

# **North Dakota Energy Emergency Response Plan NASEO/DOE Exercise After Action Report**

RECOVERY ACT – Energy Assurance Planning – state of NORTH DAKOTA

## **WORK PERFORMED UNDER AGREEMENT**

DE-OE0000112

### **SUBMITTED BY**

North Dakota State Energy Office

1600 East Century Ave., Suite 2

P.O. Box 2057

Bismarck, ND 58501-2057

### **PRINCIPAL INVESTIGATOR**

Jeff Rotenberger

Ph: 701-328-4137

Fax: 701-328-2308

[jprotenberger@nd.gov](mailto:jprotenberger@nd.gov)

### **SUBMITTED TO**

U. S. Department of Energy

National Energy Technology Laboratory

Katherine Kweder

[Katherine.Kweder@netl.doe.gov](mailto:Katherine.Kweder@netl.doe.gov)

## Overview

On August 31<sup>st</sup> and September 1, 2011 a Midwest Energy Assurance Exercise entitled White Prairie was conducted in Chicago, IL. The intent of the exercise was to evaluate states' responses to an energy supply emergency as well as progress of state energy response plans in accordance with Department of Energy grant DE-OE0000112.

The following people attended on behalf of the State of North Dakota:

- Jeff Rotenberger, Energy Program Manager, North Dakota Department of Commerce
- Tom Doering, State Deputy Section Chief, ND Department of Emergency Services
- Kirk Hagel, Critical Infrastructure Program Manager, ND Department of Emergency Services
- Mike Rafferty, Jacobs Consulting

States attending the exercise included:

Iowa	Illinois
Indiana	Kansas
Kentucky	Michigan
Minnesota	Missouri
North Dakota	Nebraska
Ohio	South Dakota
Wisconsin	

Additionally, several Local Energy Assurance Plan Grant recipients (cities) were also in attendance as participants in the exercise.

## Pre-Exercise

Prior to the exercise the state was required to complete at least one in-state exercise as well as answer a number of pre exercise related questions regarding potential responses and priorities. The background information related to the exercise and questions is shown below:

### Background Pre-event Information

This exercise begins in the first week of December 2011. The following set the stage for the conditions under which this Midwest Regional Energy Assurance Exercise will be conducted:

- Crude oil prices have once again taken a sharp jump over the fall increasing from just under \$100 per barrel to \$175 by the end of November. Hurricanes that hit the Gulf of Mexico and Gulf Coast in September have disrupted oil and gas production and shut down a number of refineries. The devaluation of the dollar and cold weather in Europe also contributed to the increase in crude oil costs. Natural gas prices have also risen due to the decline in production from the Gulf of Mexico.
- The jump in crude oil prices has in turn increased the prices of gasoline, diesel fuel and propane. Retail gasoline prices are now above \$5.00 per gallon and there are concerns that it may peak above \$6.00 per gallon, diesel and propane have increase proportionally. Petroleum companies have begun to limit sales to non-contract customers and are holding contract customers to 100% of their contract volumes.

- The public and business are increasingly vocal about how high prices are hurting them, there are fears of a potential recession, and Governor's throughout the Midwest have turned to their State Energy Agencies for recommendations on what might be done.
- The onset of winter was earlier this year with temperatures running below normal. The upper Midwest saw a snow storm the last week of November and the longer term outlook is for colder than normal for December and January.
- Propane inventories have been drawn down in response to higher heating demand, and concerns about even higher prices later in the heating season. Inventories are within the lower end of the normal range for this time of year.
- Cyber Security threats are ongoing. "Critical infrastructure has taken an even more prevalent position in being primary targets for terrorist groups. These groups are seeking to infiltrate critical facilities and assets through employment opportunities and then using this inside information to conduct physical or cyber attacks on these sites."<sup>[1]</sup> The Department of Homeland Security, National Cybersecurity and Communication Integration Center issued a Bulletin titled "Anonymous" and Associated Hacker Groups Continue to be Successful Using Rudimentary Exploits to Attack Public and Private Organizations", a copy is attached. (*Plases note this Statement and the attached Bulletin are real.*)
- Situation Reports issued by State Intelligence Fusions Centers indicate a growing potential threat from domestic groups that could signal possible attacks on infrastructure targets.

