Energy Generation and Transmission in the Great Lakes Region

Critical Infrastructure Protection Research

Developed by:
The National Center for Security & Preparedness

On behalf of:
NYS Division of Homeland Security and Emergency Services
Office of Counter Terrorism

In support of:
The Great Lakes Hazards Coalition
Executive Summary
Executive Summary

Energy is the lifeblood of U.S. industry, commerce, financial systems, and indeed, our very way of life. The critical energy infrastructure is a highly interdependent web of fuel, transmission, and power generation resources. In the Great Lakes Region, this web extends throughout the U.S. states of Illinois, Indiana, Michigan, Minnesota, New York, Ohio, Pennsylvania, and Wisconsin, as well as the Canadian province of Ontario.

The governments, operators, and utilities within the region must work together to continually improve the resilience and security of our critical energy infrastructure. The Great Lakes Hazard Coalition (GLHC) was formed to facilitate this effort. The coalition includes members from federal, state, provincial, and local government, the private sector, and academic partners from throughout the region.

PURPOSE:
The purpose of this study is to conduct an open source literature review to provide an analysis of the vulnerabilities, consequences, and resilience related to critical energy sites located within the Great Lakes Region. This study endeavors to answer the following questions provided by The New York State Division of Homeland Security and Emergency Services (NYSDHSES), Office of Counter Terrorism (OCT):

1. What are the current levels of resilience of the electric and pipeline infrastructure in this region?
2. What federal, state, and local security initiatives have occurred since the 2003 outage?
3. What owner/operator or association activities have taken place to increase the security and resilience of the electric infrastructure since the 2003 outage in this region?
4. What pipeline and electrical connectivity exists?
5. What dependencies exist between electric and pipeline infrastructure and essential community services or other major critical infrastructure?
6. What are the direct relationships between employment, technology, and innovation as it relates to the concentration of very important energy infrastructure in this region?
7. What are the economic dependencies within the U.S. of Canadian-produced power sold to the GLHC members?

Scope and Approach

To answer these questions, the research team conducted a comprehensive review of literature related to the critical energy infrastructure, focusing on threats, vulnerabilities and resilience. Additionally, the review analyzed the economic and logistical consequences of major blackouts as they relate to the 18 critical infrastructure sectors. To supplement this discussion, the research team facilitated a focus group including regional industry experts in electric transmission, generation, and physical security. Meta-analysis of the information collected from the literature review and the focus group formed the basis of the conclusions. The information is
supplemented with descriptive statistical analysis on data related to major outages, Canadian imports, and annual sales data for the United States.

Conclusions

While the conclusions all relate specifically to the above research questions and scope, it is important to note several common threads that were prevalent throughout the literature and other information collected. First, cyber infrastructure will continue to play a major role in future grid development initiatives. This presents both an opportunity and a challenge for the industry. On the one hand, cyber systems, such as self-healing smart grid technology, have the potential to greatly increase the resilience of the power grid through automation and dynamic information sharing; on the other hand, these systems bring with them increasing cyber security concerns.

Another common thread is the concern over the aging power infrastructure, especially transmission lines. As the infrastructure gets older, it becomes more costly and difficult to maintain. Outdated infrastructure also creates a barrier to innovation. The specific conclusions are listed below, organized by the topics brought up in the research questions.

Current Levels of Resilience

1. The energy industry in the Great Lakes Region, and around the country, has built in highly redundant mechanisms to withstand hazards and prevent disruptions from cascading. Efforts to maintain and improve this capability in the power grid present challenges to the electric industry.

2. There is a dearth of open source literature on trends describing how quickly the power grid recovers from an outage. Data collected suggests that the industry may not be improving in this capacity.

Government and Utility Security Initiatives and Activities

3. Federal, state, and local governments and energy utilities are working together in a strong push to improve energy security and resilience throughout the region.

Interdependencies between Pipelines and Electric Infrastructure

4. Petroleum pipelines are dependent on electricity; natural gas pipelines are typically not.

5. Electric generation in the region is dependent on natural gas supply, but not on petroleum.

Dependencies with Critical Infrastructure and Essential Community Services

6. The first and second order effects of a long-term power disruption in the region would impact every critical infrastructure sector—most prominently, banking and finance, food and agriculture, manufacturing, transportation, emergency services, and water.

Employment and Technology

7. As the energy sector looks for new technologies to replace and improve our aging electric and pipeline infrastructure, the market for skilled workers and innovative ideas will continue to expand.
The Partnership between the United States and Canada

8. Canada is a vital and highly interdependent part of the Great Lakes Region’s energy infrastructure. Cooperation between the two countries through the GLHC reflects this relationship.

Threats and Vulnerabilities

9. Natural forces are the most significant threat to the electric grid, and equipment failure is the most significant threat to petroleum and natural gas pipelines.

10. Terrorism remains a significant concern for the energy sector; however, in the study period there were no open source indications of a specific threat made against critical energy infrastructure.

11. Transmission lines are the most vulnerable aspect of the power grid; pipelines are the most vulnerable in petroleum and natural gas transmission systems.

Recommendations

Based on the conclusions of this study, the following recommendations are offered for future work:

1. Explore methods of improving and replacing the aging electrical transmission infrastructure in the region and ways the industry can further mitigate the impact of hazards on these assets.
2. Study the pipeline network’s ability to maintain its performance over the next 15-20 years, considering the impacts of aging infrastructure and new technologies.
3. Develop a specific definition and measure for post-outage recovery as it relates to the resilience of critical energy infrastructure.
4. Study key customers’ efforts to mitigate the effects of outages. Determine how these resilience efforts relate to the collective ability to recover.
5. Study the energy sector’s need for skilled workers over the next 10-15 years and determine where gaps exist or are likely to develop.
6. Maintain and continue to improve collaboration and information sharing efforts between federal, state, provincial, and local governments and energy utilities.
Acknowledgements

The National Center for Security & Preparedness wishes to acknowledge and thank the following for their contributions to this report:

External Reviewers

Mr. Scott Bailey  
*Great Lakes Region Information Exchange Broker, HIFLD*  
*U.S. Department of Homeland Security*

Ms. Karen Guziel  
*Decision and Information Sciences Division*  
*Argonne National Laboratory*

Mr. Jeff Pillon  
*Director of Energy Assurance Programs*  
*NASEO*

Mr. Bruce Nelson  
*Operations and Analysis*  
*Emergency Management Ontario*

Felix A Kwamena, Ph.D.  
*Director & Special Advisor*  
*Energy Infrastructure Security*  
*Natural Resources Canada*

Mr. Brian Ballinger  
*Director, Operations and Wholesale Markets Division*  
*Michigan Public Service Commission*

Mr. Bob Bensko  
*Director*  
*Office of Homeland Security*  
*Illinois Commerce Commission*

Mr. Hal Dalson  
*CMS Energy*

Mr. Mack Argentieri  
*Director of Operations*  
*NYPA Niagara Power Project*
Mr. Gian DiGaiamattista  
*Director, Emergency Management and Business Continuity*  
*Ontario Power & Gas*

Vicki Bier, Ph.D.  
*Chair, Department of Industrial and Systems Engineering*  
*University of Wisconsin-Madison*

LTC Alec Hay (ret)  
*Centre for the Resilience of Critical Infrastructure*  
*University of Toronto*

**Other Grateful Acknowledgments**

Ms. Kristina Leonardi  
*Michigan Department of Military and Veterans Affairs*

Mr. Alan Leider  
*Northeast Regional Information Exchange broker*  
*HIFLD to the Regions (HTTR)*  
*U.S. Department of Homeland Security*

New York State Division of Homeland Security and Emergency Services  
*Office of Counter Terrorism*  
*Critical Infrastructure Protection Unit*

New York State Division of Homeland Security and Emergency Services  
*Office of Cyber Security*  
*NYS GIS Coordinating Body*

New York Power Authority  
*Clark Energy Center*
The Research Team

The research team from The National Center for Security & Preparedness was comprised of:

Roderick MacDonald, Ph.D.
*Senior Researcher*

Michael Fagel, Ph.D.
*Internal Subject Matter Expert Reviewer*

Hwa-young Sin, Ph.D.
*Internal Subject Matter Expert Reviewer*

Carl Filbrich, M.A.
*Technical Writer*

Marie Reilly, M.A.
*Project Coordinator*

*Graduate Student Research Team from the Rockefeller College of Public Affairs and Policy and the National Center for Security & Preparedness, University at Albany, SUNY*
  - David Gottesman
  - Jayson Kratoville
  - Benjamin Spear
  - Brandon Kennedy

Rick C. Mathews, M.S.
*Director*
*National Center for Security & Preparedness*
# Contents

1. Introduction.......................................................................................................................... 1
2. Critical Infrastructure and Key Resources ........................................................................... 5
3. The Great Lakes Region at a Glance .................................................................................... 9
4. The Power Grid.......................................................................................................................... 13
5. The Pipeline Network ............................................................................................................. 21
6. Threats ...................................................................................................................................... 27
7. Vulnerabilities............................................................................................................................. 31
8. Blackouts.................................................................................................................................. 41
9. Consequences of Blackouts ...................................................................................................... 49
10. The Resilience of Energy Resources ................................................................................... 57
11. The U.S. – Canada Relationship .......................................................................................... 65
12. Initiatives................................................................................................................................. 69
13. Conclusions.............................................................................................................................. 73
14. Recommendations.................................................................................................................... 79
15. Bibliography............................................................................................................................ 81

Appendix A: Major Power Plants Within 75 Miles of the Great Lakes ......................... 97
Appendix B: Chronology of Events of the 2003 Blackout ............................................... 99
Appendix C: TSA-Led Programs, Projects, and Activities ............................................... 104
Appendix D: Major Outages in the Great Lakes Region, 2003-2010 ......................... 107
Appendix E: Transmission Lines and Urban Areas, Northeastern U.S.A. and Southeastern Canada .............................................................. 110
List of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2-1</td>
<td>6</td>
</tr>
<tr>
<td>3-1</td>
<td>9</td>
</tr>
<tr>
<td>3-2</td>
<td>10</td>
</tr>
<tr>
<td>5-1</td>
<td>22</td>
</tr>
<tr>
<td>5-2</td>
<td>25</td>
</tr>
<tr>
<td>6-1</td>
<td>28</td>
</tr>
<tr>
<td>7-1</td>
<td>35</td>
</tr>
<tr>
<td>8-1</td>
<td>42</td>
</tr>
<tr>
<td>8-2</td>
<td>43</td>
</tr>
<tr>
<td>8-3</td>
<td>45</td>
</tr>
<tr>
<td>8-4</td>
<td>46</td>
</tr>
<tr>
<td>10-1</td>
<td>62</td>
</tr>
<tr>
<td>10-2</td>
<td>63</td>
</tr>
<tr>
<td>10-3</td>
<td>63</td>
</tr>
</tbody>
</table>

List of Tables

<table>
<thead>
<tr>
<th>Table</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4-1</td>
<td>15</td>
</tr>
<tr>
<td>4-2</td>
<td>16</td>
</tr>
<tr>
<td>4-3</td>
<td>17</td>
</tr>
<tr>
<td>7-1</td>
<td>38</td>
</tr>
<tr>
<td>10-1</td>
<td>59</td>
</tr>
</tbody>
</table>
1. Introduction
1. Introduction

In the modern era, energy is essential to everything we do, from powering an entire industry’s supply chain to turning on a blender. The ubiquitous nature of this resource has made it something most people in North America take for granted; however, it is dependent on a system that many refer to as “the largest machine ever devised by man.” This machine has taken shape over the last 100 years.

As the energy infrastructure has grown, so too has our understanding of how to protect it; however, new challenges are continually emerging. Protecting the power grid and the pipeline network is a necessity to maintain the operation of most critical infrastructure sectors. When the critical infrastructure is not operating, everything, from the national economy to individuals’ lifestyles, is adversely affected. Public and private sector organizations share responsibility for maintaining this vital resource.

The challenges these organizations face were brought to the forefront in the summer of 2003, when a series of events caused the infrastructure that powers much of the northeastern United States to fail. The 2003 blackout primarily affected the region surrounding the Great Lakes, a highly populated area that represents a vital part of the U.S. and Canadian economies. Policymakers and industry professionals in this region require a more comprehensive understanding of the potential causes of this kind of disruption so that they can take steps to prepare for, mitigate, and potentially prevent future disturbances.

Regional partnerships across the public and private sectors are crucial in maintaining and improving the collective resilience and security of critical energy resources. The Great Lakes Hazard Coalition (GLHC) was formed to promote this cooperation by advancing critical infrastructure protection activities at the strategic level, and across state and international borders. The coalition includes federal, state, local, private sector, academic, and provincial partners from the Great Lakes region.
1. Introduction

1.1 Scope

Based on the requirements set forth by NYSDHSES, OCT, this report focuses on the generation and transmission of electrical energy, as well as the transportation of natural gas and petroleum through pipelines in the eight states (New York, Pennsylvania, Ohio, Michigan, Indiana, Illinois, Wisconsin and Minnesota) and the Canadian province of Ontario that surround the Great Lakes. The discussion of pipelines is limited to the transmission of natural gas and petroleum. The primary study period covers the years 2003 to 2010. The research team examined power outages that affected over 50,000 customers and lasted at least 24 hours, which are defined as either a “major outage” or “major blackout.” The research team primarily focused on high voltage transmission lines of at least 138 kV and generating sites of at least 500 MW.

1.2 Methodology

The study conducted a literature review of the major threats and vulnerabilities to the electric and pipeline networks, and the consequences of an electric blackout on the 18 CI/KR sectors, as outlined in the National Infrastructure Protection Plan. The study also looked at the factors affecting resilience, both in responding to a disruption and in recovering from one.

Using this framework, the research team performed an analysis to answer the research questions using the openly available literature and data. The results of this analysis led to conclusions that guided the development of recommendations.

PURPOSE:
The purpose of this study is to conduct an open source literature review to provide an analysis of the vulnerabilities, consequences, and resilience related to critical energy sites located within the Great Lakes Region. This study endeavors to answer the following questions provided by The New York State Division of Homeland Security and Emergency Services (NYSDHSES), Office of Counter Terrorism (OCT):

1. What are the current levels of resilience of the electric and pipeline infrastructure in this region?
2. What federal, state, and local security initiatives have occurred since the 2003 outage?
3. What owner/operator or association activities have taken place to increase the security and resilience of the electric infrastructure since the 2003 outage in this region?
4. What pipeline and electrical connectivity exists?
5. What dependencies exist between electric and pipeline infrastructure and essential community services or other major critical infrastructure?
6. What are the direct relationships between employment, technology, and innovation as it relates to the concentration of very important energy infrastructure in this region?
7. What are the economic dependencies within the U.S. of Canadian-produced power sold to the GLHC members?
To supplement the literature review, the study team met with a focus group of industry experts in electric transmission, generation, and infrastructure security. The goal in meeting with this focus group was to discuss the approach and to clarify the trends and consistencies that evolved from the literature review and meta-analysis. The discussion focused on the threats to vulnerabilities within the power grid, efforts to mitigate those vulnerabilities, and the industry’s concerns moving forward. The participants corroborated the major trends in the literature review while adding anecdotal discussions where appropriate.

1.3 Research Team

The research team consisted of subject matter experts from the areas of homeland security, emergency management, infrastructure protection, public safety, public health, and law enforcement. In addition to these experts, the team included a senior policy research professor and four graduate students from the Rockefeller College of Public Affairs and Policy studying homeland security, information management, finance, and economics.

1.4 Limitations

The study and its subsequent reports were conducted and written as “unclassified” and, in general, are based on “open source” materials. In addition, the study does not include materials or sources considered to be “sensitive” and protected as Protected Critical Infrastructure Information (PCII). Some material used may, however, be labeled as “For Official Use Only (FOUO).” As a result it should be noted that the following limitations are inherent in excluding classified or sensitive information. As it pertains to the energy infrastructure:

A.) Useful information pertaining to U.S. and Canadian power sharing is limited.

B.) Structural connections and key linkages between the U.S. and Canada are limited for security purposes.

The scope of this report is confined by the questions established to guide this study. As a result, there are innate research limitations relevant to energy production, transmission and distribution. Moreover, further studies are paramount in providing a comprehensive understanding as to how reliable, robust, and stable the current energy infrastructure is.

Several key recommended research topics beyond the scope and purpose of this report that should be examined include:

A.) Independent studies that define, assess and measure existing levels of system robustness, reliability, and stability while accounting for individual levels of customer resilience.

B.) Research that assesses the short and long term effects of alternative energy sources on the energy grid.

C.) An analysis of improvement incentives in place domestically and internationally to bolster critical energy infrastructure.

D.) An examination of threats and vulnerabilities that exist in distribution pipelines.
1.5 Layout of the Report

This study addresses the key issues involved in protecting the critical infrastructure and key resources in the Great Lakes Region. Specifically, it:

- Defines the terms “critical infrastructure” and “key resources” as they are used in federal legislation.
- Describes the economic breakdown of the Great Lakes Region.
- Provides an introduction to the power grid and the regulatory agencies responsible for it.
- Describes the pipeline network and its importance to the Great Lakes Region.
- Defines the major threats and vulnerabilities affecting the critical infrastructure in the Great Lakes Region.
- Provides an overview of blackouts and their consequences.
- Discusses the concept of resilience and the literature on the resilience of critical energy infrastructure.
- Outlines the initiatives taken by federal, state, and local governments, along with the energy industry.
- Summarizes the conclusions of the study and offers recommendations for future work.

Notes

1 Amin and Gellings, 2006.
2. Critical Infrastructure and Key Resources
2. Critical Infrastructure and Key Resources

The production and transmission of energy are supported by facilities that are referred to in the context of homeland security as “critical infrastructure” and “key resources.” These terms are widely understood, but for the sake of clarity it is worthwhile to see how they are defined in federal legislation. Critical infrastructure is defined in the USA PATRIOT Act of 2001 under the Critical Infrastructure Protection Act of 2001 as:

…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. (Sec. 1016e)

The Department of Homeland Security (DHS) uses a network of questions, diagrammed in Figure 2-1, to determine whether a piece of infrastructure is critical.

Key Resources are defined under the Homeland Security Act of 2002 as “publicly or privately controlled resources essential to the minimal operations of the economy and government.”

2.1 Protection of Critical Infrastructure and Key Resources

Under Homeland Security Presidential Directive 7, the protection of Critical Infrastructure and Key Resources (CIKR) falls under the responsibilities of the Secretary of Homeland Security. The directive establishes 18 critical infrastructure sectors and designates a federal agency to implement a sector-specific plan (SSP) for each. Each SSP conforms to the framework established in the National Infrastructure Protection Plan (NIPP) in an effort to create unified goals and enhance cross-sector collaboration. The following six goals are established in the energy sector SSP:

**Goal 1**: Establish robust situational awareness within the sector through timely, reliable, and secure information exchange among trusted public and private sector partners.

**Goal 2**: Use sound risk management principles to implement physical and cyber measures that enhance preparedness, security, and resilience.

**Goal 3**: Conduct comprehensive emergency, disaster, and continuity of business planning, including training and exercises, to enhance reliability and emergency response.

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

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

**Goal 6**: Strengthen partner and public confidence in the sector’s ability to manage risk and implement effective security, reliability, and recovery efforts.

DHS and the agencies responsible for the individual sectors coordinate with Government Coordinating Councils (GCC) comprised of federal, state, provincial, local, tribal, and territorial organizations, and Sector Coordinating Councils (SCC) comprised of private sector partners, to execute their respective SSPs.
Critical Infrastructure and Key Resources

Sector-Specific Agencies

The nation’s energy infrastructure (electric, petroleum, and natural gas) encompasses two of the 18 sectors: energy and transportation. The national electric grid falls under the energy sector and is managed by the Department of Energy (DOE). The gas and petroleum pipeline infrastructure falls under both the energy and transportation sectors. While the distribution of petroleum and natural gas is overseen by the energy sector, this report focuses on the protection

Figure 2-1. Determining Criticality of Infrastructure (Source: TSA Pipeline Security Guidelines, 2011, p. 14)
of the national pipeline infrastructure, which is administered by the Transportation Security Administration (TSA).\(^6\)

---

**Notes**


3. The Great Lakes Region at a Glance
The Great Lakes region encompasses eight U.S. states and the Canadian province of Ontario (Figure 3-1). It is home to over a quarter of the U.S. population and includes eight of the country’s fifty largest cities, including New York (1), Chicago (3), Philadelphia (5), and Indianapolis (12). With a net GDP of over $4 trillion, the states bordering the Great Lakes account for over 27% of the U.S. economy. The Canadian Province of Ontario is home to approximately 12.6 million people, almost 40% of the national population, and contributes almost 40% of the country’s GDP.

The industrial breakdown of the economy is fairly homogenous across the Great Lakes region in both the U.S. and Canada (see Figure 3-2). The region’s economy relies mainly on service sectors that encompass finance, insurance, real estate and leasing, health and education, and wholesale and retail trade. Manufacturing accounts for approximately 13 and 15 percent of the Great Lakes states’ and Ontario’s GDPs respectively. Trade accounts for a little over 10% of the region’s economic activity.
Figure 3-2. Economies of Ontario and the Great Lakes states. (Sources: U.S. Department of Commerce, Ontario Ministry of Finance)
Notes

7 The eight states are New York, Pennsylvania, Ohio, Michigan, Indiana, Illinois, Wisconsin, and Minnesota.
8 2010 U.S. Census.
4. The Power Grid
4. The Power Grid

4.1 How it Works

The North American power grid is a machine that consists of over 200,000 miles of transmission lines.\textsuperscript{11} These lines carry power from various generating stations that have a nameplate capacity of over 950,000 megawatts to over 143 million customers.\textsuperscript{12} Providing people with power is done through three steps: generation, transmission, and distribution.

