WITH THE MANAGEMENT AND COORDINATION OF THE

1 COMMONWEALTH'S EMERGENCY MANAGEMENT PROGRAMS AND ADMINISTERS THE
2 COMMONWEALTH'S EMERGENCY OPERATIONS CENTER (EOC); AND

3 WHEREAS, THE PENNSYLVANIA EMERGENCY MANAGEMENT COUNCIL IS
4 RESPONSIBLE FOR OVERALL POLICY AND DIRECTION OF STATEWIDE
5 DISASTER PROGRAMS AND RESPONSE CAPABILITIES, IS CHAIRED BY THE
6 LIEUTENANT GOVERNOR AND HAS A MEMBERSHIP THAT INCLUDES STATE
7 AGENCIES, COUNTY AND LOCAL GOVERNMENTS; AND

8 WHEREAS, The General Assembly deregulated Pennsylvania's
9 electricity market in 1996 and its natural gas market in 1999,
10 which resulted in privately owned and operated utility
11 generating facilities; and

12 WHEREAS, PJM Interconnection is a ~~privately managed~~ PRIVATE ←
13 limited liability corporation which operates the largest
14 centrally controlled dispatched electric system in North
15 America, providing 23 million consumers in five states with
16 reliable electric service; and

17 WHEREAS, The United States Nuclear Regulatory Commission
18 regulates commercial nuclear power reactors, nonpower research,
19 testing and training reactors, fuel cycle facilities, medical,
20 academic and industrial uses of nuclear materials and the
21 transport, storage and disposal of nuclear materials and waste;
22 therefore be it

23 RESOLVED, That the General Assembly direct the Pennsylvania
24 Public Utility Commission AND THE PENNSYLVANIA EMERGENCY ←
25 MANAGEMENT AGENCY, in cooperation with other Federal and State
26 agencies, the United States Nuclear Regulatory Commission,

27 regulated public utilities, ~~privately owned and municipally~~ ←
28 ~~owned utility companies and independent grid system operators to~~
29 ~~conduct a comprehensive review and evaluation of the safety and~~

30 OPERATIVE AND NONOPERATIVE NUCLEAR POWER PLANTS, ELECTRIC ←

1 GENERATING COMPANIES, NATURAL GAS PRODUCERS, INDEPENDENT
2 ELECTRIC SYSTEM OPERATORS, COOPERATIVE ASSOCIATIONS, MUNICIPAL
3 CORPORATIONS AND MUNICIPAL AUTHORITIES, TO REVIEW AND EVALUATE
4 security policies implemented in and around ~~the~~ PENNSYLVANIA'S <—
5 CRITICAL utility infrastructures ~~in this Commonwealth~~ since the <—
6 September 11, 2001, terrorist attack; and be it further
7 RESOLVED, That the Pennsylvania Public Utility Commission AND <—
8 THE PENNSYLVANIA EMERGENCY MANAGEMENT AGENCY analyze existing
9 utility infrastructure protection and continuity programs and
10 utility-specific proposals to implement counterterrorism threat
11 assessment and risk mitigation policies; and be it further
12 RESOLVED, THAT RECOMMENDATIONS BE MADE BY THE PENNSYLVANIA <—
13 PUBLIC UTILITY COMMISSION AND THE PENNSYLVANIA EMERGENCY
14 MANAGEMENT AGENCY TO THE GENERAL ASSEMBLY CONCERNING STATUTORY
15 CHANGES TO ENABLE COST RECOVERY MECHANISMS FOR ANY SECURITY
16 MODIFICATIONS TO UTILITY INFRASTRUCTURES RECOMMENDED BY THE
17 PENNSYLVANIA PUBLIC UTILITY COMMISSION AND THE PENNSYLVANIA
18 EMERGENCY MANAGEMENT AGENCY; AND BE IT FURTHER
19 RESOLVED, THAT PROPRIETARY, SECURITY AND COMPETITIVELY
20 SENSITIVE INFORMATION AND TRADE SECRETS OF REGULATED PUBLIC
21 UTILITIES, OPERATIVE AND NONOPERATIVE NUCLEAR POWER PLANTS,
22 ELECTRIC GENERATING COMPANIES, NATURAL GAS PRODUCERS,
23 INDEPENDENT ELECTRIC SYSTEM OPERATORS, COOPERATIVE ASSOCIATIONS,
24 MUNICIPAL CORPORATIONS AND MUNICIPAL AUTHORITIES SHALL NOT BE
25 PUBLIC RECORDS FOR PURPOSES OF THE ACT OF JUNE 21, 1957
26 (P.L.390, NO.212), REFERRED TO AS THE RIGHT-TO-KNOW LAW, AND
27 SHALL NOT BE SUBJECT TO MANDATORY PUBLIC DISCLOSURE WHICH WOULD
28 COMPROMISE THE SECURITY AND INTEGRITY OF CRITICAL UTILITY
29 INFRASTRUCTURES; AND BE IT FURTHER
30 RESOLVED, That the Pennsylvania Public Utility Commission AND <—