The following questions were posed to all participants:

**Questions:**

1. What actions are included in your Energy Assurance Plan(s) that you may take, or be prepared to take, if these events impact your State and communities? What State and local contingencies may be needed to assure supply and/or reduce demand for petroleum, electricity, and natural gas? If not explicitly identified in your plan, what other action might you take to be prepared to undertake?
2. How will these conditions potentially affect your State? How can you determine likely consequences and what information and how will it be communicated, to:
  - a) State and local decision makers;
  - b) The public;
  - c) Other States; and
  - d) Federal government?
3. What State agencies would become involved if the situation worsened? What would their role be and how would you coordinate your actions? What if any actions might local governments take at this point?
4. What other critical sectors might be affected by this situation, what are the top 3 critical interdependencies, and how might they be addressed?

North Dakota's responses to the pre-exercise questions are shown in Appendix A.

## **Workshop and Exercise**

Prior to the start of the Energy Assurance Exercise, participants were given a half day workshop covering several important EA topics such as Energy Sector Interdependencies, Driver Hour Waivers, Cybersecurity and the Energy Sector as well as an overview of Midwest Petroleum markets. All of these topics were relevant not only to the exercise but also to current events. Additionally a large energy background packet was given to each participant. This packet is detailed in Appendix B. Following the workshop, scientists from the Argonne National Laboratory reviewed the pre-exercise conditions and began the presentation of scenario one of the exercises.

### **Scenario One**

The first scenario covered six days and included the following 'events':

- Natural Gas delivery issues on major interstate pipelines are being reported by news agencies
- Pipeline control issues are being reported on the Natural Gas Pipeline of America (NGPL) as well as Marathon Pipeline (MPL).
- Control Issues expand to other pipelines carrying petroleum and natural gas.
- Restoration is attempted manual
- The issues may be cyber related.

A detailed timeline for scenario one is shown in Appendix C.

After the presentation, participants broke out into five working groups to discuss issues, concerns and potential responses to the scenario to this point. Following the working groups, the entire group was brought back to discuss in general how each group addressed key issues within the scenario. The hot topic from this scenario was the cyber component and it fostered some interesting discussion. Namely, what is the state's role in responding to a cyber attack and where does restoration impact investigation of a potential crime.

### **Scenario Two**

The second scenario expanded on the first and included suspicious fires at ethanol plants followed by terrorist attacks on the electrical grid which causes cascading failures. The detailed timeline is included in Appendix D. Discussion response dealt with how states deal with man-made events vs. natural disasters as well as restoration priorities from the state and the utilities' point of view.

### **Scenario Three**

The final scenario took place approximately two weeks after the previous scenario and involved an independent truckers strike throughout the United States. The impact of the strike affects petroleum deliveries in the region as well as delivery of key goods. The detailed timeline is shown in Appendix E. Discussion on this scenario focused on interdependencies, state priorities for fuel, and state set-aside programs.

## Lessons Learned

Some of the key lessons learned from this exercise:

- The Cyber security issue brought up in scenario one highlighted a number of issues related to this topic for states:
  - Most states have yet to address this in their plans (including North Dakota).
  - The seriousness of this issue was illustrated in the pre-event information, the workshop presentation and numerous infrastructure bulletins and recent news. Examples are shown in Appendix F and G.
  - States do not have resident experts on cyber security that understand energy infrastructure which is vital for addressing the intricacies of response. For most states this is an 'additional duty as required'. The Department of Energy and NASEO recommend making this a permanent responsibility written into a job description.
  - Response plans for cyber attacks need to address restoration needs vs. crime investigation.
  - The man-made/crime/terrorism aspect of this issue makes response a challenge due to the quick elevation to federal involvement.
  - Communication between state, local, federal and private industry is absolutely critical or key investigative data can be lost.
  - Understanding who is in charge and when a handoff occurs is vital.
- Communication between states is imperative in most energy supply disruptions. Excluding local natural disasters, most events impact multiple states. Understanding neighboring state's issues and planned response can mitigate potential trickle down problems. Memorandums of Understanding might be important as well.
- Utilities are well positioned and trained to quickly restore energy when a disruption occurs. Their planned restoration priorities may not coincide, however, with the state's needs.
- States are very good at dealing with energy issues related to natural disasters but are less well prepared for man-made events. Man-made disruptions typically come without warning, have a significant psychology attached and require additional agencies with varied responsibilities. Communication to the public in this situation needs to be addressed. The unfamiliarity of this type of disruption was obvious.
- Interdependencies are common and critical in an energy emergency. All three scenarios highlighted this fact and it is one that needs to be addressed with the state's plan.
- Local business needs are important during long term supply disruptions and those concerns should be in the plan.
- Most states had not included ethanol contacts within their plans.