Electricity is generated at power plants from a variety of sources, including water, wind, oil, coal, natural gas, and nuclear energy. These plants are owned by customers, utilities, and independent power producers.\textsuperscript{13} They operate in one of two ways:

- They convert the latent energy in the source (e.g., coal, uranium) into mechanical energy and finally into electrical energy, or
- They convert the mechanical energy in a source such as flowing water into electrical energy.\textsuperscript{14}

Once this power is generated it cannot be stored, so it must be transmitted and consumed immediately.\textsuperscript{15}

4.1.1 Transformers

Transformers transfer electrical energy from one circuit to another. There are two types of transformers: power transformers, which are greater than 500kVA, and distribution transformers, which are less than 500kVA. Large power transformers often have to use external cooling devices, which are typically filled with oil.

Step-up transformers increase the voltage of the electricity through generating magnetic flux from a coil winding that is connected to the generation source and a second coil winding that is attached to the transmission line, while step-down transformers do the opposite. To effect these voltage changes, alternating current is passed through the first coil, which causes voltage to be induced in the second coil.

Unlike generators, transformers have zero moving parts, and therefore require less maintenance. The repairs they do need are essential to ensure reliability and prolong the transformer’s lifespan.\textsuperscript{16} Larger transformers (those supporting lines >345kV) are manufactured outside the United States. This greatly impacts repair time, so many utilities have backup transformers in place in the event the operating one fails.

4.1.2 Substations

There are three types of substations in the power grid: switching substations, distribution substations, and transmission substations.

- Switching substations provide switching flexibility and to enhance circuit protection.
- Distribution substations safely reduce voltages from transmission line levels to distribution line levels.
• Transmission substations reduce voltage from transmission to sub-transmission voltages.\(^{17}\)

Substations form nodes that allow substation and control center operators to switch the configuration of networks by opening or closing circuit breakers. This can be done by the substation system operators or remotely from control centers.\(^{18}\) Most substations in the United States are operated remotely from control centers.\(^{19}\)

SCADA (supervisory control and data acquisition) systems are control systems with three different parts: sensors and actuators, remote terminal units (RTUs) and a master system.

• The sensors and actuators measure and control (respectively) various aspects of the power grid.
• RTUs display the data from the sensors. They also display input and output, as well as any sort of alarms. The display functions operate through a programmable logic controller.
• Master systems obtain data from the RTUs and can control remote parts of the grid through the operator station.\(^{20}\)

Once power is generated, the voltage is increased through a step-up transformer and then the electricity is sent along the thousands of miles of transmission wires. Transmitting at higher voltages reduces the amount of electricity that is lost to heat as it travels\(^{21}\). Power losses from transmission and distribution are usually 6% to 8%.\(^{22}\) These wires carry alternating current electricity at 138 kV, 230 kV, 345 kV, 500 kV or 765 kV. Voltage fluctuations must be tightly controlled; the system continually operates at a frequency of 60Hz.\(^{23}\) Transmission lines are connected through substations and switching stations to help form what is colloquially known as the power grid.\(^{24}\) In transit, electricity follows the path of least resistance to its destination, limiting utilities’ ability to directly control the flow. The only way to control the flow is to open or close circuit breakers or to increase or decrease generation.\(^{25}\) The electricity’s voltage is lowered at a step-down transformer and eventually reduced to the 120 to 240 volts that most residential customers use.\(^{26}\)

### 4.2 Power in the Great Lakes Region

The United States has 184 major power plants\(^{27}\) operating in the states bordering the Great Lakes, using primarily coal, but also oil, hydro, natural gas, and nuclear sources. Ontario plants had an installed capacity of 36,975 MW in 2010. There are 14 major power plants in Ontario, powered primarily by hydro and nuclear, as well as coal and natural gas.\(^{28}\) The major electrical corridors in this region are:

• Between Toronto and Ottawa, into New York City and Long Island
• Between Cleveland and Akron, the Detroit area, the Cincinnati area, the Indianapolis area
• Between Fort Wayne and Chicago, the Chicago area and the Minneapolis-St. Paul area
The Great Lakes region also has two of the U.S.’s critical congestion areas, as identified in the National Electric Transmission Congestion Study, one of which extends from New York City up the Hudson River, and the other through eastern Pennsylvania.

<table>
<thead>
<tr>
<th>U.S. Great Lakes States Generation Capacity (All Plants, 2007): 273,208.70 MW</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Fuel Source</strong></td>
</tr>
<tr>
<td>-----------------</td>
</tr>
<tr>
<td>Coal</td>
</tr>
<tr>
<td>Hydro</td>
</tr>
<tr>
<td>Natural Gas</td>
</tr>
<tr>
<td>Nuclear</td>
</tr>
<tr>
<td>Oil</td>
</tr>
<tr>
<td><strong>TOTAL (&gt;500MW)</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Ontario Generation Capacity (All Plants, 2010): 36,975 MW</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Fuel Source</strong></td>
</tr>
<tr>
<td>-----------------</td>
</tr>
<tr>
<td>Coal</td>
</tr>
<tr>
<td>Hydro</td>
</tr>
<tr>
<td>Natural Gas</td>
</tr>
<tr>
<td>Nuclear</td>
</tr>
<tr>
<td>Dual Cycle</td>
</tr>
<tr>
<td>(Oil &amp; Gas)</td>
</tr>
<tr>
<td><strong>TOTAL (&gt;500MW)</strong></td>
</tr>
</tbody>
</table>

Table 4-1. Nameplate Capacity of Major Power Plants (>500MW) in the Great Lakes Region by Fuel Source (U.S. and Ontario). N.B. The remaining percentage of regional capacity is supplied by plants with a capacity less than 500MW.

4.3 Regulatory Agencies

The power grid is the responsibility of a variety of federal agencies and departments, each of which is responsible for a certain aspect of the system (see Table 4-2 below). While these agencies are responsible for different aspects of energy infrastructure, FERC has the power to issue safety requirements and oversees approval and enforcement of all electric reliability standards. These standards are developed by the North American Electric Reliability Corporation (NERC), which acts as the FERC-designated Electric Reliability Organization pursuant to the Energy Policy Act of 2005.

The overlapping missions and functions of agencies involved with energy infrastructure require them to collaborate dynamically to be successful. The Department of Energy (DOE) coordinates with several different organizations in its oversight function, for example, when conducting environmental reviews for new transmission line siting. In this case, the following agencies must be consulted: the Department of Energy, the Department of Agriculture, the
Department of Defense (DOD), the Department of the Interior, the Department of Commerce (DOC), the Federal Energy Regulatory Commission, the Environmental Protection Agency, the Council on Environmental Quality (CEQ), and the Advisory Council on Historic Preservation (ACHP). These intricacies must be worked out to the satisfaction and clear understanding of all agencies to decrease the chance of a blackout and improve efficiency. This sort of cooperation is also vital to expediting the process of acquiring and maintaining adequate infrastructure as well as delineating duties during the recovery stages after major damage to the system.
<table>
<thead>
<tr>
<th>Name of Agency [Parent Agency]</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department of Agriculture (USDA)</td>
<td>Funding and supporting rural electrical activities</td>
</tr>
<tr>
<td>United States Army Corps of Engineers (USACE) [Department of Defense (DoD)]</td>
<td>Maintaining the nation’s dams</td>
</tr>
<tr>
<td>Department of Homeland Security (DHS)</td>
<td>Coordinating and leading critical infrastructure protection projects including nuclear and hydroelectric power, implementing chemical safety regulations</td>
</tr>
<tr>
<td>United States Coast Guard (USCG) [DHS during peacetime and DoD during wartime]</td>
<td>Protecting offshore electrical assets, enforcing the Maritime Transportation Security Act in as far as it applies to the energy sector, and dealing with issues that arise at terminals and waterways</td>
</tr>
<tr>
<td>Office of Cyber Security and Communications (OCSC) [DHS]</td>
<td>Working with and enhancing the cyber security of all critical infrastructure sectors</td>
</tr>
<tr>
<td>Mineral Management Service (MMS) [Department of the Interior (DOI)]</td>
<td>Managing the nation’s natural resources on the Outer Continental Shelf</td>
</tr>
<tr>
<td>Power Marketing Administrations (PMAs) [DoI]</td>
<td>Monitoring coal mines, siting power plants and geothermal areas</td>
</tr>
<tr>
<td>Department of State (DOS)</td>
<td>Brokering agreements with Canada and Mexico for the importing and exporting of energy</td>
</tr>
<tr>
<td>Environmental Protection Agency (EPA)</td>
<td>Enforcing the Clean Air Act</td>
</tr>
<tr>
<td>Federal Energy Regulatory Commission (FERC) [Department of Energy (DOE)]</td>
<td>Regulating the interstate transmission of electricity and natural gas and hydropower products, overseeing approval of all electric reliability standards and the enforcement of those standards.</td>
</tr>
<tr>
<td>Nuclear Regulatory Commission (NRC)</td>
<td>Coordinating with energy providers dealing with security issues arising from nuclear fission</td>
</tr>
</tbody>
</table>

**Table 4-2. Federal Power Sector Regulatory Agencies (adapted from the NIPP, pp. 20-22)**

1 The Mineral Management Service has been reorganized into several different sub-agencies. The version of the NIPP where this chart originates predates this change.
There are also many state, local and private agencies and organizations tasked with regulatory oversight of the power grid at a more local level. Table 4-3 shows the applicable organizations as displayed in the NIPP.

<table>
<thead>
<tr>
<th>Agency/Group Name [Parent Agency]</th>
<th>Type of Agency</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>National Association of State Energy Officials (NASEO)</td>
<td>Regional, State and Local</td>
<td>Coordinating responses to energy crises, developing state energy emergency plans, and developing mechanisms to improve reliability and security</td>
</tr>
<tr>
<td>Regional Consortium Coordinating Councils [DHS]</td>
<td>Regional</td>
<td>Coordinating efforts to protect critical infrastructure and key resources in geographic areas, which is done to strengthen regional collaboration to enhance resilience in these areas, and to share lessons learned</td>
</tr>
<tr>
<td>Fusion Centers [DHS]</td>
<td>Federal, State and Local</td>
<td>Providing better communication between the federal, state, and local levels, establishing relationships with owners of critical infrastructure and key resources, and providing expertise to the state and local governments through the use of subject matters experts</td>
</tr>
<tr>
<td>State Public Utility Commissions</td>
<td>State</td>
<td>Regulating utilities at the state level</td>
</tr>
<tr>
<td>Governor’s Offices and State Legislatures</td>
<td>State</td>
<td>Coordinating with Federal and industry groups to craft policies to deal with emergency energy crises</td>
</tr>
<tr>
<td>State Homeland Security Offices</td>
<td>State</td>
<td>Assessing critical infrastructure protection and vulnerability analysis</td>
</tr>
<tr>
<td>Local Governments</td>
<td>Local</td>
<td>Major stakeholders, particularly interested in energy sector security, preparedness and protection</td>
</tr>
<tr>
<td>Critical Infrastructure Protection Advisory Council (CIPAC) [DOE]</td>
<td>Federal, State, Local and Private</td>
<td>Facilitating interactions between owners of key resources and critical infrastructure and the government</td>
</tr>
<tr>
<td>Electricity Sharing Information and Analysis Center (ES-ISAC) [DOE]</td>
<td>Federal and Private</td>
<td>Sharing and analyzing information on vulnerabilities and providing support to the Federal Government</td>
</tr>
<tr>
<td>Homeland Security Information Network (HSIN) [DOE and DHS]</td>
<td>Federal and Private</td>
<td>Sharing and analyzing information on vulnerabilities and providing support to the Federal Government</td>
</tr>
<tr>
<td>North American Electric Reliability Corporation</td>
<td>Private</td>
<td>Developing electrical reliability standards and enforcing those standards</td>
</tr>
</tbody>
</table>

Table 4-3. Other Federal, State and Local Power Sector Organizations and Associations (Adapted from NIPP, pp. 22-24)
4.4 Regulations

The regulatory environment for the electric industry has changed over time as the industry has matured. Several key events have enhanced the government and industry’s understanding of the causes of major disruptions and ways to avoid them. Further, as electric infrastructure became less of a commodity and more of a necessity, regulations began to employ stricter oversight mechanisms. This section provides a brief discussion of the development of regulations for the electric industry prior to the 2003 Blackout.

The Public Utility Holding Company Act of 1935 (PUHCA) promoted self-regulation and treated utilities as state-operated monopolies. While grid reliability standards were put into place, compliance was voluntary. This lax regulatory environment came under scrutiny after a massive outage in 1965 that affected millions of Americans and blacked out much of the northeastern United States. An analysis of the blackout’s causes contained many recommendations, one of which Congress acted on when it passed the Energy Reliability Act of 1967, establishing regional reliability councils.

Energy shortages in the 1970s led to increased conservation efforts and a reduction in energy consumption. Utilities promoted overinvestment in power supply while prices were high, which resulted in a shift to a cost-avoidance approach that sought to maximize the use of the existing infrastructure. Beach and Dilts explain that this decision-making environment has had far-reaching consequences, reducing the reliability of infrastructure, which typically has a useful life of approximately 30 to 50 years.

In 1978, President Carter signed the Public Utility Regulatory Policies Act (PURPA). The main aim of this legislation was to promote energy efficiency through financial incentives for power plants producing 100 megawatts or less of electricity. These plants tended to be more energy efficient than larger plants. Scholars indicate that PURPA also had three unintended side effects: it jump-started the creation of new technologies, reduced the control of power company managers, and was the beginning of deregulation.

The next significant piece of legislation to influence the utility industry was the Energy Policy Act of 1992. Beach and Dilts explain that this act created the blueprint for a wholesale competitive generation market. It created a new category of energy producer, the exempt wholesale generator (EWG), which existed outside of the PUHCA framework. EWGs were granted the ability to use a larger utility’s infrastructure if that utility was also in the market for wholesale power sales.

While FERC was not empowered to order direct retail competition, it was given access to the grids and the ability to regulate them. In 1996, FERC Order 888 created a wholesale electricity market, which increased the number of transactions between different utilities. The goal of this and subsequent orders (889, 2000 and 2001) was to drive down electricity prices. This resulted in the construction of hundreds of new natural gas turbines and the emergence of an enormous wholesale power market. The increased collaboration between utilities placed more stress on the grid while transmission investment remained relatively low, failing to return to 1975 levels until 2005.
Notes

22 ABB Inc., 2007, p. 3.
27 For the purposes of this paper, a “major power plant” is a generation site with a nameplate capacity greater than or equal to 500MW. Appendix A contains a list of the 184 major power plants.
31 Beach and Dilts, 2006, p. 9.
32 “History,” n.d.
34 Beach and Dilts, 2006, p. 9.
35 Hirsh et al., 2005, p. 7.
36 Dillon, 1979, p. 519; Hirsh et al., 2005, p. 7.
38 Beach and Dilts, 2006, p. 10.
39 Amin, 2004, p. 2; Beach and Dilts, 2006, pp. 7-11.
5. The Pipeline Network
5. The Pipeline Network

Pipelines are an important mode of transportation in the United States, bringing fossil fuel products to the consumer from distant sources. Both petroleum and natural gas are important fuel sources on which the U.S. is greatly dependent. Petroleum accounts for 37 percent of U.S. energy consumption while natural gas accounts for 25 percent. They are essential in heating homes and businesses, fueling vehicles, providing electrical generation, and as a resource for industrial processes. This section describes petroleum and natural gas transport through pipelines in the GLHC states and the agencies, regulations, and initiatives in place nationwide to secure this method of transport.

5.1 How it Works

5.1.1 Pipelines

Petroleum and natural gas are primarily transported through pipelines, which are usually laid underground. The largest pipelines, called “trunklines,” travel interstate in order to bring fuel from the source of production to multiple consumer markets. Petroleum products are delivered to storage facilities for distribution locally. Natural gas is processed through a local control station and either moved to underground storage to build reserves or distributed to consumers through a localized grid system. While the largest markets for petroleum and natural gas are the Midwest and Northeast, the majority of petroleum supply and natural gas production is located in the Gulf Region. As a result, the states that make up the GLHC rely heavily on trunkline distribution. With such a large distance between production and consumption, a disruption in pipeline structures outside of the region can greatly impact infrastructure and processes within the GLHC states.

There are five major domestic gas pipeline routes into the Great Lakes states, with New York City and Chicago serving as the major delivery points. Two major pipeline systems supply the Northeast, including Pennsylvania and New York, with natural gas from the Gulf: one through the Mississippi and Ohio River Valleys, the other along the East Coast. In the Midwest, three pipeline systems provide much of the supply. According to the U.S. Energy Information Administration (EIA), nearly 61% of the natural gas supply for the Midwestern states is delivered through pipelines that originate in the Gulf and others from the Oklahoma and Texas panhandles. Additionally, the Midwest has recently been supplied by a pipeline originating in the Rocky Mountain states. This system is currently being upgraded to meet greater demand in the Great Lakes region. Figure 5 illustrates the flow of natural gas from source regions in the Southwest and Rocky Mountain states to major delivery centers.

The Great Lakes region also imports natural gas from Canada through Minnesota and Michigan for distribution to the Chicago region as well as at Niagara, NY for distribution in New York and Pennsylvania. The pipelines into the Midwest accounted for about 41% of total U.S. natural gas import capacity in 2006. A large amount of the gas imported from Canada through the Midwest is exported in order to supply Ontario. Figure 5-1 shows major import/export centers as well as the amount of gas they transport.
Figure 5-1. Major U.S. Natural Gas Pipeline Corridors. Source: Energy Information Administration, Office of Oil and Gas, Natural Gas Division, GasTran Gas Transportation Information System. The EIA has determined that the information displayed here does not raise security concerns, based on the application of the Federal Geographic Data Committee’s Guidelines for Providing Appropriate Access to Geospatial Data in Response to Security Concerns.

Like natural gas, petroleum products are sourced from the Gulf region where they are refined. The pipelines supporting the transport of these products follow very similar, or even share, rights of way to those supplying natural gas.\(^\text{48}\)

### 5.1.2 Compressor/Pump Stations

Pipelines are designed to transport petroleum and natural gas of a very specific quality at a very specific pressure. Transported at high pressures, gas must be processed and scrubbed for impurities that might condense.\(^\text{49}\) If fuels entering a system do not meet specific requirements, they could cause extreme damage, typically through rupture. To avoid damage it is important that the pressure be maintained over the length of transmission.

For natural gas pipelines this is achieved by compressor units located every 40 to 100 miles along the pipeline.\(^\text{50}\) These systems, typically powered by the natural gas flowing through the pipeline, re-pressurize the system to maintain the continuous flow of gas. Compressor stations are unmanned and controlled by Supervisory Control and Data Acquisition (SCADA) systems that monitor a number of stations along the pipeline.\(^\text{51}\)
Petroleum pipelines use pump stations, located every 20 to 100 miles, to keep the flow of liquid consistent. These stations are not powered by the product in the pipeline, but rather by electric motors that require other methods of fueling. They typically have backup power so the system can be properly shutdown in the event of a failure.

Pressure sensors and relief valves built into the pipeline and compressor/pump units guard against over-pressurization. Also, most pump and compressor stations are equipped with multiple units that can provide the necessary pressurization in the event the working unit is disrupted.

5.2 Regulatory Agencies

The safety and security of pipeline infrastructure have primarily been handled at the federal level. The Natural Gas Pipeline Safety Act of 1968 and the Hazardous Liquid Pipeline Act of 1979 laid the groundwork for federal protection rules by requiring the Secretary of Transportation to oversee pipeline “design, construction, operation and maintenance, and spill response planning.” In 2002, further legislation was enacted to strengthen DOT’s existing programs. The Pipeline Safety Improvement Act of 2002 set forth requirements for operators to conduct risk analyses on critical facilities to ensure basic integrity. These requirements were further strengthened under the Pipeline Safety Improvement Act of 2006 and the Implementing Recommendations of the 9/11 Commission Act of 2007. In addition, the Homeland Security Act of 2002 and HSPD-7 made DHS the lead for all forms of transportation security previously handled by DOT, including pipelines.

Under the statutes enacted, two agencies are charged with monitoring pipelines: the Office of Pipeline Safety (OPS) within the Pipeline and Hazardous Materials Safety Administration (PHMSA) regulates regular safety and maintenance, while the Division of Pipeline Security within the Transportation Security Administration (TSA) deals with security measures. The monitoring roles of these two agencies are closely related and intertwined, and thus require them to collaborate in a number of ways. Under the National Infrastructure Protection Plan (NIPP), these two agencies must coordinate with each other to protect the pipeline infrastructure. In 2004, DOT and DHS entered into an MOU that laid out a framework for how the two departments would coordinate on all forms of transportation security moving forward. This MOU was expanded by an Annex contracted between TSA and PHMSA to delineate their separate roles in pipeline security in 2006, and to meet the various legislative requirements governing this sector.

According to the Annex, besides its safety programs, PHMSA is required to act as a surrogate of TSA, providing the agency with the data required to conduct security reviews. TSA also provides information to PHMSA based on its various risk assessments. The two agencies are charged with coordinating the “standards, regulations, guidelines, or directives affecting transportation security.” If TSA requires assistance, it can request the use of PHMSA personnel. The Annex also provides implementation guidelines.

