

Critical Infrastructure Protection in the National Capital Region

**Risk-Based Foundations for Resilience and
Sustainability**

**Final Report, Volume 2:
Energy Sector**

September 2005

University Consortium for Infrastructure Protection

Managed by the
Critical Infrastructure Protection Program
School of Law
George Mason University

This Page Intentionally Blank

Critical Infrastructure Protection in the National Capital Region

Risk-Based Foundations for Resilience and Sustainability

Final Report, Volume 2: Energy Sector

Submitted in fulfillment of:

Department of Homeland Security Urban Areas Security Initiative (UASI) Grant 03-TU-03; and
Department Justice Office of Community Oriented Policing Services (COPS) Grant 2003CKWX0199

September 2005

John E. Bigger and Michael G. Willingham

University Consortium for Infrastructure Protection

Managed by the
Critical Infrastructure Protection Program
School of Law
George Mason University



– **Notice** –

This research was conducted as part of the National Capital Region Critical Infrastructure Project, carried out by the University Consortium for Infrastructure Protection, managed by the Critical Infrastructure Protection Program, George Mason University, John A. McCarthy, Director and Principal Investigator.

It was sponsored by the U.S. Department of Homeland Security's Urban Area Security Initiative grant #03-TU-03, and by the U.S. Department of Justice Community Oriented Policing Services Program grant #2003CKWX0199, under the direction of the Senior Policy Group of the National Capital Region.

The views expressed are those of the authors, and do not necessarily reflect the views of the Department of Homeland Security, the Department of Justice, or the Senior Policy Group of the National Capital Region.

Copyright © 2005 by George Mason University

Published in 2006 by George Mason University

Table of Contents

Executive Summary	3
1. Sector Background.....	7
1.1 Sector Profile	7
1.1.1 General.....	7
1.1.2 Definitions.....	7
1.1.3 Features	8
1.2. Regional Sector Characteristics	9
1.2.1 Service Areas.....	9
1.2.2 Energy Supply Companies: Employees and Customer Base.....	9
1.3 Review of Regulatory Authorities	10
1.3.1. Acts and Statutes.....	10
1.3.2 Regulatory Agencies.....	12
1.3.3 Energy Industry Security Guidelines & Standards.....	13
1.4 Mapping of Interdependencies.....	16
1.4.1 Upstream and Downstream Sectors.....	16
1.4.2 Other Dependencies	17
2. State of Security Assessment.....	18
2.1 Assessment of status and application of CIVA/RM in sector.....	18
2.1.1. Awareness of value of CIP and CIVA/RM	19
2.1.2 Availability of appropriate tools.....	19
2.1.3 Extent to which tools are being used through resource allocation.	23
2.1.4 Extent of implementation of CIP measures.....	23
2.1.5 Extent of Evaluation of CIP Effectiveness	24
3. Risk Reduction Programs and Processes.....	25
3.1 Measuring Effectiveness.....	25
3.2 Managing Continuous Improvement	26
4. Conclusion	25
Appendix A: Project Approach and Data Collection.....	29
Appendix B: Vulnerability Assessment Methodologies – Summaries.....	31
Appendix C: Energy Sector Stakeholder Organizations.....	43
Appendix D: Bibliography.....	51
Appendix E: Endnotes	54

List of Figures

Figure 1: Major Transmission Lines – NCR and Virginia.....	48
Figure 2: Major Natural Gas Pipelines – NCR and Virginia.....	48
Figure 3: Electric Utilities in Virginia.....	49
Figure 4: Natural Gas Utilities in Virginia.....	49
Figure 5: Electric Utilities in Maryland.....	50
Figure 6: Gas Utilities in Maryland.....	50
Figure 7: Department of Energy Vulnerability Assessment Methodology Reports.....	35

List of Tables

Table 1: Principal Energy Organizations Serving the NCR.....	10
Table 2: Key Energy-Related Regulatory Acts and Statutes.....	11
Table 3: Publicly Available Vulnerability Assessment Methodologies.....	46

Energy Sector Report

Executive Summary

This report is designed to help the Senior Policy Group (SPG) who represent the state/local public sector, and energy sector personnel of the National Capital Region (NCR) office, to determine vulnerabilities and risks within the energy infrastructure, and to lay the groundwork for a systematic approach to threat and risk evaluation.

A two-fold approach was used to obtain the original energy infrastructure data. First, a literature search was conducted to identify and obtain publicly available documents relating to both energy infrastructure security and vulnerability assessments. Second, energy industry personnel were interviewed to document their organization's activities and experiences related to vulnerability assessments. At each participating organization, interviewers talked with personnel from departments that had participated in the firm's vulnerability assessment and with an executive of the firm who has responsibility for security. A detailed description of the project approach and data collection process is presented in Appendix A.

Most energy organizations have gone through the vulnerability assessment process at least once, using more than one approach and relying heavily on private, proprietary methodologies. Most firms believe that no one vulnerability assessment methodology will suffice for all energy organizations. In particular, publicly available vulnerability assessment methodologies examined do not adequately address the area of infrastructure interdependencies, either within a single sector or among infrastructures. Other issues worth noting include: assessments were usually conducted only to the organization's property line; in fact, no small firm participated in assessments involving their upstream or downstream counterparts; and, limited in-house technical capability of small utilities often restricted use of sophisticated assessment methodologies.

Specific factors may limit a firm's voluntary security-related investments. For instance, there is concern over disclosure of security and vulnerability details during subsequent rate hearings. Further, a lack of awareness exists, in both executive and operating areas, of the organization's growing use and dependence on the Internet and inherent vulnerability to outside intrusion.

This report underscores one critical ancillary concern: the high failure rate of on-site emergency generation equipment at both public and private facilities, including Emergency Operation Centers (EOC's). In addition, the owners-operators of facilities for vulnerable populations in the NCR do not adequately prepare for natural disasters or other situations where electric service may be interrupted.

Conclusions

Based on interviews with energy infrastructure firm personnel as well as energy industry association staffs, and supported by direct review of a number of publicly available vulnerability assessment/risk management methodologies, the energy sector team developed these conclusions:

- With few exceptions, mainly in the natural gas and petroleum areas, the publicly available methodologies examined do not adequately address the area of infrastructure interdependencies, either within a single sector or among infrastructures. Presently, how

NCR electric utility organizations handle or use these methodologies is unknown. Consequently, vulnerabilities of infrastructure interdependencies in this area is still unknown both outside the firms, and in most instances inside firms as well.

- All but one energy organization has gone through the vulnerability assessment process at least once. With the exception of some gas and petroleum product companies, energy organizations did not rely solely on publicly available methodologies found in this project.
- Energy infrastructure organizations did not normally interact with upstream suppliers of critical services during the assessment process. In fact, the assessment process was conducted to the organization's physical property lines, to common interconnection points, and no further. Worth noting is that no energy organization was invited to participate in other infrastructure organization's process even though energy is a critical supplier to these other organizations.
- Industry organizations, along with some government agencies including the Rural Utility Service (RUS) of the U.S. Department of Agriculture (USDA), stated that one single vulnerability assessment methodology will not work for all energy organizations.
- For small utilities and firms, public, private, or cooperative, the in-house technical capability can be very limited. Moreover, some organizations have very few or no engineers. In these instances, utilizing an assessment methodology that is very technically based and requires significant data collection and technical support is not useful for or usable by smaller energy organizations.
- Considerable action initiated by the federal government – Federal Energy Regulatory Commission (FERC) and the RUS – and industry organizations – North American Electric Reliability Council (NERC) – is expected to increase security-related actions, including vulnerability assessments, by electric utilities before the end of July 2005. However, it is not clear whether any action will be taken to validate these actions or individual organization certifications.
- Some energy utilities that serve the NCR are reluctant to initiate actions with state or District Public Utility Commissions (PUC's) to obtain reimbursement for security-related expenditures because of the possibility of disclosure of security and vulnerability details during subsequent rate procedures. The major problem is potential liability if information is made public. Likewise, this may limit the extent of voluntary investment because the cost is presently being borne by company stockholders.
- More and more energy management, SCADA, and other energy infrastructure communications and control functions depend on the Internet for services; and thousands of new systems are added each year. Yet, many utility personnel, in both the executive and operating areas, do not realize that this growing use and dependence on the Internet increases vulnerability to outside intrusion.
- Small electric and gas utilities are concerned with what they see as “looming security requirements” that they cannot afford or that the results will not benefit their customers. Without outside support, utilities with a few tens of thousands of customers cannot adopt a complex assessment methodology and invest in a number of mitigation measures that may be imposed on them by federal legislation or mandate.
- Electric utility personnel, emergency managers, and NCR Emergency Operations Center (EOC) personnel continue to be concerned over the high failure rate of on-site emergency generation facilities at both public and private facilities. An additional perspective came to light during these interviews. The owners/operators of facilities for a range of vulnerable

populations (hospitals, nursing homes and critical care facilities) in the NCR also do not adequately prepare for natural disasters or other situations where their electric service may be interrupted. These facilities include nursing homes, convalescent facilities, intermediate medical facilities, retirement communities, and especially multi-story facilities that cater to these populations.

- In those instances where risk reduction measures had been completed or implemented, organizations often either had not reviewed the assessment findings with the mitigation measures in place or were not confident in the exact changes in security or vulnerability the mitigation measures had achieved.
- One surprising finding was the vulnerability and sensitivity of energy organization workers, whether equipment operators, maintenance personnel, or telephone operators manning call centers during emergencies. Extreme workplace demands often compete for their attention with personal and family concerns, especially during long-duration situations (e.g., Hurricane Isabel). This human resource issue appears to receive little attention.

Recommendations

The principal recommendations from the study are grouped into four major categories:

Assessment Methodology

1. The NCR infrastructure organizations should modify their procedures to conform to the model, where appropriate, for their next (usually annual) assessment.
2. Relations should be established with selected private firms, with the assistance of high-level DHS and its advisory panel members, to obtain at least limited access to private sector methodologies for review.
3. All vulnerability assessments should include participation of critical upstream suppliers from the same and other infrastructures.
4. Tools need to be developed to allow NCR energy infrastructure organizations to establish the actual extent of infrastructure interdependency vulnerability in the NCR area.

Tactical Steps for Immediate Benefit

- An in-depth evaluation of the growing dependence of the energy infrastructure on the Internet is needed. A number of modest efforts are looking at various aspects of this situation; however, there are no comprehensive studies examining the increasing threat of future vulnerabilities of products being developed for future adoption by the energy industry.
- An independent monitoring and review pilot program should be initiated in order to assess and document electric utilities' (private, public, and cooperative) response to increased federal (North American Electric Reliability Council (NERC) and Rural Utilities Service (RUS) security recommendations and guidelines.
- An in-depth survey of on-site emergency generators needs to be conducted--units tested and refueling strategies developed to increase the reliability and security of the hundreds of existing emergency units in the NCR.
- A credentialing process for key energy sector personnel should be established to ensure priority access to incident sites in order to coordinate sector assessment, restoration and repair efforts.

Governance Recommendation at Sector-Level

- The regional Public Utility Commissions (PUC) should consider procedures to explore the prudence of security investments and expenditures to limit the distribution of critical security data and information. A joint FERC – PUC pilot project may offer a suitable venue to address this question.
- A regional workshop should be held in the NCR to address how utilities could recover their security-related investments via rate hearings without having to reveal sensitive security-related information in a public forum.

Service to Vulnerable Populations

- Owners/operators of facilities that serve vulnerable populations should prepare and implement plans to ensure energy availability and continuity of operations in the event of extended power outage. Emergency managers, utilities, and fuel distribution firms and associations should participate in the process with emphasis on identifying business opportunities to serve these populations during emergencies

1. Sector Background

The National Capital Region is not only a large metropolitan area with considerable recent economic growth, but it also is the seat of the nation's federal government, making the infrastructures serving this area of critical importance not only to the NCR and the surrounding region but also to the entire country. Each of the energy infrastructures examined in this chapter (electric power, natural gas and petroleum products) is itself made up of complex physical, cyber, institutional, functional and human networks – a network of networks. For the most part, the electric transmission and distribution facilities are above-ground and visible; the natural gas and petroleum products transmission and distribution facilities are below ground and out of sight. As shown in the regional section of this report, the energy infrastructure is complex, multi-faceted and recursive.

1.1 Sector Profile

1.1.1 General

The energy infrastructures examined in this chapter are those included in Presidential Decision Directive 63 (PDD-63), namely, electric power, natural gas, and petroleum products. Solid fuels – coal and nuclear – were not included in the PDD-defined energy infrastructure and thus are not included in this discussion.

Figures in Appendix C show the major electric generation and transmission facilities in and around the NCR and shows the natural gas transmission and distribution facilities serving the same area.¹ Individually, these figures show the complicated nature of each infrastructure; when superimposed, they show the complexity of the total physical network. Information for the natural gas sector specifically in Maryland was not available; the Virginia information is included because it illustrates two major interstate pipelines servicing the northeast U.S.

1.1.2 Definitions

Infrastructure

A generally-accepted definition of infrastructure is that of a framework of interdependent networks and systems comprising identifiable industries, institutions, and distribution capabilities that function collaboratively and synergistically to produce and distribute a continuous flow of essential goods and services.²

NCR Project Energy Sector Descriptions

The definitions of specific energy infrastructure sub-sectors used in this report differ slightly from those given above. In the natural gas and petroleum products sector, for example, there are no oil or natural gas production fields, gathering pipeline systems, or primary processing facilities in the NCR. All fossil fuel products come into the area via pipelines, train, and trucks from outside the NCR. In the electric power sector, fuels are brought into the NCR via pipeline, train, and truck. Northern Virginia, the District, and Western Maryland do not generate sufficient electric energy to serve the NCR loads; therefore, high voltage transmission lines are also needed to bring electric power into the NCR.

Electrical Power Systems³

The electric power systems that service the NCR include generation stations, transmission and distribution networks that create and supply electricity to end-users (customers). This includes the transportation and storage of fuels and disposal of waste products essential to the systems.

Natural Gas and Petroleum Systems⁴

The natural gas and petroleum systems within the NCR include the pipelines, trucks, and rail systems that transport these commodities from their sources to end-users (wholesale and retail customers) in any one of their many forms.

Project Infrastructure Boundaries

The boundaries between energy sector organizations and other sectors are defined as the points where products and services are exchanged between sector customers. The boundary facilities depend upon the mode of transportation of the product or service including wire, pipeline, truck, ship, or train.

1.1.3 Features

In the electrical sector, the physical structures are owned and/or operated by private firms, government agencies e.g., municipalities, or customers themselves (electric cooperatives). In addition to the physical and cyber networks, there are a myriad of social, institutional, and functional networks in the sector that are necessary to conduct business, including industry-wide associations. These associations are divided into investor, public, and customer oriented associations and function-related associations.

In the natural gas and petroleum sectors, considerable amounts of petroleum products are brought by ships to various East Coast ports, however, these are all outside the NCR. The closest point to the NCR where liquefied natural gas (LNG) is brought is the Cove Point facility in Southern Maryland, where it is stored, gasified and put into the pipelines.

Electric and Gas Utilities

Service boundaries defining the geographic areas where service is provided for electric and gas distribution utilities are established by state regulatory and local agreements e.g., franchises. The electric generation facilities owned by either utilities (public or private) or independent power producers can be located wherever there is an economic confluence of land, fuel, water, transmission access, regulatory approval, and public acceptance –facility sites are not limited to service areas.

Interface boundaries are usually transmission or distribution substations or service connections where the electric utility connects to industrial, commercial, government, or other customer service points, depending upon the voltage level of service and magnitude of load. For the protection of the public, interface connection designs are controlled by various federal and state regulatory agencies (principally FERC and PUC's), industry and local code requirements (e.g., National Electrical Code, National Fire Protection Code) and professional industry standards (e.g., IEEE design standards).⁵

Oil and Petroleum Liquids

There are no service boundaries for firms in the oil and petroleum products industries. Boundaries are normally established by economics: the cost of the crude oil at the wellhead or port of entry, the cost of all necessary refining and processing, and the cost of transporting the intermediate and end products to customers.

Interface boundaries for this segment of the energy sector depend specifically on the mode of delivery of the product to the customer and can include tanker/port facilities, pipelines, or delivery trucks. For bulk oil, petroleum products, and natural gas, the interface is usually a pipeline metering and supply service installation and is normally at or near the customer's facility perimeter. Smaller quantities of oil and petroleum products are delivered by truck and these require pipeline-to-truck transfer equipment at the supplier's facilities and, at the customer's location, offloading and storage facilities.