## Recommendations

For the sake of clarity, I've annotated the responsibility for each recommendation at the end of each using the following abbreviations:

- Department of Commerce **(NDDOC)**
  - Department of Emergency Services **(NDDDES)**
  - Jacobs Consulting **(JC)**
1. North Dakota needs to develop a cyber security expertise related to energy assurance. ND ITD is well positioned to handle cyber security related to state agencies but is less familiar with critical energy infrastructure and disaster response concerns. Given that ND Department of Commerce has been the lead agency in developing the Energy Assurance Plan for the state, it makes sense for that expertise to reside within this agency. This expertise should be trained and the responsibilities written into a job description as recommended by NASEO and the US Department of Energy. **(NDDOC)**
  2. The North Dakota Energy Assurance plan should be an annex to the state's Emergency Operations Plan. **(NDDDES)**
  3. Interdependencies for the different types of energy disruptions should be addressed within the plan. **(NDDOC, NDDDES, JC)**
  4. Because North Dakota is a net supplier of numerous types of energy, effort should be made to neighboring states to understand what their needs might be in a disruption situation. **(NDDOC, NDDDES, JC)**
  5. Supply Disruption Tracking needs to be updated and included within the plan. **(NDDOC)**
  6. The State Set Aside included in the plan needs to be updated. **(NDDOC)**
  7. The fall in state exercise should focus on man-made disruptions and address these concerns:
    - a. Interdependencies **(NDDOC, NDDDES, JC)**
    - b. State response and communication plan **(NDDOC and NDDDES)**
    - c. Long term disruption effect. **(NDDOC)**
  8. The Energy Assurance Plan needs the following additions:
    - a. A cyber security section detailing response and communication plan in the event of a cyber attack on critical energy infrastructure. **(NDDOC, NDDDES, JC)**
    - b. Ethanol Contacts need to be added to the transportation fuels section of the plan. **(NDDOC)**
    - c. Local Chambers of Commerce should be included in the contacts listing. **(NDDOC)**
    - d. Mapping needs to be updated **(NDDDES, NDDOC)**

## Final Thoughts

Given North Dakota's position as a net energy supplier it was obvious that large scale energy disruptions in petroleum or natural gas would have less of an impact here in the short term than in other states. However, depending on time of year and weather those impacts could be acerbated significantly and quickly. Also, the state currently has no plan to address cyber security issues related to energy infrastructure and this needs to be addressed as recommended above. In a general sense, man-made disruptions should be covered in the plan regardless of type.

My thanks to North Dakota Department of Emergency Services for their efforts in mapping much of North Dakota's energy infrastructure (Jon Tonneson should be commended) and for sending Kirk and Tom to the exercise. Their input in the discussions was important for my understanding and gave good insight into where there are gaps in the current draft of the plan.

Respectfully submitted,

---

Jeff Rotenberger  
Energy Program Manager  
North Dakota Department of Commerce

## APPENDIX A Pre-Exercise Question Responses

### Basic ND Information Summary

**Electric Generation:** Less than 0.1% of ND electric produced by petroleum. No natural gas-fired electric generation

**Heating:** 40% residences use natural gas

**Petroleum:** substantial reserves in Williston Basin, ND produces 2% of US crude, transports Canadian crude, 7 pipelines, ND has 3% US crude oil reserves (573 million barrels)

**Refining:** Mandan at 5.9% of US capacity accounts for 17% of ND gasoline and 42% of diesel fuels. Days of consumption: gasoline -12, diesel - 13.