In spite of their traditional regulatory roles, the agencies have held back from issuing hard rules and regulations. Historically the PHMSA, and now TSA have preferred to use a system of self-enforcement in the industry. The agencies provide “voluntary guidelines” on what safety and security measures should be in place, but expect operators to implement them. Facility operators
develop their own private security plans that must be updated and shared regularly with PHMSA and TSA. The agencies conduct on-site reviews of facilities, but rarely take enforcement action against operators.\textsuperscript{61}

Inspections require considerable time in the field and PHMSA and TSA have very limited staff to commit to pipeline security. Because of this, and because of the seriousness of the threat, the agencies are required by statute to “develop and implement a plan for reviewing the pipeline security plans and an inspection of the critical facilities of the 100 most critical pipeline operators.”\textsuperscript{62} It is these facilities that receive the most attention and require the most security measures as recommended by TSA guidance. PHMSA and TSA are also expected to maintain a system of shared inspection and enforcement in which inspectors from both agencies jointly monitor important facilities.

While standards are set federally, the states do have a role through their respective public utility commissions. These institutions work with PHMSA and TSA to institute the programs that are developed to increase safety and security. They also establish more specific regulations for the individual states regarding construction and safety, and monitor compliance with both state and federal regulations.

### 5.3 Regulations and Initiatives

Security requirements for pipelines are set forth in the NIPP Transportation Sector Specific Plan and the TSA Pipeline Security Guidelines. These guidelines require corporate security plans, regular risk analysis, physical security measures, as well as protection from cyber-attack. While adherence to security guidance is typically voluntary, collaboration at the industry level, as well as through the Pipeline Working Groups in the Energy Sector Government Coordination Council and Oil and Natural Gas Sector Coordinating Council, has seen these measures implemented. Various initiatives have been developed by TSA and operators, as well as industry trade groups such as the American Petroleum Institute (API), American Gas Association (AGA) and Interstate Natural Gas Association of America (INGAA). These are discussed in more detail in the Initiatives section.

### 5.4 Natural Gas in the Great Lakes Region

For the Great Lakes region, natural gas is particularly important. Five Great Lakes States consistently fall within the EIA list of the top ten states in annual natural gas consumption. The region as a whole consumed over 5.5 trillion cubic feet (Tcf) in 2009, approximately 25% of total U.S. consumption.\textsuperscript{63} According to the EIA, 18\% of the over 300,000 miles of natural gas pipelines in the United States run through the region. This figure does not account for the infrastructure these states rely on to carry and control natural gas from other states. The map in Figure 5-2 demonstrates the region’s reliance on natural gas from out-of-state sources. States colored in gray import more than 85\% of their gas from elsewhere. The map also shows the layout of the interstate gas pipelines in the region.
While the GLHC states are also among the largest consumers of petroleum products as well, this is mostly in the form of home heating oil. The region is not reliant on petroleum for electric generation, with only 1% of generation coming from oil generating plants. There are 175,000 miles of petroleum pipelines in the United States, many of them serving the Great Lakes region. Many of these pipelines transport products that have already been refined such as gasoline or heating oil, rather than crude oil, though there is a large refinery base in the Midwest.

Notes
41 U.S. Pipeline and Hazardous Materials Administration, PHMSA Stakeholder Communications: Petroleum Pipeline Systems: From Well Head to the Consumer n.d..
42 U.S. Energy Information Administration, Natural Gas Pipeline Network: Natural Gas Import/Export Locations Map n.d.
43 McCrossin, DiLeo & Benton, 2002; National Infrastructure Simulation and Analysis Center 2006; Stower, 2005.
44 U.S. Energy Information Administration, Natural Gas Pipeline Network: Interstate Pipeline Segment 2011
45 U.S. Energy Information Administration, Natural Gas Pipeline Network: Major Natural Gas Transportation Corridors 2011


5. The Pipeline Network

48 Stower, 2005, p. 17.
52 U.S. Pipeline and Hazardous Materials Safety Administration 2005
59 Annex to DHS/DOT MOU 2006
60 Annex to DHS/DOT MOU 2006
64 U.S. Energy Information Administration, *Use of Natural Gas* 2011.
6. Threats
6. Threats

The National Infrastructure Protection Plan (NIPP) defines a threat as “a natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property.” Threats exploit vulnerabilities in critical infrastructure, achieving a harmful impact. This is the generally accepted definition, used to direct regulations and guidelines by the government as well as industry. In keeping with that definition, this section outlines the threats to the electric and pipeline infrastructures.

6.1 Electricity Sector

In the Energy Sector Specific Plan, threat is framed using the definition proscribed in the NIPP. The threats posed to the electric sector, in order of importance, include natural forces, accidents or human error, and deliberate attack.

Natural forces include such things as rain, snow, heat and lightning. These forces can strain the electric infrastructure, increasing vulnerabilities, and leading to eventual failure. Apart from weather, encroaching vegetation has the potential to damage lines and disrupt the flow of electricity if not properly maintained. The electric sector is also vulnerable to freak natural incidents such as solar flares, which can disrupt an entire electric system, or earthquakes which can damage equipment and substations.

Accidents or human error, including the threat of equipment failure, can expose vulnerabilities. Corrosion and mechanical failure threaten transmission lines and their related infrastructure, reducing transmission capacity or putting a line of out commission. Poor communication can lead to human error in the control room as systems are improperly monitored.

Deliberate attack could come from any number of individuals or groups including terrorists and disgruntled employees. Amin designed a framework that describes three possible types of deliberate attacks related to the electric grid: attacks upon the power system, attacks by the power system, and attacks through the power system. This report looks at attacks on the power system, in which the electric system is targeted in order to disrupt its operation. Deliberate threats could include attacks on transmission lines, generators and control centers, as well as forms of cyber-attack. A review of the available open source literature reveals there has been no direct threat made against the electricity infrastructure within the scope of the study.

6.2 Pipelines

While an integral part of the energy sector, pipelines are a transportation system protected by guidelines set forth in the related sector-specific plan. The Transportation Systems Sector Specific Plan defines threat differently than the NIPP, calling it “the intention and capability of an adversary to undertake actions that would be detrimental to CI/KR.” This definition presumes a malicious actor serving as a threat, or deliberate attacker. The scope of this report includes threats that are not of a deliberate nature, particularly accidents or human error and natural forces. These threats must therefore also be examined under the broader definition.
provided in the NIPP. Figure 6-1 illustrates the causes of significant pipeline incidents from 1991 to 2010.

![Significant Incident Cause Breakdown](image)

**Figure 6-1. Causes of significant pipeline incidents, 1991–2010.**

Based on incident data which must be reported to PHMSA, accidents or human error, particularly excavation damage and equipment failure, are the primary threat to pipeline infrastructure. Based on incident data which must be reported to PHMSA, accidents or human error, particularly excavation damage and equipment failure, are the primary threat to pipeline infrastructure. Figure 6-1 shows this accounts for over 60% of all incidents. Third parties engaging in construction can threaten pipelines by digging near an unmarked line. Corrosion and other forms of equipment failure also have the potential to cause a line rupture and leak.

Natural forces are the next largest threat to the pipeline system, potentially disrupting the lines or their source of supply. Earthquakes and flooding pose a direct threat as they can undermine the soil where pipelines are laid, disrupting the pipeline. Hurricanes and other storms could also threaten the supply of petroleum or natural gas, indirectly impacting the pipeline system.

Deliberate attacks from terrorists and/or insider threats continue to be a concern as well, with potential attacks against physical and/or cyber assets. A review of the available open source literature reveals there has been no direct threat made against the pipeline infrastructure during the study period.
Notes

71 U.S. Congress Office of Technology Assessment, 1990, p. 11, p. 14
74 Daily Mail, 2011.
76 Amin, 2002.
77 Amin, 2002.
80 U.S. Pipeline and Hazardous Materials Safety Administration, PHMSA Stakeholder Communications: Excavation Damage 2004; U.S. Pipeline and Hazardous Materials Safety Administration, PHMSA Stakeholder Communications: Significant Pipeline Incidents by Cause 2011
81 National Infrastructure Simulation and Analysis Center, 2006.

6. Threats
7. Vulnerabilities
7. Vulnerabilities

The NIPP explains that, in order to cause damage, a threat needs to intersect with a vulnerability, or “a physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard.” Electric and pipeline infrastructure are both vulnerable to attacks or disruptions, which, if severe enough, can cause widespread physical and economic damage.

7.1 Electric Infrastructure

7.1.1 Exposed Transmission Lines

The power grid is composed of three main infrastructure systems: transmission lines and related infrastructure (including substations), generating plants, and control centers. Transmission lines are the most vulnerable to attack because they are the most exposed. High voltage lines that carry the bulk of electricity to major markets travel through rural areas. Because of their remoteness there is little surveillance over, or physical security protecting, these parts of the infrastructure. This makes high voltage lines easy targets for a small-scale attack aimed at disrupting the power supply from a large source. A disruption at one of these points could take time to rebuild as many of the parts used in larger lines are manufactured overseas. This could inhibit the delivery of electricity for an extended period of time if redundancies were not built into the transmission system.

Transmission lines are also exposed to severe natural forces, such as high winds and rain. This often causes localized outages in the transmission system as lines become damaged or collapse. Heat waves can also contribute to electrical dysfunction as customers draw increasing power from the grid for cooling. As power use increases, the amount of electricity being transported over transmission lines begins to increase as needed. The increased flow of electricity burdens lines that begin to droop from the increased load and heat.

Without proper vegetation management, a drooping line can come into contact with vegetation, causing it to trip. Vegetation grows into transmission lines, and utilities must regularly monitor critical areas to ensure overgrowth is contained. A line trip as a result of vegetation encroachment, together with drooping, is what initiated the 2003 blackout. If a line trips, the electricity that was supposed to be passed through that line must find another medium to travel through. If the secondary lines do not have the capacity to support increased load, the grid may experience a cascading failure as other lines fail to support the excess load resulting from the preceding line trips. Ultimately, transmission lines must have proper maintenance and construction in order to ensure that unnecessary outages do not occur.
7.1.2 Power Quality

Electricity is produced in generators at a constant current of 60 Hz. This must be maintained continuously through transmission to ensure quality power flow. As it travels through a wire, electricity experiences voltage fluctuations. In order to maintain optimal load and prevent loss of power, reactive power maintains a stable current. According to FERC, “reactive power supports the voltages that must be controlled for system reliability.”\(^9\) Voltage naturally fluctuates in power lines; reactive power is used to adjust for these fluctuations as they happen. If the voltage rises too high, the reactive power needs to be scaled back to lessen the load. If the voltage falls too low, reactive power needs to be increased.\(^9\)

Reactive power is used to maintain a consistent current of the “real” power delivered to customers. This is achieved through a series of capacitors, inductors, and compensators on transmission lines that supply and consume reactive power as necessary.\(^9\) The nature of reactive power contributes to the grid’s propensity to cascade. There must be sufficient reactive power in order for the current of real power to continue. “Inadequate reactive power supply lowers voltage; as voltage drops, current must increase to maintain the power supplied, causing the lines to consume more reactive power and the voltage to drop further.”\(^9\) As reactive power is lost, the flow of real power must be increased to ensure continued transmission. This further reduces the available reactive power to support continued transmission. Ultimately, this cycle will cause the line to trip as it cannot support the load. The nature of reactive power and the grid’s inability to support its supply at all times is a vulnerability that must be mitigated through proper grid management techniques.

7.1.3 Transmission Congestion

Transmission congestion is a vulnerability that has arisen because of the electric grid’s historical development. In its 2009 National Electric Transmission Congestion Study, the DOE sought to understand the problem of congestion in electric power transmission. Congestion exists when “actual or scheduled flows of electricity across a line or piece of equipment are restricted below desired levels.”\(^9\) It results from a historical focus on the development of generation without adequate development of transmission to match.\(^9\)

In New York, the most severe congestion area surrounds New York City, where the transmission lines struggle to support the power that flows into the city to satisfy the high demand. There is particular congestion on the corridor running from western New York to the eastern part of the state as imports from the Midwest and Canada have increased.\(^9\) According to the DOE, congestion leads to poor electricity delivery, impacting the total reliability of the system. New York has worked to reduce congestion, which costs the industry hundreds of millions of dollars each year. Generally, congestion has been reduced in the critical areas in New York as low capacity, fast start natural gas turbines built throughout the city have been able to support increased demand when necessary.\(^9\) The Great Lakes states in the Midwest do not exhibit the same congestion issues as on the East Coast.\(^9\)
7.1.4 Aging Infrastructure

By many accounts, the age of the power grid, especially transmission infrastructure, is of growing concern.\(^1\) The last major boom in energy infrastructure was in the 1950’s and 60’s in the wake of World War II. Because of this new wave of infrastructure, “those reaching senior positions today and those who trained them through the 1970’s and into the early 1990’s did not view aging and aging-related problems as particularly important, because at the time they were not.”\(^2\) As a result, the culture in the industry promoted the idea that equipment failure is not a trend-based phenomenon and should be managed exclusively on a case-by-case basis. Companies focused their equipment investments on periodic repair rather than infrastructure renewal.\(^3\) As it stands, Li and Guo explain, “the U.S. electricity infrastructure, in terms of its age and the trend of development, is a ‘third world grid.’”\(^4\) As of 2008, over 70 percent of transmission lines and power transformers in the United States were 25 years old or older. Experts strongly contend that the industry needs to shift its focus and begin addressing the issue of aging infrastructure.\(^5\)

Many of the key threats that have the potential to disrupt the power grid also contribute to the grid’s deterioration. Natural disasters, weather, and even high temperatures slowly wear out the infrastructure. Brown and Willis explain that this is cause for concern because:

- “The likelihood of outright, end of life failure tends to increase with age.
- Maintenance and breakdown-repair costs tend to increase with age.
- Replacement parts can become difficult and expensive to obtain for older equipment.
- Old equipment may be technologically obsolete and incompatible with newer systems.”\(^6\)

All of these factors, absent of improvement efforts, contribute to a downward trend in grid reliability.\(^7\)

7.1.5 Centralization of the Grid

Using the 2003 blackout as a model, Albert, Albert & Nakarado show that the structure of the power grid can contribute to its vulnerability. The authors examine the connection of nodes and substations and relative power loss and find that while grids are designed to withstand the loss of a minor node or substation, it would be hard to continue operation if a more significant “hub” were to go offline.\(^8\) In addition, there has been a trend towards “centralizing control of electric power systems.”\(^9\) Amin relates that while this will increase efficiency and reliability, a centralized system is more susceptible to attack because an attacker would be able to target one specific node, whereas in a smaller localized system there would be greater resilience.\(^10\) Prior to energy deregulation the electric system was comprised of vertically integrated generation and distribution companies. Deregulation led to a system of independent system operators (ISO) and regional transmission organizations (RTO) that facilitate transmission from independent power producers to separately owned distribution grids.\(^11\) This market-based system requires control centers to manage transmission and generation across ISO/RTO regions that used to be managed at the local utility level.\(^12\) These control centers provide a single point of vulnerability for a system that used to have many.

7. Vulnerabilities
To increase reliability and support centralized control centers, utilities have developed communications systems that operate along the electrical pathways. Supervisory Control and Data Acquisition (SCADA) systems control the main systems in the power infrastructure, and are connected to these networks. These systems have increased the reliability of the grid, providing alarms that alert workers to potential problems so they can be contained, but they have also increased the vulnerability to damaging cyber intrusion. Some access control systems include the ability to connect remotely, opening utilities to intrusions and disruptions that could have a large detrimental impact. The interconnectedness of the network that has developed requires “highly reliable, secure control and information management systems” in order to mitigate the threat of malicious hackers or disgruntled employees.

7.1.6 Physical Security

All forms of electrical infrastructure are vulnerable to physical threats. Most of the infrastructure is above ground and has poor physical security. Substations and basic generating plants do not typically have heavy security measures outside of physical barriers, while nuclear facilities have developed very strict security plans, including physical barriers and armed security.

7.1.7 Fuel Supply

While the inability to deliver power would have wide-reaching impacts across the affected area, the inability to generate would be equally detrimental. While much of the Great Lakes region has access to hydroelectric and other forms of renewable energy, the generation of electricity is still reliant on external fuel sources such as oil, coal, and natural gas. Generation plants are thus reliant on a continuous supply of these fossil fuels. Natural gas in particular is a large source of generation in the Great Lakes region. Disruption of gas pipelines could create major disruptions in the ability to provide power as well. Figure 7-1 shows the breakdown of generating sources in the Great Lakes region.
7.2 Pipeline Infrastructure

The pipeline network in the United States has vulnerabilities at compressor/pump stations, control centers, and through supply lines. An important source of fuel and heating in the Great Lakes states, most petroleum and natural gas originates from outside the region. As a net importer of these fuels, the region is put at the disadvantage of having third party vulnerabilities in other sectors. Data on significant pipeline incidents provide a strong baseline for a discussion on the system’s vulnerabilities. PHMSA defines a significant incident as:

- Fatality or injury requiring in-patient hospitalization.
- $50,000 or more in total costs, measured in 1984 dollars.
- Highly volatile liquid releases of 5 barrels or more or other liquid releases of 50 barrels or more.
- Liquid releases resulting in an unintentional fire or explosion.

The natural gas industry has witnessed an average of 55 significant onshore pipeline incidents a year over the past five years (2006-2010). These incidents accounted for an average of $92.5 million dollars a year in property damage. The average cost of incidents has greatly increased when compared to the averages from the previous ten years. While gas pipeline incidents may be financially costly, they have only resulted in an average of three fatalities in any given year. There has been an average of 109 significant onshore petroleum pipeline incidents a year over the past five years (2006-2010). There have been few fatalities, averaging only two a year. Compared to natural gas pipelines, the disruption of petroleum pipelines seems much more
Vulnerabilities

costly, averaging $204 million dollars a year. But this data is skewed by a large pipeline incident in Michigan in the last year. The data shows typical damage per year ranging from $60-70 million.\textsuperscript{118}

7.2.1 Pipelines

The pipeline industry does not attribute failures to aging of pipeline infrastructure, but rather poor management. According to the Association of Oil Pipelines (AOPL), the number of incidents attributed to age decreased by 36\% between 2002 and 2009.\textsuperscript{119} Based on data provided by PHMSA, aging pipelines account for only 10\% of the total transmission infrastructure. This number has decreased significantly since the 1960s, where aging lines were approximately 23\% of total infrastructure.\textsuperscript{120} AOPL suggests that excellent integrity management improves pipeline reliability. Actual pipelines are still a large vulnerability accounting for the majority of incidents, rupture being the primary cause.\textsuperscript{121} According to PHMSA, corrosion or equipment failure are the primary threats that lead to a significant incident. Poor maintenance and an inability to regularly monitor pipelines can increase the potential that a line will rupture due to regular deterioration. Pipelines are also poorly marked and buried fairly close to the surface. Markers only indicate that a pipeline is nearby and not its exact location.\textsuperscript{122} This makes them extremely vulnerable to rupture as a result of digging. Construction and other industries often build in areas where they come into contact with a pipeline. While it is a common incident, there are numerous mitigation techniques that can decrease the magnitude of this vulnerability. PHMSA and many states have developed programs to prevent construction workers from accidentally striking a pipeline. Under Federal requirements, states have established “one-call” centers that can provide information on nearby lines and alert the local utilities of an impending action.\textsuperscript{123} The combination of these one-call centers with proper marking of pipelines and public education campaigns can help mitigate the threat posed to vulnerable underground lines.\textsuperscript{124}

While pipelines are generally built underground, this does not preclude them from the threat of natural forces. Pipelines can be made vulnerable because of the soil in which they are laid. Heavy flooding and earthquakes can cause the soil to become uneven or erode.\textsuperscript{125} While a report by NISAC suggests pipelines would withstand an earthquake, without proper support from the soil a pipeline would be susceptible to displacement and/or rupture.

Pipelines are also vulnerable to physical attack. They travel across large distances of uninhabited land and surveillance is very minimal.\textsuperscript{126} Attacks in other countries have seen adversaries use improvised explosive devices to disrupt pipelines in these vulnerable remote areas.\textsuperscript{127} While there have been no similar attacks in the United States, the threat still exists.

While the Great Lakes region may not be particularly prone to earthquakes, the major transport systems that supply natural gas to the region could be at risk. NISAC examined the possibility of an earthquake along the relatively quiet, but powerful New Madrid fault line in the center of the country and found that it could disrupt large portions of the trunklines that support the New York and Chicago delivery points, thereby cutting off supply. NISAC explains, however, that in addition to existing reserves of natural gas, were this pipeline to fail, the trunkline along the East Coast provides a redundancy in the system that would ameliorate much of the consequences. More specifically, the “simple aggregation of supply and consumption shows that the maximum supply disruption (8.1 BCF per day) is less than the sum of gas used by
industrial users and power generators. If the supply routes traversing the New Madrid fault were lost, the total loss of supply would not be sufficient to cause a shortage in the near term.

The sources of supply and productions centers are also vulnerable due to their location in the hurricane-threatened Gulf of Mexico. Hurricanes could significantly damage facilities that, if out of commission for an extended period of time, would begin to dramatically impact the Great Lakes region. Natural gas would have to be imported from Canada or domestic sources in other regions. NISAC reports that while this would result in an increase in natural gas prices and contribute to consequences in other sectors, the price increase would naturally reduce consumption, and therefore lead to the development of greater reserves. Following large storms such as Hurricane Katrina, history has shown the impact of large hurricanes on the price structure in natural gas markets, with prices increasing for an amount of time before settling once more.