Liquefied natural gas (LNG) is transported to the U.S. by ship, converted to gas, and then injected into the gas transmission pipeline system. Presently, there are four LNG facilities operating in the U.S., with one in southern Maryland in Chesapeake Bay. Port, offloading, liquid and gas storage, and gasification facilities are required at these locations. The LNG facility product (in gaseous form) is pumped into gas transmission pipelines through pipeline metering and supply service installations.

1.2. Regional Sector Characteristics

1.2.1 Service Areas

The service areas for the different electric and natural gas utilities serving the Virginia portion of the NCR are shown in Figures 3 and 4⁶, while the electric and natural gas utilities serving the Maryland portion of the NCR are shown in Figures 5 and 6⁷ (see all figures in Appendix C). Washington Gas serves both inside and outside the NCR and only two electric utilities – Potomac Electric Power Co. and the City of Manassas – serve only areas inside the NCR.

Implications of the NCR Boundary

With the exceptions of the Potomac Electric Company and the City of Manassas Electric Department, energy infrastructure organizations have facilities - and provide products and services to customers - both inside and outside the NCR boundary; therefore, the NCR “boundary” does not coincide with energy infrastructure organization service areas.

1.2.2 Energy Supply Companies: Employees and Customer Base

Infrastructure organizations that provide various energy products and services directly to customers in the NCR are listed in Table 1. Detailed information about individual organizations is included in Appendix C: Energy Sector Stakeholder Organizations.

Table 1: Principal Energy Organizations Serving the NCR

Company	Total Employees	Total Customers
Electric		
City of Manassas, Elec. Dept.	100	14,700
Dominion Virginia Power	16,700	3,900,000
Mirant Mid-Atlantic, Inc.	515	Sells to PJM market Formerly PEPCO supplier (see below)
No. Virginia Electric Coop	300	125,000
Potomac Electric Power Co.	2,500	713,581 ⁸
Natural Gas		
Columbia Gas of Virginia	300	212,000
Washington Gas Light Co.		980,000
Petroleum Products		
British Petroleum	102,900	NA
Chevron Texaco	50,582	NA
Exxon-Mobil Corp.	88,300	NA
Shell Oil Co.		NA

1.3 Review of Regulatory Authorities

1.3.1. Acts and Statutes

An extensive array of federal authorities, acts, and statutes relate to either the energy infrastructure generally, or the electric, natural gas, and petroleum sectors specifically. Three initiatives in particular are relevant for the energy sector of the NCR because of their focus on critical infrastructures and related information sharing. The Homeland Security Presidential Directive/HSPD-7, the Critical Infrastructure Information Act of 2002 and FERC Final Ruling controlling access to critical energy infrastructure information (CEII) are summarized below, while others are listed in Table 2 following.

Homeland Security Presidential Directive/HSPD-7

This directive establishes a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks.

The implementation phase calls for a comprehensive, integrated National Plan for Critical Infrastructure and Key Resources Protection that will include, in addition to other homeland security-related elements as the secretary deems appropriate, a strategy to identify, prioritize, and coordinate the protection of critical infrastructure and key resources, including how the department intends to work with federal departments and agencies, state and local governments, the private sector, and foreign countries and international organizations.

The National Plan, which is now being codified as the interim National Infrastructure Protection Plan (NIPP), also must include (1) a summary of activities to be undertaken in order to: define and prioritize, reduce the vulnerability of, and coordinate the protection of critical infrastructure and key resources, as well as (2) a summary of initiatives for sharing critical infrastructure and key resources information and for providing critical infrastructure and key resources threat warning data to State and local governments and the private sector.⁹

Critical Infrastructure Information Act of 2002 (CIIA)

CIIA consists of a group of provisions that address the circumstances under which the Department of Homeland Security may obtain, use, and disclose critical infrastructure information as part of a critical infrastructure protection program. CIIA establishes several limitations on the disclosure of critical infrastructure information voluntarily submitted to DHS. The CIIA was enacted, in part, to respond to the need for the federal government and owners and operators of the nation's critical infrastructures to share information on vulnerabilities and threats, and to promote information sharing between the private and public sectors in order to protect critical assets.¹⁰

FERC Critical Energy Infrastructure Information Final Ruling

The Federal Energy Regulatory Commission (Commission) issued this final rule amending its regulations for gaining access to critical energy infrastructure information (CEII). These changes were made based on comments filed in response to the February 13, 2004 notice seeking public comment on the effectiveness of the Commission's CEII rules. The final rule [[Page 48387]] primarily eases the burden on agents of owners or operators of energy facilities that are seeking CEII relating to the owner/operator's own facility. The rule also simplifies federal agencies' access to CEII. These changes will facilitate legitimate access to CEII without increasing vulnerability of the energy infrastructure.¹¹

Table 2: Key Energy-Related Regulatory Acts and Statutes

Homeland Security Presidential Directive (HSPD)-5	Executive Order 12038
	Power Plant and Industrial Fuel Use Act
Federal Information Security Management Act of 2002	Clean Air Act
	Natural Gas Act
Bonneville Project Act of 1937	Natural Gas Policy Act
Federal Power Act	Public Utilities Regulatory Policies Act of 1978
Defense Production Act of 1950	Ports and Waterways Safety Act, Natural Gas Pipeline Safety Act, Hazardous Liquids Pipeline Safety Act
Robert T. Stafford Disaster Relief and Emergency Assistance Act	Emergency Reconstruction (FERC Order 633)
Executive Order 11912, Energy Policy and Conservation Act	Energy Policy and Conservation Act

Merchant Marine Act of 1920	Department of Energy Organization Act
Communications Act of 1934	

1.3.2 Regulatory Agencies

Regulatory authority in the energy sector for the National Capital Region is shared between federal, state and local jurisdictions, with federal oversight focused on interstate aspects. The primary federal organizations include the following:

Federal Energy Regulatory Commission (FERC)

FERC is an independent federal agency that regulates the interstate transmission of natural gas, oil, and electricity. FERC jurisdictional responsibility does not include regulation of retail electricity and natural gas sales, regulation of municipal power systems, rural electric cooperatives, pipeline safety or local natural gas distribution pipelines.

Office of Pipeline Safety (OPS) U.S. Department of Transportation

OPS has federal oversight for the nation’s 2.3 million miles of natural gas and hazardous liquid pipelines. The primary mission of OPS is to ensure the safe, reliable, and environmentally sound operation of the nation’s pipeline transportation system. Federal pipeline statutes provide for exclusive federal authority to regulate interstate pipelines. OPS may authorize a state to act as its agent to inspect interstate pipelines, but retains responsibility for enforcement of the regulations. The OPS federal/state partnership is the cornerstone for assuring uniform implementation of the pipeline safety program nationwide. Toward that end, the Eastern Region OPS office routinely works with the Maryland and D.C. Public Service Commissions and the Virginia State Corporation Commission.

U.S. Department of Energy (DOE)

DOE provides a context for federal regulation by developing policies designed to protect national security and other critical assets entrusted to the department, as well as managing security operations for DOE facilities in the NCR. In particular, the Office of Electricity Delivery & Energy Reliability (OE) works in collaboration with state and local governments and the private sector to protect the nation against severe energy supply disruptions.

U.S. Environmental Protection Agency (EPA)

EPA is the designated lead agency for Emergency Support Functions (ESF) #10 (Hazardous Materials) of the Federal Response Plan (FRP).¹² The intent of ESF #10 is to provide support to state and local governments in responding to an actual or potential discharge and/or release of hazardous materials (including releases of chemicals, oil, gasoline, and propane) following a major disaster or emergency.

District/State Regulatory Organizations

All states have established commissions vested with regulatory authority over many business and economic interests in that state. Commission authority is usually described by state constitution and state law. Commission authority can encompass utilities, insurance, state-chartered financial

institutions, securities, retail franchising, and railroads; it also includes monitoring operations and setting rates for investor-owned gas and electric utilities.

The energy firms serving customers in the NCR are subject to the authority and regulation of three commissions, one in each jurisdiction:

- District of Columbia Public Service Commission
- Maryland Public Service Commission
- Virginia State Corporation Commission

Municipal Regulatory Authority

One municipally-owned electric utility - Manassas Electric Department – serves electric customers within the municipal boundaries of the City of Manassas. The City is completely inside the NCR. The Electric Department is regulated by the City of Manassas.

1.3.3 Energy Industry Security Guidelines & Standards

Electric Utility Sector

Until recently, there were no required security standards addressing design, installation, operation, or maintenance for the electric utility portion of the energy infrastructure; this included requirements for both physical and cyber systems. However, the North American Electric Reliability Council (NERC), the Federal Energy Regulatory Agency (FERC), and the U.S. Department of Agriculture’s Rural Utility Service (RUS) recently approved actions requiring electric utilities and others under their jurisdiction to take specific procedures to increase system security. These requirements were scheduled to take effect during the first half of 2005.

U. S. Federal Energy Regulatory Commission Actions

On February 9, 2005, FERC issued the “Supplement to Policy Statement on Matters Related to Bulk Power System Reliability.” The supplement stated that the term “Good Utility Practice” in their Open Access Transmission Tariff was “...to include compliance with the reliability standards developed by the North American Electric Reliability Council (NERC).” The Open Access Transmission Tariff (OATT) is part of FERC Order No. 888, which was initially issued in 1996.

North American Electric Reliability Council Actions

Until recently, the various standards and guidelines established by NERC covering various operations of its members – including utilities, merchant plant owners and industry associations - were all voluntary.

“NERC's mission is to ensure that the bulk electric system in North America is reliable, adequate and secure. Since its formation in 1968, NERC has operated successfully as a voluntary organization, relying on reciprocity, peer pressure and the mutual self-interest of all those involved. Through this voluntary approach, NERC has helped to make the North American bulk electric system the most reliable system in the world.”¹³

However, the North American Electric Reliability Council (NERC) issued a press release in December 2000 noting that the year 2000 saw only a 90% compliance rate with NERC and regional reliability council reliability policies and standards. This meant that at least some utilities were not complying with the voluntary reliability standards established by NERC and the regional councils.¹⁴

In 1998, at the request of the Secretary of Energy, NERC began working with the U. S. Department of Energy to develop a program for “information sharing, cooperation, and coordination between private industry and the government.”¹⁵

Since the events of 9/11, the entire electric utility industry has been reexamining its approach to security; since early 2002, NERC has been developing new security procedures for operating utilities. Two major security procedures that relate directly to the NCR are presently in draft form and are going through NERC’s rigorous validation process: Security Guidelines for the Electricity Sector, and Standard 1300 – Cyber Security.

In continuing discussions with security personnel from various electric utilities in the U.S., almost all indicate that although these NERC guidelines and standards are presently voluntary, their organizations are following them as if they were required. The utility personnel fully expect that at some point in the near future, these will become required, either through federal legislation or as a condition for continued membership in NERC.

After the major blackout in the northeastern United States and southern Canada on August 14, 2003, a joint U.S.-Canada Outage Task Force was formed to investigate the causes of the blackout. In its final report, the task force made a number of recommendations regarding the need for restating and clarifying the NERC standards and guidelines, both those approved and those under development. In response, on February 8, 2005, the NERC Board of Trustees approved Version 0 - Reliability Standards which became effective April 1, 2005 and addresses system security issues in electric utility operations.

The Department of Energy has designated NERC as the sector coordinator for the Electric System Information Sharing and Analysis Center (ES-ISAC), a joint industry-government effort to share security-related information among the many industry organizations, government agencies, and other critical infrastructure industries directly involved with infrastructure security. Recently, NERC established a Critical Infrastructure Protection Committee (CIPC) to “...advance the physical and cyber security of the critical electricity infrastructure of North America.”¹⁶ It should be noted that NERC has, in addition to U.S. utility members, both Canadian and Mexican electric utility members. The role of (CIPC) is to act as an expert advisory panel for NERC activities, the ES-ISAC, and all levels of government.

U. S. Department of Agriculture Rural Utility Service (RUS) Actions

On January 7, 2005, RUS Bulletin 1730B-2, “Guide for Electric System Emergency Restoration Plan,” was approved. The Guide “...contains information to assist RUS borrowers in the development of vulnerability and risk assessment (VRA) and an Emergency Restoration Plan (ERP).” Under the Bulletin, RUS borrowers must: a) conduct a VRA, b) using the results of the VRA, develop an Emergency Restoration Plan, and c) submit a Self-Certification letter to RUS by July 2005.¹⁷

Although the guideline does not require or dictate that a specific VRA methodology be used because of the variety of utility systems and their consumers, it does urge their electric program

borrowers to refer to the NERC-developed security and reliability guidelines and standards. RUS, by federal mandate, has adopted the five-level color coded Threat Alert System.¹⁸

Oil & Gas Pipeline Industry

Natural Gas Sector – Transmission and Distribution

Two statutes provide the framework for the federal pipeline safety program. The Natural Gas Pipeline Safety Act of 1968 as amended (NGPSA) authorizes the Department of Transportation (DOT) to regulate pipeline transportation of natural (flammable, toxic, or corrosive) gas and other gases as well as the transportation and storage of LNG. Similarly, the Hazardous Liquid Pipeline Safety Act of 1979 as amended (HLPSA) authorizes DOT to regulate pipeline transportation of hazardous liquids (crude oil, petroleum products, anhydrous ammonia, and carbon dioxide). Both of these acts have been re-codified as 49 U.S.C. Chapter 601.

Regulations

The federal pipeline safety regulations (1) assure safety in design, construction, inspection, testing, operation, and maintenance of pipeline facilities and in siting, construction, operation, and maintenance of LNG facilities; (2) set out parameters for administering the pipeline safety program; and (3) delineate requirements for onshore oil pipeline response plans. The regulations are written as minimum performance standards. The regulations are published in the Code of Federal Regulations, 49 CFR Parts 190-199.

Federal Actions

On September 5, 2002, the Department of Transportation's Office of Pipeline Safety (OPS), in cooperation with DOE and DHS, issued a pipeline security information circular, entitled "Security Guidance for Natural Gas, and Hazardous Liquid Pipelines and Liquefied Natural Gas Facilities". The Circular: 1) defined critical facilities in the industry, 2) identified appropriate measures for protecting these critical facilities for owners/operators, 3) required submittal of a self-certification letter to OPS indicating actions taken, and 4) defined the process by which the federal government would verify that pipeline operators had taken appropriate action. By April 2003, the Office of Pipeline Safety had received certifications from operators of 95% of the regulated pipelines in the U.S. (> 150,000 miles). DOT and DHS personnel have been trained and are now verifying these certifications by on-site environmental and safety inspections.

Industry Actions

In 2002, in cooperation with DOE, the U.S. Coast Guard, and DOT, the American Petroleum Institute developed and published Security Guidance for the Petroleum Industry. Based upon feedback from industry members and input from a security contractor, a second edition was published in April 2003, and is now available. These voluntary guidelines apply to all major sectors of the petroleum industry: exploration and production; refining; pipeline transportation; marine transportation; petroleum product distribution, marketing, and service; and cyber systems.

The document includes a thorough discussion of the vulnerability assessment (VA) process, what a proper VA methodology should include, and organization and data requirements to conduct an assessment. For each major sector of the industry, the document contains a more detailed

discussion of security plans, vulnerability assessments, security conditions, and response measures. Although not a risk assessment per se, the process allows the user to systematically develop information required for a full risk assessment.

This document also contains a 43-page discussion and check list specifically designed to identify infrastructure interdependencies. This is one of the most logical and systematic tools for evaluating infrastructure interdependencies in the public domain.

1.4 Mapping of Interdependencies

The terms interdependency and dependency frequently are used interchangeably when the infrastructures are examined. To eliminate ambiguity, this report defines the terms as follows:

“Interdependency is a bi-directional relationship between infrastructures through which the state of each infrastructure is influenced by or correlated to the state of the other. More generally, two infrastructures are interdependent when each is dependent on the other for some aspect of their operation”¹⁹

“Dependency is a unidirectional relationship between infrastructures through which one provides a product or service to the other under a formal agreement for a specified fee.”

Classes of Interdependencies

There are generally considered four classes of interdependencies between or among infrastructures. These are briefly described below along with an example for each.²⁰

- *Physical Interdependency* – Two infrastructures are physically interdependent if the state of each depends upon the material products or services of the other. For example, a rail network and a coal-fired electrical generation plant are physically interdependent, given that each supplies commodities that the other requires to function properly.
- *Cyber Interdependency* – An infrastructure has a cyber interdependency if its state depends on information transmitted through the information infrastructure. Cyber dependencies include the reliance on telecommunications for supervisory control and data acquisition (SCADA) systems and information technology for e-commerce and business systems
- *Geographic Interdependency* – Infrastructures are geographically interdependent if a local environmental event can create state changes in all of them. Geographic dependencies include, for example, common corridors that natural gas pipelines share with electric power lines and/or telecommunications lines.
- *Logical Interdependency* – Two infrastructures are logically interdependent if the state of each depends upon the state of the other. An example of a logical dependency is the impact that oil futures have on natural gas prices and ultimately the natural gas infrastructure via changes in infrastructure investment.