1 THE PENNSYLVANIA EMERGENCY MANAGEMENT AGENCY report ~~its~~ THEIR ←
2 findings and recommendations to the House of Representatives on
3 or before ~~July 15, 2002~~ SEPTEMBER 1, 2002. ←

WORKPLACE SECURITY SURVEY

1. GENERAL

- 1.1. Does the Company participate in the FBI InfraGard program?
- 1.2. What changes in security plans, procedures and policies has the Company made since 9/11/01
- 1.3. Has the Company updated security plans since the Y2K plan was put into place?
- 1.4. Has the Company participated in any assessment by an outside organization of their security plans, policies and procedures?
- 1.5. How recently has the company updated their emergency personnel listing?
- 1.6. How recently has the company updated their contact information?
- 1.7. How recently has the company conducted a drill on their procedures? Does the company conduct such drills on a regular basis? If so, how often?
- 1.8. How recently have plans been updated for individual facilities?
- 1.9. How recently have company facilities contacted their local law enforcement contacts?
- 1.10. For each of the past 3 years please provide an estimate of security-related capital and operating costs.
- 1.11. What regulatory oversight does the company perceive in its security-based obligations?
- 1.12. Have there been any major changes in insurance requirements and premiums since the 9/11/01 incidents? Please describe in detail.
- 1.13. Has your insurance coverage been altered since 9/11/01? Was the alteration made by the company or the insurer? Please explain.
- 1.14. Have you participated in any security reviews with your insurance provider? Describe the extent of the review.

- 1.15. Please describe your internal processes for handling security related planning in your corporation?
- 1.16. Please describe your internal organization for security planning in your corporation?
- 1.17. Please describe any changes in your organization and planning since the 9/11/01 incidents?
- 1.18. As an example of your corporate policies please describe your most recent security related incident prior to 9/11/01 and how it was handled by the corporation?
- 1.19. Describe the Company's procedures to notify customers in case of an emergency?
- 1.20. Explain pre 9/11/01 and post 9/11/01 policy for facility tours.
- 1.21. Explain the emergency procedures implemented on September 11th.
- 1.22. What is the protocol for alerting the public when an incident takes place?

2. BUSINESS CONTINUITY

- 2.1. Does the company possess a formal and/or approved succession plan for its corporate affairs?
- 2.2. Does the company have policies that restrict traveling of corporate officials in common transportation vehicles?
- 2.3. Does the company have an emergency plan for corporate decision making?
- 2.4. Does the company maintain multiple means for contacting its decisions makers?
- 2.5. How often are the contact systems updated and tested?

3. CYBER SECURITY

- 3.1. Please describe your planning process for security of your computer networks and information?
- 3.2. Please describe your policies for use of your computer networks?

- 3.3. Please describe your maintenance of computer based records?
 - 3.4. Does the company maintain a disaster recovery plan?
 - 3.5. What arrangements have been made to process data offsite in the event of a disaster?
 - 3.6. When was the most recent test of the disaster recovery plan?
 - 3.7. Please describe your discipline policy for misuse of company records?
 - 3.8. Has the company conducted any drills regarding cyber security?
 - 3.9. How does the company disseminate information regarding computer viruses and alerts?
 - 3.10. What instruction is provided to employees for use of virus software?
 - 3.11. Are procedures in place for reporting threats received via email?
 - 3.12. Is all e-mail able to be reviewed corporately?
 - 3.13. How has internal access to computer programs and data files been restricted?
 - 3.14. Is Internet and e-mail policy disseminated to employees regularly?
 - 3.15. Do employees perceive their e-mail as private?
 - 3.16. Is encryption used for any communications?
 - 3.17. Approximately what proportions of your employees have access to corporate facilities for Internet and e-mail?
 - 3.18. Does the company believe that it has adequate legal tools to document and prosecute any cyber sabotage?
- 4. ACCESS CONTROL (Clarify if for Corporate Headquarters or all buildings).**
- 4.1. Do visitors need to secure passes before they enter?
 - 4.2. Are visitor passes distinctive from employee passes?

- 4.3. Is there a record of when and to whom the organization issues passes?
- 4.4. Does the organization collect passes when visitors depart?
- 4.5. Are passes or badges difficult to forge?
- 4.6. Is the perimeter of the office or building adequately illuminated?
- 4.7. Is the roof illuminated?
- 4.8. Are the parking lots adequately illuminated?
- 4.9. Do time-sensitive or motion sensor devices control the lights?
- 4.10. Does the organization replace burnt-out light bulbs immediately?
- 4.11. Are light fixtures protected against breakage?
- 4.12. Are passageways and storage areas illuminated?
- 4.13. Is lighting at night sufficient for police surveillance?
- 4.14. Does a fence or wall protect the place of business on all sides?
- 4.15. Are fences or walls in good repair?
- 4.16. Do groundskeepers keep the fence or wall clear of nearby trees, bushes and tall grass?
- 4.17. Does Security check locks regularly?
- 4.18. Do gates remain locked when not in use?
- 4.19. Is there an alarm system?
- 4.20. Are there security-locking devices on each door and window?
- 4.21. Are doors constructed of sturdy materials?
- 4.22. Are there only the barest minimum of access doors to the facility?
- 4.23. Are door hinges spot-welded or secured, in order to prevent removal?
- 4.24. Are the hinges facing the inward side of the doors?