7.2.2 Compressor / Pump Stations

Major hubs in the infrastructure, such as compressor and pump stations, are located above ground, making them the most visible vulnerability in the pipeline system. As mentioned, these units are particularly important to the pipeline network because they maintain the pressure of the transmission flow. As a result, a disruption at a compressor or pump station could lead to loss of flow or rupture in the system. Many of these sites do not require onsite staff and are operated remotely from a control center. Perimeter fences are the only security requirement for compressor stations, so they do not have much physical security protecting them. Despite the lax regulatory environment, some operators do maintain alarm and surveillance systems.

7.2.3 Control Centers

With the advent of new computer-based technologies, much of the energy infrastructure has become more interconnected. Like the electric grid, the pipeline infrastructure is connected and controlled through large SCADA systems that have access to and control over all the systems in an operator’s networks. This creates a single point of vulnerability through which a cyber attack could be executed. These systems are vulnerable to remote access and control, and proper cybersecurity protocols are necessary to ensure that systems are protected from intrusion. TSA has issued guidelines on the protection of these connected systems. All pipeline operators are required to take basic steps to mitigate the threat from cyber intrusion, while facilities deemed “critical” by the TSA and PHMSA are required to implement more enhanced measures. Table 7-1 provides a more detailed look at the cyber security measures that should be employed at all pipeline facilities.
## Baseline Cyber Security Measures
The baseline measures should be applied to all pipeline control system cyber assets

| General Cyber Security Measures | Provide physical security and access controls to cyber assets  
| monitored and periodically review, not to exceed 18 months, network connections, including remote and third-party connections  
| Evaluate and assess the role of wireless networking for risk before implementation  
| Review and reassess all cyber security procedures annually. Update as necessary  
| Review and reassess cyber asset criticality periodically, not to exceed 18 months |

| Information Security Coordination and Responsibilities | Develop a cross-functional cyber security team and an operational framework to ensure coordination, communication, and accountability for information security on and between the control systems and enterprise networks  
| Define information and cyber security roles, responsibilities, and lines of communication among the operations, IT, and business groups, as well as with outsources, partners, and third-party contractors  
| Establish and document standards for cyber security controls for use in evaluating systems and services for acquisition. Encourage vendors to follow software development standards for trustworthy software through the development lifecycle |

| System Lifecycle | Incorporate security into cyber system design and operation, whether designing a new system or modifying an existing system. Secure design and operation of the SCADA control system architecture is critical for the creation of a sustainable and reliable system. Mitigate any security deficiencies found in control system hardware and software  
| Establish and document policies and procedures for assessing and maintaining system status and configuration information, for tracking changes made to the control systems network, and for patching and upgrading operating system and applications  
| Establish and document policies and procedures for the secure disposal of equipment and associated media |

| System Restoration & Recover | Plan and prepare for the restoration and recovery of control systems in a timely fashion as specified in the operator’s recovery procedures |

| Intrusion Detection & Response | Establish policies and procedures for cyber intrusion monitoring, detection, incident handling, and reporting |

| Training | Provide training in information security awareness for all users of control systems before permitting access to the control systems and on an annual basis or as necessitated by changes in the control system. Individuals with significant control systems security roles should have training specific to their roles |

| Access Control and Functional Segregation | Segregate and protect the control systems network from the business network and the Internet through the use of firewalls and other protections. This applies both to wired and wireless networks  
| Use control systems hosts and workstations only for approved control system activities  
| Establish and enforce access control policies for local and remote users, guests, and customers. Procedures and controls should be in place for approving and enforcing policy for remote and third-party connections to control networks |

| Enhanced Cyber Security Measures | In addition to baseline measures, operators should apply enhanced measures to all cyber assets that have been designated critical |

| Access Control | Restrict physical and logical access to control systems and control networks through the appropriate combination of locked facilities, passwords, communications gateways, access control lists, authenticators, and separation of duties, invocation of least privilege, and/or other mechanisms and practices  
| Conduct a risk assessment to weigh the benefits of implementing wireless networking against the potential risks for exploitation. Evaluate the need for enhanced networking control technologies for wireless networks prior to implementation |

| Vulnerability Assessment | Conduct periodic vulnerability assessments of the control system security, including testing as appropriate in a non-production environment, not to exceed 36 months |


7. Vulnerabilities 38
Notes

83 DHS, 2007, p. 112.
84 Argonne National Laboratory, 2008, 7.
85 Congressional Research Service, 2005; Argonne National Laboratory, 2008, 7
86 U.S. Energy Information Administration, Electric Power Monthly 2010
87 Overbye, 2010.
88 LCRA; Overbye, 2010.
90 Overbye, 2010.
91 U.S. Federal Electric Regulatory Commission, 2005, p. 3
92 U.S. Federal Electric Regulatory Commission, 2005, p. 17
93 U.S. Federal Electric Regulatory Commission, 2005, p. 1
95 U.S. Department of Energy, 2009, p.1
96 Beach & Dilts, 2006; U.S. Department of Energy, 2009, p. 11
100 Brown and Willis 2006; Li and Guo 2006; National Infrastructure Advisory Council 2010;
    Owens 2008; Shahidehpour 2006.
103 Li & Guo, p. 50.
105 Brown and Willis, 2006; Li and Guo, 2006; Owens, 2008.
107 Brown and Willis, 2006; Li and Guo, 2006.
110 Amin, 2010, p. 15.
111 Beach & Dilts, 2006, p. 10.
112 Gruen, 2010; New York Independent Service Operator, 2011; Pennsylvania-New Jersey-
    Maryland Independent Service Operator, 2011.
116 U.S. Energy Information Administration, Net Generation by State by Type of Producer by
117 U.S. Pipeline and Hazardous Materials Safety Administration, PHMSA Stakeholder
    Communications: Significant Pipeline Incidents 2011.
118 U.S. Pipeline and Hazardous Materials Safety Administration, PHMSA Stakeholder
    Communications: Significant Pipeline Incidents by Cause 2011.
119 Association of Oil Pipe Lines 2011.

7. Vulnerabilities
120 U.S. Pipeline and Hazardous Materials Safety Administration, *Pipeline Incidents and Mileage Reports* n.d.
128 National Infrastructure Simulation and Analysis Center, 2006, p. 27.
129 National Infrastructure Simulation and Analysis Center, 2006, p. 35.
130 National Infrastructure Simulation and Analysis Center, 2006.
131 9 CFR 192.163.
132 The Williams Companies, n.d.
8. Blackouts
8. Blackouts

This section presents a broad picture of blackouts, which put simply, occur when threats meet vulnerabilities. By analyzing what happens during blackouts, a better understanding of how to reduce vulnerabilities and guard against threats can be gained.

8.1 Blackouts Pre-2003

Most blackouts occur when multiple threats meet multiple vulnerabilities. The two threats responsible for the major blackouts that occurred in the U.S. before 2003 were natural forces and accidents/human error. In 2004, the U.S.-Canada Power System Outage Task Force composed a report on the major blackout that occurred on August 14, 2003. The study described the causes and effects of the blackout and made a number of recommendations. It also reviewed multiple blackouts from 1960 through 1998. All of the blackouts reviewed in the study began with transmission line failures caused by factors such as inadequate vegetation management, poor system visibility, and issues involving reactive power supply. The research team used these blackouts as examples of when threats meet vulnerabilities.

8.1.1 Poor Vegetation Management

One of the primary causes of power outages is contact of trees and other vegetation with transmission lines, which cause the lines to trip. If the lines are sagging due to higher loads or warm weather, they are more likely to come in contact with surrounding vegetation. One prominent example of this problem was a cascading power outage on July 2, 1996, caused by a tripped sagging line. This outage led to a major blackout in the western United States, Canada and Mexico that left 2,000,000 people without power for several hours. Another blackout a month later (August 10, 1996), also due to poor vegetation management, left 7.5 million people without power for up to nine hours. Within one summer, poor vegetation management, a major issue in the 2003 blackout, temporarily cut power to approximately ten million people.

8.1.2 Poor System Visibility and Communication

The Blackout Report also lists limited system visibility, a failure to receive accurate and timely condition information, as a significant contributor to past outages. In terms of Amin’s framework, accidents and errors (a threat) can alter decision making. The insufficient flow of information prevents system operators from understanding the full range of impacts that their decisions have. It also hinders operators’ ability to share accurate information with other utilities. This was evident in the 1982 power outage when poor communication prevented the safety net from being implemented in time. (A safety net is a plan previously put in place to minimize the number of people being blacked out if the system is put under excessive stress.) A similar problem occurred during the August 1996 blackout. Following the first two line trips, operators were not aware that the system was in an insecure state.
8.1.3 Reactive Power

Reactive power supply issues also commonly contribute to blackouts. Shunt capacitors and generating resources are the primary sources of reactive power. While it is not difficult for utilities to estimate how much reactive power they have in shunt capacitors, it is far more difficult for utilities to monitor the amount that comes from generators when the system is under stress. Often, the estimated available reactive power is higher than the actual available reactive power, which results in significant voltage discrepancies. A better simulation method that gives the system operator more insight into an accurate picture of the available reactive voltage would be a way of detecting and preventing a loss of current in transmission lines.

8.2 The 2003 Blackout

On August 14, 2003, a major blackout left over 50 million people without power for up to 96 hours.137 This disaster had wide-ranging consequences and was the result of multiple threats meeting multiple vulnerabilities. The major problems that were pervasive throughout this blackout were ineffectual communication, poor vegetation management, and reactive power issues.138

A detailed chronology of the events of August 14, 2003 can be found in Appendix B, while Figure 8-1 shows a timeline and categorizes the events that started the blackout.

8.2.1 High Demand

One of the contributory factors in the early stages of this blackout was the high load that the Cleveland-Akron area of Ohio had on August 14, 2003. The grid typically reaches peak loads in the summer when demands of air conditioning and appliances are greatest.\(^{139}\) As shown in Figure 8-2, the greatest amount of electricity sold per month (which is the same as the load since as power cannot be stored, the power consumed is the same as the power sold in a state) is in the summer months.\(^{140}\)

![Figure 8-2. Total electricity sales by month in 2003 ("Monthly Electric Utility Sales/Revenue data - EIA-826 data file," n.d.)](image)

This is also when transmission lines are most vulnerable because they are carrying their greatest load, and it would take the removal of fewer lines for there to be inadequate transmission capacity. Furthermore, these lines were sagging due to the high load that they were carrying.

8.2.2 Reduced Capacity

Another factor affecting this blackout was the 3.178 gigawatts of generators that were offline. The energy industry plans to ensure that enough power is available to meet peak demand; however, regular and emergency maintenance must be considered when balancing
demand and supply.\textsuperscript{141} Even though the temporary loss of these generators did not cause a power shortage, it made managing reactive power much more challenging. In conjunction with multiple trips on lines of varying loads (from carrying less than half the critical load to carrying over 150\% of the critical load), this led to the shifting of load to wires serving the Cleveland area.\textsuperscript{142}

8.2.3 Poor Vegetation Management

Poor vegetation management was the root cause of the blackout. Most of the lines that tripped early on (e.g., the Stuart-Atlanta line and the Harding-Chamberlain line) were lightly loaded lines, which would indicate that they did not sag much before tripping.\textsuperscript{143} This indicates that the utilities controlling these lines did not adhere to the vegetation management standards in place prior to the blackout, which would have prevented a line trip during normal operating conditions. This issue was common in most of the earlier major blackouts, in particular the August 10, 1996 blackout, in which lightly loaded lines also tripped, which began a cascading blackout.

8.2.4 Poor System Visibility and Communication

Ineffective communication and alert mechanisms prevented system operators from having an accurate picture of what was occurring in the grid in real time. The threat of accidents, equipment failures, and errors met the vulnerability of ill-advised actions or inaction.\textsuperscript{144} There was also poor system visibility, which likely stemmed from an inability to monitor the electric grid under stress.\textsuperscript{145} This was evident when First Energy was unaware that the Stuart-Atlanta line had tripped.\textsuperscript{146}

MISO’s (Midwest Independent System Operator) state estimator and real time contingency analysis software was also offline during most of the events leading up to the blackout. Were they operational, these systems could have provided more advanced warning.\textsuperscript{147} This prevented the system from operating within safe limits and inhibited implementation of any safety net procedures that might have prevented or mitigated the effects of the blackout. This issue had been problematic in the past, most specifically in the August 1996 blackout.\textsuperscript{148} As in the 2003 blackout, system operators were unaware of the status of their lines, though it was pointed out to First Energy that their lines were down by MISO and PJM an hour and a half after the issue occurred.\textsuperscript{149}

8.2.5 Reactive Power

Improper management of reactive power likely played a role in the blackout as well as the wild power swings that were occurring in the later stages of the blackout. In previous blackouts utilities also had trouble estimating the amount of reactive power available, as it is difficult to model the generating systems under stress.\textsuperscript{150}
8.2.6 Conclusion

In these cases the threats meeting the vulnerability led to many Americans and Canadians losing power. These extended and wide ranging power outages affected almost every sector of the economy and people’s everyday lives, showing how indispensable the electric system has become.

8.3 Blackouts Post-2003

Since 2002, blackouts have been predominantly caused by weather. (For the purposes of this study, the research team has defined blackouts as power outages lasting more than 24 hours and affecting at least 50,000 people within the study region. The 2003 blackout was excluded from this data set as it was an outlier.) As Figure 8-3 shows, 97% of the 101 blackouts examined were caused by weather. Sixty-two percent were caused by severe storms (e.g., thunderstorms). Also, 23% of the blackouts were caused by snow or ice storms. This pattern seems to be consistent throughout the years, as shown in Figure 8-4.

![Figure 8-3. Causes of blackouts, 2003–2010.](image-url)

Notes

133 Hoffman & Nilchiani, 2008, p. 32.


9. Consequences of Blackouts
9. Consequences of Blackouts

An attack, disruption or failure within the energy sector has the potential to significantly impact all 18 CIKR sectors because they all require power to function. Consequently, it is crucial to understand the dependencies and interdependencies that exist across all CIKR sectors when evaluating the potential implications of a major blackout.

The NIPP defines a dependency as, “the one-directional reliance of an asset, system, network, or collection thereof, within or across sectors, on input, interaction, or other requirement from other sources in order to function properly”; and interdependency as a “mutually reliant relationship between entities (objects, individuals, or groups). The degree of interdependency does not need to be equal in both directions.”

This section summarizes the essential connections that exist between the energy infrastructure and each of the 17 other CIKR sectors. Subsequently, it examines the consequences of blackouts using the August 14, 2003, blackout as an example to illustrate these interrelationships.

9.1 Agriculture

Crop growth, food production and distribution, and livestock maintenance all comprise the Food and Agriculture Sector. An adequate water supply is essential to the functionality of these components. Furthermore, food wholesalers and retailers are dependent on these products to generate revenues. While the water sector manages distribution equipment in supply systems, the energy sector provides fuel sources to power irrigation and refrigeration systems that preserve food resources for distribution. A disruption in the energy infrastructure can lead to spoilage and livestock loss, causing disturbances in the supply-chain, which is critical in assuring market stability and meeting consumer demand.

Moreover, wholesalers and retailers face shortages, spoilage, or shutdowns resulting in significant revenue loss.

In the Great Lakes region, dairy is a very large industry that is particularly vulnerable to power outages because products must be kept at a specific range of temperatures to prevent health risks from consumption. While agriculture accounts for only 1% of the region’s economy (see Figure 3-2), the Great Lakes region produces a large amount of the United States’ food. According to AUS Consultants, one hour of outage time can reduce one week’s food production by up to 10%. In the 2003 blackout, food spoilage accounted for between $380 million and $940 million worth of loss. Many food retailers were also forced to close as a result of the blackout.

9.2 Banking and Finance

The banking and finance sector involves everything from local banks to the stock market. Banks and markets rely on power to conduct daily trading and transactions. A disruption in the power infrastructure can significantly hamper operations and have a widespread economic impact. Local banks and ATMs, exchange markets, and security systems rely heavily on the
power grid. A power loss leads to overtime for critical personnel, and closures that result in a loss of financial transactions and employee production.

The banking and finance sector accounts for about 24 percent of the region’s economy (see Figure 3-2). During the 2003 blackout, retail banking was the hardest hit portion of this sector, as branches and ATMs rely on electronic systems to do most of their business. Commercial banking and general financial headquarters were able to withstand the blackout using backup generators. In addition, the markets were closed when the blackout began. Still, additional costs were experienced due to employee overtime. On a second-order level, the sector experienced some problems due to a loss of telecommunications. The insurance industry saw no measurable impact on its operations.

9.3 Chemical/Critical Manufacturing

The Chemical and Manufacturing Sectors rely heavily on the energy infrastructure to distribute electricity and natural gas used to fuel manufacturing facilities. A disruption can lead to the loss of employee productivity and equipment failure. It may shut down equipment that is needed to maintain stable working conditions and critical safety features within a facility. Additionally, countless petroleum-based chemicals and products are used at other interdependent facilities that manufacture a myriad of products. A disruption to the daily supply of these key resources is detrimental to the manufacturing sector and poses the risk of substantial economic loss. Similar to agriculture, wholesalers and retailers on the other end of the supply-chain experience shortages or closures that result in significant economic loss.

In the Great Lakes region, manufacturing is an especially important sector, accounting for 13% of total GDP. According to AUS consultants, in 2003 broken equipment from the outage accounted for up to $800 million in damages. One steel mill witnessed an explosion and fire due to an interrupted process during the blackout. Most manufacturing plants suffered lost productivity due to insufficient backup generation, leaving many workers idled. The chemical industry also suffered, particularly “Chemical Valley” in Ontario, where producers lost $10-20 million per hour without electricity.

9.4 Commercial Facilities (CF)

The CF sector is broad and includes a wide range of commercial infrastructure. The CF SSP highlights the following as major components of the CF sector: entertainment and media, gaming, lodging, outdoor events, public assembly, real estate, retail, and sports leagues. The most significant consequences associated with a loss of power in the CF sector involve loss of production as a result of idle workers and disabled machinery. Other major effects result from the operating expenses associated with shutting down and restarting major facilities that encompass this sector.

The available literature does not address commercial facilities as a broad subject area impacted by blackouts. There is a greater focus on individual commercial sectors.
9.5 Communications

Communications are vital to the functionality of all 18 sectors. This sector has evolved to include wire line, telecommunication, wireless, satellite, cable, internet, and broadcasting networks.\textsuperscript{170} A disruption in the power grid can have a crippling effect on these systems. In addition to the day-to-day functions, each sector contains components that are dependent on networks for critical operations. For instance, public health facilities, emergency services, and the transportation sector rely heavily on communication networks to coordinate everything from daily operations to emergency situations.\textsuperscript{171} The energy sector as well is dependent on networks to ensure reliability in regulating the distribution and transportation of energy sources.\textsuperscript{172} Broadcasting networks face obstacles in delivering urgent information. Ultimately, a partial or full loss of these services, as a result of a power outage, will potentially impact residential, commercial, industrial, and governmental users.

During the 2003 blackout, mobile telecommunications were able to maintain most operations even though there was a large increase in phone calls. Calls for emergency services were prioritized in order to ensure there was a reliable communications system for responders.\textsuperscript{173} Some wire line providers required assistance to ensure their backup generators continued service.\textsuperscript{174} In addition, some media outlets had trouble broadcasting due to a loss of backup power.\textsuperscript{175}

9.6 Dams

Dams and the energy sector are interdependent as dams are central to hydro power facilities. The dam sector also includes navigation locks, levees, dikes, hurricane barriers, and waste impoundments that rely on power for water regulation equipment.\textsuperscript{176} Therefore, a failure in the power infrastructure can result in a failure in the dam infrastructure. This can cause significant disruptions, especially in power supplies, creating cross-sector implications that occur as a result of a power loss.

The available literature does not provide any documentation for the impact of blackouts on dam infrastructure.

9.7 Defense Industrial Base

The Defense Industrial Base comprises an array of government and private sector organizations partnered with the Department of Defense (DOD). This sector comprises thousands of contractors and companies that assume research and development capacities in support of the DOD systems, information, and equipment.\textsuperscript{177} As current levels of interdependency are not clearly identified by the Defense Sector, the defense SSP acknowledges that it has a particular concern in identifying interdependencies with the energy, transportation, water, IT, and communications sectors.\textsuperscript{178}

The available literature shows that DoD is currently unaware of the direct impacts of blackouts on its critical assets. From 2006-2008, DoD facilities experienced outages that lasted up to 7 days, accounting for at least 70% of critical assets. About 9% of the missions in that period were adversely affected by the loss of power.\textsuperscript{1} DoD is currently performing a vulnerability assessment as it relates to the effects of a prolonged power outage on critical
facilities.\textsuperscript{1} However, it is critical to recognize that the DOD relies heavily on power to mobilize and carry out military operations in utilizing cyber-communication systems. Consequently, this CIKR sector is dependent on the energy sector to operate.\textsuperscript{179}

### 9.8 Government Facilities/Education Facilities

The Government Facilities Sector encompasses facilities owned, leased, or operated by the Federal government. These facilities are located domestically and in foreign nations. These facilities maintain an array of public and official purposes ranging from commercial and recreational activities and business transactions to operating and housing highly sensitive information and equipment. In total, the facilities that comprise this CIKR sector amount to 3 billion square feet. Government Facilities are maintained directly by the federal government; therefore, there is not a sector plan outlining specific cross-sector interdependencies. However, as many of these facilities are representative of the federal government, they face both natural and terroristic events. Consequently, a disruption to critical energy infrastructure poses security and operational risks.\textsuperscript{180}

The Education Sector’s falls under the Government Facilities Sector. The Education Facilities SSP does not stipulate specific interdependencies with the energy sector. However, facilities in general rely on energy sources to operate on a daily basis. More specifically, information technology systems, their security, and functionality all rely on power. A loss of power jeopardizes security features and education software as a result.\textsuperscript{181}

The available literature on blackouts does not address impacts on the education sector.