1.4.1 Upstream and Downstream Sectors

The energy sector is the primary driving force behind almost all other infrastructure systems, and in that sense can be characterized as an ‘upstream’ (input) sector for these systems. For example, disruption of energy systems could also affect potable water supplies, since water treatment facilities use large amounts of energy for on-site processing.

At the same time, the mix of contributions from other sectors necessary to produce, transform and transmit the various forms of energy illustrate that the sector itself is a ‘downstream’ sector,

itself often reliant on other sector inputs to function properly. As a rule, the most critical upstream sectors are communications, transportation and water infrastructures. As a case in point, in the event of outages of gas pipelines, the curtailment of natural gas supplies to gas-fired generators without dual-fuel capacity could constrain the power system operation and even lead to additional outages.

To a great extent, characterizing the energy sector as either an upstream or downstream sector depends on site-specific or process-specific criteria. More important when considering system vulnerabilities is the use of a methodology that explicitly recognizes the sector as either (or both) upstream or downstream to its counterpart sectors, as well as providing the means for systematically analyzing how degradation of the energy sector affects (or is affected by) its upstream or downstream counterparts.

1.4.2 Other Dependencies

Co-Location of Facilities

Locating new infrastructures in existing rights-of-way may reduce the need for new permits and can expedite the development process. However, this increases the risk of simultaneous loss of service in the event of an accident, natural disaster or terrorist attack.

Common Right-of-Ways and Crossings

Electric utility transmission and railroad right-of-ways are also being used as sites for regional and local fiber-optic cable installations. In some instances, the utilities and the railroads are getting into the communications business; in other cases they are just leasing part of their right-of-way to a communications company. In the NCR, a significant number of high-capacity fiber-optic cables come into the District of Columbia on the railroad right-of-ways northeast of Union Station. At the beginning of 2000, telecommunications firms had installed more than 650,000 miles of fiber optic cable in major corridors in Virginia; these installations were, in many cases, along existing railroad and utility transmission line right-of-ways between major cities, including Washington, D.C., Fredericksburg and Richmond, Virginia.²¹

Emergency Services in the NCR

Almost every political jurisdiction in the NCR – city, county, state, and federal – has an Emergency Operating Center (EOC) to coordinate the response of various types of resources during emergencies. Each infrastructure organization also usually has at least one operating/dispatching center; when an emergency occurs, its operations are expanded to handle the increased staff, functions, and coordination with outside organizations. The resulting network of Emergency Operating Centers within a single state can easily number over one hundred.

In addition to their requiring electric service in order to function, EOCs also coordinate information regarding energy services required by other infrastructures. In this context, EOCs are both dependencies and coordinators of interdependencies.

2. State of Security Assessment

2.1 Assessment of status and application of CIVA/RM in sector

Vulnerability Assessment Methodologies Presently in Use in NCR

During on-site interviews, a number of questions were asked pertaining to the vulnerability assessment methodology used by each organization. These questions related to the methodology used, development of the methodology, the assessment conduct, and others relating to the assessment process. The organizations used a variety of methodologies, briefly described below, to conduct their vulnerability assessments

Private/proprietary methodology – A private firm was contracted to conduct an assessment, usually using contract personnel. In all cases, infrastructure organization personnel worked alongside the contract personnel.

In-house developed methodology – The infrastructure organization developed its own assessment methodology, usually with support from outside consultant(s). The assessment was conducted with the organization's own personnel.

Government/Sandia developed methodology – The methodology is publicly available or developed by Sandia National Laboratories. If used, this assessment was conducted with the organization's own personnel. When the Sandia methodology was used, Sandia personnel facilitated the process.

Survey Results – Assessment Methodologies

The results may be summarized by noting that two of the four representative energy infrastructure organizations interviewed used private firms to conduct their VAs and these private firms used their own/proprietary methodologies to guide the assessments. Two organizations also developed their own assessment methodology, utilizing consultants in both the development and conduct of the assessment. None of the organizations interviewed utilized government or Sandia methodologies.

Questions regarding the methodology and process used covered a number of areas, including:

- Resources needed to conduct the assessment
- Financial: in-house, outside contracts
- Personnel: executive, management, technical, security, and support
- Schedule (months): planning, conduct, analyses, and mitigation plans
- Outside interaction: institutional (local, regional, state, and federal agencies); critical suppliers and customers; and energy industry associations, research organizations, etc.
- Triggering mechanisms for conducting VAs (e.g., regularly scheduled, tied to DHS Index, etc.)

Without exception, the organizations answered the questions only in generalities. The organizations were not willing to share details regarding the investments in funds, number of personnel involved, and time required for the assessments.

Proprietary Vulnerability Assessment Tools and Methodologies for Energy Infrastructure Organizations

During the course of the literature and Internet searches, private firms were identified that offered assessment services to public and private entities, using their “proprietary” assessment methodologies. These included architectural and engineering firms, consulting firms, and specialty communications/computer companies.

Given the number of privately developed, proprietary assessment methodologies used today, the NCR project’s approach to the review of the methodologies –examine only publicly available methodologies for review – may not have identified a true “best practices” framework. A significant number of methodologies were left out of the review process.

2.1.1. Awareness of value of CIP and CIVA/RM

General Awareness of Infrastructure Vulnerabilities

Every organization contacted for this project indicated a growing awareness of both the vulnerability of their specific system and facilities and acknowledged a need to reduce vulnerability and increase resiliency of their systems – hardware, cyber, and people. This awareness has been reinforced by a variety of events in the NCR over the past four years.

- Many of the energy infrastructure organizations serving the NCR are accustomed to coordinating and working with a number of different security-agency personnel and other infrastructure organizations in the area regarding security and vulnerability of systems, facilities, and equipment.
- One of the four major incidents that occurred on 9/11 – the airliner crash into the Pentagon – was within the NCR and tested the emergency services and energy sector organizations and resources in Northern Virginia, especially Arlington County, and the District of Columbia. Emergency services organizations in the surrounding areas of Virginia and Maryland also supported and backed up these efforts.
- In September 2003, Hurricane Isabel struck the east coast of the U.S. in North Carolina and proceeded up through the District, Maryland, and Virginia and had a significant impact on the NCR area. All emergency operation centers at city, county, state/District, and federal levels were activated. Isabel left many areas in the NCR without electric power for a number of days, and the resulting infrastructure problems (including communications, water and transportation) during the hurricane and the recovery period led to considerable interaction among energy infrastructure organizations, EOC’s and emergency services organizations.

2.1.2. Availability of appropriate tools

Vulnerability assessment methodologies developed by private firms are usually considered proprietary, and, for the most part, are not available in the public domain; in some cases, the customers who contract for assessment services are not left with detailed copies of the methodology. Those developed by firms for their own use are also usually not available to the public. Therefore, the number of energy-related VA methodologies available for review and evaluation in this NCR project were fewer in number than originally anticipated.

Although all energy infrastructure organizations interviewed are or have examined a range of assessment methodologies in preparation for conducting their initial assessment, regional electric and gas utilities are ahead in conducting vulnerability assessments of their system.

With one exception, all the utilities interviewed for this project have conducted one or more vulnerability assessments for their physical and cyber systems. The methodologies used range from internally developed, building sometimes on the federally funded/developed efforts to those developed by private firms and consultants. No organization was found to be using the publicly available, government-supported methodologies by itself. In some cases, the government-supported methodologies and national laboratory information were used as the starting point by the consultants or private consulting firms, but they have been greatly expanded upon and/or modified.

There are few VA methodologies available in the public domain specifically addressing the energy infrastructure: electricity, natural gas, and petroleum products. Furthermore, few of the documents found were complete VA methodologies. For example, some only address electric utility control centers, some only cover Supervisory Control and Data Acquisition (SCADA) systems, and a number are high-level system guidelines and summaries. (See Appendix B for additional details.)

Initial examination of the complete vulnerability assessment methodologies showed that the basic assessment steps were present, under one name or another. Listed below are the basic assessment steps found in the methodologies:

- I. Asset Characterization:** Collect technical (physical, cyber, etc.) descriptions of facility assets; identify hazards to the facility, its surroundings and supporting infrastructures; impact of loss of facility function (temporary and permanent), and describe existing security measures (physical, electronic, human, etc.). An organization's most critical are usually identified in this step.
- II. Threat Assessment:** Identify possible threats to the facility (both from outside and inside) and the facility's attractiveness from threat perspective.
- III. Vulnerability Analyses:** Evaluate the vulnerability of each facility using methodology and assign risk/target ratings. Questions, check-off lists, and scenarios are commonly used in conducting the analysis.
- IV. Risk Assessment:** An examination of the degree of risk of the various threats identified against each facility. Attractiveness, probability of occurrence, and consequences are usually included in this step.
- V. Mitigation Analyses:** Identification and evaluation of a range of mitigation measures to address the threats, vulnerabilities, and security issues. The evaluation can include costing, risk/vulnerability reduction, and feasibility of the options. Formal trade-off analyses are often recommended in this step.

However, when viewed closer, some items are notable for their absence or their perspective. For example, top management's integration and involvement is missing in many assessment methodologies. In some instances, the human resources areas of the assessments never reach above the middle-management levels such as head of security, emergency planner, etc. The NCR region's energy organization's response to Hurricane Isabel demonstrated that top-level management and executives are key players in the preparation for, operation during, and timely

recovery from emergency events. This aspect was emphasized in the James Lee Witt report²² which examined all aspects of the Potomac Electric Power Company's (Pepco) response to the Hurricane Isabel.

To provide more detailed information concerning the assessment methodologies and related documents listed in Table 3, brief overviews of a number of the documents are included in Appendix B: Vulnerability Assessment Methodologies. Appendix B includes a summary of the major federal vulnerability assessment methodology reports developed with support of the U. S. Department of Energy's Office of Critical Infrastructure Assurance, Office of Energy Assurance, and Office of Emergency Operations. The methodologies were developed by KPMG Peat Marwick LLP, Battelle Northwest, and Sandia National Laboratories. DOE and Battelle personnel confirmed that none of the draft assessment methodology reports have been put into final form, and that there were no plans to do so.²³

Two assessment reviews, from the federal and private sector respectively, have been selected and summarized below as examples of the material contained in Appendix B.

Federal: Vulnerability Assessment and Survey Program: Lessons Learned and Best Practices. U.S. Department of Energy, Office of Energy Assurance, September 2001.

Abstract: "This report summarizes initial lessons learned and best practices that have been captured as part of a multifaceted effort by the U.S. Department of Energy's Office of Energy Assurance (OEA) to work with the Energy Sector in developing the capability required for protecting the nation's energy infrastructures. Over the last three years, a team of national laboratory experts, working in partnership with the energy industry, has performed a series of VAs as part of OEA's Vulnerability Assessment and Survey Program. Because the assessments are conducted on a confidential basis, the information in this report is intentionally presented at a high level so as not to reflect on specific companies or industry segments."

Comment: This report briefly and generally describes fourteen "best practices" and ten "lessons learned" that resulted from Sandia National Laboratories' validation of the VA methodology at 11 gas and electric utilities around the U.S. With 11 assessments to draw upon, the number and extent of the "best practices" and "lessons learned" documented in this report were disappointing. Results obtained from the assessments could be described in a manner that would not lead to specific identification of organizations but would be of significant value to the hundreds of other utilities involved in similar efforts.

Best Practices: In the "best practices" list, no information was included that indicated the metrics that were used to grade individual practices, what criteria were established and used to identify best practices, and what ranges of practice were found among the organizations assessed; also, the potential economic impact of adopting these specific practices was not discussed. It is not clear if the "lessons learned" were by the national laboratory personnel developing and validating the methodology or by the participating utilities' personnel based upon the range of present industry practices.

Lessons Learned: A total of 38 bulleted lessons were listed and they were grouped in 10 categories.²⁴ In the brief bullet descriptions of each lesson, there was again neither a discussion of the range of practices found across the 11 organizations nor a justification

for, value of, or expected increase in the level of security that could be expected by following the "...should be ...should not be..." descriptive statements.

Interdependency Awareness: There were no "best practices" identified in the report that related to infrastructure interdependencies.

Petroleum: Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries²⁵

Abstract: "This methodology was prepared by the American Petroleum Institute (API) and the National Petrochemical & Refiners Association (NPR) Security Committees to assist the petroleum and petrochemical industries in understanding Security Vulnerability Assessment (SVA) and in conducting the assessments. The guidelines describe an approach for assessing security vulnerabilities that is widely applicable to the types of facilities operated by the industry and the security issues they face. During the development process it was tested at two refineries, two tank farms, and a lubricating oil plant, which included typical process equipment, storage tanks, marine operations, infrastructures, pipelines, and distribution terminals for truck and rail. Based on these trials and the generic nature of the overall methodology, its use at other types of petroleum and petrochemical facilities is expected to be suitable. Future editions will address other operations within the petroleum industry. The methodology is presented as one approach for assessing security vulnerabilities at petroleum and petrochemical industry facilities, and is not intended to supplant measures previously implemented or to offer commentary regarding the effectiveness of any individual company efforts."²⁶

Comment: This is a comprehensive vulnerability assessment document, with a systematic set of questions and check-off boxes to guide the team through the assessment process.

The methodology identifies six basic elements of a proper SVA:

1. Characterize the facility to understand what critical assets need to be secured, their importance and their interdependencies and supporting infrastructure;
2. Identify and characterize threats against those assets and evaluate the assets in terms of attractiveness of the targets to each adversary and the consequences if they are damaged or stolen;
3. Identify potential security vulnerabilities that threaten the asset's service or integrity;
4. Determine the risk represented by these events or conditions by determining the likelihood of a successful event and the consequences of an event if it were to occur;
5. Rank the risk of the event occurring and, if high risk, make recommendations for lowering the risk;
6. Identify and evaluate risk mitigation options (both net risk reduction and benefit/cost analyses) and re-assess risk to ensure adequate countermeasures are being applied.

Interdependence Awareness: The methodology stresses that SVA teams should identify the critical internal and external infrastructures and their interdependencies (e.g., electric power, petroleum fuels, natural gas, telecommunications, transportation, water, emergency services, computer systems, air handling systems, fire systems, and SCADA systems) that support the

critical operations of each asset. For example, the electrical substation may be the sole electrical supply to the plant, or a supplier delivers raw material to the facility via a single pipeline.

Much of the methodology's value with respect to interdependencies lies in a comprehensive checklist for infrastructure and interdependencies that can be used both before and after a SVA for ensuring completeness.

2.1.3 Extent to which tools are being used through resource allocation.

Organizations had differing criteria for prioritizing expenditures on mitigation measures after an assessment had been made. One organization utilized decision support software that the assessment contractor had, and developed priorities for security investments in that manner. Others utilized in-house approaches to set investment priorities.

As the size of the energy organization got smaller the range of mitigation options that could be funded was significantly reduced. Items such as a small number of surveillance cameras and card entry systems at a few facilities were affordable, but high-priced items were out of range. In general, larger organizations sometimes fund significant efforts that could not even be considered by small organizations, either public or private.

For smaller organizations security and mitigation investment decisions appear to have been made higher up in the organization. With the small organizations, boards of directors and commissions were directly involved in the process and decisions, in addition to organization management personnel.

Both the industry organization and the industry association personnel interviewed indicated that results of specific vulnerability assessments and risk management processes did result in changes in capital construction and operating budgets and, in some cases, modification of the organization's insurance programs.

2.1.4. Extent of implementation of CIP measures

Implementation of Mitigation Measures

Identification of the top critical facilities in their system almost always led to installation of new/increased security systems: physical, electronic, surveillance, some changes in operating procedures, and some changes in personnel training. However, individual infrastructure organizations and their industry associations were not willing to share details regarding their mitigation or correction activities, either what they were spending or what they were doing. The best information shared indicated that first, it was a direct function of the size of utility, and second, expenditures ranged from less than one million dollars to tens of millions of dollars.

The public disclosure of details related to identification of system vulnerabilities, mitigation activities undertaken, or levels of security-related expenditures are the principal reason most utilities give for not having gone to state utility commissions for reimbursement for these expenditures. In a recent study,²⁷ the National Association of Regulatory Commissioners (NARUC) surveyed actions taken by utilities and utility commissions in all states. Some state PUC's have implemented expedited approval procedures and some have developed special handling procedures. However, all procedures end in a full rate case where all utility actions are open to public review. Many utilities seem unwilling to risk release of their security-related

efforts, so they have chosen not to initiate a formal process for reimbursement of these expenses. Due to the sensitive and proprietary nature of these investments, the study did not assess the impact of utility risk-aversion on actual investments.