- 4.25. Are there time locks to detect unauthorized entrance?
- 4.26. If there are padlocks, do they comprise high-quality materials?
- 4.27. Are padlock hasps made of heavy-duty materials?
- 4.28. Do opening alarms protect all fire doors?
- 4.29. Is the alarm system connected to all doors and windows?
- 4.30. Does the organization follow a specific lock-up procedure?
- 4.31. Is someone responsible for checking all doors and windows to make sure they are closed and locked every night?
- 4.32. Are all alarms connected to a central control center?
- 4.33. Do personnel man the central control station at all times?
- 4.34. Are there periodic checks on response times to alarms?
- 4.35. Does the organization test alarms on a regular basis?
- 4.36. Is there a backup emergency power source for the alarm system?
- 4.37. Are surveillance cameras in place for all exits and entrances?
- 4.38. Are surveillance cameras in place for all parking lots and alleys?

5. VEHICLE CONTROL

- 5.1. Is there a separate area for employee parking?
- 5.2. Is there a separate area for visitor parking?
- 5.3. Do personnel verify all service vehicles?
- 5.4. Is there a log of service vehicles?
- 5.5. Are all delivery vehicles scheduled in advance?
- 5.6. Are delivery drivers identified in advance?
- 5.7. Does the organization fence in or secure parking areas?
- 5.8. Does the organization illuminate parking areas?

5.9. Do guards patrol parking areas?

6. OFFICE SECURITY

6.1. Do personnel properly greet and/or challenge strangers?

6.2. Do personnel protect billfolds, purses and other personal belongings while on the job?

6.3. Does only one person issue all keys?

6.4. Does the organization keep a record of who has received what keys and if the individual(s) return them?

6.5. Do all keys clearly state "Do Not Duplicate?"

6.6. Does the organization have a lost key policy?

6.7. Are maintenance personnel, visitors, etc. required to show ID to a receptionist?

6.8. Is there a clear line of sight from the reception area to the entrance, stairs and elevators?

6.9. Is it possible to reduce the number of entrances without a loss of efficiency or safety?

6.10. Do personnel keep office doors locked when unattended for a long period of time?

6.11. Do personnel keep items of value secure in a locked file or desk drawer?

6.12. Has Security briefed the supervisor of each office on security problems and procedures?

6.13. Do all office employees receive some security education?

6.14. Do office-closing procedures require that important information be secure at night?

6.15. Does the organization keep office entrance doors locked except during business hours?

6.16. Do personnel shred confidential material before placing it in the trash?

- 6.17. Does the organization log in and out all janitorial and cleaning service personnel?
- 6.18. Does a security force protect the facility or building?
- 6.19. Are security personnel company employees or contractors?
- 6.20. Are security employees or contractors licensed and trained pursuant to 22 Pa. C.S. §§11-50.1?
- 6.21. How often do they receive training?
- 6.22. Do they receive live fire training?
- 6.23. Do guards understand their role?
- 6.24. Are guards prepared to act in case of an emergency?
- 6.25. Do guards carry arms legally?
- 6.26. Are guards alert?
- 6.27. Is there an effective system for communication in emergency situations? How often is it tested?
- 6.28. Please describe the handling of mail and packages at your facilities?
- 6.29. Is all mail centrally received and checked?
- 6.30. Where is mail opened?
- 6.31. Have mail personnel received training on procedures for biological or incendiary threats?
- 6.32. Are all packages verified prior to opening on source and request?
- 6.33. Have personnel received training in procedures for handling and reporting suspicious packages?
- 6.34. Have phone personnel received training on handling bomb threats?
- 6.35. Are procedures in place for reporting bomb threats and/or threats to company property?

7. HIGH SECURITY AREAS

- 7.1. Do personnel keep high security areas locked at all times?
- 7.2. Do managers and/or security personnel keep high security areas under supervision?
- 7.3. Do badges bear clear markings to designate those who may enter security areas?
- 7.4. Do procedures require employees to verify their identity when entering security areas?
- 7.5. Is access to high security areas controlled?
- 7.6. Have any areas had their designation as "high security" changed since 9/11/01?
- 7.7. Have budget decisions affected the designation of areas as "high security"?