### 9.9 Postal and Shipping Sector

The Postal and Shipping sector encompasses the agencies responsible for shipping small packages and flat mail. As a result, virtually every public and private sector organization is dependent on a component of this CIKR sector to deliver time-sensitive packages. The Banking and Finance, Commercial Government Facilities, and Healthcare and Public Health sectors are among those most dependent on the functionality of this CIKR sector. Conversely, the Postal and Shipping Sector is dependent on the energy sector to power its facilities. Consequently, there is a significant interdependency on the power infrastructure, and a disruption could have major consequences in all of the CIKR sectors.\textsuperscript{182}

### 9.10 Emergency Services

Emergency Services are responsible for ensuring security in all 18 CIKR sectors. Emergency services rely heavily on energy to operate systems and communication networks that are vital to mobilizing and coordinating response efforts. Additionally, facilities require power, water, and natural gas to function. In the event of a disabled facility, emergency services face the necessity of transferring critical personnel and equipment to alternate sites to maintain services. This sector is also dependent on the transportation sector to maintain critical transportations systems. For instance, power is required to operate traffic signals and mass transit systems. If functionality of these systems is lost, the ability of emergency services to swiftly mobilize can be hampered by accidents or delayed traffic.

9. Consequences of Blackouts
Emergency services are primarily affected on a second-order level by impacts in other sectors. Blackouts in summer have resulted in an increase in the number of heat-related illnesses that require emergency medical treatment, with the number of emergency calls more than doubling during these times. This increase in calls ultimately lengthens response times.\textsuperscript{183} Disabled traffic and transit systems increase the number of accidents that require emergency response, and make roadways difficult to travel on.\textsuperscript{184} Emergency response can also be impacted by an inability to communicate with the Emergency Operations Center.\textsuperscript{185}

### 9.11 Healthcare and Public Health

Public health agencies and healthcare facilities rely heavily on several sectors to provide crucial medical services. These facilities, which include life-saving equipment such as operating rooms, clinical information systems, and life support systems, are powered by electricity. Cross-sector impediments that result from power outages also have a significant and direct impact on healthcare facilities. Disabled transportation systems inhibit the movement of critical patients, personnel, vehicles, materials and pharmaceuticals. Loss of water filtration systems impacts sanitation systems and procedures fundamental to healthcare practices. Supply-chain shortages due to power loss in the Chemical and Agriculture sectors pose the risk of food and drug shortages throughout the healthcare sector.\textsuperscript{186} Simultaneously, communication with emergency services via telecommunications is hampered affecting coordination during healthcare emergencies.\textsuperscript{187}

While there are often backup power systems at hospitals, an extended blackout can result in total loss of power. The loss of refrigeration required for the storage of various vaccinations and medicines could have deleterious effects as they start to deteriorate after two hours without power.\textsuperscript{188} Most hospitals have enough backup power to operate life support systems for one to two days.\textsuperscript{189}

### 9.12 Information Technology (IT)

IT systems are utilized in every sector to carry out all levels of functionality. Moreover, IT systems store, secure, and share information within and across CIKR sectors.\textsuperscript{190} The energy infrastructure relies heavily on IT systems to maintain control and regulation systems, critical in accurately distributing supplies to prevent power outages.\textsuperscript{191}

The available literature does not discuss the impact of blackouts on information technology systems in general, focusing more on systems within each sector.

### 9.13 National Monuments and Icons

While this sector does not highlight direct dependencies on energy in its SSP, there are many secondary consequences that face this sector as a result of a power outage. For instance, interdependency exists with the CF sector as it provides lodging and accommodations for visitors. Power loss results in a partial or full shutdown in these facilities, causing economic loss and low visitation levels.\textsuperscript{192}
The available literature does not discuss the direct impact of blackouts on national monuments and icons.

9.14 Nuclear Reactors, Materials, and Waste

Nuclear facilities and the power infrastructure are interdependent. Nuclear reactors produce a large portion of the energy distributed throughout the power grid. In exchange, back-up and emergency systems within nuclear facilities rely on alternative power sources. Consequently, any disturbance can result in widespread blackout as an outage in one facility can mandate that another facility be shut down.

Nuclear facilities have a number of protective measures that will cause the facility to standby or shutdown in the event of a loss of offsite power. These facilities have various safety systems that must be running in order to prevent reactor failure and ensure safe shutdown. During the loss of external power, diesel generators power these safety systems. Should the loss of external power be for an extended period generators may not have the fuel to support the safe shutdown of a nuclear facility’s processes.

9.15 Transportation Systems

The energy sector is dependent on transportation systems to provide all the materials necessary to produce power. Petroleum, natural gas, coal, and oil fueled facilities rely on pipelines, ships, waterways, roadways, and railroads to deliver these materials; hydroelectric producing facilities rely on canals and dams that utilize waterways. A disruption in the supply of these resources can reduce distribution capabilities resulting in power failure. Conversely, the energy sector powers many of the transportation systems (such as pipeline and rails) responsible for delivering these materials. Additionally, the national transportation infrastructure (rails, mass-transit systems, traffic signals, and airports) rely on electricity to operate communication networks and operating technologies. Power loss can result in stressed IT systems and affect the movement of personnel, goods, and services, impacting revenue and functionality in all CIKR sectors.

The 2003 blackout saw large impacts across public transportation systems in the Great Lakes region with all major airports in the affected area shut down. The New York City mass transit system was disabled and the loss of traffic lights impeded most travel during the region’s evening rush hour.

9.16 Water

Water is essential to the functions of every sector. It is vital to emergency services, healthcare, sanitation, agriculture, and transportation. Additionally, significant interdependency exists between the water and energy sectors. Water is utilized by the energy sector as a primary source in running hydroelectric producing facilities as well as a source for cooling. Conversely, the water sector relies on energy to power pumps and equipment vital to water treatment facilities, sanitation plants, regulation, and distribution.
Blackouts have the potential to affect the safety of the water supply. In 2003, boil-water advisories affected 4.3 million people in the U.S. and Canada and some wastewater treatment plants released partially treated or untreated water into the public areas.\textsuperscript{201}

\textbf{Notes}


\textsuperscript{156} AUS Consultants, p. 10.

\textsuperscript{157} AUS Consultants, p. 12; Electricity Consumers Resource Council, p. 10.


\textsuperscript{160} Electricity Consumers Resource Council, p. 9; Financial and Banking Information Infrastructure Committee, p. 1.

\textsuperscript{161} Financial and Banking Information Infrastructure Committee, p. 1.

\textsuperscript{162} Financial and Banking Information Infrastructure Committee, p. 2.

\textsuperscript{163} Financial and Banking Information Infrastructure Committee, p. 5.


\textsuperscript{165} AUS Consultants, p. 5.

\textsuperscript{166} Electricity Consumers Resource Council, p. 6.

\textsuperscript{167} Electricity Consumers Resource Council, p. 3.

\textsuperscript{168} Electricity Consumers Resource Council, p. 7.


\textsuperscript{173} Public Safety and Emergency Preparedness Canada, p. 2.

\textsuperscript{174} Electricity Consumers Resource Council, p. 10.

\textsuperscript{175} Public Safety and Emergency Preparedness Canada, p. 2.


183 Beatty et al., p. 36; Freese et al., p. 374; Kile et al., p. 95.
184 Public Safety and Emergency Preparedness Canada, 3
185 Kile et al., p. 94.
188 Beatty et al., p. 36; Hinrichs et al., p. 16.
189 Hinrichs et al., p. 16.
197 DeBlasio, p. 3; Financial and Banking Information Infrastructure Committee, p. 4; Electricity Consumers Resource Council, p. 10; Public Safety and Emergency Preparedness Canada, p. 3.
201 Kile et al., p. 94; Public Safety and Emergency Preparedness Canada, pp. 2-3.
10. The Resilience of Energy Resources
10. The Resilience of Energy Resources

While DHS and the energy sector can take steps to prevent issues related to the vulnerabilities inherent in the power system, the system needs to be prepared should threat meet vulnerability. In light of this, the region’s critical energy infrastructure needs to be as resilient as possible to mitigate the effects of functional disruptions. Resilience is one of the “three key concepts” outlined in DHS’s 2010 Quadrennial Homeland Security Review (QHSR) as “essential to and [formative in] a comprehensive approach to homeland security.” The report defines resilience as “foster[ing] individual, community, and system robustness, adaptability, and capacity for rapid recovery” and outlines four goals that are crucial to “ensuring resilience to disasters”:

1. Mitigate Hazards;
2. Enhance Preparedness;
3. Ensure Effective Emergency Response; and
4. Rapidly Recover

Under the industry’s Sector Specific Plan, “energy infrastructure resilience is defined as the ability to reduce the magnitude and/or duration of disruptive events.”

This section focuses on the opinions of government agencies, private sector entities, and the academic community regarding the power grid’s current level of resilience and how it can be improved.

While there are governmental policies that establish security and preparedness frameworks and recommendations, it is largely private companies’ responsibility to implement practices to match them. Business executives need to balance this responsibility with that to their financial stakeholders and customers; therefore, the ideal disaster prevention initiatives are not always feasible. Resilience programs provide a way to bridge that gap by ensuring that if there is an attack, the government and critical infrastructure operators can limit the damage it causes and quickly get services back on line.

As demonstrated earlier in this report, threats to critical energy infrastructure are varied and unpredictable. A disruption as simple as tree branches can cause a failure that the grid needs to be able to respond to immediately.

10.1 Evaluating Power Grid Resilience

Private-public partnerships are a key aspect in managing critical energy infrastructure in the United States. In recent years, DHS has worked with energy experts from academia and private sector organizations to answer one simple question: how can the industry become more resilient? In answering that question, the homeland security and energy communities need to have a sense of how resilient they are. This section outlines frameworks that have come out of public-private partnerships for assessing the resilience of critical power infrastructure.

The National Infrastructure Advisory Committee (NIAC) recently conducted a “stress test” on the U.S. power grid to assess its resilience under a variety of conditions. Based on their observations during this test, the NIAC established four “high-level…prospective sector resilience goals” for the agencies and organizations in charge of managing critical infrastructure sectors to consider adopting:
1. Withstand a shock from any hazard with no loss of critical functions.

2. Prevent a power disruption from cascading into interconnected systems.

3. Minimize the duration and magnitude of power outages through rapid recovery strategies.

4. Mitigate future risks by incorporating lessons from past disruptions, simulations and exercises, and sound risk assessment processes.

Aspects of the infrastructure’s design and interconnectedness further affect the sector’s resilience, in general (Table 10-1).

There are several lessons that can be gleaned from the NIAC’s measures of resilience. First, the vulnerability of the cyber systems that control the flow of electricity and the non-cyber redundancies in place hold tremendous weight in this discussion. Experts agree that if the structural resiliency mechanisms within the power grid (locations of transmission lines, built-in redundancies and alternate pathways, etc.) are all controlled by computers, they do not provide resilience in the event of a cyber-attack (or similar attack on cyber infrastructure).

Second, the emphasis on industry-wide standards and information sharing mechanisms highlights the fact that cooperation is a key to resilience. As explained in the overview of the power grid and its history, the grid has become more interdependent over time. Within the Great Lakes region alone, there are several private and public sector organizations in control of critical energy resources. If one company or region’s transmission line goes down, that company or region needs to be able to dynamically coordinate across regional controls to reroute power. This would rectify the issues that plagued the 2003 blackout, when PJM, MISO and FE did not communicate effectively while attempting to get the situation under control.

When examining the reliability of the electric grid, there are more specific resiliency concerns that need to be assessed. At the regional level, it is important to understand the relative densities of CIKR structures (e.g. transmission lines, power plants). Documenting the load or flow capacity of transmission lines and pipelines (respectively) is also important. At certain points in the power grid, there are “bottlenecks,” i.e. where many transmission lines or pipelines come together, making it difficult to reroute the electricity or fuel if needed. Along the same lines, engineers should document all the potential rerouting paths to assist in vulnerabilities assessments, etc. Finally, an analysis of structural and functional interdependencies is also important for assessing both the level of resilience and where it can be improved.
1. Infrastructure Design and Asset Characteristics
   a. **Interconnectedness:** Are products and services mostly facility-based or systems-based? How reliant are individual providers on the operational integrity of the entire sector? How interconnected are sector assets?
   b. **Asset Profile:** Are the majority of sector assets tied up in long-lived capital assets? Does the sector have rapid equipment turnover that can absorb new technologies quickly?
   c. **Product/Service Profile:** Can the product be inventoried or is it delivered in real time?
   d. **Design Limitations:** Are there technical, social, environmental, or policy barriers that limit the ability to design more resilience into the infrastructure?
   e. **Cyber Dependence:** Are the operations of the infrastructure controlled by cyber assets? If cyber assets go down, can the infrastructure still provide products and services?

2. Supply Chain Vulnerabilities
   a. **Availability of Critical Components:** Are key components readily available? Are lead times and cost of critical spares acceptable?
   b. **Domestic Sources:** Are domestic manufacturing capabilities adequate?

3. Sector Interdependencies
   a. **Dependencies:** Can the sector function long without key inputs from other sectors? Are executives fully aware of inherent risks from sectors they depend on? If the sector is disrupted, how will it affect other critical infrastructure sectors?
   b. **Co-Location:** Are sector assets vulnerable due to co-location with other infrastructures?

4. Sector Risk Profile
   a. **High-Profile Target:** Is the sector a high-profile target for physical or cyber-attacks?
   b. **Strategic Assets:** Does the sector contain assets that are critical for national security?

5. Markets and Regulatory Structure
   a. **Regulatory Constraints:** Do regulations create barriers to increased resilience?
   b. **Market Structure:** How do company size, industry concentration, and profitability affect the ability of the sector to finance investments to enhance resilience?

6. Public-Private Roles and Responsibilities
   a. **High-Impact, Low-Frequency Risks:** Are government and industry roles and responsibilities clearly understood for high-impact, low-frequency risks?
   b. **Disaster Coordination:** Are the responsibilities and expectations of the sector during a disaster clearly understood by the government and the public?

7. Standards
   a. **Standard Bodies:** Does the sector have an existing, highly regarded organization or body to create standards for the sector using a stakeholder process?

8. Information Sharing
   a. **Threat Information:** Does the sector have adequate access to timely, actionable threat information?
   b. **Clearances:** Do companies have a cleared executive who can receive classified information and commit company resources?

9. Workforce Issues
   a. **Capabilities:** Does the sector have a workforce with adequate technical operating experience? Is an aging workforce an issue?

---

**Table 10-1. Questions to be considered when assessing resilience (NIAC, 2010, p. 20)**
10.2 Barriers to Enhancing Resilience

Reports resulting from recent public-private information sharing have made some acute observations regarding the resiliency of the power grid. As explained earlier, the national attention and economic fallout generated by the August 2003 blackout have focused many different stakeholders’ attention on ensuring resiliency. On the technical side, the power companies and authorities have developed a better understanding of how to make the structure of the grid more resilient—mainly by making it more flexible. Following the 2003 blackout, for example, a significant percentage of companies installed emergency preparedness plans and some of the affected companies also installed more backup generation.

Though federal, state, local, and private sector interests in resiliency overlap, they are not the same. Under the Energy Sector Specific Plan, federal agencies are tasked with protecting critical structure as it relates to national security, providing governance and planning, and fostering information sharing. State and local governments have a more narrowly defined role, focusing on preserving government continuity and coordinating initial emergency response in the event of a critical energy infrastructure failure. The private sector places a greater emphasis on service reliability (through system robustness), risk management, innovation, and value for their shareholders. The key is for members of the three stakeholder categories to coordinate based on their mutual interests and understand where they differ in developing policies or practices.

Based on the construct of critical infrastructure definitions, redundancies in the cyber control construct are crucial to determining the resilience of the power grid. The NIAC explains that:

...federal agency responsibilities regarding cyber vulnerabilities, information sharing, emergencies, and mitigations are still unclear to many utilities. In addition, the difficulty in assessing cyber risks may be creating a culture of compliance at the expense of a culture of security.

The implications of this are far-reaching. As the response to the 2003 blackout indicates, explicit guidelines often come in the wake of a problem, not before it happens. If energy providers are not taking advantage of their expertise and innovation to develop resiliency above and beyond established guidelines, the CIP community is in danger of treading behind the curve in mitigating risks.

10.3 Moving Forward: Smart Grid Technology

To address resiliency gaps and the challenges to filling them, the businesses responsible for critical power infrastructure are beginning to move toward smart grid technology. The idea behind smart grid initiatives is to allow the grid to sense and adapt to threats on its own. Put simply, a smart grid works through a network of sensors that alert the system to a threat. Consider the example of a tripped line. A sensor would detect the trip and automatically reroute power in a way that would prevent other lines from taking on too much load and tripping themselves. Failures leading up to the 2003 blackout cascaded the way they did, in part, because the engineers at the control stations had no way of knowing that the transmission lines had tripped in time to take the necessary actions. Smart grid technology, if fully implemented, would
allow the grid to both detect and respond to disturbances on its own so that failures are less likely to cascade.\textsuperscript{214}

The widespread success of this idea relies heavily on technology. This includes:

\textquote{...overcoming today’s limitations on temperature, robustness, versatility, and size [of sensors]} in order to “facilitate fulfillment of a number of long-standing power system needs, including real-time characterization of plant emissions and waste streams, distributed measurement of transformer winding temperatures, and on-line monitoring of pH in steam plant circulation water.}\textsuperscript{215}

Fiber optics are also crucial for implementation because they are small and are not adversely affected by magnetic interference.\textsuperscript{216}

While society has come a long way technologically, scholars note that a large barrier to smart grid implementation is institutional. As the grid has grown, its processes have become more interwoven. This is especially true when discussing a specific region like the Great Lakes, where different ISOs’ areas of responsibility are inherently connected. While regional authorities and public-private partnerships have increased cooperation between individual companies and ISOs, scholars note that these institutions are not nearly as well networked as the critical energy infrastructure they oversee.\textsuperscript{217}

There are also major security concerns that arise with the advent of smart grid technologies. As more infrastructure becomes reliant on control systems, control centers become a more significant vulnerability for the power grid.\textsuperscript{218}

Aging infrastructure is also a concern for the adaptation of new technologies. Much of the grid’s current assets are not compatible with these new technologies. Since self-healing smart grid initiatives require widespread implementation to be successful on a regional or national scale, obsolete infrastructure will need to be replaced for these initiatives to reach their full potential.\textsuperscript{219}

The academic community, as well as homeland security companies and partnerships, widely contend that the most immediate challenge in making the power grid more resilient lies in coordination and information sharing. Despite the technical measures in place and in development to monitor the grid and help it respond to threats, the information is only useful if it is shared effectively. Smart grid technology would enable different parts of the system to communicate with each other and react to threats, but requires universal adaptation to work effectively. This issue presents both an opportunity and a challenge to the critical power infrastructure community going forward.

\textbf{10.4 Recovery}

As part of the study, the team collected data from the EIA that fell within the scope of major blackouts (at least 50,000 people affected for at least 24 hours) from 2003-2010 (see Appendix D). The raw data demonstrates a virtually level trend within the scope in the average number of people affected per blackout over time. The team further examined the data in terms of the Customer Average Interruption Duration Index (CAIDI), (i.e., how long the average customer affected by a major outage in a given year was out of power) to control for the number of people affected (see Figure 10-3). A descriptive analysis of the data using this measure demonstrates fluctuating values with an upward trend over the study period.
As snow and ice tend to make roads far more impassable than rain or wind, one can expect that blackouts caused by snow and ice storms would take longer to fix than ones caused by rain. The data in Figure 10-1 corroborates this assumption. However, the data found little variation in the number of people affected by the cause of blackouts, though snow and ice storms tended to affect fewer people, as shown in Figure 10-2.

These observations lend further weight to a Carnegie Mellon study’s findings, which indicated that the frequency of large blackouts has not decreased in recent years.220

While these data provide useful insight about our ability to recover, they are not sufficient to assess recovery as a general concept. Other variables, such as the size of the area impacted, can affect recovery time. For example, an outage affecting 50,000 people in a rural area would take longer to recover from than one in an urban area because the infrastructure is more dispersed. There is no open-source metric to assess recovery considering this complexity.

![Average Duration (Hours)](image)

**Figure 10-1.** Average duration of blackouts, by cause
Figure 10-2. Average number of people affected by blackouts, by cause.

Figure 10-3. Length of time without power due to blackouts, 2000–2010.
Notes


209 National Infrastructure Advisory Council, 2010, p. 46-48; U.S. Department of Homeland Security and U.S. Department Energy 2010, p. 48. For a more technical explanation of these key concerns, see Appendix D of the cited report, which explains a mathematical model that can be used to assess resilience.


214 Amin, 2010; Amin and Stringer, 2011; Gellings, Samotyj, and Howe, 2004; Moslehi et al., 2005.


218 Campbell, 2011, p. 6.

219 Brown and Willis, 2006, p. 37; Gellings, et al., 2004, p. 44.

11. The U.S. – Canada Relationship
11. The U.S. – Canada Relationship

The eastern interconnect, which encompasses the power structure in the Eastern United States and Eastern Canada, is a structurally interdependent system. The legal and regulatory environment needs to be able to support this interdependency while adhering to the two countries’ policies governing energy generation and transmission. As a result, power that moves between Canadian provinces and U.S. states is controlled in much the same way as power that moves between different U.S. states and ISOs. Also similar to the way transfers are handled within the U.S., different ISOs have different policies for trading power with Canada. This section discusses the basic regulations that govern the transfer of electricity between the United States and Canada and provides a few examples of the way this works for different ISOs.