Extent of Implementation of Cyber Mitigation Measures

With one exception, utility personnel interviewed indicated that their organizations had contracted with various software and computer systems consulting firms to periodically conduct exercises to test the vulnerability, defense, and penetrability of their SCADA, communications, and computer systems. Those organizations that have the testing programs in place for their cyber systems indicated that each time these exercises are conducted, the organizations learn a great deal about their level of cyber security.

For the most part, electric utilities own their SCADA networks. These are primarily microwave-based but a growing portion use fiber optic cable. As most of the original SCADA systems at electric utility facilities were installed by contractors using proprietary software and platforms, their vulnerability to cyber intrusion was considered low. However, many of these facilities, including those for power plants, transmission and distribution substations and system operating centers are being upgraded or replaced, and in the process moving to common software platforms and operating systems. Because of the level of public knowledge about these platforms, associated hardware and operating systems, their vulnerability to intrusion has increased significantly. The trend toward merging of utilities into regional transmission organizations (RTO's) can only be expected to accelerate the adoption of common operating systems.

Even though electric utilities own most of their own systems, they contract with commercial communications companies for a wide range of support services for SCADA, computer and communications systems. These actions have also increased the system vulnerability. High security circuits and systems are available from commercial vendors, but they can be very expensive to use.

However, the majority of natural gas and petroleum transmission companies' SCADA systems operate exclusively on commercial communication company transmission facilities. As a consequence, the exposure to security and reliability problems is much higher than for electric systems. The refining and processing sector of the oil industry has only added new processing capacity to existing facilities in the U.S. in a number of decades and many of the older facilities continue to use their original, proprietary hardware and software. As a result, the facility owners do not believe their cyber systems have high degrees of vulnerabilities to outside intrusion. SCADA systems for expansion projects at existing oil refining and processing facilities are, like new electric facilities, beginning to use common platform control systems and thus their vulnerability to outside intrusion will increase.

2.1.5 Extent of Evaluation of CIP Effectiveness

With the not insignificant number of privately developed, proprietary assessment methodologies being used today, the NCR Project's approach – examine publicly available methodologies for review and analysis – may not result in the development of a true “best practices” framework. A considerable number of methodologies are being left out of the process. In order to ensure a

“better practices” approach, a mechanism will be needed to establish relations with private firms –to allow limited access to these private sector methodologies.

With respect to the metrics used to determine levels of security, the study revealed that some VA methodologies produce a single number, others compare VA results to a series of security levels, and others don’t produce a numerical result at all. With this range of results, it will be difficult to obtain a single, comparable, level of security from each segment of the infrastructure, let alone for the energy infrastructure as a whole.

Organizations were also asked about reexamining assessment results and ratings after various risk reduction measures had been completed or implemented. In some instances, the organizations had not redone that portion of the assessment so they did not know how the mitigation measures had changed their security or vulnerability level. In other cases, the organizations had gone back and reviewed the assessment findings with the mitigation measures in place. In general, the organizations were not confident in the exact changes in security or vulnerability the mitigation measures had achieved.

All organizations interviewed indicated that their preparation for, operation during, and recovery from Hurricane Isabel taught them a number of valuable lessons about their system security and vulnerability. All have made a number of changes including upgraded design parameters for facilities, changes in operating procedures, increases in coordination of communications with similar infrastructure organizations located nearby, and heightened need for exercising their emergency plans and operations.

Electric, gas, or petroleum organizations were asked whether they had evaluated and were using the Sandia-developed Risk Assessment Methodologies. These computer-guided tools were developed for electric transmission systems (RAM-T), hydroelectric facilities (RAM-D), and petroleum/chemical facilities (RAM-CF). The responses were usually [paraphrased] “...yes we looked at them, our security personnel conducted a detailed review of the tool(s), and in some instances, even sent company personnel to the formal training workshops. But, for a variety of reasons, we are not using them.” These comments came from both individual infrastructure organizations and industry association personnel. One federal agency and one large private chemical firm were identified as using these tools. The study team believes that at least part of this reduced enthusiasm is based on the data-intensive nature of these methodologies.

3. Risk Reduction Programs and Processes

3.1 Measuring Effectiveness

One approach to measuring effectiveness is to develop a comprehensive “methodology framework.” NCR infrastructure organizations could then compare their methodologies and the recommended framework and modify their procedures for subsequent assessments. To be truly effective, the methodology should encourage firms to clearly articulate the extent of their infrastructure vulnerability and interdependency, the cost of implementing identified mitigation measures and the resulting increase in security.

3.2 *Managing Continuous Improvement*

While organizations should be encouraged to continuously modify their vulnerability assessment methodologies, an in-depth evaluation of the growing dependence of the energy infrastructure upon the Internet for SCADA, energy management, and other critical energy sector functions needs to be conducted. In addition, an in-depth survey of on-site emergency generators and their operating status and refueling strategies would go far to increase the reliability and security of emergency units in the NCR.

In parallel with these efforts, an independent monitoring and review pilot program should be initiated to assess and document firm response to federal (FERC and RUS) and NERC security actions related to increasing levels of security. This also needs to be accompanied by a credentialing process to ensure access to incident sites for key energy sector personnel in order to coordinate sector assessment, restoration and repair efforts.

4. **Conclusions**

Based on direct interviews with energy infrastructure firm personnel as well as energy industry association staffs, and supported by direct review of a number of publicly available vulnerability assessment/risk management methodologies, the energy sector team developed a number of conclusions:

- With very few exceptions, mainly in the natural gas and petroleum areas, the publicly available methodologies examined do not adequately address the area of infrastructure interdependencies, either within a single sector or among infrastructures. However, how the methodologies actually used by NCR electric utility organizations handle this aspect is presently unknown. Therefore, the actual vulnerability of infrastructure interdependencies in this area is still unknown outside the specific firms and in most instances unknown inside the firm.
- All but one of the energy infrastructure organizations interviewed in the NCR have gone through the vulnerability assessment process at least once. With the exception of some gas and petroleum product companies, they did not rely solely on publicly available methodologies found in this project.
- The energy infrastructure organizations interviewed did not normally interact with upstream suppliers of critical services during the assessment process. The assessment process was conducted to the organization's physical property lines, to common interconnection points, and no further. None had been invited to participate in other infrastructure organization's process where they were a critical supplier to the other organization.
- Industry organizations, along with some government agencies including the Rural Utility Service (RUS) of the U.S. Department of Agriculture (USDA), have stated that one single vulnerability assessment methodology will not work for all energy organizations.
- For small utilities and firms, public, private, or cooperative, the in-house technical capability can be very limited. At some organizations, there may be very few or no engineers. In these instances, utilizing an assessment methodology that is very technically based and requires significant data collection and technical support is not useful for or usable by smaller energy organizations.
- Considerable action by the federal government – Federal Energy Regulatory Commission (FERC) and the RUS – and industry organizations – North American Electric Reliability

Council (NERC) – has been initiated that is expected to result in increased security-related actions, including vulnerability assessments, by electric utilities before the end of July 2005. However, it is not clear whether any action will be taken to validate these actions or individual organization certifications.

- Some energy utilities that serve the NCR state they are reluctant to initiate actions with state or District Public Utility Commissions (PUC's) to obtain reimbursement for security-related expenditures because of the possibility of disclosure of security and vulnerability details during subsequent rate procedures. The major problem stated is potential liability if the information is made public. This may limit the extent of voluntary investment since the cost is presently being borne by company stockholders.
- More and more energy management, SCADA, and other energy infrastructure communications and control functions are dependent upon the Internet for services; and thousands of new systems are added each year. Many utility personnel, in both the executive and operating areas, do not realize their organization's growing use and dependence upon the Internet and their increasing vulnerability to outside intrusion.
- Small electric and gas utilities are very concerned with what they see as "looming security requirements" that they cannot afford or that the results will not benefit their customers. Small utilities with a few tens of thousands of customers do not have the resources to adopt a complex assessment methodology and invest in a number of mitigation measures that may be imposed upon them by federal legislation or mandate without outside support.
- Electric utility personnel, emergency managers, and NCR Emergency Operations Center (EOC's) personnel again brought one aspect up that has been identified in a number of earlier NCR-related infrastructure studies: the high failure rate of on-site emergency generation facilities at both public and private facilities. An additional perspective came to light during these interviews. The owners/operators of facilities for a range of vulnerable populations (hospitals, nursing homes and critical care facilities) in the NCR also do not adequately prepare for natural disasters or other situations where their electric service may be interrupted. These facilities include nursing homes, convalescent facilities, intermediate medical facilities, retirement communities, and especially multi-story facilities that cater to these populations.
- In those instances where risk reduction measures had been completed or implemented, organizations often either had not reviewed the assessment findings with the mitigation measures in place or were not confident in the exact changes in security or vulnerability the mitigation measures had achieved.
- One surprising finding was the vulnerability and sensitivity of energy organization workers, whether equipment operators, maintenance personnel, or telephone operators manning call centers during emergencies. Extreme workplace demands often compete for their attention with personal and family concerns, especially during long-duration situations (e.g., Hurricane Isabel). This human resource issue appears to receive little attention.

Recommendations:

The principal recommendations from the study are grouped into four major categories:

Assessment Methodology

- The NCR infrastructure organizations should modify their procedures to conform to an established model based upon best practices, where appropriate, for their next (usually annual) assessment.
- Relations should be established with selected private firms, with the assistance of high-level DHS executives and its advisory panel members, to obtain at least limited access to private sector methodologies for review.
- All vulnerability assessments should include participation/ interaction by critical upstream suppliers from the same and other infrastructures.
- Tools need to be developed to allow NCR energy infrastructure organizations to establish the actual extent of infrastructure interdependency vulnerability in the NCR area.

Tactical Steps for Immediate Benefit

- An in-depth evaluation of the growing dependence of the energy infrastructure on the Internet is needed. A number of modest efforts are looking at various aspects of this situation; however, there are no comprehensive studies examining the increasing threat of vulnerabilities of products being developed for future adoption by the energy industry.
- An independent monitoring and review pilot program should be initiated in order to assess and document electric utilities' (private, public, and cooperative) response to increased federal North American Electric Reliability Council and Rural Utilities Service security recommendations and guidelines.
- An in-depth survey of on-site emergency generators needs to be conducted--units tested and refueling strategies developed to increase the reliability and security of the hundreds of existing emergency units in the NCR.
- A credentialing process for key energy sector personnel should be established to ensure priority access to incident sites in order to coordinate sector assessment, restoration and repair efforts.

Governance Recommendation at Sector-Level

- The regional Public Utility Commissions should consider procedures to explore the prudence of security investments and expenditures to limit the distribution of critical security data and information. A joint FERC–PUC pilot project may offer a suitable venue to address this question.
- A regional workshop should be held in the NCR to address how utilities could recover their security-related investments via rate hearings without having to reveal sensitive security-related information in a public forum.

Service to Vulnerable Populations

- Owners/operators of facilities that serve vulnerable populations should prepare and implement plans to ensure energy availability and continuity of operations in the event of extended power outage. Public agency emergency managers, utilities, and fuel distribution firms and associations should participate in the process with emphasis on identifying business opportunities to serve these populations during emergencies.

Appendix A: Project Approach and Data Collection

Introduction

Literature search and review

- Commercial search engines: AltaVista, Yahoo, etc.
- Government databases and search engines: DOE's Office of Scientific and Technical Information (OSTI), FirstGov.gov U.S. Government Web Portal.

Field work

In the Energy Infrastructure area, after the initial telephone contact was made and the proper person(s) identified, an introductory package of materials was sent which included: 1) an introductory letter requesting the firm's cooperation and support, signed by NCR Senior Policy Group members; 2) one-page description of the overall project the organization; and 3) a brief topical outline of the areas where questions would be asked. It was made very clear from the very first contact that the interviews would concentrate on the assessment process and the methodology used and NOT on any results of the assessment. Because of the large number of energy organizations that serve customers in the NCR, especially in the oil and petroleum products area, interviews from all the organizations were not possible. The firms selected for interviews were considered reasonable representatives of the industry organizations serving the region.

Initially, industry associations in the electric power, natural gas, and petroleum industries were contacted and personnel whose area of responsibility included security were interviewed. This was done to ensure that no significant factors or issues were overlooked by the fact that not all firms serving the NCR were interviewed. Also, it was desired to know if the energy firms serving this area were further along in upgrading levels of security or were representative of their industry sectors. Personnel from the following industry associations were interviewed as part of this project:

- American Gas Association – Represents investor-owned gas distribution utilities
- American Petroleum Institute – Represents investor-owned oil companies
- American Public Power Association – Represents publicly owned electric utilities
- Edison Electric Institute – Represents investor-owned electric utilities
- National Rural Electric Cooperative Association – Represents consumer-owned electric utilities

After the association personnel were interviewed, then interviews were conducted with representatives at the selected energy firms themselves. With only one exception, the energy infrastructure organizations contacted all agreed to cooperate with the project. In some instances, Non-Disclosure Agreements were required to be signed by the interviewers prior to the meetings.

At each Energy Infrastructure organization where interviews were conducted, the objectives were to first talk with personnel from a number of areas that had actually participated in the

vulnerability assessment conducted by the firms and then speak with an executive of the firm who has responsibility for security. The original letter inquiry included a request to speak with representatives in the areas listed below.

- Security - Physical
- Operations
- Information/Communications
- Human Resources/Personnel
- Engineering/Design
- Company Executive – Responsible for Security

The group interviews normally lasted about 60 to 90 minutes and the executive interviews about 60 minutes. Although the titles of the personnel in the group interviews varied from organization to organization, most of the areas listed above were covered by one or more interviewees.

Other Utility Input

During the course of this project, Virginia Tech personnel were involved in two other projects that involved interviewing energy utility personnel who managed or were involved with emergency management, security, and/or insurance programs at their utilities. This provided an opportunity to inquire about whether the individual organizations had conducted risk and/or vulnerability assessments and ask a few general questions related to the methodologies used and their experience with the assessment process. The inquiries made as part of these other projects, however, were not full interviews as described above. And again, questions related to the results of the assessment were not asked.

Although, the information obtained from these sources outside the NCR was kept separate from the results of the NCR project, the information was similar to and tended to confirm the responses being provided by energy organizations within the NCR.

The following is a list of the utilities that were contacted as part of these other two projects and where their personnel graciously responded to the inquiries related to topics of interest in this project:

- Duke Power Company, NC
- Kissimmee Utilities Authority, FL
- Long Island Power Authority, NY
- Orlando Utilities Commission, FL
- Progress Energy, NC
- Reedy Creek Energy, FL
- Salt River Project, AZ
- Sumter Electric Cooperative, Inc. FL
- Tampa Energy Corp. – Peoples Gas, FL

Appendix B: Vulnerability Assessment Methodologies – Summaries

1. Review of Cross-Sector Tools

Computer modeling of individual infrastructures has been done since the 1950s when analog network analyzers were used to support system design and steady-state operation. Since the early 1960s, digital computers have been used to conduct both steady-state and dynamic analyses of entire infrastructure systems; the computer models examined system flows, operation under both normal and emergency conditions; system stability under a variety of situations, economic control and dispatch, and planning options. These early computer models were primarily for individual systems; interdependencies were usually not examined.

As the capabilities of digital computers grew, the models expanded to allow evaluation of operation and reliability of multiple infrastructure organizations over large regions of the U.S.

2. Review of Sector-Specific Tools

Beginning in the late-1990s, DOE began supporting the development of more advanced computer models because of heightened security concerns of the nation's infrastructures. These advanced models included interconnection and interdependency aspects. A number of DOE's laboratories participated in these efforts, including Argonne, Berkeley, Los Alamos, Oak Ridge, and Sandia National Laboratories. In addition, individual industry organizations are also supporting development of advanced infrastructure system models (e.g., Electric Power Research Institute).

It has only been recently that infrastructure interdependencies have come to the fore as a critical issue. The Presidential Decision Directive 63 (PDD-63) on Critical Infrastructure Protection raised the level of concern for the infrastructures and their interdependencies. Their importance has become even more significant as a result of the events of September 11, 2001. During recent major natural disasters – earthquakes in California, tornados in Oklahoma, hurricanes in Florida, and floods in the Midwest – most or all of the service infrastructures were put out of service over a wide area for a period of time. However, during some events, for instance in September 2003 Hurricane Isabel impact on the Mid-Atlantic coastal states, the electric power distribution system infrastructure was devastated, water and wastewater facilities significantly damaged in certain areas, and many local roads and highways were obstructed for significant periods. Isabel dramatically demonstrated the high level of interdependency of all the infrastructures on each other and society's increasing dependency on all of them.