**Ethanol:** 6 plants produce 123 million gallons (3.9 million barrels) annually

**Fuels storage:**

- |                               |                 |
|-------------------------------|-----------------|
| 1. Motor Gasoline             | 289,000 Barrels |
| 2. Distillates (incl. Diesel) | 435,000 Barrels |

**Questions:**

1. **What actions are included in your Energy Assurance Plan(s) that you may take, or be prepared to take, if these events impact your State and communities? What State and local contingencies may be needed to assure supply and/or reduce demand for petroleum, electricity, and natural gas? If not explicitly identified in your plan, what other action might you take to be prepared to undertake?**

**Steps:**

- Encourage voluntary reductions
  - Mass transit
  - Ride share
  - Changes in work patterns
  - State employee initiatives
- Reduction of state fleet gasoline and diesel oil usage.
- Modification of driving hours/load restrictions.
- NDDOT fuel reduction contingency plan.
- Fuel Set-aside Program

Transportation Fuel Shortage Contingency Measures By Type
<b>1. Distribution and Supply Management</b>
<ul style="list-style-type: none"> <li>• Minimum Purchase Program</li> <li>• Odd/Even Day Purchase Program</li> <li>• Limited Hour of Operation by Transportation Fuel Retailers</li> <li>• Geographic Distribution Plans by Primary Suppliers</li> <li>• Hours of Service Waiver for transportation fuel</li> </ul>
<b>2. Demand Reduction</b>

- Stricter Enforcement of Speed Limits
- Carpool/Vanpool, Mass Transit Promotion
- Flexible Work Hours
- No-Drive Day
- Parking Facility Limitations
- One-Day Closure Retail Stores

### 3. Information Acquisition

- Market Area and Market Share of Prime Suppliers
- Inventories and Capacity Utilization of Refineries
- Inventories in Regional Terminals
- Retail Sales at Gasoline Stations
- Traffic Volume Counts

### 4. Public Information

- How Motorists Comply with Conservation Strategies
- Additional Energy-Saving Measures
- Regular updates on Fuel Supplies Information to include:
  - News Releases
  - Daily Media Response
  - Fact Sheets and Publications
  - Information to Retail Gasoline Stations
  - TV and Radio announcements
  - PSA Campaign

**2. How will these conditions potentially affect your State? How can you determine likely consequences and what information, and how will it be communicated, to:**

- a) State and local decision makers;**
- b) the public;**
- c) other States; and**
- d) Federal government?**

Because North Dakota has significant energy resources within its boundaries, the impact will be lessened compared to other states. The ND Office of Renewable Energy and Energy Efficiency would monitor state supplies via the ND Petroleum Marketers Association and the local Tesoro refinery to stay on top of potential supply concerns. Working with the state Emergency Operations Center contingency plans would be discussed based on potential consequences. Depending on the circumstances, communication with state agencies, local government, and other states would happen via the EOC's joint information center. The cyber security information would be distributed to critical infrastructure via regular traffic.

**3. What State agencies would become involved if the situation worsened? What would their role be and how would you coordinate your actions? What if any actions might local governments take at this point?**

Potential State Agencies involved:

- NDOREE lead
- PSC

- Office of the Governor
- Department of Commerce
- Joint Information Center
- NDDDES (to include ND National Guard)
- ND Highway Patrol

All state emergency response actions are coordinated through the state's emergency operations center. Local government actions could draw from the list shown in answer to question 1.

**4. What other critical sectors might be affected by this situation, what are the top 3 critical interdependencies, and how might they be addressed?**

**North Dakota Critical Service Providers Priority List (not in order)**

- Sanitation services
- Snow removal and other non-normative road service
- Emergency services and public works
- Aviation ground support vehicles and equipment
- Cargo, freight and mail hauling by trucking
- Energy production
- Health care facilities
- Public passenger transportation
- Telecommunication services
- Utility services
- Agricultural production including agricultural trucking and aviation
- Gas/Pipeline Operators

Top 3 given time of year:

- 1) Emergency services and public works
- 2) Energy Production
- 3) Utility services