8. PERSONNEL

- 8.1. Does Security require personnel to wear badges or identification cards?
- 8.2. Does Security require employees to display ID badges at entrances?
- 8.3. Does Security include card numbers on all identification cards?
- 8.4. Does Security include employee photographs on all ID cards?
- 8.5. Does Security keep a record of all lost or stolen badges?
- 8.6. Does Security keep a record of all badges issued?
- 8.7. Does Security institute standard screening procedures for all employees before hiring?
- 8.8. Does Security fingerprint all employees?
- 8.9. Does Security photograph all applicants?
- 8.10. Does Security keep personnel files of all employees?

- 8.11. Does Security require employees to produce official identification at the time of hiring?
- 8.12. Does Security check references?
- 8.13. Does Security require employees to present a list of past employers?
- 8.14. Does Security check employees past employers?
- 8.15. Does Security require employees to provide any pseudonyms?
- 8.16. Does Security instruct employees on all security and emergency operating procedures in place?
- 8.17. Does Security believe there are regulatory or legal barriers to performing background checks on employees? Which barriers?
- 8.18. Are their formal procedures in place for notifying management of problems in an employee's background check and current activities?



**COMMONWEALTH OF PENNSYLVANIA
PENNSYLVANIA PUBLIC UTILITY COMMISSION
P.O. BOX 3265, HARRISBURG, PA 17105-3265**

May 31, 2002

M-00021590

To Utilities Participating in House Resolution 361 Security Review:

As you are aware, the Pennsylvania Public Utility Commission ("PUC") and the Pennsylvania Emergency Management Agency ("PEMA") were tasked by the Pennsylvania House of Representatives, pursuant to House Resolution 361, to review, analyze, and evaluate utility infrastructure security protection. This tasking also includes an evaluation of risk mitigation policies and other related security issues, and requires the PUC and PEMA to recommend prudent strategies to enhance the standards for physical security and integrity of utility industry infrastructure in the Commonwealth. The report to the House of Representatives is due September 1, 2002.

As part of this effort, we asked utilities to complete a "Workplace Security Survey" and participate in an on-site interview process with PUC and PEMA Staff. This interview process covered five areas of discussion: emergency response and contingency plans; business continuity plans; cyber security and disaster recovery; security costs & insurance liability; and, recommendations on regulatory policy changes to assist the industries in improving security at critical facilities.

Staff members of the PUC and PEMA recently attended the "Pennsylvania Regional Counter-Terrorism Task Force Symposium" with other emergency management professionals. During the interview process with the utility industries and from discussions during the Symposium, it became apparent that none of the surveyed utilities were aware of, or belonged to, any of the nine regional Task Forces located throughout Pennsylvania. We believe that utility participation in the Task Forces will help the utilities to better respond to terrorist threats and provide the Task Forces with a utility perspective.

Enclosed please find a map showing the nine task force regions in Pennsylvania, a list of the counties that make up the region, and a list of contacts and telephone numbers for each region. In addition to these documents, we are providing you with the five Threat Condition Levels and Readiness Actions.

We strongly encourage each utility to participate and become a part of its respective Regional Counter-Terrorism Task Force. If you do choose to

participate in a Task Force, we ask that you provide written notification to the PUC's Bureau of Fixed Utility Services after you have contacted the Task Force and before June 21, 2002. We would like to track the level of utility participation in order to assess whether further action is required.

Please file an original and one copy of the notification at Docket No. M-00021590 with James J. McNulty, Secretary, Pennsylvania Public Utility Commission, P. O. Box 3265, Harrisburg, PA 17105-3265. Please be assured that any information provided that is proprietary or confidential in nature will be protected from disclosure pursuant to the Public Utility Code, 66 Pa. C.S. § 335(d) and as mandated in House Resolution 361.

Any questions concerning this matter should be directed to either Robert A. Rosenthal (717-783-5242) or David T. Newcomer (717-787-6381) at the PUC. Thank you for your cooperation in this important matter.