Because of the length of the electric service outage in parts of the District of Columbia, Maryland, and Virginia – for some customers in these areas electric service was not restored for almost two weeks – the shorter term emergency provisions that had been made by government agencies, businesses, and citizens were not adequate.

3. General Assessment Methodologies

To provide a general view of the assessment methodologies and related documents listed in Table 3, the following are brief overviews of a number of the documents. The approach used in these reviews was to examine what the report itself said, to specifically look at key areas where weaknesses have been identified in other methodologies (e.g., interdependencies), and finally

provide brief comments and/or comparisons to other methodologies. The overviews here are not complete area-by-area or question-by-question comparisons.

Vulnerability Assessment Framework 1.1, U.S. Department of Energy, Critical Infrastructure Assurance Office, October 1998.

Abstract: “Presidential Decision Directive 63 directs every department and agency of the Federal Government to develop a plan by November 18, 1998, to protect its own critical infrastructure, including but not limited to its cyber-based systems...The Vulnerability Assessment Framework (VAF) is designed to assist your agency’s work on these issues... Based on existing security requirements and standards, the VAF can be applied across the federal government as well as to private sector infrastructures.

“Through a three-step process, the VAF will enable your organization to define your Minimum Essential Infrastructure (MEI), identify and locate interdependencies and vulnerabilities of your MEI, and provide the basis for developing your remediation plans. The VAF has been designed with inherent scalability so that it is applicable to all levels of government as well as broad sectors of the National infrastructure.”

Comment: Although primarily developed for federal departments and agencies, this Framework is a good approach to vulnerability assessments and can serve as a basis for public and private infrastructure organization’s conduct of assessments. The Preface, Chapter I: Introduction, and the Appendix G White Paper – The Clinton Administration’s Policy on Critical Infrastructure Protection: PDD 63, provide a foundation for understanding the logic and reasoning behind the Vulnerability Assessment process in the 1998 time period. The contractor that developed the Framework, KPMG Peat Marwick LLP, “...has taken a business approach to developing this vulnerability assessment tool as opposed to a national security approach. The former incorporates established business risk assessment measurements in a holistic approach to assessing physical and cyber vulnerabilities. The latter has historically been primarily driven by the known or suspected capabilities of identified adversaries.”

This Framework discussion also emphasizes the critical nature of the direct involvement of an organization’s senior executives in the security program and the vulnerability assessment process.

The major emphasis of this Framework is on Information Technology (IT) but the range of areas in the assessment process includes physical facilities. If this Framework is used by Energy infrastructure organizations as a starting point for the development of their assessment methodologies, it will have to be considerably expanded in the areas of physical plant, SCADA and other control systems, institutions, and functions.

This Framework uses a three-step approach that follows, in general, that of other publicly available Vulnerability Assessment methodologies; the steps are briefly described below. Each step includes Objectives, Critical Success Factors, Expected Outcomes, and Activities. The discussion in each area provides reasonably good, if general, information regarding the various aspects of each step.

Step 1: Establish Agency Minimum Essential Infrastructure (MEI) – Determine the minimum specific infrastructure components that are absolutely fundamental to achieving an organization’s core mission.

Step 2: Gather Data to Identify MEI Vulnerabilities – Review actions, devices, procedures, techniques, and other measures that potentially place the organization’s MEI resources at risk.

Step 3: Analyze and Prioritize Vulnerabilities – Define and analyze vulnerabilities identified enabling at least a first order of prioritization for purposes of remediation or minimization.

Specific questions for obtaining information related to each step area are provided in appendices. Each is divided into Control Objectives, Control Technique, and Compliance Procedures. However, in a large number of the questions, the Compliance Procedures state that the assessment team should “Interview Senior Management.” In many instances covered, Senior Management personnel may not know the answers and are looking to the assessment team to provide the information.

Interdependency Awareness: The discussion in the Framework’s Introduction stresses the importance of understanding an organization’s interdependencies and the “substantial vulnerabilities” to threats, both domestic and international, associated with these interdependencies. However, the language of the Framework is very general; it states that interdependencies are “... addressed at the high-end macro level” (Pages 32-33). And in the appendices, interdependencies are covered on one-half page and ask only two questions; these are reproduced below.

Interdependence Awareness (Page D-22)

Control Objective	Control Technique	Compliance Procedures
8.1 Organization is aware of interdependencies	Has management considered the effect of the loss of a national infrastructure component, such as: Loss of power for an extended period of time Loss of water supply Loss of telecommunications Loss of transportation system Loss of oil or gas	Interview senior management
8.2 Management has recognized dependence on outside sources.	Has the organization constructed redundant resources in critical areas?	Interview senior management Review architecture diagrams

Vulnerability Assessment and Survey Program: Overview of Assessment Methodology. U.S. Department of Energy, Office of Energy Assurance, September 2001.

Abstract: “This report provides a high-level overview of the vulnerability assessment methodology that is being developed and validated by the U.S. Department of Energy’s Office of Energy Assurance (OEA) as part of its multifaceted mission to work with the Energy Sector in developing the capability required for protecting the nation’s energy infrastructure.”

Comment: As stated above, this is a high-level overview that briefly describes “what” the steps in the OEA-funded VA methodology are. Sandia and Battelle National Laboratory personnel were involved in developing and validating the methodology. This document does not present any detail and speaks only in generalities about the process. It also does not provide the reader with an idea of the resources necessary to use this methodology nor to conduct a vulnerability assessment.

The report introduction states that the OEA effort is to “...develop, validate, and disseminate a VA methodology with associated tools to assist in the implementation; provide training and technical assistance; and stimulate action to mitigate significant problems.”

To validate the methodology, eleven utility assessments – under the guidance of national laboratory personnel – were conducted with voluntary electric and gas utilities in the U.S. One (1) electric and one (1) gas utility in the NCR participated in these early assessment efforts. The original agreements between DOE/Sandia and the utilities indicated that all materials developed in the course of the assessment that related to results and specific findings would be returned to the participating utility at the completion of the effort; this material was considered extremely sensitive by the utilities. However, problems arose when DOE headquarters personnel wanted to retain copies of the assessment results for use in other projects; this led to at least the NCR utilities terminating further assessment activities with Sandia.

Interdependency Awareness: The discussion and guidance related to infrastructure interdependencies in the body of the report are very short, consisting of a general definition and only a brief discussion (Section 4.9 – Page 18); these are reproduced below:

“The term ‘infrastructure interdependencies’ refers to the physical and electronic (cyber) linkages within and among our nation’s critical infrastructures – energy (electric power, oil, natural gas), telecommunications, transportation, water supply systems, banking and finance, emergency services, and government services. This task identifies the direct infrastructure linkages between and among the infrastructures that support critical facilities as recognized by the organization. Performance of this task requires a detailed understanding of the organization’s functions, internal infrastructures, and how these link to external infrastructures.

“The purpose of the infrastructure interdependencies assessment is to examine and evaluate the infrastructures (internal and external) that support critical facility functions, along with their associated interdependencies and vulnerabilities.”

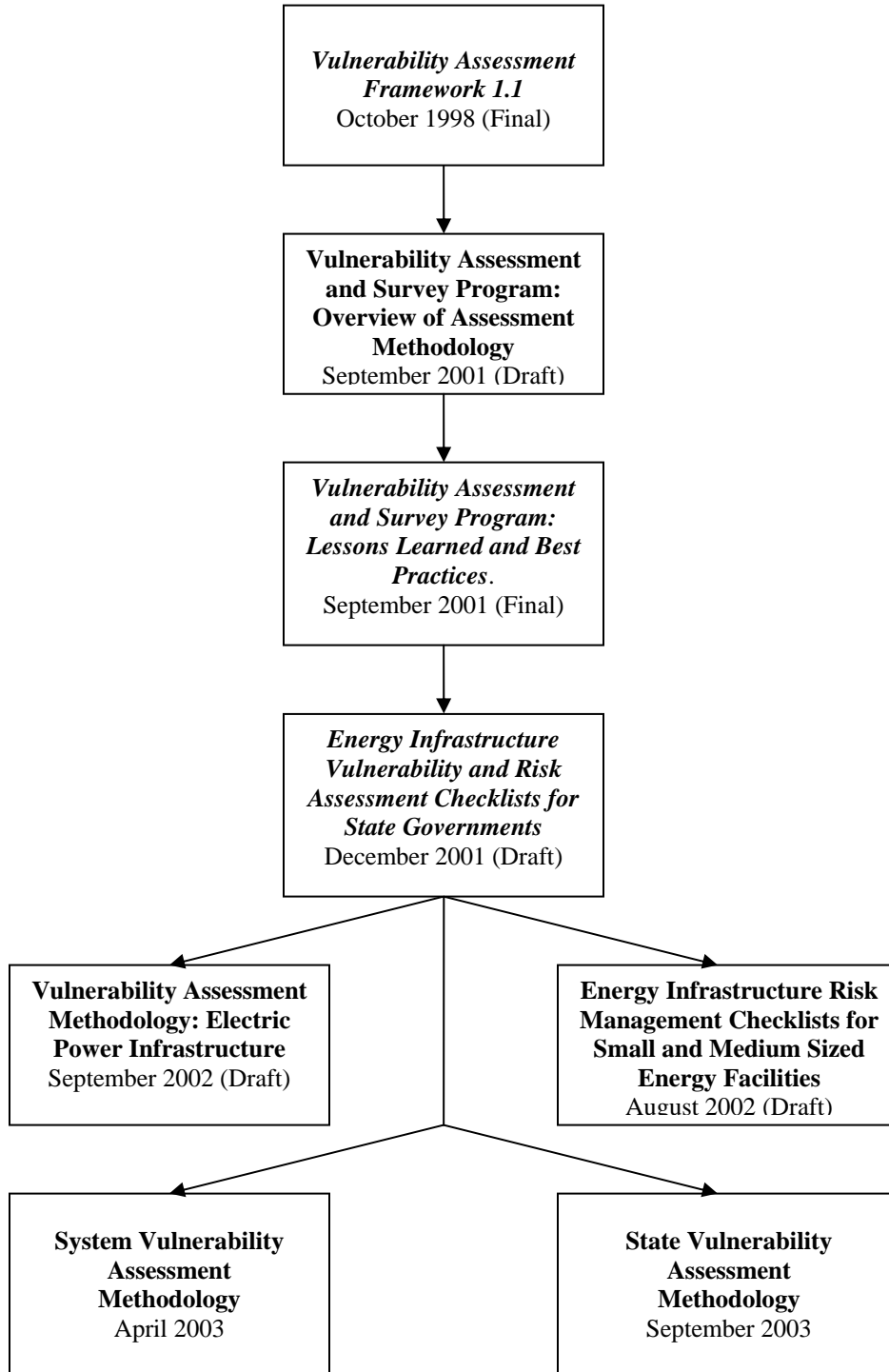
In Appendix B of this report, there is a one-page listing of types information needed – to be obtained and/or developed – to respond to questions relating to infrastructure interdependencies in the assessment. The major emphasis in the items listed relate to an organization’s buildings and facilities and the outside utilities that serve them.

Federal VA Reports

Figure 7 provides a schematic representation of the major federal Vulnerability Assessment methodology reports developed with support of the U. S. Department of Energy’s Office of Critical Infrastructure Assurance, Office of Energy Assurance, and Office of Emergency Operations. The methodologies were developed by KPMG Peat Marwick LLP, Battelle Northwest, and Sandia National Laboratories. In discussions with DOE and Battelle personnel,

it was confirmed that none of the draft assessment methodology reports have been put into final form, and also that there were no plans to do so.

Figure 7: Department of Energy Vulnerability Assessment Methodology Reports
(Offices of Critical Infrastructure Assurance, Emergency Operations, and Energy Assurance)



Vulnerability Assessment Methodology: Electric Power Infrastructure (Draft), U.S. Department of Energy, Office of Energy Assurance, September 30, 2002.

Abstract: “This report is an update of the “*Vulnerability and Risk Analysis Program: Overview of Assessment Methodology,*” report, dated September 28, 2001. [See above] The initial report provided a high-level overview of the vulnerability assessment methodology being developed and validated by DOE’s Office of Energy Assurance (OEA) “... This updated report focuses specifically on a methodology that has been applied to the electric power infrastructure and at a more detailed level. Over the last five years, a team of national laboratory experts, working in partnership with the energy industry, has successfully applied the methodology as part of the OEA’s Vulnerability Assessment Program (VAP) to help energy sector organizations identify and understand the threats to and vulnerabilities (physical and cyber) of their infrastructures. Lessons learned from these assessments, as well as best practice approaches to mitigate vulnerabilities, are continuing to be documented in related reports ...”

“The purpose of this report is to provide a methodology resource for the electric power industry ...”

“Fourteen vulnerability assessments (and 20 vulnerability surveys/quick-turnaround assessments) have been completed under this initiative (several more are in progress and in the planning stages). To date, 13 of the vulnerability assessments and 10 of the vulnerability surveys have focused on the electric power infrastructure ...”

Comment:

Interdependency Awareness:

The discussion of Infrastructure Interdependencies (Section 4, page 18) in this Vulnerability Assessment Methodology is very general and does not provide in-depth guidance for a user. The discussion is reproduced below:

“The term ‘infrastructure interdependencies’ refers to the physical and electronic (cyber) linkages within and among our nation’s critical infrastructures – energy (electric power, oil, natural gas), telecommunications, transportation, water supply systems, banking and finance, emergency services, and government services. This task identifies the direct infrastructure linkages between and among infrastructures that support critical facilities as recognized by the organization. Performance of this task requires a detailed understanding of the organization’s functions, internal infrastructures, and how these link to external infrastructures.

“The purpose of the infrastructure interdependencies assessment is to examine and evaluate the infrastructures (internal and external) that support critical facility functions, along with their associated interdependencies and vulnerabilities.”

There are 12 items on the Information Request list that relate to infrastructure interdependencies (Appendix B.9, Page 38-39) and a list of 13 people to interview – all internal to the organization. The four Issues to be addressed are: 1) single-point infrastructure failures, 2) infrastructure backup, 3) commercial infrastructure reliance, and 4) historic/current problems and concerns. Appendix B.9 also contains a series of checklists that indicate the heading of areas to be investigated. These are:

9.1 Infrastructure Oversight and Procedures	9.8 Emergency Services*
9.2 Electric Power Supply and Distribution	9.9 Internal Computers and Servers*
9.3 Petroleum Fuels Supply and Storage	9.10 HVAC Systems
9.4 Natural Gas Supply	9.11 Fire Suppression and Fire Fighting
9.5 Telecommunications	9.12 SCADA System
9.6 Transportation	9.13 Physical Security System
9.7 Water and Water System	9.14 Financial System*

* These three Checklist areas included the following: “NOTE: This infrastructure area is not of primary concern for this survey and can be eliminated if useful information is not readily available.”

Vulnerability Assessment and Survey Program: Lessons Learned and Best Practices. U.S. Department of Energy, Office of Energy Assurance, September 2001.

Abstract: “This report summarizes initial lessons learned and best practices that have been captured as part of a multifaceted effort by the U.S. Department of Energy’s Office of Energy Assurance (OEA) to work with the Energy Sector in developing the capability required for protecting the nation’s energy infrastructures. Over the last three years, a team of national laboratory experts, working in partnership with the energy industry, has performed a series of VAs as part of OEA’s Vulnerability Assessment and Survey Program. Because the assessments are conducted on a confidential basis, the information in this report is intentionally presented at a high level so as not to reflect on specific companies or industry segments.”

Comment: This report briefly and generally describes 14 “best practices” and 10 “lessons learned” that resulted from Sandia National Laboratories’ validation of the VA methodology at 11 gas and electric utilities around the U.S. With 11 assessments to draw upon, the number and extent of the “best practices” and “lessons learned” documented in this report were disappointing. Results obtained from the assessments could be described in a manner that would not lead to specific identification of organizations but would be of significant value to the hundreds of other utilities involved in similar efforts.

Best Practices: In the “best practices” list, no information was included that indicated the metrics that were used to grade individual practices, what criteria were established and used to identify best practices, and what ranges of practice were found among the organizations assessed. This omission raises the critical question: How were these 14 best practices selected?

The 14 “best practices” were grouped into three issue categories: organization (9), education and awareness (4), and staffing (1). In most cases, the practices described could be classified as “things to do” but were not the “best way of accomplishing” a specific goal or practice. There was no discussion of the range of practices that were found and how the best practice was identified and why it was selected to accomplish a specific goal. There was also no discussions of how, why, or by how much this specific best practice would decrease vulnerability or increase security of a facility, system, or organization.