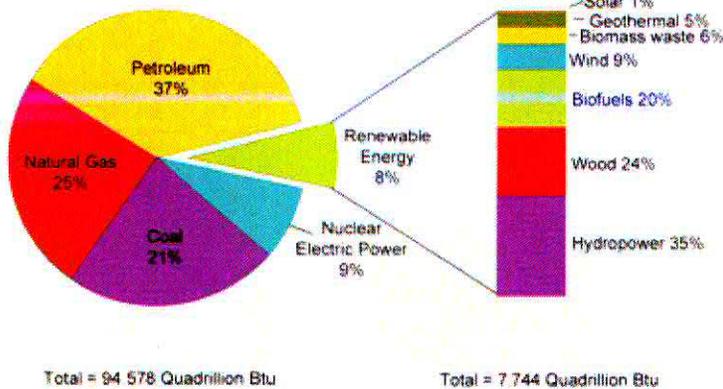


# Midwest States Regional Energy Assurance Exercise Chicago, Illinois - August 31 & September 1, 2011

Sponsored by the U.S. Department of Energy (DOE) Office of Electricity Delivery and Energy Reliability (OE)

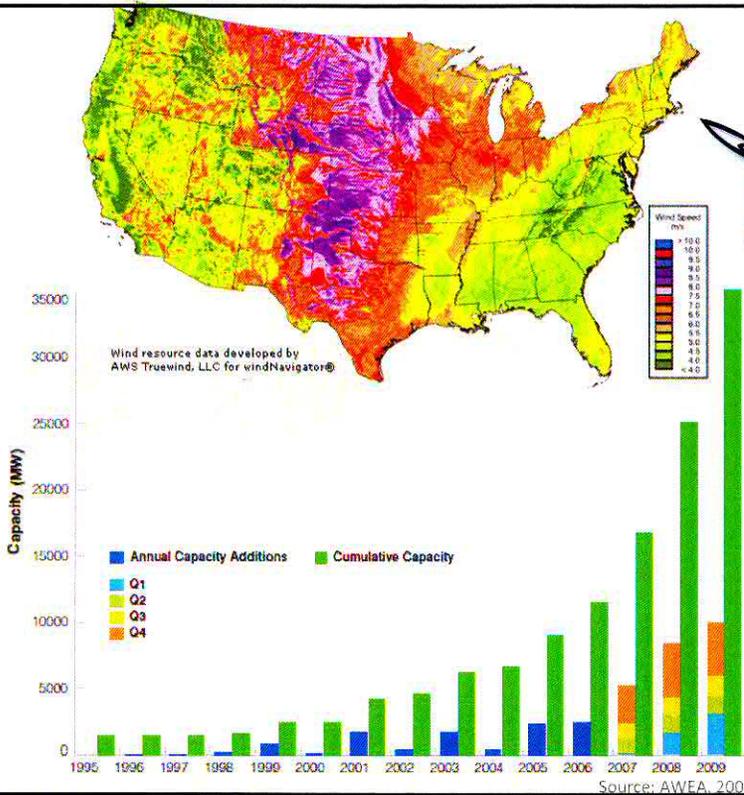
## Renewable Energy

U.S. Energy Consumption by Energy Source, 2009 Source: EIA, 2009.



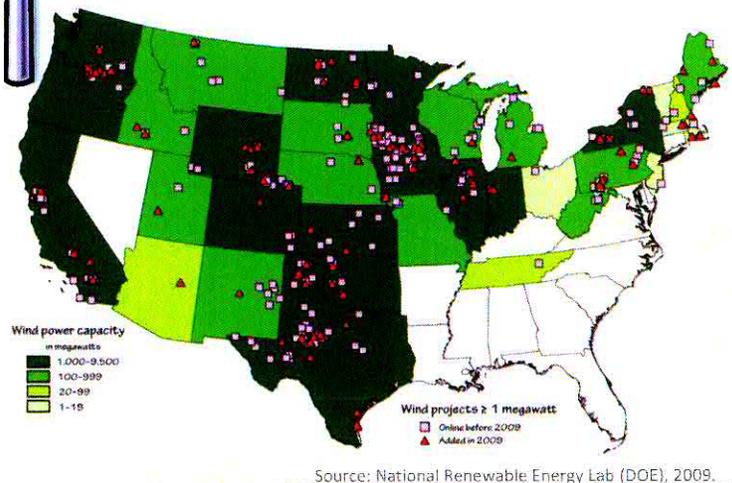
Renewable energy is energy, which comes from natural resources such as sunlight, wind, rain, tides, and geothermal heat that are naturally replenished. Renewable energy replaces conventional fuels in four distinct areas: power generation, hot water/space heating, transport fuels, and rural (off-grid) energy services. This handout is focused on commercially available forms of renewable energy other than hydropower and include wind power, solar energy, biomass, biofuel and geothermal energy.