Sincerely,

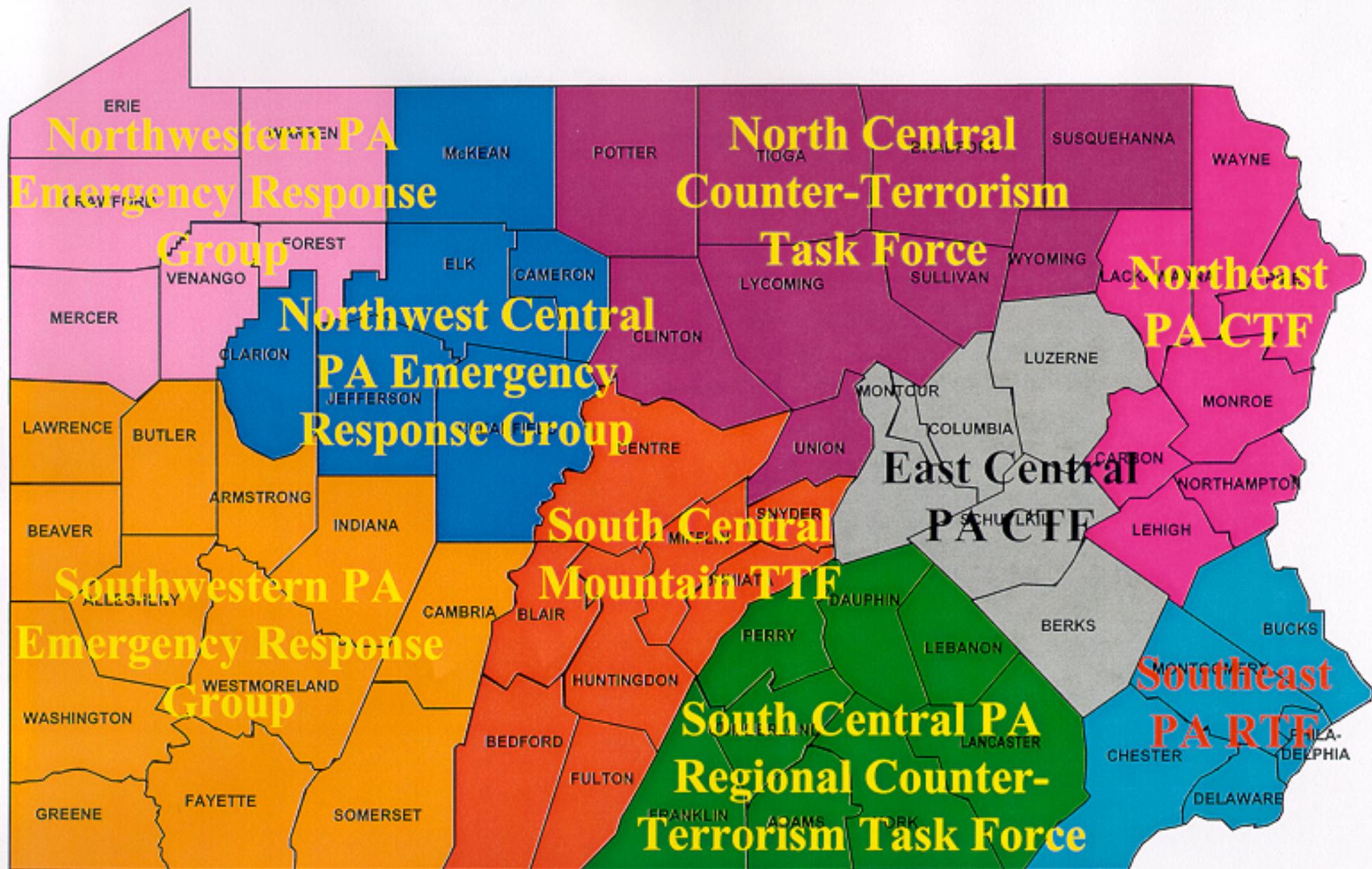
Glen R. Thomas
Chairman
Pennsylvania Public Utility Commission

David L. Smith
Director
Pennsylvania Emergency Management Agency

Attachments

cc: Veronica Smith, PUC Executive Director
Karen Moury, PUC Deputy Executive Director
J. J. McNulty, PUC Secretary
Robert Rosenthal, PUC Director FUS
David Newcomer, PUC Emergency Management Coordinator
David Zambito, Counsel to PUC Chairman
Earl Freilino, PA Director of Homeland Security
Donna Zack, PEMA Director's Office
File

REGIONAL COUNTER-TERRORISM TASK FORCES



APPENDIX D

NRC Advisories Issues Since September 11, 2001

Note: Advisory Numbers were not assigned until November 6, 2001.

Advisory Number	Tab	Date Issued	Subject	# of Pages
N/A	A	09/11/01	IAT Advisory for Power Reactors, Non-Power Reactors, Category 1 Fuel Facilities and Gaseous Diffusion Plants <u>Subject:</u> Initial threat advisory recommending Security Level III be established according to Information Notice 98-35	1
N/A	B	09/04/98	NRC Information Notice 98-35: Threat Assessments and Consideration of Heightened Physical Protection Measures	5
N/A	C	09/12/01	IAT Advisory Update for Power Reactors, Non-Power Reactors, Category 1 Fuel Facilities and Gaseous Diffusion Plants <u>Subject:</u> Continuation of Security Level III	1
N/A	D	09/14/01	IAT Advisory Update for Power Reactors, Non-Power Reactors, Category 1 Fuel Facilities Decommissioning Reactors, Independent Spent Fuel Storage Installation, and Gaseous Diffusion Plants <u>Subject:</u> Continuation of Security Level III with sensitivity to personnel with temporary access, security personnel with temporary access not serving in an armed capacity, access of vehicles, potential activation of Site Operations Centers. Encouragement to licensees to report suspicious or unusual activity, or threats	1
N/A	E	09/21/01	IAT Advisory Update for Power Reactors, Non-Power Reactors, Category 1 Fuel Facilities Decommissioning Reactors, Independent Spent Fuel Storage Installation, and Gaseous Diffusion Plants <u>Subject:</u> Continuation of Security Level III with clarification regarding personnel with temporary access, increased awareness of personnel activities, continuation of limitation on use of security personnel with temporary access, heightened level of awareness of vehicle access, and continuation of 09/14/01 IAT recommended conditions	1