Also, the potential economic impact of adopting these specific practices was not discussed. For instance, Item 5 in the list (Page 5) was: “Best Practice: Implement structured security requirements for critical suppliers and partners. Make security reviews an element of contracts for critical services and periodically evaluate compliance.” Imposing additional security requirements on suppliers could have major contract cost implications for a utility but no mention of increased costs vs. increased security levels was made.

Other best practices listed simply discussed the obvious, such as Item 8 in the list (Page 6): “Best Practice: Periodically review and update emergency plans to include newer threats and vulnerabilities, and test these plans regularly.”

In addition, after working with 11 gas and electric utilities around the U.S., a reader of this report should expect to have a considerable number of “best practices” identified and discussed for each part of the VA methodology’s three major segments.

Lessons Learned:

In the list of “lessons learned,” each lesson was identified by a bullet with a one or two sentence description. A total of 38 bulleted lessons were listed and they were grouped in 10 categories: Network Architecture (5), Threat Environment (4), Penetration Testing (2), Physical Security (7), Physical Asset Analysis (2), Operations Security (6), Policies and Procedures (3), Impact Analysis (2), Infrastructure Interdependencies (4), and Risk Characterization (3).

There were again a few gems of value among the lessons identified, such as in Section 3.1 Network Architecture (Page 9 – Third bullet): “The trend in IT is to outsource more and more functions. Cyber security, however, should remain as an enterprise function, and not become a contractor function.”

In the brief bullet descriptions of each lesson, there was again neither a discussion of the range of practices found across the 11 organizations nor a justification for, value of, or expected increase in the level of security that could be expected by following the “...should be ...should not be...” descriptive statements.

Interdependency Awareness:

There were no “best practices” identified in the report that related to infrastructure interdependencies. There were four bulleted “lessons learned” that related to interdependencies (Page 12); however, as reproduced below, the descriptions were all very general:

- “Interdependencies among the infrastructures must be thoroughly investigated because they can create subtle interactions and feedback mechanisms ...
- “Interdependencies increase the complexity of the infrastructures and introduce additional vulnerabilities.
- “Interdependencies among the infrastructures vary significantly in scale and complexity and they typically involve many system components ...
- “Contingency and response plans need to be evaluated from an infrastructure interdependencies perspective and coordination with other infrastructure providers needs to be enhanced.”

It is not clear if the “lessons learned” were by the national laboratory personnel developing and validating the methodology or by the participating utilities’ personnel based upon the range of present industry practices.

Energy Infrastructure Risk Management Checklists for Small and Medium Sized Energy Facilities. U.S. Department of Energy, Office of Energy Assurance. August 19, 2002 (Draft Version 1).

Abstract: “The purpose of this document is to provide some general guidance and a starting point so that a smaller energy facility is able to identify its critical functions and assets, become aware of threats and vulnerabilities, evaluate and rank the threats in terms of the incidents they may cause, and initiate a security enhancement program, if appropriate.” The approach outlined in this Risk Management Checklist uses a six-step process which is similar to the vulnerability assessment process:

- Step 1: Identify critical assets and the impacts of their loss
- Step 2: Identify what protects and supports the critical assets
- Step 3: Identify and characterize the threat
- Step 4: Identify and analyze vulnerabilities
- Step 5: Assess risk and determine priorities for asset protection
- Step 6: Identify mitigation options, costs, and trade-offs”

Comment: This Risk Management Checklist is a reasonable starting point for an organization manager asking questions about a small energy facility’s vulnerability, risk, and security for the first time. Questions and check-off boxes are used for the process. However, little or no guidance is provided on how to go about answering the questions asked; what data and information needs to be collected to help answer the questions; how the information collected is to be interpreted or analyzed; or how the answers developed are to be interpreted and used. Also, this document does not include a list of resources – federal, state, or private – where an organization that owns a small energy facility could obtain help in the vulnerability and security assessment process.

Petroleum Product-Specific Assessment Methodologies

Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries, American Petroleum Institute and National Petrochemical & Refiners Association, May 2003. Available electronically: api-ec.api.org/filelibrary/SVA_2003.pdf

Abstract: “This methodology was prepared by the American Petroleum Institute (API) and the National Petrochemical & Refiners Association (NPRA) Security Committees to assist the petroleum and petrochemical industries in understanding Security Vulnerability Assessment (SVA) and in conducting the assessments. The guidelines describe an approach for assessing security vulnerabilities that is widely applicable to the types of facilities operated by the industry and the security issues they face. During the development process it was tested at two refineries, two tank farms, and a lubricating oil plant, which included typical process equipment, storage

tanks, marine operations, infrastructures, pipelines, and distribution terminals for truck and rail. Based on these trials and the generic nature of the overall methodology, its use at other types of petroleum and petrochemical facilities is expected to be suitable. Future editions will address other operations within the petroleum industry. The methodology is presented as one approach for assessing security vulnerabilities at petroleum and petrochemical industry facilities, and is not intended to supplant measures previously implemented or to offer commentary regarding the effectiveness of any individual company efforts.”

Comment: This is a comprehensive vulnerability assessment document, with a systematic set of questions and check-off boxes to guide the team through the assessment process.

The methodology identifies six basic elements of a proper SVA:

1. Characterize the facility to understand what critical assets need to be secured, their importance and their interdependencies and supporting infrastructure;
2. Identify and characterize threats against those assets and evaluate the assets in terms of attractiveness of the targets to each adversary and the consequences if they are damaged or stolen;
3. Identify potential security vulnerabilities that threaten the asset’s service or integrity;
4. Determine the risk represented by these events or conditions by determining the likelihood of a successful event and the consequences of an event if it were to occur;
5. Rank the risk of the event occurring and, if high risk, make recommendations for lowering the risk;
6. Identify and evaluate risk mitigation options (both net risk reduction and benefit/cost analyses) and re-assess risk to ensure adequate countermeasures are being applied.

Interdependence Awareness: The methodology stresses that SVA teams should identify the critical internal and external infrastructures and their interdependencies (e.g., electric power, petroleum fuels, natural gas, telecommunications, transportation, water, emergency services, computer systems, air handling systems, fire systems, and SCADA systems) that support the critical operations of each asset. For example, the electrical substation may be the sole electrical supply to the plant, or a supplier delivers raw material to the facility via a single pipeline.

Appendix C: Interdependencies and Infrastructure Checklist can be used to identify and analyze these issues. Much of the methodology’s value with respect to interdependencies lies in Appendix C, which is a comprehensive checklist for infrastructure and interdependencies that can be used both before and after a SVA for ensuring completeness. The questions in the appendix address interdependencies both internal to the facility and with external infrastructures. The methodology notes that some of these issues may be beyond the control of the owner/operator, but it underscores the need to understand the dependencies and interdependencies of the facility, and the result of loss of these systems on the process.

Securing Oil and Natural Gas Infrastructures in the New Economy: A Report by the National Petroleum Council Committee on Critical Infrastructure Protection, June 2001

Abstract: This report was prepared to consolidate the National Petroleum Council’s advice “on cooperative approaches to protecting the critical infrastructure of the United States oil and gas industry.” The two principal foci of the report requested by the Secretary of Energy were:

1. Review the potential vulnerabilities of the oil and gas industries to attack, both physical and cyber; and
2. Provide advice on policies and practices that industry and government, separately and in partnership, should adopt to protect or recover from such attacks.

According to the Executive Summary, "... (t)his NPC report suggests actions for identifying and reducing infrastructure vulnerabilities within the oil and natural gas industry sector. It raises the level of awareness and understanding of these new critical infrastructure protection challenges within our industry and government. It presents the business case for moving forward in this new business environment, adopting critical infrastructure protection thinking as part of the foundation of acting in the best interests of a company. It identifies the issues and the steps forward that the oil and natural gas industries and the government will need to implement, in partnership, to ensure the integrity and continuity of the industries' infrastructure."

Comment: The report stresses that universally and instantaneous availability of information required for the closely linked business network, has resulted in a marked increase in the interdependence of entities in the petroleum sector. As a result, information is more transparent, difficult to protect, and easily transferred. These electronic systems are interconnected globally, making traditional physical boundaries less important. One of the keys to a more secure infrastructure thus involves a commensurate ability to both provide and protect needed information

The report does not identify specific vulnerability assessment methodologies, and states only that these should be employed. For example, under the section entitled Vulnerability/Risk Management Assessments, the report notes that "(e)ach company should regularly conduct vulnerability assessments of its own systems and operations and take action as appropriate. In addition, each company should conduct assessments of its partners' vulnerabilities. Risk management processes should be reviewed to ensure that both electronic and physical security is included."

The report is somewhat more focused with regard to the information aspect of vulnerability assessment. In the section entitled Information Assurance Process, it states that "... industry and government should advocate the development, adoption, and implementation of global IT management processes to reduce vulnerabilities of the cyber and other electronic systems on which the oil and natural gas industries are dependent. A good example of such a process is the International Standards Organization (ISO) 17799, "The Standard for Information Security Management."

Interdependence Awareness: The report stresses the importance of recognizing the increasingly interdependent nature of the oil and gas sector, but does not discuss specific approaches to mapping interdependencies for site-specific applications. As noted earlier, the primary emphasis is on information sharing and analysis as shown in the following excerpt from the report:

"The National Petroleum Council recommends the development and implementation of an oil and natural gas Information Sharing and Analysis Center (ISAC). Such an ISAC would help mitigate the sector's collective risk considering its dependency on IT, telecommunications, and SCADA systems. Additionally, because of the convergence of oil, natural gas, and electric power into an energy industry, these industries can no longer be examined independently. Most energy companies have activities in two or more of these energy commodities. It is

recommended that after the oil and natural gas industries ISAC is operational, consideration should be given to include other entities, as interrelationships become apparent.

While there are issues and challenges to some types of information sharing, they do not prohibit the development of the ISAC. Initially, information will not be shared with government until current barriers are removed. As more of these barriers are removed, the value of the ISAC will increase even further.

It is recommended that an arrangement be initiated with government to permit certain industry personnel to obtain national security clearances in order to access classified threat information. Access to such classified information would enhance vulnerability assessment for the sector.

In order to facilitate information sharing without an encumbrance of the antitrust legislation, it is recommended that the ISAC obtain a business review letter from DOJ to allow information sharing regarding cyber security.

The industry-directed service provider model is recommended as the most efficient and appropriate for the oil and natural gas sector. The “information sharing requirements” of an ISAC, described earlier in this chapter, should be utilized in selecting the best service provider. Information technology and telecommunications vulnerabilities should be the immediate focus, but inclusion of physical vulnerabilities and threat information should be included in the evolution of the ISAC. The National Petroleum Council found that some energy companies do not receive enough of this crucial information, and some companies may not receive any at all. Additionally some companies may not have a physical or IT security staff to act on this crucial information. A cost-effective ISAC would permit those companies access to timely vulnerability and threat information along with solutions.

In determining the structure and operating procedures of an ISAC, the NPC recommends that an industry board be established to investigate, develop, and implement an appropriate ISAC for the sector. This board would address issues such as membership, legal structure, costs, selection of a service provider, etc.”

Proprietary Vulnerability Assessment Tools and Methodologies for Energy Infrastructure Organizations

During the course of the literature and Internet searches, a number (few tens) of private firms were identified that offered assessment services to public and private entities, using their “proprietary” assessment methodologies. These included architect and engineering firms, consulting firms, and specialty communications/computer companies.

With the not insignificant number of privately developed, proprietary assessment methodologies being used today, the NCR Project’s approach to the review of the methodologies –examine only publicly available methodologies for review – may not result in the identification of a true “best practices” framework. A significant number of methodologies are being left out of the review process. An effort should be made to establish relations with a number of these private firms to obtain at least limited access to these private sector methodologies for review.

Appendix C: Energy Sector Stakeholder Organizations

The types of organizations in the Energy Sector are of an extremely wide range, including private, public (all levels), and customer owned. This results in a complex set of roles, relationships, and competition and complicates the legal, business, regulatory, and financial relationships among the Energy Sector organizations. Listed below is a sampling of energy infrastructure organizations serving the NCR, along with brief descriptions of the organization.

Private (Investor Owned) Companies & Subsidiaries

British Petroleum. British Petroleum Amoco (BP) operates in over 100 countries throughout the world with about 103,000 employees. It explores for, produces, refines, and markets petroleum products and natural gas on most continents. BP Solar produced 100 MW of photovoltaic modules in 2004.

Dominion Virginia Power. Dominion Virginia Power provides electric service to more than 2 million homes and businesses in Virginia and North Carolina. Its service area is over 30,000 square miles. Dominion Virginia Power is a subsidiary of Dominion Corporation, a large energy holding company involved in a wide range of energy (electric, gas, and liquids) activities throughout North America.

In 2003, Dominion Virginia Power sold 76.1 billion KWhs to its 2 million customers. Power is purchased from Dominion Generation and from electricity markets with short- and long-term contracts.

ExxonMobil Corporation. ExxonMobil operates in almost every country in the world exploring and producing oil and natural gas. It has 17 refineries located throughout the world; one is located in California. ExxonMobil markets and distributes petroleum, petroleum products, and chemicals in the NCR, both wholesale and retail.

Potomac Electric Power Co. Pepco Electric Power Company (Pepco) provides electric service to 725,000 customers in the District of Columbia and the majority of areas in two counties in Maryland, Prince George and Montgomery, with a total land area of 640 square miles. In 2000, Pepco sold over 27.4 billion kWh to its electric customers. In 2002, Pepco merged with Conectiv, an electric and gas utility serving more than one million customers in Delaware, Maryland, New Jersey and Virginia and both are now subsidiaries of Pepco Holdings, Inc.

Pepco purchases electric power from Pepco Energy Services, Mirant Corp., and the developing electricity markets with spot and both short- and long-term contracts.

Mirant Mid-Atlantic Mirant is an Independent Power Producer with generation facilities throughout the U.S. and Caribbean. Corporate headquarters are located in Atlanta, Ga. Mirant Mid-Atlantic has four generating stations in the NCR area that were purchased from Pepco during their restructuring. Mirant Mid-Atlantic has power supply agreements with Pepco and also sells power through the developing electricity markets with both short- and long-term contracts.

Shell Oil Company. Shell Oil Company is an affiliate of the Royal Dutch/Shell Group of Companies, which operates in over 135 countries. Approximately 24,000 Shell employees are based in the US. Shell Oil Company is one of leading oil and natural gas producers, natural gas marketers, gasoline marketers and petrochemical manufacturers. Shell Renewables is involved in wind, solar (photovoltaics), and hydrogen projects in the U.S. Shell distributes and markets retail petroleum and petroleum products throughout the NCR region, although Shell refineries are located in the Western U.S.

Washington Gas Light Company (Washington Gas) is a regulated natural gas distribution company that serves over 930,000 customers in the District of Columbia, Western Maryland, and Virginia, above Richmond. Washington Gas is a wholly owned subsidiary of the public utility holding company WGL HOLDINGS, INC., headquartered in Washington, D.C.

In 2001, Washington Gas delivered 1.69 billion therms of natural gas to its customers. The Washington Gas service area abuts service areas of the City of Richmond (a municipally owned gas utility), Dominion Energy, Columbia Gas of Virginia, and Baltimore Gas & Electric Co.; therefore, Washington Gas provides natural gas service to customers throughout the NCR. Washington Gas purchases natural gas from suppliers and contracts with a number of gas transmission companies for transportation to its service area. The gas purchased usually originates in Texas and Louisiana on-shore and off-shore gas fields. The gas obtained through the Cove Point LNG facility usually originates in Algeria, but can come from any number of worldwide sources.

Cooperative Electric Distribution (Customer Owned)

Northern Virginia Electric Cooperative Northern Virginia Electric Cooperative (NOVEC) is a rural electric cooperative that serves customers in six counties in Northern Virginia. Its headquarters are in Manassas, Va. NOVEC purchased 2.71 billion KWhs in 2004 for resale to its customers.

Publicly Owned (Government Owned Systems)

City of Manassas, Electric Department. There is one municipally-owned electric utility - Manassas Electric Department – serves electric customers within the municipal boundaries of the City of Manassas; the City boundaries are completely inside the NCR. The Electric Department is regulated by the City of Manassas.

Quasi-Public (Non-Profit)

PJM Interconnection - Electric Transmission (PJM). PJM Interconnection is a regional transmission organization (RTO) that plays a vital role in the U.S. electric system. PJM ensures the reliability of the largest centrally dispatched control area in North America by coordinating the movement of electricity in all or parts of Delaware, Illinois, Indiana, Kentucky, Maryland, Michigan, New Jersey, North Carolina, Ohio, Pennsylvania, Tennessee, Virginia, West Virginia and the District of Columbia.