11.1 The Regulatory and Trade Environment

While the power systems in the U.S. and Canada are interconnected, the two countries have different laws that guide the movement and control of assets, such as energy, across borders. The current regulatory environment allows for the transfer of energy under guidelines that adhere to the respective countries’ policies. As mentioned earlier in this report, the power grid is broken up into several regional ISOs for control purposes. ISOs work to prevent unexpected power flows into their region by scheduling hourly flows between regions (called intertie flows). While this allows system operators to focus more heavily on their own area, it complicates the transportation of electricity over long distances. One of the issues that can arise is that each system operator involved in a transaction can terminate it at any given time. Furthermore, anytime the electricity crosses an international border, it is subject to tariffs and taxes, since in the absence of coordinating agreements, there are transmission service charges between the Canadian and American transmission systems. Utilities must also obtain an Order of Commission to import energy from or export energy to Canada.

Despite the initial red tape, regulations have sought to facilitate energy trade between the two countries. When exporting to the United States, all Canadian provinces must abide by standards laid out in the Energy Policy Act of 2005 (EPAct 2005). In an attempt to ameliorate the international power trade, an April 2002 FERC order made the markets in Canada and the U.S. more uniform by standardizing generator interconnection agreements. To further aid in making power transfers between countries smoother, the power lines that cross borders are monitored by the Canadian NEB (National Energy Board) and the US NERC per a 2008 MOU between the US and Canada.

11.2 ISO International Market Policies

11.2.1 IESO

IESO, the ISO for Ontario, uses a single energy price for the entire ISO and treats adjacent ISOs in the same manner. To trade power using Ontario’s ISO, a utility must submit import and export bids, which are accepted or rejected independently. There is also no mechanism to ensure that these are simultaneously scheduled. One hour before the transactions are to be managed
Ontario sends out a schedule of the intertie flows, but this does not account for Ontario’s transmission capacity, which is much different from NYISO’s. Also, participants in IESO decide for themselves when to turn generators on and off, which is not a luxury granted to utilities in most other ISOs. Ontario provides net importers an “intertie offer guarantee” to protect against changes in electricity prices that are reset every five minutes, so that transactions are not reneged because it is not economic to do them.226

11.2.2 NYISO

Unlike Ontario, New York uses a “nodal” energy market; i.e., prices are not constant throughout the ISO to account for the transmission capacity in the region (e.g., energy is far more expensive in Long Island than in northern New York). New York sets its energy prices a day ahead of time and deals with power exports and imports for the entire neighboring ISO as opposed to each individual intertie. Similar to IESO, exports from NYISO and their corresponding imports are not reported simultaneously but rather through two transactions with each ISO, which means that one transaction could be approved, while the other may not be, negating the transaction. While NYISO strives to have all imports and exports scheduled in the day-ahead market, it sometimes accommodates neighboring ISOs by scheduling transactions less than a day in advance, which is what Ontario tends to do.

11.2.3 PJM

PJM also operates in a different fashion than IESO or NYISO. For PJM the location of the buyer and seller impacts the price depending on how congested the transmission lines in the area are. Also, PJM uses an auctioning system that matches bids and offers in a spot market where transactions can take place almost immediately, which contrasts heavily with NYISO’s policy. As a result, PJM’s market is very volatile. PJM also has a day ahead market, which functions similar to NYISO’s, in which electricity is purchased for a specified time the following day.227 Excess or insufficient purchases are often rectified with additional transactions on the spot market.

11.2.4 MISO

MISO is the only ISO in the study region that oversees U.S. states and a Canadian province (Manitoba); therefore, Manitoba’s relationship with MISO provides a different perspective on the energy relationship between the U.S. and Canada as Manitoba has maintained a coordinating agreement with MISO since 2001. Manitoba is required to follow NEB and provincial regulations, though it may also have to follow some NERC regulations as defined by the coordinating agreement (for example, Manitoba must let MISO know how much available transmission line space there is).228 MISO permits Manitoba to sell its excess energy to any other MISO member, as opposed to having to have to sell through multiple contracts. That being said, the four major ISOs which make up the Great Lakes Region (IESO, NYISO, PJM and MISO), all operate in different manners.229
Notes

221 Ring, Ruff, & Hannan, 2008, p. 2.
225 National Energy Board n.d.
226 Ring et al., 2008, p. 4.
229 Manitoba Hydro 2011, pp. 3, 6.
12. Initiatives
12. Initiatives

In order to address concerns brought about by the blackout on August 14, 2003, as well as general security in the wake of September 11th, 2001, the pipeline and electric industries have taken a number of measures to improve the reliability and security of their systems. Industry has partnered with state, federal, and local agencies to accomplish this broad safety and security approach.

12.1 Electric

Following the August 14, 2003, blackout, the federal government and electric industry took many steps to improve the reliability of the grid. The blackout was an impetus for a task force that examined the reliability of the grid, not just in 2003, but also in earlier blackouts dating back to 1965. It provided a number of recommendations, many of which have been enacted in some way in federal law and regulation or industry standards.

12.1.1 Federal, State and Local Initiatives

The Federal government has taken an active role in enhancing the reliability of the grid through legislation, as well as the regulatory power of the FERC. Perhaps the greatest step in improving grid reliability and security was the passage of the Energy Policy Act of 2005. This law issued many requirements; some key ones are listed below:

- Designated an Electric Reliability Organization (ERO) to develop reliability standards with FERC approval. FERC designated NERC as the ERO.
- Empowered FERC and NERC to enforce existing standards through sanctions
- Empowered FERC to develop incentives for utilities to promote efficient generation and transmission
- Assigned DOE to study electric grid transmission congestion every three years
- Initiated provisions to ease the process of constructing transmission lines in designated congestion areas
- Permitted Federal Power Authorities to join ISOs/RTOs
- Established provisions to promote the development of a smart grid
- Established provisions to promote demand response programs
- Enhanced physical security and screenings at nuclear energy facilities

Another law, the Energy Independence and Security Act of 2007, included provisions to promote the use of Smart Grid technologies.
At the regulatory agency level, FERC and NERC have instituted standards to comply with EPAct 2005, as well as to correct issues that resulted in the 2003 Blackout, such as vegetation management under NERC order FAC-003-1. They have also sought to improve training for individuals involved in transmission and reliability management.\textsuperscript{252} In dealing with issues of security, NERC has issued guidelines for physical security, including annexes for specific pieces of infrastructure, as well as cyber security.\textsuperscript{235}

To promote information sharing among security agencies and utilities, as well as other private industries, DHS developed the Protected Critical Infrastructure Information (PCII) program.\textsuperscript{234} DHS has also sought to curtail the threat of high voltage transformer loss by developing the National Emergency Energy Spare Parts Program, which sought to fund the development of transformers that could fit in standard shipping containers. A strong focus has also been placed on increasing physical security around critical facilities.\textsuperscript{235}

12.1.2 Owner/Operator Initiatives

Owners and operators have undertaken many steps to protect electric infrastructure through increased security and reliability. In particular, utilities in the Great Lakes region rely on the management and requirements of their ISOs/RTOs to help determine what steps are necessary to improve reliability. ISOs/RTOs in turn take many of their standards and requirements from those delineated by FERC and NERC. Many of these organizations cooperate with each other and with the federal regulatory agencies in order to draft standards.

One reliability program instituted at the utility level is the establishment of demand response programs. These programs, supervised at the ISO/RTO level, allow private customers to contract a reduction in power consumption upon request during high demand periods. These customers are provided with incentives in order to respond to a request and can be removed from the program if they fail to comply.\textsuperscript{236}

Owners and operators have also sought to improve the training of their control and reliability employees.

12.2 Pipelines

Overseen by the PHMSA in matters of safety, and the TSA in matters of security, the pipeline industry has taken numerous steps to improve both in recent years. Industry organizations such as the API, AGA, and INGAA have worked together to develop a number of initiatives. These organizations are part of their respective coordinating committees, as outlined by the NIPP.

12.2.1 Federal, State and Local Initiatives

Under the NIPP, the federal government has sought to take a much larger role in the development of security procedures for the pipeline sector. Discussed in the Pipeline Modal Annex of the Transportation Systems Sector Specific Plan are many of the guidelines laid out for the industry to follow.
TSA has taken numerous steps organizationally in order to improve pipeline security including:

- Development of pipeline security guidelines for all facilities, not just critical ones\textsuperscript{237}
- Development of cyber security education\textsuperscript{238}
- Guidelines for various security reviews (Threat, Risk and Vulnerability Assessments)
- The development of an on-site Corporate Security Review Program\textsuperscript{239}
- Development of a critical facilities list
- Inspection of critical facilities\textsuperscript{240}
- Ten stakeholder conference calls annually\textsuperscript{241}
- International Pipeline Security Forum\textsuperscript{242}
- Information Sharing Portal\textsuperscript{243}

These major initiatives have allowed TSA to set goals to measure the success of increased pipeline security. While many of these programs have been successful, a review by the Government Accountability Office (GAO) found TSA to be lacking in proper performance measures. Specifically, after providing recommendations during a review, TSA does not follow up with a critical facility.\textsuperscript{244} The GAO recommends a system be developed to allow for this kind of review. TSA must also be able to measure its role in monitoring the security posture of the pipeline industry\textsuperscript{245}

From a safety perspective the PHMSA has implemented guidelines in order to protect pipelines from common threats. PHMSA regulations require the development of public awareness programs.\textsuperscript{246} In addition, to mitigate the threat of excavation damage, 811 one-call centers were established under federal law in 2007. These numbers provide diggers with information on pipeline infrastructure near a dig site.\textsuperscript{247}

\textbf{12.2.2 Owner/Operator Initiatives}

Operators have been cooperative with TSA, implementing the voluntary security measures and improving their security posture.\textsuperscript{248} In addition, industry organizations, representing pipeline operators, have played an important role in improving the security of the pipeline system through participation in many federal programs and the development of their own industry-wide programs. For instance the API has developed an informative report on proper security guidelines for the petroleum industry.\textsuperscript{249} These organizations have also developed programs that train operators in security subjects and provide forums for security discussion.\textsuperscript{250}

Operators and their organizations also play a large role in the development of safety programs related to the reliability of pipeline infrastructure. These institutions host public education and awareness workshops regarding excavation issues and what to do in the event of a leak.\textsuperscript{251} A listing of government and owner/operator initiatives from the Pipeline Model Annex is available in Appendix C.
Notes

235 Congressional Research Service 2005, 5
236 New York State Independent Service Operator, n.d.
239 U.S. GAO 2010, p. 28.
240 U.S. GAO 2010, p. 32.
242 U.S. GAO 2010, p. 49.
244 U.S. GAO, p. 39.
245 U.S. GAO, p. 57.
246 Pipeline and Hazardous Materials Safety Administration, *PHMSA Stakeholder Communications: Public Awareness Programs* n.d
249 American Petroleum Institute, 2005.
13. Conclusions
13. Conclusions

This study was designed to assess the current level of resilience, security posture, and economic dependencies of critical energy infrastructure in the U.S. states and Canadian provinces surrounding the Great Lakes. In particular, the research team set out to answer seven questions:

1. What are the current levels of resilience of the electric and pipeline infrastructure in this region?
2. What federal, state, and local security initiatives have occurred since the 2003 outage?
3. What owner/operator or association activities have taken place to increase the security and resilience of electric infrastructure in this region?
4. What pipeline and electrical connectivity exists?
5. What dependencies exist between electric and pipeline infrastructure and essential community services or other major critical infrastructure?
6. What are the direct relationships between employment, technology, and innovation in regard to the concentration of very important energy infrastructure in this region?
7. What are the economic dependencies within the U.S. of Canadian-produced power sold to the GLHC members?

This section outlines the research team’s conclusions concerning these questions as well as the general threats, vulnerabilities, consequences, and resilience related to the critical energy infrastructure in the region.

The major themes that are pervasive throughout the conclusions are the benefits and security challenges that cyber infrastructure brings to the electric grid and the implications of aging electric infrastructure on the industry. Utilities and authorities in charge of the power grid are beginning to implement self-healing smart grid technologies designed to facilitate real-time information sharing and further automate the grid’s response to threats. These technologies have the potential to dramatically increase the grid’s resilience and reliability but bring with them significant cyber security concerns. The aging infrastructure within the grid threatens to decrease the grid’s resiliency and make it more vulnerable to failure. Both trends create opportunities for innovation and employment moving forward.

Current Levels of Resiliency

1. The energy industry in the Great Lakes Region, and around the country, has built in highly redundant mechanisms to withstand hazards and prevent disruptions from cascading. Efforts to maintain and improve this capability in the power grid present challenges to the electric industry.
Scholars and industry experts agree that the power grid in the United States operates at over 99.9 percent reliability at any given time. This statistic reflects the industry’s strong efforts to continually and reliably provide power to its customers. As the demand for electricity climbs, the issues and difficulties the industry faces increase in terms of mitigating hazards and containing failures to prevent them from cascading into major outages. As discussed in the description of the power grid, generation and transmission operators use a variety of systems to monitor the grid in real time. Information and support are shared dynamically between utilities, states/provinces, and ISOs to manage any loss of transmission or generation capability. The regulatory environment also provides annual feedback to ISOs, utilities, and governments in the form of reliability reporting so that the industry can continue to improve. The experts consulted during the focus group further explained that, as a result of these measures, it would take a series of well-timed, coordinated disruptions to cause serious damage.

The industry is working to further improve on its ability to share and react to real-time information through self-healing grid and smart grid initiatives. These technological advances present both an opportunity and a challenge. Widespread implementation would benefit everyone involved, but it would be costly. As mentioned in the section on resiliency, a portion of the region’s current infrastructure may be outdated to the point where it is incompatible with new technologies. Further, as the grid becomes more reliant on digital systems, it becomes more vulnerable to cyber intrusion. The industry will need to continue its efforts to secure its SCADA systems as they become an even more integral and automated part of the grid’s operation.

Sources in the literature that discuss vulnerabilities and the industry also present evidence that maintaining resilience levels is becoming more costly. Maintenance costs increase as lines get older. During the focus group, the industry experts agreed that if left unchecked, aging infrastructure will contribute to a downward trend in grid reliability. Utilities will need to determine when it becomes more efficient to replace the infrastructure than to repair it.

The literature on pipeline security portrays a highly-resilient system that isolates failures to small portions of the infrastructure. Most petroleum and natural gas pipelines are underground, making them difficult to access and less vulnerable to most weather events, such as wind and snow storms. In the event of a pipeline rupture, the flow is immediately and automatically cut off by sensors in the line. Redundancies within the system often make up for the short-term loss of flow. Sources explain that operators are quick to replace the ruptured section of pipeline to get it back in service.

2. There is a dearth of open source literature on trends describing how quickly the power grid recovers from an outage. Data collected suggests that the industry may not be improving in this capacity.

The survey of the literature did not uncover any discussion on how quickly the industry recovers from blackouts. As mentioned in the section on resilience, the “recovery” is difficult to measure; however, the data collected from the EIA suggests that, despite the industry’s efforts and government initiatives, the industry may not be improving in its ability to recover from an outage. While this trend is not definitive, it demonstrates a need for more open-source study on
the industry’s ability to recover from major events. The industry experts who participated in the focus group cite aging infrastructure as a possible reason for this trend. They point out that while the capacity for recovery may be improving, it is becoming more difficult to do so quickly as the infrastructure ages.

**Government and Utility Security Initiatives and Activities**

3. Federal, state, and local governments and energy utilities are working together in a strong push to improve energy security and resiliency throughout the region.

*Electric*

The Report of the U.S.-Canada Task Force on the August 14, 2003, blackout presented many recommendations to the federal government and utilities in order to guide their efforts to mitigate potential events moving forward. Congress and FERC worked with the utilities to develop legislation and regulations seeking to improve the reliability and security of the grid. These gave the FERC and NERC enforcement powers over utilities. The collaboration has seen much of the Task Force recommendations implemented nationwide and even further standards established at the state and local levels. Efforts have been made to reduce congestion, promote the development of a smart grid, and reduce demand concerns. Better security measures have also been put into place across the industry.

*Pipelines*

Since September 11th, 2001, the federal government has partnered with the petroleum and natural gas industries to increase the security of the pipeline network. The Pipeline Modal Annex to the Transportation Sector Specific Plan, along with security guidelines at the federal and industry levels, has driven the successful implementation of voluntary measures in most facilities across the region. A Corporate Security Review process ensures that these measures are properly in place.

PHMSA has led the initiatives to increase safety and reliability of the pipeline network through its own efforts to collect information on incidents. Public education campaigns led by the industry, partnered with federally mandated one-call centers, have sought to mitigate the most common threat to pipelines, excavation damage.

**Interdependencies between Pipelines and Electric Infrastructure**

4. Petroleum pipelines are dependent on electricity; natural gas pipelines are typically not.

The literature’s discussion on vulnerabilities shows interdependencies between the pipeline and electric infrastructures in which each sector is dependent on the other. Natural gas pipeline networks are generally not dependent on the electrical infrastructure because most compressor stations are powered by the gas transported in the system. Should the electric system be disrupted, natural gas pipelines have the means to continue operation. Meanwhile, petroleum pipelines are completely dependent on the electric system to power pumps and other infrastructure. Should the electric system be disrupted, petroleum pipelines have enough backup generation to properly shutdown the system; however, the pipelines would be unable to transport petroleum until the power is restored.

13. Conclusions
5. Electric Generation in the region is dependent on natural gas supply, but not on petroleum

As explained in the electric vulnerabilities section, the electric network is dependent on the supply of natural gas to generators. In the Great Lakes region, natural gas accounts for 10% of all generation, and even greater in certain states. While reserves would be able to support the system in the off-season, if there was a loss of supply in the peak use period for natural gas (winter) it could impact generation capacity. This would need to be offset with imports of gas from elsewhere. Petroleum only accounts for about 1% of the region’s generation, so power infrastructure in the Great Lakes States and Ontario is not critically dependent on petroleum.

Dependencies with Critical Infrastructure and Essential Community Services

6. The first and second order effects of a long-term power disruption in the region would impact every critical infrastructure sector—most prominently, banking and finance, food and agriculture, manufacturing, transportation, and water.

In the critical infrastructure Sector-Specific Plans, DHS and its partner agencies reveal a web of resources that is highly dependent on energy. This implies that if energy is cut off in a region, the critical infrastructure in that region would be severely crippled across the board. Government and financial reporting following the August 14, 2003, blackout indicated serious financial losses to the Banking and Finance, Food and Agriculture, and Manufacturing sectors. Many essential community services were also limited or shut down, including public transportation, traffic control, and in some cases, water treatment facilities.

Employment and Technology

7. As the energy sector looks for new technologies to replace and improve the aging electric and pipeline infrastructure, the market for skilled workers and innovative ideas will continue to expand.

In a presentation to the EIA’s 2008 Energy Conference, David Owens, Executive Vice President of the Edison Electric Institute, emphasized the importance of “creating excitement around engineering, mathematics and science...to replace the aging workforce and encourage the next round of technical and strategic leaders.” The experts the team spoke to agree with the concern that the incoming generation of leaders in the energy field may not be able to fill the gap that will be left when the current generation retires. New leaders in the field must have the expertise to deal with the problems facing the current generation and usher in new and innovative ideas for modernizing the grid. The market for this expertise in the Great Lakes region, where critical power infrastructure is older and more concentrated than in most other regions, should expand rapidly over the next decade.

The industry’s continued progress toward a self-healing smart grid should also spark demand for innovative ideas on how to efficiently and effectively implement and improve these systems across the grid. As explained in the section on resilience, there are significant but surmountable technological, structural, and organizational barriers to implementing these new technologies.
13. Conclusions

grid-wide. The region has a need for ideas and technologies that help efficiently overcome these barriers.

The Partnership between the United States and Canada

8. Canada is a vital part of the Great Lakes Region’s energy infrastructure.

Canada and the United States are strong partners in the power grid. Structurally, energy is transferred between the two countries in the same way that it is transferred between U.S. states. The regulatory environment is designed to facilitate both a seamless transfer of energy and a highly cooperative environment while adhering to both countries’ laws. The GLHC is a strong example of how the U.S. and Canada work together to improve the mutual security posture and resilience of their critical energy infrastructure.

Threats and Vulnerabilities

9. Natural forces are the most significant threat to the electric grid, and equipment failure is the most significant threat to petroleum and natural gas pipelines.

Electric

Industry experts and the literature have expressed that natural forces are the greatest threat to the electric grid, exploiting openly accessible transmission systems. The data collected and presented in the discussion of blackouts from 2003 to 2010 shows that weather instances such as rain, wind and snow have been the primary cause of electric failure.

Additional threats exist from equipment failure and other accidental incidents. The aging infrastructure in the electric grid (70% of current transmission lines are 25 years old or more) has contributed to increasing equipment failure, making this an area of growing concern. There is also the constant threat of deliberate attack by terrorists or disgruntled employees. While these threats are always a concern the industry must pay attention to, regulators and utilities must focus on mitigating the failures that result from natural events.

Pipeline

The pipeline infrastructure is considered the safest transportation system in the country; however, there are still natural and man-made threats that could disrupt the flow of natural gas or petroleum. When examining threats to the pipeline infrastructure, the data shows that equipment failure is the most prevalent cause of incident. Corrosion and welding issues materialize with age and improper maintenance. Excavation damage is of special concern because it is an easily avoidable human threat. Natural forces pose less of a threat to pipelines because they are underground, but this does not protect the system from changes in the environment such as flooding or earthquakes. Finally, as with the electric system, the pipeline industry must always be prepared for a deliberate attack from malicious actors.