## Wind Generation

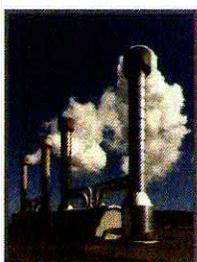


Wind power is growing exponentially. For utility-scale sources of wind energy, a large number of turbines are usually built close together to form a *wind farm* that provides grid power. Several electricity providers use wind farms to supply power to their customers.

## Locations of Wind Farms, 2009



## Geothermal Energy



**Geothermal energy.** As used at electric generating facilities, hot water or steam extracted from geothermal reservoirs in the Earth's crust is supplied to steam turbines at electric utilities that drive generators to produce electricity. Moderate-to-low temperature geothermal resources are used for space heating.

In 2010, the United States led the world in geothermal electricity production with 3,086 MW of installed capacity from 77 power plants. The largest group of geothermal power plants in the world is located at The Geysers, a geothermal field in California.

## Solar Power

**Solar Power.** Solar power is created either using:

- Photovoltaic (PV) or "solar cells"
- Concentrated Solar Power (CSP) systems - concentrate solar energy to heat a fluid and produce steam to drive turbines.

The largest solar power installation in the world is the Solar Energy Generating Systems facility in California with a total capacity of 354 MW. As of 2010, the U.S. total production capacity was 9,724 MW. Less than 1% of the Nation's electricity is solar power (SEPA).





# Midwest States Regional Energy Assurance Exercise Chicago, Illinois - August 31 & September 1, 2011

Sponsored by the U.S. Department of Energy (DOE) Office of Electricity Delivery and Energy Reliability (OE)

Renewable Energy

## Biomass --> Biofuels: Ethanol & Biodiesel

### Types of Biomass



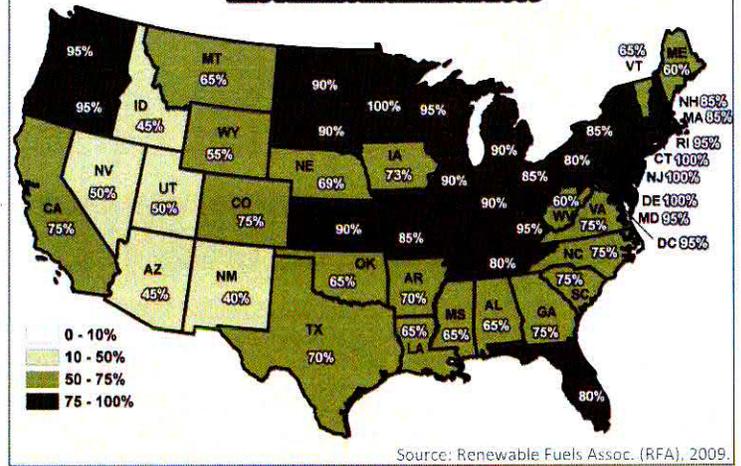
**Converting Biomass to Other Forms of Energy.** Biomass can be converted to useable forms of energy, such as methane gas or transportation fuels, such as ethanol and biodiesel. Today the two most common types of biofuels are ethanol and biodiesel.

- Ethanol, an alcohol, is commonly produced by fermenting corn and sugar cane. Nearly half of the U.S. gasoline contains ethanol in a low-level blend, E10 (10% ethanol, 90% gasoline). E85 is increasingly becoming available that can be used in flexible fuel vehicles.
- Biodiesel is made by combining alcohol (usually methanol) with leftover food products like vegetable oils and animal fats. The most common biodiesel blend is B20 (20% biodiesel, 80% petroleum). B20 can be used in nearly all diesel equipment and is compatible with most storage and distribution equipment.