PJM, acting neutrally and independently, operates the largest competitive wholesale electricity market in the world. PJM manages a sophisticated regional planning process for generation and transmission expansion to assure future electric reliability. It does this by facilitating a collaborative stakeholder process. Stakeholders include participants that produce, buy, sell, move and regulate electricity. PJM's 350-plus members transact much of their business on this Web site. Using online tools that give them real-time data about the electric system, they buy and sell power, arrange transmission service, schedule contract purchases, carry out business strategies and make critical business decisions.

Other Organizations

North American Electric Reliability Council. NERC's mission is to ensure that the bulk electric system in North America is reliable, adequate and secure. Since its formation in 1968, NERC has operated successfully as a voluntary organization, relying on reciprocity, peer pressure and the mutual self-interest of all those involved. Through this voluntary approach, NERC has helped to make the North American bulk electric system the most reliable system in the world.

NERC is a nonprofit New Jersey corporation whose members are ten regional reliability councils. The members of these councils come from all segments of the electric industry: investor-owned utilities; federal power agencies; rural electric cooperatives; state, municipal and provincial utilities; independent power producers; power marketers; and end-use customers. These entities account for virtually all the electricity supplied and used in the United States, Canada and a portion of Baja California Norte, Mexico.

Electric Energy Buyers, Sellers, Brokers, and Marketers. Since the electric utility industry began its restructuring and deregulation efforts in the mid-1990s, a very large number of electric energy buyers, sellers, brokers, and marketers have come into the industry to operate in the market development and operation part of the industry. These range from one-person firms to independent subsidiaries of large corporations that own utility companies. Because of the large number of firms (numbering over a thousand) doing business in this area today, only a brief sampling of those headquartered on the East Coast is listed below:

- Alpha Energy
- Constellation Power Source Inc
- LG&E Energy Marketing Inc.
- Merchant Energy Group of the Americas

Industry Associations

- American Gas Association
- American Petroleum Association
- American Public Power Association
- Edison Electric Institute
- National Rural Electric Cooperative Association

Table 3: Publicly Available Vulnerability Assessment Methodologies and Related Documents

No.	Type/Sponsor	Document Title
	Infrastructure VA Methodologies - General	
1*	U.S. Department of Energy, Critical Infrastructure Assurance Office	Vulnerability Assessment Framework 1.1, October 1998.
	Infrastructure VA Methodologies Electric	
2*	U.S. Department of Energy, Office of Energy Assurance	Vulnerability Assessment Methodology: Electric Power Infrastructure, September 30, 2002.
3*	U.S. Department of Energy, Office of Energy Assurance	Energy Infrastructure Risk Management Checklists for Small and Medium Sized Energy Facilities, (Draft Version 1), August 19, 2002.
4*	U.S. Department of Energy Office of Emergency Operations	Energy Infrastructure Vulnerability and Risk Assessment Checklists for State Governments, December 2001
5*	U.S. Department of Energy, Office of Energy Assurance and U.S. Department of Homeland Security	State Vulnerability Assessment Methodology, April 3, 2003
6	U.S. Department of Energy, Office of Energy Assurance and U.S. Department of Homeland Security	System Vulnerability Assessment Methodology, September 29, 2003
	Infrastructure VA Methodologies – Natural Gas	
7*	American Gas Assoc., Interstate Natural Gas Assoc., and American Public Gas Association.	Security Guidelines Natural Gas Industry Transmission and Distribution September 6, 2002
	Infrastructure VA Methodologies – Petroleum Products	
8*	American Petroleum Institute and National Petrochemical & Refiners Association	Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries, Second Edition, October 2004.
9	American Petroleum Institute	Security Guidelines for the Petroleum Industry Second Edition, April 2003
	Partial Infrastructure Assessment Methodologies/ Guidelines/Approaches	
10	U. S. Department of Transportation, Office of	Pipeline Security Information Circular: Security Guidance for Natural Gas, and Hazardous Liquid

	Pipeline Safety	Pipelines and Liquefied Natural Gas Facilities, September 5, 2002
11*	National Communications System	National Security Telecommunication Advisory Committee, Information Assurance Task Force: Electric Power Risk Assessment, March 1997
12	U.S. Department of Defense, Defense Advanced Research Projects Agency	The Vulnerability Assessment & Mitigation Methodology, 2003
	Related Infrastructure Documents	
13	North American Electric Reliability Council (NERC)	The Electricity Sector Response to the Critical Infrastructure Protection Challenge May 2002.
14	North American Electric Reliability Council	Gas/Electric Interdependencies and Recommendations, June 15, 2004
15	National Petroleum Council	Securing Oil and Natural Gas Infrastructures in the New Economy, June 2001
16	U.S. Department of Energy, National Nuclear Security Administration	Common Vulnerabilities in Critical Infrastructure Control Systems, May 2003
17	British Columbia Institute of Technology	SCADA Report: The Myths and Facts Behind Cyber Security Risks for Industrial Control Systems, October 2004.
18	U.S. Department of Energy, Office of Energy Assurance	Vulnerability Assessment and Survey Program: Overview of Assessment Methodology, September 2001
19	U.S. Department of Energy, Office of Energy Assurance	Vulnerability Assessment and Survey Program: Lessons Learned and Best Practices, September 2001.
20	U.S. Department of Energy, Office of Critical Infrastructure Protection	Lessons Learned from Industry Vulnerability Assessments and September 11 th , December 2001. (PowerPoint Presentation)
21	U.S. Department of Energy, Office of Critical Infrastructure Protection	Critical Infrastructure Interdependencies: Impact of the September 11 Terrorist Attacks on the World Trade Center – A Case Study, November 2001

Figure 1: Major Transmission Lines – NCR and Virginia

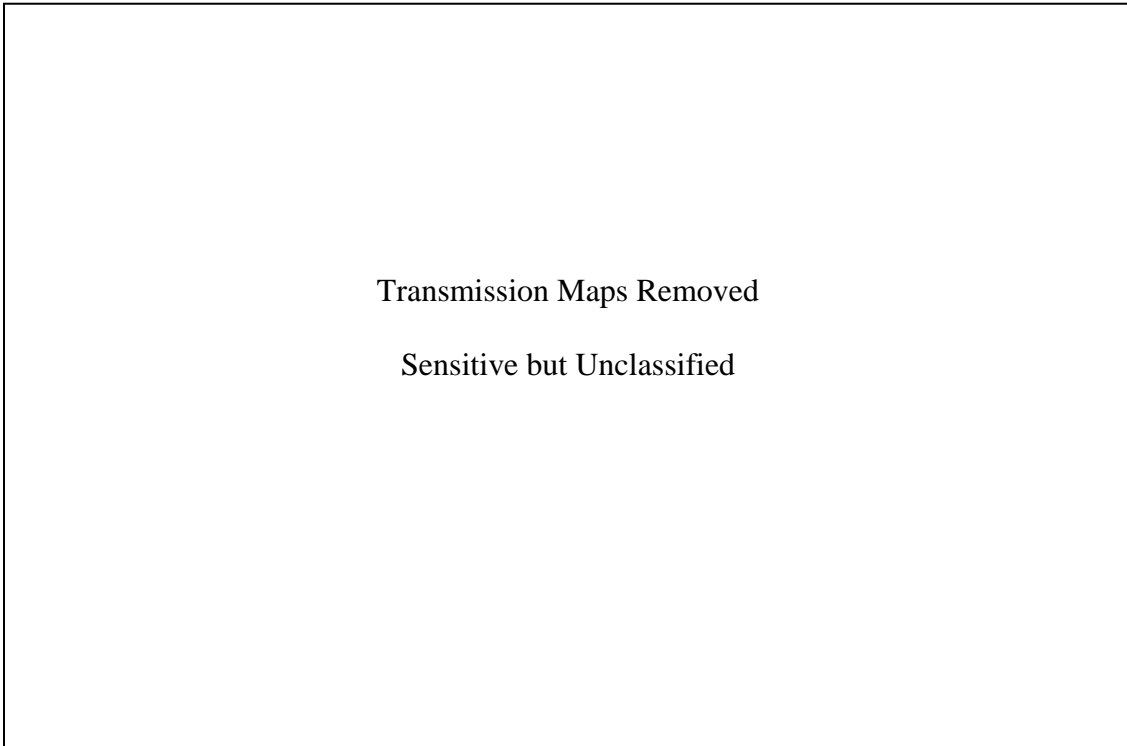


Figure 2: Major Natural Gas Pipelines – NCR and Virginia

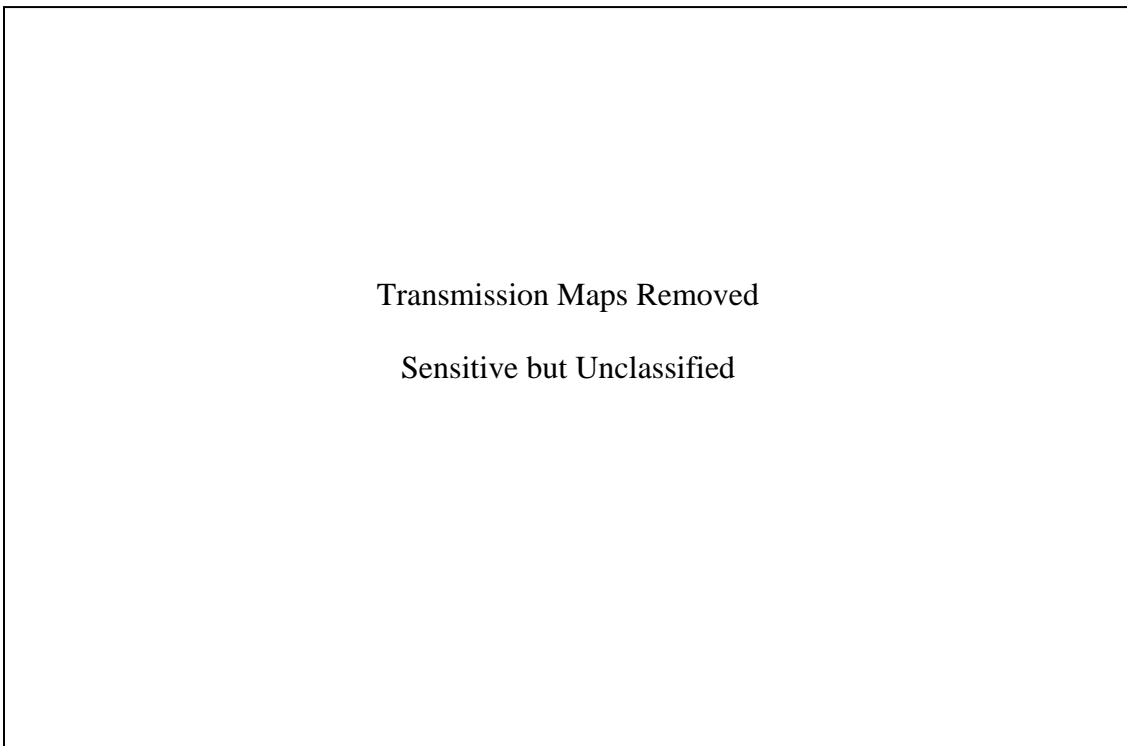
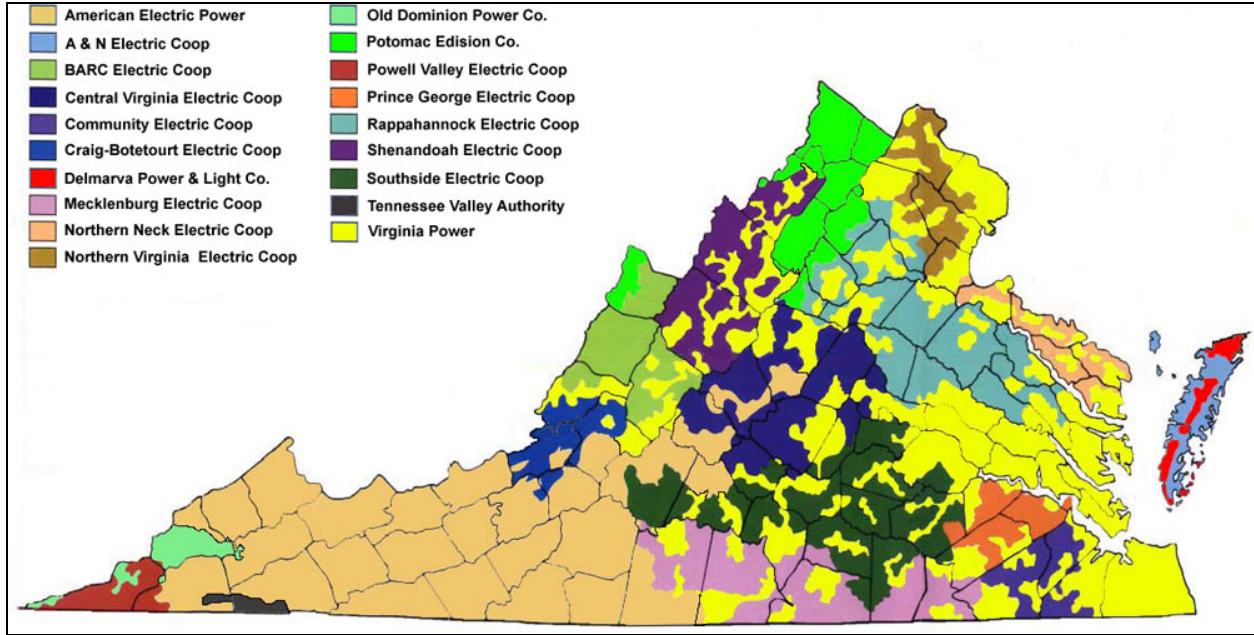
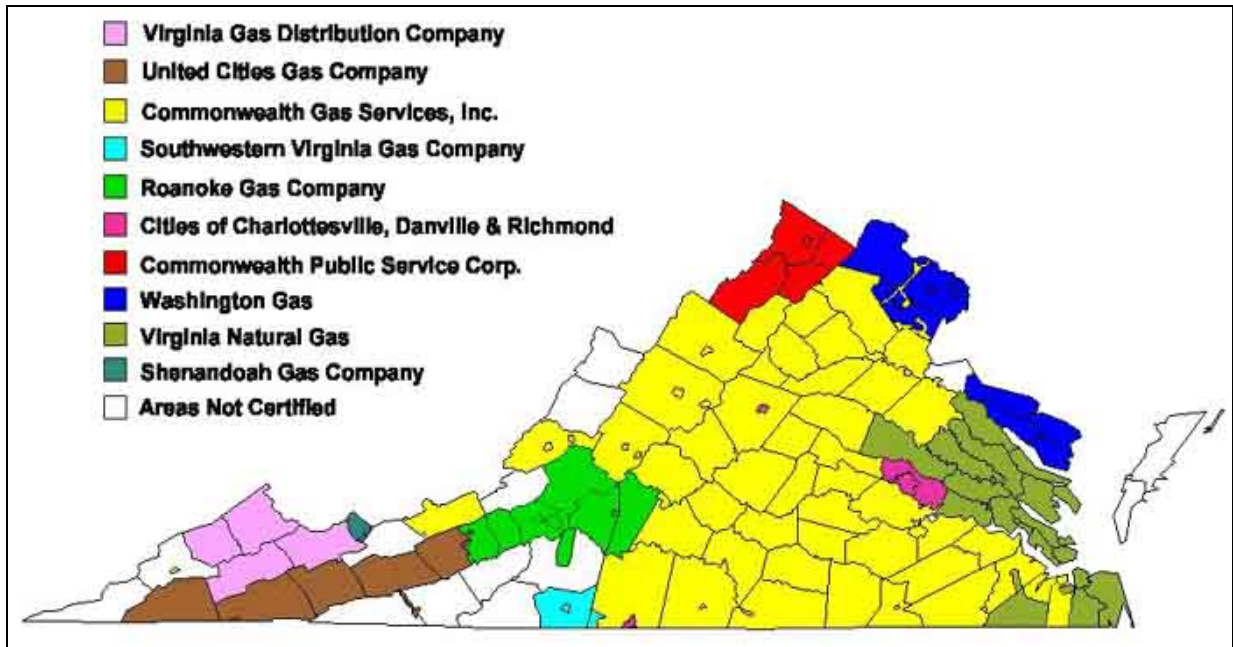