10. Terrorism remains a significant concern for the energy sector; however, in the study period there were no open source indications of a specific threat made against critical energy infrastructure.
While natural forces and equipment failure are the primary threats to electric and pipeline infrastructure, respectively, evidence in the threat literature has shown terrorists willing to attack critical energy infrastructure in other countries. The success of attacks abroad suggest that even though openly available information shows no direct threat made against the United States energy infrastructure, the industry must be prepared to protect critical facilities with proper physical and cyber security. Regulatory agencies and both industries have taken steps to increase physical security and develop protocols to defend against cyber intrusion. While during the study period no threat has been made, the industry must remain vigilant in the face of a persistent enemy.

11. Transmission lines are the most vulnerable aspect of the power grid; pipelines are the most vulnerable in petroleum and natural gas transmission systems.

Electric

Industry experts and the literature agree that transmission lines are the most vulnerable infrastructure in the electric grid. From an attack perspective, this arises from a lack of physical security and the remote nature of the transmission system. Transmission lines are also vulnerable to natural forces because they are exposed. The increasing age of the transmission infrastructure further contributes to its vulnerability. The literature shows that there has been a lack of real investment in transmission infrastructure since the 1960s because the industry’s focus, until very recently, was on generation. Sources in the literature have found that age of the transmission system increases the chance of failure as well as the cost of repair.

Pipeline

In the pipeline sector, the actual pipeline segments are the greatest vulnerability. The threat of corrosion and excavation is exacerbated by deterioration and poorly marked lines, respectively. Regulatory agencies report that while not the number one cause of incidents, vulnerability to excavation can be mitigated through public education and awareness programs. The industry suggests that aging has little role in increasing the vulnerability of a pipeline system, arguing good integrity management can prevent most failure. Pipeline segments are also vulnerable to environmental changes that disrupt their foundation soil, such as earthquakes and flooding. These incidents could disrupt a pipeline by displacing the sediment bed.

Notes

252 Owens 2008, p. 26
14. Recommendations
14. Recommendations

Based on the conclusions of this study, the research team offers the following recommendations for future work:

1. Explore methods of improving and replacing the aging electrical transmission infrastructure in the region and ways the industry can further mitigate the impact of hazards on these assets.
2. Study the pipeline network’s ability to maintain its performance over the next 15-20 years, considering the impacts of aging infrastructure and new technologies.
3. Develop a specific definition and measure for post-outage recovery as it relates to the resilience of critical energy infrastructure.
4. Study key customers’ efforts to mitigate the effects of outages. Determine how these resilience efforts relate to the collective ability to recover.
5. Study the energy sector’s need for skilled workers over the next 10-15 years and determine where gaps exist or are likely to develop.
6. Maintain and continue to improve collaboration and information sharing efforts between federal, state, provincial, and local governments and energy utilities.
15. Bibliography
15. Bibliography


15. Bibliography


15. Bibliography


15. Bibliography

89


Appendices
## Appendix A: Major U.S. Power Plants within 75 miles of the Great Lakes

### Major Power Plants within 75 Miles of the Great Lakes (Op. MW >500)

<table>
<thead>
<tr>
<th>Name of Plant</th>
<th>Utility</th>
<th>County</th>
<th>State</th>
<th>Op. MW (2007)</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES Somerset LLC</td>
<td>AES Somerset LLC</td>
<td>Niagara</td>
<td>NY</td>
<td>655.1</td>
</tr>
<tr>
<td>Aurora</td>
<td>Reliant Energy Power Gen Inc</td>
<td>DuPage</td>
<td>IL</td>
<td>1275</td>
</tr>
<tr>
<td>Avon Lake</td>
<td>Orion Power Midwest LP</td>
<td>OH</td>
<td></td>
<td>870</td>
</tr>
<tr>
<td>B C Cobb</td>
<td>Consumers Energy Corp.</td>
<td>Muskegon</td>
<td>MI</td>
<td>519.6</td>
</tr>
<tr>
<td>Bailly</td>
<td>Northern Indiana Pub Serv Co.</td>
<td>Porter</td>
<td>IN</td>
<td>641</td>
</tr>
<tr>
<td>Bay Shore</td>
<td>Toledo Edison Co.</td>
<td>Lucas</td>
<td>OH</td>
<td>655.4</td>
</tr>
<tr>
<td>Belle River</td>
<td>Detroit Edison Co</td>
<td>St Clair</td>
<td>MI</td>
<td>1664.4</td>
</tr>
<tr>
<td>Covert Generating Project</td>
<td>Covert Generating Co LLC</td>
<td>Van Buren</td>
<td>MI</td>
<td>1176</td>
</tr>
<tr>
<td>D E Karn</td>
<td>Consumers Energy Corp.</td>
<td>Bay</td>
<td>MI</td>
<td>1946.3</td>
</tr>
<tr>
<td>Davis Besse</td>
<td>Toledo Edison Co.</td>
<td>Ottawa</td>
<td>OH</td>
<td>925.2</td>
</tr>
<tr>
<td>Dean H Mitchell</td>
<td>Northern Indiana Pub Serv Co.</td>
<td>Lake</td>
<td>IN</td>
<td>537.6</td>
</tr>
<tr>
<td>Donald C Cook</td>
<td>Indiana Michigan Power Co</td>
<td>Berrian</td>
<td>MI</td>
<td>2285.3</td>
</tr>
<tr>
<td>Dresden</td>
<td>Exelon Generating Co. LLC</td>
<td>Grundy</td>
<td>IL</td>
<td>1824</td>
</tr>
<tr>
<td>Dunkirk Generating Station</td>
<td>Dunkirk Power LLC</td>
<td>Chautauqua</td>
<td>NY</td>
<td>627.2</td>
</tr>
<tr>
<td>Eastlake</td>
<td>Cleveland Electric Illuminating Co</td>
<td>Lake</td>
<td>OH</td>
<td>1289</td>
</tr>
<tr>
<td>Edgewater (WI)</td>
<td>Wisconsin Power &amp; Light Co</td>
<td>WI</td>
<td></td>
<td>770</td>
</tr>
<tr>
<td>Elgin Energy Center</td>
<td>Ameren Energy Generating Co</td>
<td>Kane</td>
<td>IL</td>
<td>540</td>
</tr>
<tr>
<td>Elwood Energy</td>
<td>Dominion Elwood Services Co</td>
<td>Will</td>
<td>IL</td>
<td>1728</td>
</tr>
<tr>
<td>Fermi</td>
<td>Detroit Edison Co</td>
<td>Monroe</td>
<td>MI</td>
<td>1281</td>
</tr>
<tr>
<td>Fisk Street</td>
<td>Midwest Generations EME LLC</td>
<td>Cook</td>
<td>IL</td>
<td>662.8</td>
</tr>
<tr>
<td>Fox Energy Center</td>
<td>Fox Energy Center LLC</td>
<td>WI</td>
<td></td>
<td>620</td>
</tr>
<tr>
<td>Greenwood</td>
<td>Detroit Edison Co</td>
<td>St Clair</td>
<td>MI</td>
<td>1071.3</td>
</tr>
<tr>
<td>Independence Station</td>
<td>Sithe/Independence Power Part LP</td>
<td></td>
<td>NY</td>
<td>1086.1</td>
</tr>
<tr>
<td>J H Campbell</td>
<td>Consumers Energy Corp.</td>
<td>Ottawa</td>
<td>MI</td>
<td>1604.5</td>
</tr>
<tr>
<td>James A Fitzpatrick</td>
<td>Entergy</td>
<td>Oswego</td>
<td>NY</td>
<td>882</td>
</tr>
<tr>
<td>Joliet 29</td>
<td>Midwest Generations EME LLC</td>
<td>Will</td>
<td>IL</td>
<td>1320</td>
</tr>
<tr>
<td>Kendall County Generation Facility</td>
<td>LSP-Kedall Energy LLC</td>
<td>Kendall</td>
<td>IL</td>
<td>1256</td>
</tr>
<tr>
<td>Kewaunee</td>
<td>Wisconsin Public Service Corp.</td>
<td>Kewaunee</td>
<td>WI</td>
<td>560.1</td>
</tr>
<tr>
<td>Kinder Morgan Power Jackson</td>
<td>Kinder Morgan Power Co</td>
<td>Jackson</td>
<td>MI</td>
<td>649</td>
</tr>
<tr>
<td>Lincoln Energy Center</td>
<td>Lincoln Generating Facility LLC</td>
<td>Will</td>
<td>IL</td>
<td>692</td>
</tr>
<tr>
<td>Ludington</td>
<td>Consumers Energy Corp.</td>
<td>Mason</td>
<td>MI</td>
<td>1978.8</td>
</tr>
<tr>
<td>Michigan City</td>
<td>Northern Indiana Pub Serv Co.</td>
<td>La Porte</td>
<td>IN</td>
<td>680</td>
</tr>
<tr>
<td>Midland Cogeneration Venture</td>
<td>Midland Cogeneration Venture</td>
<td>Midland</td>
<td>MI</td>
<td>1853.1</td>
</tr>
<tr>
<td>Monroe</td>
<td>Detroit Edison Co</td>
<td>Monroe</td>
<td>MI</td>
<td>3293.1</td>
</tr>
<tr>
<td>Moses Niagara</td>
<td>New York Power Authority</td>
<td>NY</td>
<td></td>
<td>2429.1</td>
</tr>
<tr>
<td>Moses Power Dam</td>
<td>New York Power Authority</td>
<td>NY</td>
<td></td>
<td>912</td>
</tr>
<tr>
<td>Nine Mile Point Nuclear Station</td>
<td>Nine Mile Point Nuclear Station</td>
<td>Oswego</td>
<td>NY</td>
<td>1901.1</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------</td>
<td>--------</td>
<td>----</td>
<td>--------</td>
</tr>
<tr>
<td>Oswego Harbor Power</td>
<td>NRG</td>
<td>Oswego</td>
<td>NY</td>
<td>1803.6</td>
</tr>
<tr>
<td>Palisades</td>
<td>Consumers Energy Corp.</td>
<td>Van Buren</td>
<td>MI</td>
<td>811.8</td>
</tr>
<tr>
<td>Perry</td>
<td>Cleveland Electric Illuminating Co</td>
<td>Lake</td>
<td>OH</td>
<td>1311.6</td>
</tr>
<tr>
<td>Pleasant Prairie</td>
<td>Wisconsin Electric Power Co</td>
<td>Kenosha</td>
<td>WI</td>
<td>1235</td>
</tr>
<tr>
<td>Point Beach</td>
<td>Wisconsin Electric Power Co</td>
<td>Manitowoc</td>
<td>WI</td>
<td>1072.6</td>
</tr>
<tr>
<td>Port Washington</td>
<td>Wisconsin Electric Power Co</td>
<td>WI</td>
<td>1182</td>
<td></td>
</tr>
<tr>
<td>PPL University Park Power Project</td>
<td>PPL University Park LLC</td>
<td>IL</td>
<td>540</td>
<td></td>
</tr>
<tr>
<td>Presque Isle</td>
<td>Wisconsin Electric Power Co</td>
<td>Marquette</td>
<td>MI</td>
<td>624.7</td>
</tr>
<tr>
<td>R E Ginna Nuclear Power Plant LLC</td>
<td>R E Ginna Nuclear Power Plant LLC</td>
<td>Wayne</td>
<td>NY</td>
<td>614</td>
</tr>
<tr>
<td>R M Schahfer</td>
<td>Northern Indiana Pub Serv Co.</td>
<td>Jasper</td>
<td>IN</td>
<td>2201.3</td>
</tr>
<tr>
<td>Renaissance Power LLC</td>
<td>Renaissance Power LLC</td>
<td>Montcalm</td>
<td>MI</td>
<td>680</td>
</tr>
<tr>
<td>River Rouge</td>
<td>Detroit Edison Co</td>
<td>Wayne</td>
<td>MI</td>
<td>944</td>
</tr>
<tr>
<td>South Oak Creek</td>
<td>Wisconsin Electric Power Co</td>
<td>Milwaukee</td>
<td>WI</td>
<td>1211.2</td>
</tr>
<tr>
<td>St Clair</td>
<td>Detroit Edison Co</td>
<td>St Clair</td>
<td>MI</td>
<td>1570.9</td>
</tr>
<tr>
<td>State Line Energy</td>
<td>State Line Energy LLC</td>
<td>Lake</td>
<td>IN</td>
<td>613.8</td>
</tr>
<tr>
<td>Trenton Channel</td>
<td>Detroit Edison Co</td>
<td>Wayne</td>
<td>MI</td>
<td>775.5</td>
</tr>
<tr>
<td>Troy (OH)</td>
<td>Troy Energy LLC</td>
<td>OH</td>
<td>688</td>
<td></td>
</tr>
<tr>
<td>Waukegan</td>
<td>Midwest Generations EME LLC</td>
<td>Lake</td>
<td>IL</td>
<td>914.7</td>
</tr>
<tr>
<td>West Lorain</td>
<td>Ohio Edison Co.</td>
<td>Lorain</td>
<td>OH</td>
<td>555.6</td>
</tr>
<tr>
<td>Whiting Clean Energy Inc</td>
<td>NiSource Inc.</td>
<td>Lake</td>
<td>IN</td>
<td>639</td>
</tr>
<tr>
<td>Will County</td>
<td>Midwest Generations EME LLC</td>
<td>Will</td>
<td>IL</td>
<td>1268.8</td>
</tr>
<tr>
<td>Zeeland</td>
<td>Consumers Energy Co</td>
<td>MI</td>
<td>968.1</td>
<td></td>
</tr>
<tr>
<td>Zion Energy Center</td>
<td>Zion Energy LLC</td>
<td>Lake</td>
<td>IL</td>
<td>596.7</td>
</tr>
</tbody>
</table>
# Appendix B: Chronology of Events of the 2003 Blackout

<table>
<thead>
<tr>
<th>Time (All time is Eastern Daylight Time)</th>
<th>Description of Event</th>
<th>Consequences</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prior to 12:00</td>
<td>The Davis-Besse Nuclear Unit had been offline for over a year, due to an NRC ordered outage. Sammis unit 3, Eastlake unit 4 and Cook Nuclear unit 2 were all offline dealing with unplanned power outages. Monroe unit 1 was in the midst of a planned outage. The loss of these generating stations took 3.178 gigawatts of electricity offline.</td>
<td>The remaining power generators were still adequate to meet anticipated demand. As there had been prior issues in blackouts in estimating the amount of reactive power available when the system was under stress, these outages likely limited system visibility. Also, this increased the likelihood of power imports to the Ohio area.</td>
</tr>
<tr>
<td>12:08</td>
<td>Unplanned power outages on the Cinergy, which is a subsidiary of Duke Electric Power, 345-kV, 230-kV and 135-kV lines occurred.</td>
<td>This put additional stress on the remainder of Ohio’s power grid. However, the loss of these lines was not determined to be “electrically related” to the blackout, as these issues occurred in Southwestern Ohio.</td>
</tr>
<tr>
<td>12:15-16:04</td>
<td>MISO’s state estimator and real time contingency analysis software was offline</td>
<td>This prevented MISO from being able to provide early warning assessments to First Energy.</td>
</tr>
<tr>
<td>13:31</td>
<td>Eastlake Unit 5 also tripped when the operator increased the power output. This power increase raised the reactive power to unsafe levels, which caused the reactor to go offline.</td>
<td>The loss of Eastlake Unit 5 also forced First Energy to import more energy to make up for the lost power, which stressed the First Energy electric grid and gave First Energy less room for error.</td>
</tr>
<tr>
<td>14:02</td>
<td>The Stuart-Atlanta 345-kV line tripped due to tree contact and had to be shut down for the remainder of the day.</td>
<td>While this is also not said to have caused the blackout, MISO never knew about the Stuart-Atlanta line tripping until 3:33 pm, which caused MISO to make decisions based on incorrect information.</td>
</tr>
<tr>
<td>Time</td>
<td>Event Description</td>
<td>Details</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>14:14</td>
<td>The alarm system at First Energy failed, which prevented the utility from discovering any further malfunctions in their energy grid.</td>
<td>First Energy was unaware that their alarm system had failed. This prevented First Energy from being alerted to future power outages, the same type of problem that occurred when communication systems malfunctioned in the 1982 blackout.</td>
</tr>
<tr>
<td>14:20-14:25</td>
<td>Some of First Energy’s remote terminals failed due to data queuing and overloading.</td>
<td>These terminal failures were not noticed until 14:39, and when discovered the information was incomplete in that operators thought that only some of the terminals had failed. These last two system malfunctions likely contributed to First Energy’s emergency management system servers failing.</td>
</tr>
<tr>
<td>14:42</td>
<td>First Energy’s emergency management system servers failed.</td>
<td>This slowed down the rate at which system operators could see data and drastically reduced the time in which First Energy could respond to a crisis. Again this situation was similar to what had happened in the 1982 blackout, thirty years earlier.</td>
</tr>
<tr>
<td>15:05</td>
<td>The Harding-Chamberlain 345-kV line was tripped due to tree contact.</td>
<td>This power line was only using 44% of its maximum load. A similar case of improper pruning had contributed to the July 1996 blackout when two lightly loaded lines (under 50% of maximum load) were tripped. PJM, MISO and First Energy were unaware that these lines had tripped. This also shunted the load onto the Hanna-Jupiter line.</td>
</tr>
<tr>
<td>15:32</td>
<td>The Hanna-Juniper 345-kV line was forced to carry 88% of its maximum load, which caused the line to sag and contact a tree, tripping the wire.</td>
<td>PJM, MISO and First Energy were unaware that these lines had tripped during a conference call designed to restore system visibility.</td>
</tr>
<tr>
<td>Time</td>
<td>Event Description</td>
<td>Notes</td>
</tr>
<tr>
<td>--------</td>
<td>-----------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>15:41</td>
<td>Subsequently, the Star-South Canton 345-kV tripped; was put back into operation and tripped again. This line also tripped from contacting a tree.</td>
<td>The line was carrying 120% of its normal capacity.</td>
</tr>
<tr>
<td>15:59</td>
<td>The West Akron bus tripped because of a circuit breaker failure.</td>
<td>This caused five more 138-kV lines to be out of service.</td>
</tr>
<tr>
<td>15:41-16:01</td>
<td>Seven 138-kV lines tripped either on fault or from contacting an underlying line. These lines tripped due to low air pressure problems that caused the Canton Central transformers to disconnect, further.</td>
<td>This made the energy situation in Northern Ohio more precarious</td>
</tr>
<tr>
<td>16:05</td>
<td>At this point the Cloverdale-Torrey 138-kV line was extremely overloaded, carrying a load of 160-180% of what it was intended to carry, and finally tripped.</td>
<td>This also caused the Sammis-Star Line to trip.</td>
</tr>
<tr>
<td>16:05</td>
<td>The Sammis-Star line tripped due to very high current combined with very low voltage.</td>
<td>The loss of the Sammis-Star line caused three more 138-kV lines to trip and initiated the cascading phase of this blackout and the collapse of First Energy’s power system.</td>
</tr>
<tr>
<td>16:09</td>
<td>The Gailon-Ohio Central-Muskingum 345-kV line tripped on a phase to ground fault.</td>
<td>The trip of the East Lima-Fostoria Central 345-kV line tripping from very low voltage and very high current.</td>
</tr>
<tr>
<td>16:09</td>
<td>These events were quickly followed by the East Lima-Fostoria Central 345-kV line tripping from very low voltage and very high current.</td>
<td>The trip of the East Lima-Fostoria Central line caused major oscillations in the regional power grid and voltages started to decline.</td>
</tr>
<tr>
<td>Time</td>
<td>Event</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>----------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>16:09-16:10</td>
<td>To compensate for this lack of voltage, the flow of power changed direction in Michigan and instead of moving from Michigan to Ontario started flowing from Ontario into Michigan.</td>
<td>The power swings caused multiple generators in Michigan to trip because of transformer faults and over-excitation. This was followed by multiple 345-kV lines tripping, severing Ohio's connection with Pennsylvania as well as tripping transmission lines going into Detroit at 4:10 pm. The Sumter power plant tripped and the MCV plant had to reduce its voltage by about 90%.</td>
</tr>
<tr>
<td>16:10</td>
<td>The Perry-Ashtabula 345-kV line tripped.</td>
<td>Northern Ohio and Michigan were only connected to the external power grid through Canada. This caused the power that was flowing from Ontario into Michigan to jump from 200-300 megawatts to 3,700 megawatts. This drained a significant amount of power from New York, which was exporting power to Ontario. Due to a loss of 500 megawatts of generation in the Detroit area as well as the oscillations due to the large swings of power, the Detroit area desynchronized and blacked out.</td>
</tr>
<tr>
<td>16:10</td>
<td>Further losses of 345-kV lines in the Cleveland area.</td>
<td>This caused Cleveland to become an electrical island and rapidly lose frequency, which blacked out parts of Toledo. Cleveland and Toledo were blacked out after the Perry nuclear plant tripped from being under frequency, and the Bay Shore-Monroe 345-kV line, which connected Cleveland and Detroit tripped, at 4:10 pm.</td>
</tr>
<tr>
<td>Time</td>
<td>Event Description</td>
<td>Details</td>
</tr>
<tr>
<td>-------</td>
<td>-------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>16:10</td>
<td>Detroit blacked out.</td>
<td>The blackout in Detroit caused a power shift of 5,800 megawatts across Eastern Michigan to Ontario. This power swing caused lines to trip on the border of New York and Pennsylvania, which left the tenuous line from Ontario to Minnesota via Manitoba and the lines from New York to northeastern New Jersey as the only ties connecting the northern part of the Eastern Interconnect.</td>
</tr>
<tr>
<td>16:10</td>
<td>The Wawa-Marathon 230-kV line tripped in northwestern Ontario.</td>
<td>This left northwestern Ontario connected to the grid through Manitoba and Minnesota, saving them from the impending blackout. The power lines connecting New Jersey and New York tripped shortly after, blacking out Northern Ohio, large parts of Ontario, Eastern Michigan and New York.</td>
</tr>
</tbody>
</table>