### U.S. ETHANOL BIREFINERY LOCATIONS (As of January 2010)

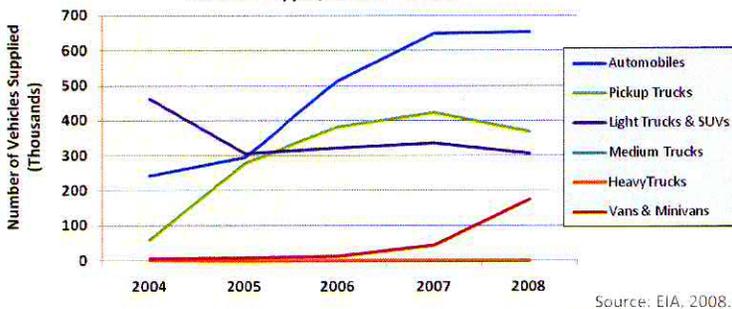


### E10 Market Estimation 2009



**Alternative Fuel Vehicle - a flexible fuel or dual-fuel vehicle designed to operate on at least one alternative fuel.**

### Trends in Alternative-Fueled Vehicles By Vehicle Type, 2004 - 2008



### Ethanol Component in Gasoline

- The concentration of ethanol in gasoline is usually no more than 10 percent by volume (excluding sales of E85).
- Gasoline cannot be delivered if ethanol supply is temporarily unavailable at a distribution terminal unless fuel waivers are obtained from the EPA.
- Ethanol resupply hubs are vulnerable to rail service disruptions. Impact would be regional and involve several gasoline distribution terminals.

### U.S. Ethanol Production Growth and Pool in Gasoline by Volume, 2000-2009

	Gasoline Pool (Million gallons/yr)	Ethanol Production (Million gallons/yr)	Annual Growth (%)	Percent of Gasoline Pool
2000	128,662	1,630	11%	1.3%
2001	129,312	1,770	9%	1.4%
2002	132,782	2,130	20%	1.6%
2003	134,089	2,800	31%	2.1%
2004	137,022	3,400	21%	2.5%
2005	136,949	3,904	15%	2.9%
2006	138,378	4,855	24%	3.5%
2007	142,287	6,500	34%	4.6%
2008	137,797	9,000	39%	6.5%
2009	137,736	10,750	19%	7.8%



### Renewable Fuels

- According to EIA, approximately 8 million flex-fuel vehicles (FFV) are on the road.
- Biodiesel has expanded from a relatively small production base in 2000, to a total U.S. production of 545 million gallons in 2009.
- For more information, visit DOE's *Alternative Fuels and Advance Vehicles Data Center* at <http://www.afdc.energy.gov/afdc/fuels/index.html>

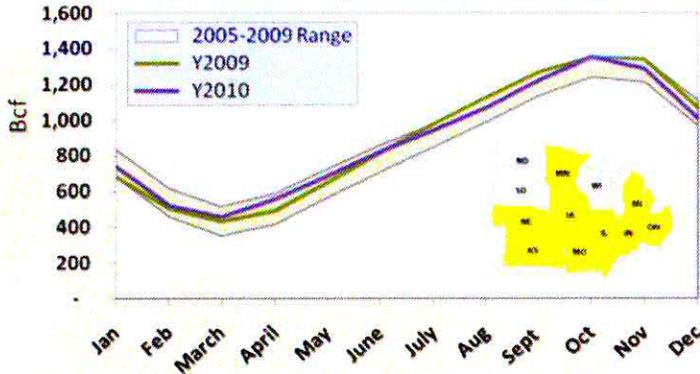


# Midwest States Regional Energy Assurance Exercise Chicago, Illinois - August 31 & September 1, 2011

Sponsored by the U.S. Department of Energy (DOE) Office of Electricity Delivery and Energy Reliability (OE)

## Natural Gas

### Working Storage Capacity: Midwest Region (5-Year Average Seasonal Variation)



Note: ND, SD and WI do not have Storage Facilities

### Natural Gas Storage Capacity: Midwest, 2009

States	Working Gas Capacity (Bcf)	Total Field Capacity (Bcf)	Max. Daily Delivery (Bcf/d)	Number of Facilities
Illinois	304	989	6.3	28
Indiana	32	114	0.8	22
Iowa	87	285	1.2	4
Kansas	119	282	2.4	19
Michigan	667	1,069	17.4	45
Minnesota	2	7	0.1	2
Missouri	3	11	0.4	1
Nebraska	14	35	0.2	1
Ohio	225	580	5.0	24
<b>Midwest</b>	<b>1,453</b>	<b>3,373</b>	<b>34</b>	<b>145</b>