N/A	F	09/25/01	IAT Advisory for Large Materials Licensees and Agreement States <u>Subject:</u> Ensure awareness of the continuing threat by large materials licensees and agreement states and ensuring control of personnel access to large amounts of radioactive materials, heightened awareness of vehicle access to facilities.	
N/A	G	10/06/01	IAT Advisory Update for Power Reactors, Non-Power Reactors, Category 1 Fuel Facilities Decommissioning Reactors, Independent Spent Fuel Storage Installation, and Gaseous Diffusion Plants <u>Subject:</u> Continuation of Security Level III with recommended additions described in previous advisories and notification that other actions would be provided under separate cover for power reactors, decommissioning reactors, Category 1 fuel facilities, gaseous diffusion plants, and Independent Spent Fuel Storage Installations	1
N/A	H	10/06/01	IAT Advisory for Power Reactors, Decommissioning Reactors, Category 1 Fuel Facilities and Gaseous Diffusion Plants <u>Subject:</u> A nine-page advisory with a list of prompt actions and additional actions for licensees to consider in order to strengthen licensee capability to respond to a terrorist attack	9
N/A	I	10/06/01	IAT Advisory for Power Reactors, Decommissioning Reactors, Category 1 Fuel Facilities and Gaseous Diffusion Plants <u>Subject:</u> An eleven-page safeguards advisory with safeguards specific lists of prompt actions and additional action for licensees to consider in order to strengthen licensee capability to respond to terrorist attack	11
N/A	J	10/07/01	IAT Advisory for Power Reactors, Decommissioning Reactors, Category 1 Fuel Facilities and Gaseous Diffusion Plants <u>Subject:</u> Notification to licensee of the initiation of US military action against targets in Afghanistan and continuance of Security Level III, including additional recommendations of previous advisories.	1

N/A	K	10/11/01	IAT Advisory Update for Independent Spent Fuel Storage Installations <u>Subject:</u> A three-page advisory with a list of prompt actions and additional actions for licensees to consider in order to strengthen licensee capability to respond to terrorist attack	3
N/A	L	10/11/01 Revised 10/12/01	IAT Advisory Update for Non-Power Reactors <u>Subject:</u> A four-page advisory with a list of prompt actions and additional actions for licensees to consider in order to strengthen licensee capability to respond to terrorist attack.	4
N/A	M	10/11/01 Revised 10/12/01	IAT Advisory Update for Category 3 Fuel Facilities and Conversion Facilities. <u>Subject:</u> A four page advisory with a list of prompt actions and additional actions for licensees to consider in order to strengthen licensee capability to respond to terrorist attack	4
N/A	N	10/12/01	Identical advisories issued October 12, 2001, reissued with the HQ Operations Center as the number to contact concerning questions on the advisories	
N/A	O	10/16/01	IAT Advisory for Power Reactors, Decommissioning Reactors, Non Power Reactors, Category 1 Fuel Facilities, Gaseous Diffusion Plants and Independent Fuel Storage Installations <u>Subject:</u> The report is divided into two sections. This first provides information regarding terrorist targets, tactics, and training and the second discusses threat indicators. Safeguards Advisory for Materials Licensees on Security of Licensed Materials. <u>Subject:</u> Urges licensees to maintain a high level of security alertness and recommends listed actions that may have significant value to address threats.	4 & 2
N/A	P	10/18/01	IAT Advisory Update for Power Reactors, Non Power Reactors, Decommission Reactors, Fuel Facilities, Gaseous Diffusion Plants and Independent Spent Fuel Storage Installations. <u>Subject:</u> Update to the threat environment. Briefly describes the TMI event that occurred on October 17, 2001	1

N/A	Q	10/23/01	IAT Advisory Update for Power Reactors, Non Power Reactors, Decommission Reactors, Fuel Facilities, Gaseous Diffusion Plants and Independent Spent Fuel Storage Installations <u>Subject:</u> Update to the threat environment. Provides routine update to current threat	1
N/A	R	10/25/01	IAT Advisory Update for Power Reactors, Non Power Reactors, Decommission Reactors, Fuel Facilities, Gaseous Diffusion Plants and Independent Spent Fuel Storage Installations <u>Subject:</u> Update regarding the termination of the Federal Bureau of Investigation's Watch List process	1
N/A	S	10/26/01	Safeguards Advisory Update for Material Licensees on Security of Licensed Material <u>Subject:</u> Recommendations specific to maintaining and improving security and control of radioactive materials	1
N/A	T	10/29/01	IAT Advisory Update for Power Reactors, Decommission Reactors, Category 1 Fuel Facilities, and Gaseous Diffusion Plants <u>Subject:</u> Strengthen perimeter security due to escalated threat environment	
N/A	U	11/01/01	IAT Threat Advisory Update for Non Power Reactors, Category III Fuel Facilities, the Conversion Plant, Large Materials Facilities, and ISFSIs. <u>Subject:</u> National threat level threat has escalated	
IA-0101	V	11/01/01	Information Assessment Team Recommended Actions in Response to a Site Specific Credible Threat at a Nuclear Power Plant (IA-01-01)	2