Figure 3: Electric Utilities in Virginia



Source: www.energy.vt.edu/vept/index.asp

Figure 4: Natural Gas Utilities in Virginia



Source: www.energy.vt.edu/vept/index.asp

Figure 5: Electric Utilities in Maryland

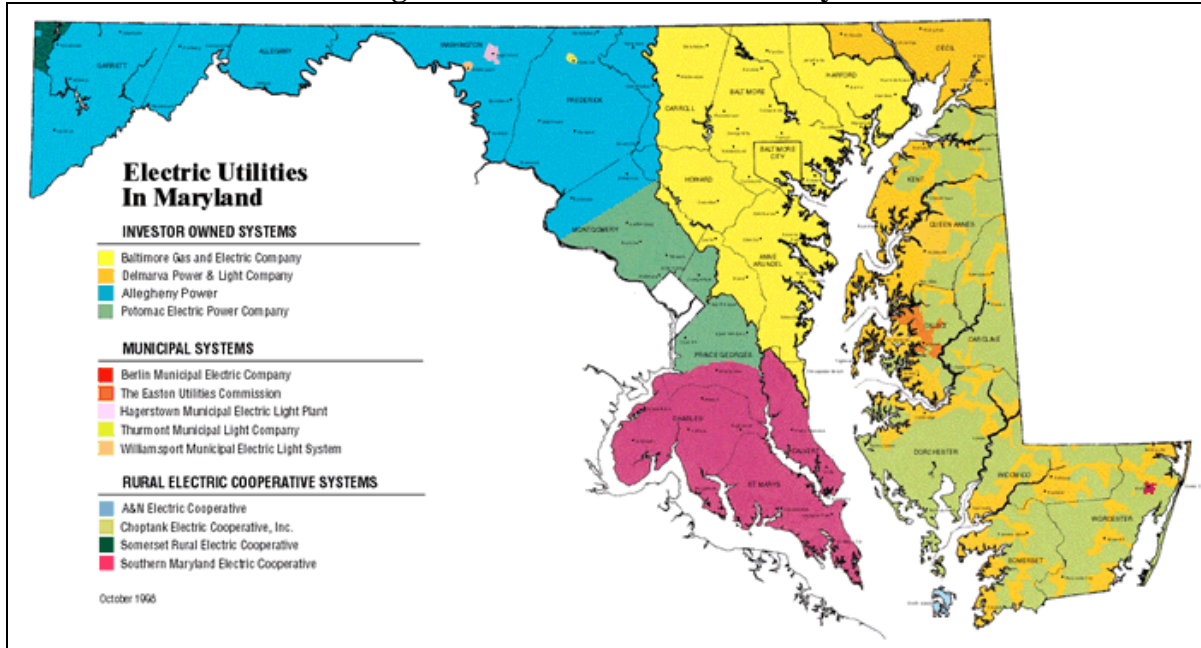
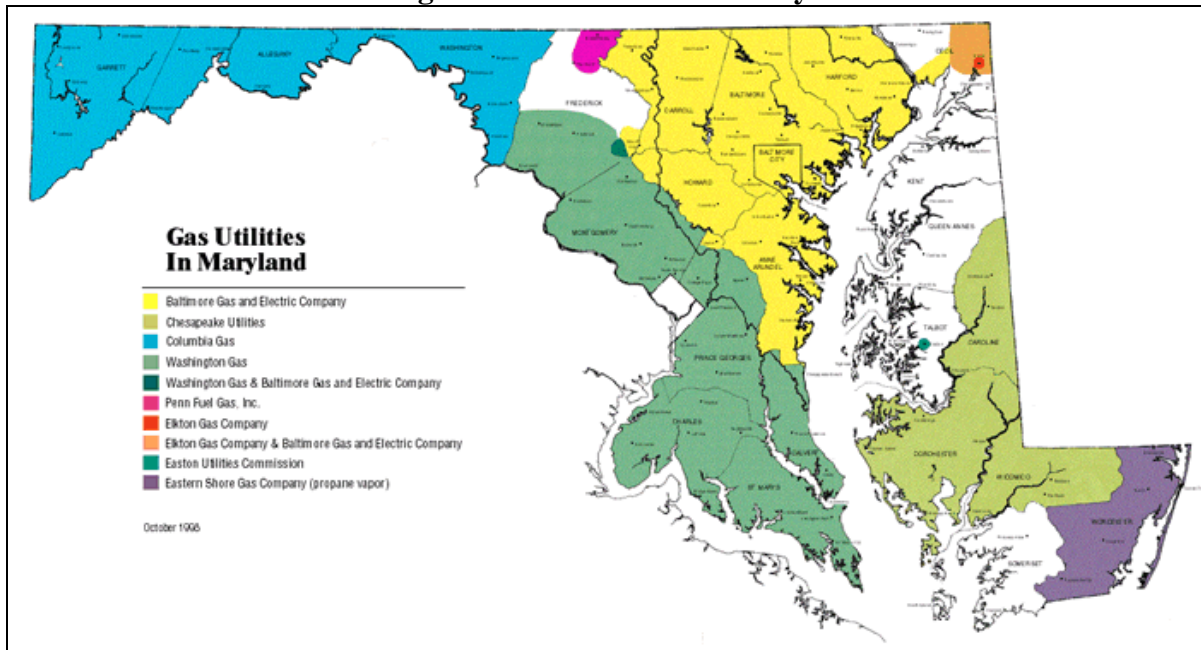


Figure 6: Gas Utilities in Maryland



Appendix D: Bibliography

- American Gas Association, Interstate Natural Gas Association, and American Public Gas Association. *Security Guidelines Natural Gas Industry Transmission and Distribution*. (2002). Washington, DC.
- American Lifelines Alliance. *Guideline for Assessing the Performance of Electric Power Systems in Natural Hazard and Human Threat Events: Part 1 Draft*. (2004). Washington, DC.
- American Lifelines Alliance. *Guideline for Assessing the Performance of Electric Power Systems in Natural Hazard and Human Threat Events: Part 2 Draft – Commentary*. (2004). Washington, DC.
- American Lifelines Alliance. *Guideline for Assessing the Performance of Oil and Natural Gas Pipeline Systems in Natural Hazard and Human Threat Events Part 1 Draft*. (2004). Washington, C.
- American Lifelines Alliance. *Guideline for Assessing the Performance of Oil and Natural Gas Pipeline Systems in Natural Hazard and Human Threat Events – Part 2 Comments Draft*. (2004). Washington, DC.
- American Petroleum Institute and National Petrochemical & Refiners Association. *Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries (2003)*. Washington, DC.
- American Society of Mechanical Engineers. *Risk Analysis and Management for Critical Asset Protection: Asset Application Handbook, Prototype for Chemical Process Industry*. (2004). Washington, DC.
- American Society of Mechanical Engineers. *Risk Analysis and Management for Critical Asset Protection: General Guidance*. (2004). Washington, DC.
- British Columbia Institute of Technology. *SCADA Report: The Myths and Facts behind Cyber Security Risks for Industrial Control Systems*. (2004). Vancouver, Canada: British Columbia Institute of Technology.
- Mussington, David. *Concepts for Enhancing Critical Infrastructure Protection: Relating Y2K to CIP Research and Development*. (2002). Santa Monica, California: Rand.
- National Communications System, National Security Telecommunication Advisory Committee, Information Assurance Task Force. *Electric Power Risk Assessment*. (1997). Washington, DC.
- National Infrastructure Advisory Council. *Cross Sector Interdependencies and Risk Assessment Guidance: Final Report and Recommendations*. (2004). Washington, DC.

- National Petroleum Council. *Securing Oil and Natural Gas Infrastructures in the New Economy*. (2001). Washington, DC.
- National Regulatory Research Institute. NRRI 04-01: NARUC/NRRI 2003 “Survey on Critical Infrastructure Security”. January 2004
- North American Electric Reliability Council (NERC). *The Electricity Sector Response to the Critical Infrastructure Protection Challenge*. (2002). Princeton, New Jersey.
- North American Electric Reliability Council. *Gas/Electric Interdependencies and Recommendations*. (2004). Princeton, New Jersey.
- The Critical Technologies Institute. *The Cyber-Posture of the National Information Infrastructure*. (1998). Vancouver, B.C.: Critical Technologies Institute.
- United Nations Development Program. *Vulnerability and Risk Assessment: Disaster Management Training Program – 2nd Edition*. (1994). New York.
- U.S. Department of Agriculture, Rural Utilities Service Bulletin 1730B-2: Guide for Electric System Emergency Restoration Plan. Effective Date: 7 January 2005
Available on RUS electric website at: <http://www.usda.gov/rus/electric/bulletins.htm>
- U.S. Department of Defense, Defense Advanced Research Projects Agency. *The Vulnerability Assessment & Mitigation Methodology*. (2003). Washington, DC.
- U.S. Department of Energy. *An Integrated Methodology for Sabotage Vulnerability Assessment* (Undated). Washington, DC.
- U.S. Department of Energy, Critical Infrastructure Assurance Office. *Vulnerability Assessment Framework 1.1*. (1998). Washington, DC.
- U.S. Department of Energy, Office of Critical Infrastructure Protection. *Critical Infrastructure Interdependencies: Impact of the September 11 Terrorist Attacks on the World Trade Center – A Case Study*. (2001)
- U.S. Department of Energy, Office of Critical Infrastructure Protection. *Lessons Learned from Industry Vulnerability Assessments and September 11th*. (2001). (PowerPoint Presentation)
- U.S. Department of Energy, National Nuclear Security. *Common Vulnerabilities in Critical Infrastructure Control Systems*. (2003). Washington, DC.
- U.S. Department of Energy, Office of Energy Assurance. *Energy Infrastructure Risk Management Checklists for Small and Medium Sized Energy Facilities, (Draft Version 1)*. (2002). Washington, DC.
- U.S. Department of Energy, Office of Energy Assurance. *Vulnerability Assessment Methodology: Electric Power Infrastructure*. (2002). Washington, DC.

- U.S. Department of Energy, Office of Energy Assurance. *Vulnerability Assessment and Survey Program: Lessons Learned and Best Practices*. (2001). Washington, DC.
- U.S. Department of Energy, Office of Energy Assurance. *Vulnerability Assessment and Survey Program: Overview of Assessment Methodology*. (2001). Washington, DC.
- U.S. Department of Energy, Office of Energy Assurance. *21 Steps to Improve Cyber Security of SCADA Networks*. (Undated). Washington, DC.
- U.S. Department of Energy, Office of Energy Assurance and U.S. Department of Homeland Security. *State Vulnerability Assessment Methodology*. (2003). Washington, DC.
- U.S. Department of Energy, Office of Energy Assurance and U.S. Department of Homeland Security. *System Vulnerability Assessment Methodology*. (2003). Washington, DC.
- U.S. Department of Homeland Security. “Overview for Non-Federal Partners on the Development of Sector-Specific Plans,” *National Infrastructure Protection Plan*. (2004). Washington, DC.
- U.S. Department of Homeland Security, Office of Domestic Preparedness. *Vulnerability Assessment Methodologies Report*. (2003). Washington, D.C.
- U.S. Department of Homeland Security, U.S. Department of Energy. “Energy Sector for Critical Infrastructure Protection,” *National Infrastructure Protection Plan*. (2004). Washington, DC.
- The Library of Congress, Congressional Research Service. *Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities, and Consequences*. (2004). Washington, DC.
- U. S. Department of Justice, National Institute of Justice. *A Method to Assess the Vulnerability of U.S. Chemical Facilities*. (2002). Washington, DC.
- U. S. Department of Transportation, Office of Pipeline Safety. *Pipeline Security Information Circular: Security Guidance for Natural Gas, and Hazardous Liquid Pipelines and Liquefied Natural Gas Facilities*. (2002). Washington, DC.
- Ware, Willis H. *The Cyber-Posture of the National Information Infrastructure*. Rand, The Critical Technologies Institute. Santa Monica, California. (1998).

Appendix E: Endnotes

- ¹ Figures 1 and 2 taken from Virginia Energy Patterns and Trends Electronic Database, maintained by the Virginia Center for Coal and Energy Research. See website: www.energy.vt.edu/vept/index.asp
- ² Wenger, A. et. al. (eds.) *Critical Information Infrastructure Protection: International CIIP Handbook*, Swiss Zurich: Federal Institute of Technology, 2002.
- ³ Modified from: Ryan, Julie (1998), *The Infrastructure of the Protection of the Critical Infrastructure*, <http://www.iwar.org.uk/cip/resources/pdd63/pdd63-article.htm> (Accessed 4/13/04).
- ⁴ Ibid.
- ⁵ The IEEE (is a non-profit, technical professional association of more than 360,000 individual members in approximately 175 countries. The full name is the Institute of Electrical and Electronics Engineers, Inc.
- ⁶ Virginia service area maps from Virginia Energy Patterns and Trends Electronic Database. See: <http://www.energy.vt.edu/vept/index.asp>
- ⁷ Maryland service area maps from Choose Maryland Web site, sponsored by Maryland Department of Business and Economic Development. See: http://www.choosemaryland.org/datacenter/utilities/terr_gas.asp
- ⁸ PEPSCO serves a total population of 2,022,000 persons with 572,000 in D.C. and 1,450,000 in Maryland
- ⁹ Information taken from White House press release, December 17, 2003. See web reference: <http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html>
- ¹⁰ Information take from Congressional Research Service report to Congress: Homeland Security Act of 2002: Critical Infrastructure Information Act, February 28, 2003
- ¹¹ Per 18 CFR Part 388, issued 10 August 2004.
- ¹² The Federal Response Plan (FRP) is designed to address the consequences of any disaster or emergency situation in which there is a need for Federal assistance under the authorities of the Robert T. Stafford Disaster Relief and Emergency Assistance Act, 42 U. S.C. 5 121 et seq. (2) The FRP is the Federal government's plan of action for assisting affected States and local jurisdictions in the event of a major disaster or emergency.
- ¹³ North American Electric Reliability Council (NERC) Web Page, <http://www.nerc.com> (accessed 12/14/04)
- ¹⁴ Testimony of the National Association of State Utility Consumer Advocates (NASUCA) in response to the Department of Energy's Notice of Inquiry relating to Electric Reliability Issues for Interstate Electric Transmission Systems. *Interstate Electric Transmission System; Electric Reliability Issues; Notice of Inquiry*, 65 Fed. Reg. 69753 (November 20, 2000).
- ¹⁵ Prepared Remarks of Michehl R. Gent, President and Chief Executive Officer, North American Electric Reliability Council, Hearing Before the United State's Senate Subcommittee on Technology, Terrorism, and Government Information, July 25, 2001, *The Electricity Sector Response To The Critical Infrastructure Protection Challenge*.
- ¹⁶ "Electricity Sector ISAC and Cyber Security", Presentation by North American Electric Reliability Council to 2004 National Hydropower Association, April 2004
- ¹⁷ U. S. Department of Agriculture, Rural Utilities Service Bulletin 1730B-2: Guide for Electric System Emergency Restoration Plan. EFFECTIVE DATE: 7 January 2005. Available on RUS electric website at: <http://www.usda.gov/rus/electric/bulletins.html>
- ¹⁸ There are no RUS electric program borrowers with current accounts in the NCR. However, the RUS loan portfolio is constantly changing, and could well include future clients from the NCR.
- ¹⁹ Wenger, A, Metzger, J, and Dunn, M. (eds.) (2002), *International CIIP Handbook: An Inventory of Protection Policies in Eight Countries*. Zurich: Swiss Federal Institute of Technology. (pg. 182)
- ²⁰ Modified from: Rinaldi, S. M. (2004) "Modeling and Simulating Infrastructures and Their Interdependencies", *Proceedings of the 37th Hawaii International Conference on System Sciences*, New York: Institute of Electrical and Electronic Engineers.
- ²¹ "Task Force on Electric Power for Virginia's High-Technology Industry: Improving Virginia's Attractiveness For High-Technology Industries", Submitted To Virginia's Center for Innovative Technology by Alexandria Research Institute, Virginia Polytechnic Institute and State University, October 31, 2001.
- ²² "Pepco Holdings, Inc. Hurricane Isabel Response Assessment: Final Report", May 2004, Prepared By James Lee Witt Associates, L.L.C., 1201 F Street, NW, Suite 850, Washington, D.C. 20004
- ²³ Personnel communications: Hank Kenchington, DOE Office of Energy Assurance (10/14/04), and Jeff Dagle, Battelle Northwest Laboratories (10/XX/04).

²⁴ Categories included: Network Architecture (5); Threat Environment (4); Penetration Testing (2); Physical Security (7); Physical Asset Analysis (2); Operations Security (6); Policies and Procedures (3); Impact Analysis (2); Infrastructure Interdependencies (4); and Risk Characterization (3).

²⁵ *Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries*, American Petroleum Institute and National Petrochemical & Refiners Association, May 2003. Available electronically: api-ec.api.org/filelibrary/SVA_2003.pdf

²⁶ Ibid.

²⁷ NRRI 04-01: NARUC/NRRI 2003 “Survey on Critical Infrastructure Security”, prepared by National Regulatory Research Institute (NRRI). January 2004.

This Page Intentionally Blank