Adapted from: U.S.-Canada Power System Outage Task Force, 2005
<table>
<thead>
<tr>
<th>Program/Project/Activity</th>
<th>Description</th>
<th>Participants</th>
<th>Strategies Supported</th>
<th>Facets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pipeline System Relative Risk Ranking and Prioritization Tool</td>
<td>Statistical data used to perform relative risk ranking and prioritize CSR findings</td>
<td>TSA, Industry</td>
<td>2, 7</td>
<td>C, H, P</td>
</tr>
<tr>
<td>Pipeline CSR Program</td>
<td>On-site security reviews of pipeline company security</td>
<td>TSA, Industry</td>
<td>1, 6</td>
<td>C, H, P, I, N</td>
</tr>
<tr>
<td>Cyber Attack Awareness</td>
<td>Training and presentations on Supervisory Control and Data Acquisition (SCADA) vulnerabilities</td>
<td>TSA, GTI</td>
<td>1, 3, 5, 7</td>
<td>C, I</td>
</tr>
<tr>
<td>Landscape Depiction and Analysis Tool</td>
<td>Incorporates combined graphic and written descriptive depiction of the pipeline domain, with risk analysis components</td>
<td>TSA</td>
<td>2, 7</td>
<td>C, H, P</td>
</tr>
<tr>
<td>Pipeline Cross-Border Vulnerability Assessment Program (International)</td>
<td>U.S. and Canadian teams assess pipeline operations, control systems, interdependencies, and assault planning in critical cross-border infrastructure</td>
<td>TSA, Natural Resources Canada</td>
<td>1, 2, 5</td>
<td>I, N, P, S</td>
</tr>
<tr>
<td>International Pipeline Security Forum</td>
<td>International forum for U.S. and Canadian Governments and industry pipeline officials to discuss security issues and topics</td>
<td>TSA, Natural Resources Canada, Government Agencies, Industry</td>
<td>5, 6</td>
<td>I, N, S</td>
</tr>
<tr>
<td>Threat, Vulnerability, &amp; Contingency Planning for Critical Pipeline Infrastructure “G8” (International)</td>
<td>Multinational-sharing threat assessment methodology. Advisory levels and effective practices and vulnerability assessment information; also develops a G8-based contingency planning document</td>
<td>TSA, DHS, Dept. of State, G8 Member Nations</td>
<td>6</td>
<td>C, H, I, N, P, S</td>
</tr>
<tr>
<td>Pipeline Policy and Planning</td>
<td>Coordination, development, implementation, monitoring national and TSA pipeline planning</td>
<td>TSA, DHS, DOT, DOE</td>
<td>4, 6</td>
<td>N, S</td>
</tr>
<tr>
<td>Regional Gas Pipeline Studies</td>
<td>Regional natural gas supplies studies for key markets nationwide</td>
<td>TSA, DOE, INGAA, GTI, NETL, Industry</td>
<td>2, 7</td>
<td>D, S</td>
</tr>
<tr>
<td>Security Awareness Training Compact Discs (CD)</td>
<td>Informational CDs about pipeline security issues and improvised explosive devices (IED)</td>
<td>TSA</td>
<td>1, 2, 6</td>
<td>S</td>
</tr>
<tr>
<td>TSA Pipeline Security Stakeholder Conference Calls</td>
<td>Periodic information-sharing teleconference calls between TSA, government, and industry security partners</td>
<td>TSA, Other Government Agencies, Industry</td>
<td>6</td>
<td>N, S</td>
</tr>
<tr>
<td>Transportation GCC, Energy GCC, and CIPAC Joint Sector Conference</td>
<td>Government Security partners participate in GCCs and CIPAC to coordinate interagency and cross-jurisdictional implementation of security for critical infrastructure</td>
<td>TSA, DOE, Government Agencies, Industry</td>
<td>1, 4, 7</td>
<td>D, P, R</td>
</tr>
<tr>
<td>Pipeline Blast Mitigation Studies</td>
<td>Research test containing explosive tests on various configurations of pipe to determine resiliency characteristics</td>
<td>TSA, DOD, TSWG</td>
<td>1, 4, 7</td>
<td>D, P, R</td>
</tr>
<tr>
<td>2006 Virtual Library Pipeline Site Development</td>
<td>TSA Web portal for information-sharing purposes</td>
<td>TSA</td>
<td>6</td>
<td>S</td>
</tr>
<tr>
<td>Program/Project/Activity</td>
<td>Description</td>
<td>Participants</td>
<td>Strategies Supported</td>
<td>Facets</td>
</tr>
<tr>
<td>---------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>----------------------</td>
<td>--------</td>
</tr>
<tr>
<td>ONG/Pipeline SCC and CIPAC Joint Sector Committee</td>
<td>Private-sector companies participate in the SCC and the CIPAC to engage with industry and government security partners in critical infrastructure protection discussions and activities</td>
<td>Industry, Government Agencies</td>
<td>6</td>
<td>N, S</td>
</tr>
<tr>
<td>Pipeline Company-Based Drill/Exercise Initiatives and Participation</td>
<td>Private-sector companies participate in drills/exercises related to infrastructure security at all levels (Federal, State, regional, local and corporate); companies have engaged in tabletop and on-site simulated exercises</td>
<td>Pipeline Companies</td>
<td>3</td>
<td>N, R</td>
</tr>
<tr>
<td>Pipeline Company-Based Training Initiatives</td>
<td>Training initiatives include corporate and field training and usually include response measures tied to the DHS Threat Advisory System; tools include briefings, manuals, CDs, and computer-based training</td>
<td>Pipeline Companies</td>
<td>5</td>
<td>N, S</td>
</tr>
<tr>
<td>API/NPRA Security and Vulnerability Assessment for the Petroleum &amp; Petrochemical Industries</td>
<td>Provides practical knowledge for performing security vulnerability assessments in multiple petroleum- and petrochemical-related industries</td>
<td>API, NPRA</td>
<td>2</td>
<td>C, H, P, S</td>
</tr>
<tr>
<td>API Security Committee and AGA Security Committee-Sponsored Training and Workshops</td>
<td>Workshops/forums and training for gas and liquid petroleum industry</td>
<td>API</td>
<td>5, 6</td>
<td>S</td>
</tr>
<tr>
<td>Pipeline Company Security Protective and Deterrence Measures</td>
<td>Pipeline operators have been enhancing protective and deterrence measures in accordance with Pipeline Security Circular 2002</td>
<td>Pipeline Companies</td>
<td>1</td>
<td>C, H, P</td>
</tr>
</tbody>
</table>

Legend for Facets Column

<table>
<thead>
<tr>
<th>C = Cyber Infrastructure</th>
<th>D = Research and Development</th>
<th>H = Human Infrastructure</th>
</tr>
</thead>
<tbody>
<tr>
<td>I= International</td>
<td>N = Network Building</td>
<td>P = Physical Infrastructure</td>
</tr>
<tr>
<td>R= Resiliency Enhancing</td>
<td>S = Information Sharing</td>
<td></td>
</tr>
</tbody>
</table>

Pipeline Modal Supporting Strategies (DHS, 2007, pp. 9-10):

1. Promote the implementation of layered threat deterrence and vulnerability mitigation programs in pipeline systems and CI/KR, considering risk analysis and making efficient use of existing resources and minimizing duplication of effort.

2. Develop and perform collaborative risk analysis processes from which mitigation measures and planning are determined using available resources with maximum efficiency.

3. Use collaborative plan development and drill/exercise participation to enhance response, restoration, and recovery capabilities while maximizing efficient use of existing resources and minimizing duplication of effort.

4. Promote pipeline system resiliency and contingency capability enhancement measures that increase pipeline system CI/KR robustness and resiliency while maximizing efficient use of resources and minimizing duplication of effort.

5. Conduct security-related training that enhances domain awareness of deterrence and mitigation measures, increases knowledge of response, restores capabilities and defines the roles and responsibilities of all stakeholders within the pipeline domain.
6. Conduct network enhancement and information-sharing activities that promote domain awareness, collaborative planning and role/responsibility defining among pipeline security partners.

7. Conduct research and development and other activities that build domain awareness in all facets of risk mitigation and resiliency enhancement through coordinated and efficient use of assets.
## Appendix D: Major Outages in the Great Lakes Region, 2003-2010
(Source: EIA)

<table>
<thead>
<tr>
<th>Year</th>
<th>People without Power</th>
<th>Hours without Power</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>2002</td>
<td>202,000</td>
<td>47</td>
<td>Ice/Snow</td>
</tr>
<tr>
<td>2002</td>
<td>190,000</td>
<td>60</td>
<td>Severe Storm</td>
</tr>
<tr>
<td>2003</td>
<td>425,000</td>
<td>70</td>
<td>Ice/Snow</td>
</tr>
<tr>
<td>2003</td>
<td>80,000</td>
<td>No Data</td>
<td>Severe Storm</td>
</tr>
<tr>
<td>2003</td>
<td>165,000</td>
<td>35</td>
<td>Severe Storm</td>
</tr>
<tr>
<td>2003</td>
<td>185,000</td>
<td>60</td>
<td>Severe Storm</td>
</tr>
<tr>
<td>2003</td>
<td>186,000</td>
<td>60</td>
<td>Severe Storm</td>
</tr>
<tr>
<td>2003</td>
<td>425,000</td>
<td>68</td>
<td>Severe Storm</td>
</tr>
<tr>
<td>2003</td>
<td>134,500</td>
<td>84</td>
<td>Severe Storm</td>
</tr>
<tr>
<td>2003</td>
<td>436,000</td>
<td>97</td>
<td>Severe Storm</td>
</tr>
<tr>
<td>2003</td>
<td>330,000</td>
<td>No Data</td>
<td>Wind</td>
</tr>
<tr>
<td>2004</td>
<td>360,000</td>
<td>211</td>
<td>Ice/Snow</td>
</tr>
<tr>
<td>2004</td>
<td>200,000</td>
<td>26</td>
<td>Severe Storm</td>
</tr>
<tr>
<td>2004</td>
<td>105,000</td>
<td>39</td>
<td>Severe Storm</td>
</tr>
<tr>
<td>2004</td>
<td>135,000</td>
<td>88</td>
<td>Severe Storm</td>
</tr>
<tr>
<td>2004</td>
<td>280,000</td>
<td>100</td>
<td>Severe Storm</td>
</tr>
<tr>
<td>2004</td>
<td>1,000,000</td>
<td>115</td>
<td>Severe Storm</td>
</tr>
<tr>
<td>2005</td>
<td>51,000</td>
<td>No Data</td>
<td>Equipment Failure</td>
</tr>
<tr>
<td>2005</td>
<td>150,000</td>
<td>96</td>
<td>Ice/Snow</td>
</tr>
<tr>
<td>2005</td>
<td>211,000</td>
<td>132</td>
<td>Ice/Snow</td>
</tr>
<tr>
<td>2005</td>
<td>360,000</td>
<td>259</td>
<td>Ice/Snow</td>
</tr>
<tr>
<td>2005</td>
<td>90,000</td>
<td>30</td>
<td>Severe Storm</td>
</tr>
<tr>
<td>2005</td>
<td>210,000</td>
<td>54</td>
<td>Severe Storm</td>
</tr>
<tr>
<td>2005</td>
<td>300,000</td>
<td>66</td>
<td>Severe Storm</td>
</tr>
<tr>
<td>2005</td>
<td>110,000</td>
<td>74</td>
<td>Severe Storm</td>
</tr>
<tr>
<td>2005</td>
<td>53,000</td>
<td>109</td>
<td>Severe Storm</td>
</tr>
<tr>
<td>2005</td>
<td>305,000</td>
<td>114</td>
<td>Severe Storm</td>
</tr>
<tr>
<td>2005</td>
<td>115,000</td>
<td>127</td>
<td>Severe Storm</td>
</tr>
<tr>
<td>2005</td>
<td>118,000</td>
<td>136</td>
<td>Severe Storm</td>
</tr>
<tr>
<td>2005</td>
<td>300,000</td>
<td>189</td>
<td>Severe Storm</td>
</tr>
<tr>
<td>2005</td>
<td>272,000</td>
<td>61</td>
<td>Wind</td>
</tr>
<tr>
<td>2005</td>
<td>200,000</td>
<td>148</td>
<td>Wind</td>
</tr>
<tr>
<td>2006</td>
<td>No Data</td>
<td>No Data</td>
<td>Ice/Snow</td>
</tr>
<tr>
<td>2006</td>
<td>50,000</td>
<td>No Data</td>
<td>Ice/Snow</td>
</tr>
<tr>
<td>2006</td>
<td>350,000</td>
<td>246</td>
<td>Ice/Snow</td>
</tr>
<tr>
<td>2006</td>
<td>470,000</td>
<td>26</td>
<td>Severe Storm</td>
</tr>
<tr>
<td>2006</td>
<td>210,000</td>
<td>37</td>
<td>Severe Storm</td>
</tr>
<tr>
<td>Year</td>
<td>Type</td>
<td>Quantity</td>
<td>Duration</td>
</tr>
<tr>
<td>------</td>
<td>------------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>2006</td>
<td>Severe Storm</td>
<td>65,000</td>
<td>50</td>
</tr>
<tr>
<td>2006</td>
<td>Severe Storm</td>
<td>142,000</td>
<td>50</td>
</tr>
<tr>
<td>2006</td>
<td>Severe Storm</td>
<td>168,000</td>
<td>51</td>
</tr>
<tr>
<td>2006</td>
<td>Severe Storm</td>
<td>146,000</td>
<td>80</td>
</tr>
<tr>
<td>2006</td>
<td>Severe Storm</td>
<td>315,000</td>
<td>106</td>
</tr>
<tr>
<td>2006</td>
<td>Severe Storm</td>
<td>493,000</td>
<td>125</td>
</tr>
<tr>
<td>2006</td>
<td>Severe Storm</td>
<td>195,000</td>
<td>129</td>
</tr>
<tr>
<td>2006</td>
<td>Severe Storm</td>
<td>112,000</td>
<td>39</td>
</tr>
<tr>
<td>2006</td>
<td>Wind</td>
<td>90,000</td>
<td>52</td>
</tr>
<tr>
<td>2006</td>
<td>Wind</td>
<td>186,000</td>
<td>55</td>
</tr>
<tr>
<td>2007</td>
<td>Equipment Failure</td>
<td>385,000</td>
<td>No Data</td>
</tr>
<tr>
<td>2007</td>
<td>Ice/Snow</td>
<td>367,000</td>
<td>58</td>
</tr>
<tr>
<td>2007</td>
<td>Ice/Snow</td>
<td>140,000</td>
<td>60</td>
</tr>
<tr>
<td>2007</td>
<td>Ice/Snow</td>
<td>130,000</td>
<td>154</td>
</tr>
<tr>
<td>2007</td>
<td>Severe Storm</td>
<td>116,000</td>
<td>No Data</td>
</tr>
<tr>
<td>2007</td>
<td>Severe Storm</td>
<td>300,000</td>
<td>43</td>
</tr>
<tr>
<td>2007</td>
<td>Severe Storm</td>
<td>69,000</td>
<td>60</td>
</tr>
<tr>
<td>2007</td>
<td>Severe Storm</td>
<td>630,000</td>
<td>127</td>
</tr>
<tr>
<td>2008</td>
<td>Equipment Failure</td>
<td>235,000</td>
<td>No Data</td>
</tr>
<tr>
<td>2008</td>
<td>Ice/Snow</td>
<td>190,000</td>
<td>76</td>
</tr>
<tr>
<td>2008</td>
<td>Ice/Snow</td>
<td>250,000</td>
<td>193</td>
</tr>
<tr>
<td>2008</td>
<td>Severe Storm</td>
<td>170,000</td>
<td>46</td>
</tr>
<tr>
<td>2008</td>
<td>Severe Storm</td>
<td>114,000</td>
<td>65</td>
</tr>
<tr>
<td>2008</td>
<td>Severe Storm</td>
<td>68,000</td>
<td>79</td>
</tr>
<tr>
<td>2008</td>
<td>Severe Storm</td>
<td>198,000</td>
<td>93</td>
</tr>
<tr>
<td>2008</td>
<td>Severe Storm</td>
<td>240,000</td>
<td>93</td>
</tr>
<tr>
<td>2008</td>
<td>Severe Storm</td>
<td>70,000</td>
<td>98</td>
</tr>
<tr>
<td>2008</td>
<td>Severe Storm</td>
<td>358,000</td>
<td>139</td>
</tr>
<tr>
<td>2008</td>
<td>Severe Storm</td>
<td>275,000</td>
<td>206</td>
</tr>
<tr>
<td>2008</td>
<td>Severe Storm</td>
<td>2,555,000</td>
<td>221</td>
</tr>
<tr>
<td>2008</td>
<td>Wind</td>
<td>186,000</td>
<td>65</td>
</tr>
<tr>
<td>2008</td>
<td>Wind</td>
<td>687,000</td>
<td>128</td>
</tr>
<tr>
<td>2009</td>
<td>Equipment Failure</td>
<td>250,000</td>
<td>No Data</td>
</tr>
<tr>
<td>2009</td>
<td>Ice/Snow</td>
<td>71,000</td>
<td>59</td>
</tr>
<tr>
<td>2009</td>
<td>Ice/Snow</td>
<td>412,000</td>
<td>389</td>
</tr>
<tr>
<td>2009</td>
<td>No Data</td>
<td>65,000</td>
<td>No Data</td>
</tr>
<tr>
<td>2009</td>
<td>Severe Storm</td>
<td>65,000</td>
<td>38</td>
</tr>
<tr>
<td>2009</td>
<td>Severe Storm</td>
<td>75,000</td>
<td>65</td>
</tr>
<tr>
<td>2009</td>
<td>Severe Storm</td>
<td>344,000</td>
<td>71</td>
</tr>
<tr>
<td>2009</td>
<td>Severe Storm</td>
<td>118,000</td>
<td>77</td>
</tr>
<tr>
<td>2009</td>
<td>Severe Storm</td>
<td>137,000</td>
<td>95</td>
</tr>
<tr>
<td>2009</td>
<td>Severe Storm</td>
<td>64,000</td>
<td>127</td>
</tr>
<tr>
<td>2009</td>
<td>Severe Storm</td>
<td>69,000</td>
<td>154</td>
</tr>
<tr>
<td>Year</td>
<td>Customers Affected</td>
<td>Duration</td>
<td>Cause</td>
</tr>
<tr>
<td>------</td>
<td>-------------------</td>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td>2009</td>
<td>70,000</td>
<td>35</td>
<td>Wind</td>
</tr>
<tr>
<td>2009</td>
<td>563,000</td>
<td>97</td>
<td>Wind</td>
</tr>
<tr>
<td>2010</td>
<td>60,000</td>
<td>31</td>
<td>Ice/Snow</td>
</tr>
<tr>
<td>2010</td>
<td>150,000</td>
<td>42</td>
<td>Ice/Snow</td>
</tr>
<tr>
<td>2010</td>
<td>135,000</td>
<td>80</td>
<td>Ice/Snow</td>
</tr>
<tr>
<td>2010</td>
<td>223,000</td>
<td>118</td>
<td>Ice/Snow</td>
</tr>
<tr>
<td>2010</td>
<td>57,000</td>
<td>158</td>
<td>Ice/Snow</td>
</tr>
<tr>
<td>2010</td>
<td>115,000</td>
<td>163</td>
<td>Ice/Snow</td>
</tr>
<tr>
<td>2010</td>
<td>250,000</td>
<td>No Data</td>
<td>Severe Storm</td>
</tr>
<tr>
<td>2010</td>
<td>51,000</td>
<td>31</td>
<td>Severe Storm</td>
</tr>
<tr>
<td>2010</td>
<td>353,000</td>
<td>45</td>
<td>Severe Storm</td>
</tr>
<tr>
<td>2010</td>
<td>192,000</td>
<td>50</td>
<td>Severe Storm</td>
</tr>
<tr>
<td>2010</td>
<td>823,000</td>
<td>67</td>
<td>Severe Storm</td>
</tr>
<tr>
<td>2010</td>
<td>82,000</td>
<td>71</td>
<td>Severe Storm</td>
</tr>
<tr>
<td>2010</td>
<td>61,000</td>
<td>75</td>
<td>Severe Storm</td>
</tr>
<tr>
<td>2010</td>
<td>80,000</td>
<td>94</td>
<td>Severe Storm</td>
</tr>
<tr>
<td>2010</td>
<td>128,000</td>
<td>101</td>
<td>Severe Storm</td>
</tr>
<tr>
<td>2010</td>
<td>355,000</td>
<td>104</td>
<td>Severe Storm</td>
</tr>
<tr>
<td>2010</td>
<td>504,000</td>
<td>176</td>
<td>Severe Storm</td>
</tr>
<tr>
<td>2010</td>
<td>63,000</td>
<td>50</td>
<td>Wind</td>
</tr>
<tr>
<td>2010</td>
<td>485,000</td>
<td>51</td>
<td>Wind</td>
</tr>
</tbody>
</table>
Appendix E: Transmission Lines and Urban Areas, Northeastern U.S.A. and Southeastern Canada

Source: Carnegie Mellon Electricity Industry Center report for the Pennsylvania Dept. of Environmental Protection, February 2005, p. 17