SA-01-01	W	11/08/01	Safeguard Advisory for Licensees Who Prepare or Receive Shipments of Highway Route Controlled Quantities of Radioactive Material (SA-01-01) <u>Subject:</u> Recommendations for Shipment of Radioactive Material Exceeding Highway Route Controlled Quantity	
SA-01-01		11/09/01	Safeguards Advisory for Licensees Who Prepare or Receive Shipments of Highway Route Controlled Quantities of Radioactive Material (SA-01-01) <u>Subject:</u> Corrected Phone Number	
SA-01-02		12/13/01	Safeguards Advisory for Licensees who prepare or receive shipments of Irradiated Reactor Fuel	
IA-01-02	X	11/12/01	IAT Advisory Update for Power Reactors, Non Power Reactors, Decommission Reactors, Category I Fuel Facilities, Category III Fuel Facilities, Gaseous Diffusion Plants, Independent Spent Fuel Storage Installations, Large Materials Licensees, and Conversion Facilities (IA-01-02) <u>Subject:</u> Update on Threat Environment and Continuation of Security Measures (re: American Airlines Flight 587)	1
IA-01-03	Y	11/14/01	IAT Advisory Update for Power Reactors, Decommission Reactors, Category I Fuel Facilities, Gaseous Diffusion Plants (IA-01-03) <u>Subject:</u> Update on Threat Environment	1
IA-01-04	Z	11/15/01	IAT Advisory Update for Power Reactors, Gaseous Diffusion Plants Conversion Facilities and Category I Fuel Facilities Associated with Office of Investigation Initiatives to Assess Unusual Events Prior to 09/11/01 (IA-01-04)	2
IA-01-05	AA	11/21/01	Credible threat guidance for Gaseous Diffusion, Conversion and Category I and III Fuel Fabrication Facilities	
IA-01-06	BB	11/21/01	Credible Threat Guidance for Independent Spent Fuel storage installation	
IA-01-07	CC	11/21/01	Credible threat guidance for Large Material Licensees	

IA-01-08	DD	12/05/01	Advisory Update for Power Reactors, Non Power Reactors, Decommission Reactors, Category I & III Fuel Facilities, Gaseous Diffusion Plants, Conversion Facilities Independent Spent Fuel Storage Installations, and Large Materials Licensees	1
IA-01-09	EE	12/14/01	Advisory Update on Threat Environment and Continuation of Security Measures	1
IA-02-01	FF	01/18/02	Advisory Update for Power Reactors, Non Power Reactors, Decommission Reactors, Category I & III Fuel Facilities, Gaseous Diffusion Plants, Conversion Facilities Independent Spent Fuel Storage Installations, and Large Materials Licensees	1
IA-02-02	GG	01/23/02	IAT Advisory Update - to same distribution as IA-02-01	1
IA-02-03	HH	05/17/02	IAT Advisory for Three Mile Island (with tearline)	1
IA-02-04	II	05/17/02	IAT Advisory for Three Mile Island (without tearline)	1

911 Section from the Governor's Task Force on Security, October 26, 2001.

D. Public Safety Answering Points (PSAPs) – 911 Centers

Description. Pennsylvania has 70 PSAPs, which are operated primarily by county or municipal government agencies. Some counties, such as Allegheny, have more than one PSAP. For the most part, PSAP facilities are housed in relatively secure facilities.

PSAPs are connected to the public switched telecommunications network (PSTN) with dedicated trunk lines. These PSAP trunks are connected to PSTN serving tandem switches. The trunks handle all incoming and outgoing emergency calls, both from the callers and to the responding emergency units. The trunks also allow communication to off-site data bases, which are required to identify, and provide information concerning incoming calling locations.

Critically. High. PSAPs, by their very nature, are critical facilities. All local emergency units, i.e., fire, police, emergency medical, etc., are dispatched by the PSAP during emergency conditions.

III. Recommendations for Action

D. Public Safety Answering Points (PSAPs) – 911 Centers

1. Managers of PSAPs, in cooperation with county and municipal government officials, should review physical security arrangements at the PSAP facility. This review is especially important for PSAPs that are co-located with other county and/or municipal government departments and agencies. Access to PSAP facilities should be strictly controlled.
2. Managers of PSAPs should also review mutual aid provisions to ensure that if one PSAP is temporarily disabled, either a backup location is available or incoming calls can be forwarded to an adjoining PSAP for dispatch of emergency response agencies.

APPENDIX F**ACRONYMS**

Acronym	Description	Industry / Agency
AAR	American Association of Railroads	Rail
AGA	American Gas Association	Gas
ANSIR	Awareness of National Security Issues and Response	Federal Agency
AWWA	American Water Works Association	Water
BRP	Bureau of Radiation Protection	DEP - State Agency
BWR	Boiling Water Reactor	Nuclear
CDL	Commercial Driver License	Transportation
CLEC	Competitive Local Exchange Carrier	Telecommunications
CO	Central Office	Telecommunications
DEP	Department of Environmental Protection	State Agency
DMVA	Department of Military and Veterans Affairs	State Agency
DOD	Department of Defense	Federal Agency
DOE	Department of Energy	Federal Agency
DOT	Department of Transportation	Federal Agency
EAP	Energy Association of PA	Electric & Gas
EAS	Emergency Alert System	Emergency Management
EDC	Electric Distribution Company	Electric
EI	Edison Electric Institute	Electric
EGS	Electric Generation Supplier	Electric
EMA	Emergency Management Agencies	Emergency Management
EMAC	Emergency Management Advisory Council	Pittsburgh Mayor's Office
EPA	Environmental Protection Agency	Federal Agency
EPRI	Electric Power Research Institute	Electric
FBI	Federal Bureau of Investigation	Federal Agency
FCC	Federal Communication Commission	Federal Agency - Telecommunications
FERC	Federal Energy Regulatory Commission	Federal Agency - Electric & Gas
FPA	Federal Pipeline Authority	Federal Agency - Gas
FRA	Federal Railroad Authority	Federal Agency - Rail
HAZMAT	Hazardous Material	Emergency Management
HR	House Resolution	
ILEC	Incumbent Local Exchange Carrier	Telecommunications
InfraGard	FBI program	Federal Agency
INGAA	Interstate Natural Gas Association of America	Gas
IOGCC	Interstate Oil and Gas Compact Commission	Gas

ISO	Independent System Operator	Electric
IT/IS	Information Technology/Information Systems	Computer
IXC	Inner Exchange Carrier	Telecommunications
LDC	Local Distribution Company	Gas
LNG	Liquid Natural Gas	Gas
LPG	Liquid Propane Gas	Gas
MW	Mega Watt	Electric
MWh	Mega Watt hour	Electric
NCIC	National Crime Information Center	Federal Agency
NERC	North American Electric Reliability Council	Electric
NG	National Guard	Military
NGS	Natural Gas Supplier	Gas
NIPC	National Infrastructure Protection Center	Federal Agency
NOC	Network Operations Center	Telecommunications
NOPR	Notice of Proposed Rulemaking	
NRC	Nuclear Regulatory Commission	Nuclear
NSTB	National Safety Transportation Board	Transportation
OPS	Office of Pipeline Safety	Federal Agency
PA	Pennsylvania	
PEMA	Pennsylvania Emergency Management Agency	State Agency
PJM	Pennsylvania New Jersey Maryland Interconnection	Electric
POLR	Provider of Last Resort	Electric
POP	Point of Presence	Telecommunications
PREA	Pennsylvania Rural Electric Association	Electric
PSAP	Public Safety Answering Points	Telecommunications
PSP	Pennsylvania State Police	State Agency
PTA	Pennsylvania Telephone Association	Telecommunications
PUC	Public Utility Commission	State Agency
PWR	Pressurized Water Reactor	Nuclear
RCTTF	Regional Counter-Terrorism Task Forces	Emergency Management
SCADA	Supervisory Control and Data Acquisition	Electric, Gas, Water, Wastewater, Steam
SDWA	Safe Drinking Water Act	Water
SEOC	State Emergency Operations Center	Emergency Management
SERT	Special Emergency Response Team	PSP - State Agency
ST ISAC	Surface Transport Information Sharing & Analysis Center	Railroad
STRACNET	Department of Defense Rail	Military
T & D	Transmission and Distribution	Electric
The Strategy	National Strategy for Homeland Security	Federal Agency Report

TIPS	Terrorism Information and Prevention System	The Strategy
TMI	Three Mile Island Nuclear Plant	Nuclear Plant
USAPA	USA Patriot Act	Federal Act
USTA	US Telecommunications Association	Telecommunications
Y2K	Year 2000 Computer Investigation	Computer
24/7	Every day all day. 24 hours per day seven days per week.	



PENNSYLVANIA PUBLIC UTILITY COMMISSION
P.O. BOX 3265
HARRISBURG, PA 17105



PENNSYLVANIA EMERGENCY MANAGEMENT AGENCY
2605 INTERSTATE DRIVE
HARRISBURG, PA 17110