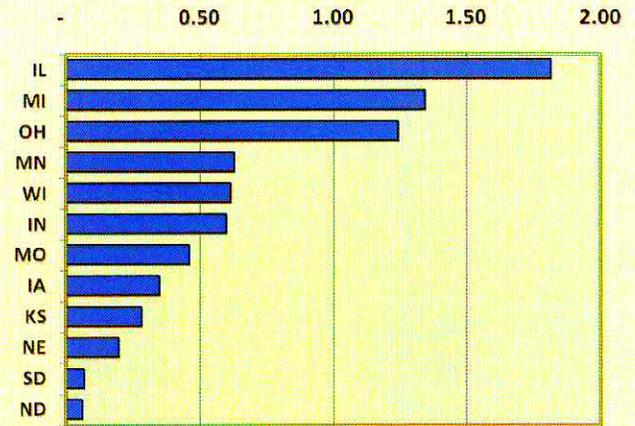
EIA. Form EIA-191a Working Storage.

### Importance of Storage

- The Midwest does not have a ready supply of locally produced natural gas and is therefore dependent upon storage reserves.
- Demand is highest in the winter because natural gas is used to heat residential and commercial buildings.
- Natural-gas fired power plants have increased the demand for natural gas. While consumption by electric power plants constitutes a smaller portion of overall consumption, it is vital component.

### Natural Gas Consumption by State

#### Residential and Commercial Consumption (Bcf/d), 2009



Source: EIA. "Consumption by End Use"

### Natural Gas Consumption

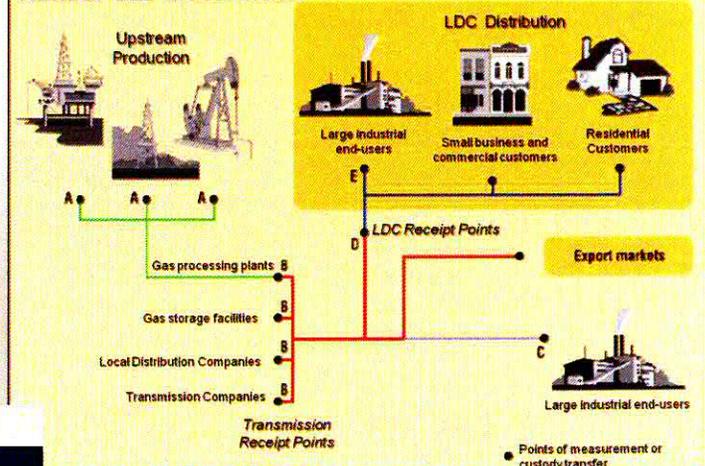
- Seventy-six percent of households use natural gas as primary heating source (Census, 2000).
  - Total residential consumption in 2009 was 4.9 Bcf/d (EIA, 2009).
  - There are a total of 18.8 million residential customers
- Midwest states consume about 12.8 Bcf/d or 22% of the 57.4 Bcf/d of U.S. total natural gas demand (EIA, 2009).
  - Relative to the U.S. the portion of the natural gas used by the Electric Power Sector is small, constituting only 7% of total consumption in 2009 (EIA, 2009).

### Natural Gas Consumption by Sector: Midwest (Bcf/d), 2009

Sector	Midwest Total	Percent by Sector	U.S. Total	Percent by Sector	Midwest Portion of U.S.
Residential	4.9	38%	13.1	23%	8.5%
Commercial	2.8	22%	8.5	15%	4.9%
Industrial	4.3	33%	16.9	29%	7.4%
Electric Power	0.9	7%	18.8	33%	1.6%
<b>Total</b>	<b>12.8</b>	<b>100%</b>	<b>57.4</b>	<b>100%</b>	<b>22.4%</b>

EIA. Consumption by End Use, 2009.

### Natural Gas Movements



Source: <http://www.ic.gc.ca>

- Distribution is the final step in delivering natural gas to end users. While some large industrial, and electric generation customers receive natural gas directly from high capacity pipelines, most other users receive natural gas from LDCs or Local Distribution Companies (ESA, 2011).



# Midwest States Regional Energy Assurance Exercise Chicago, Illinois - August 31 & September 1, 2011

Sponsored by the U.S. Department of Energy (DOE) Office of Electricity Delivery and Energy Reliability (OE)

Natural Gas

## Natural Gas Pipelines

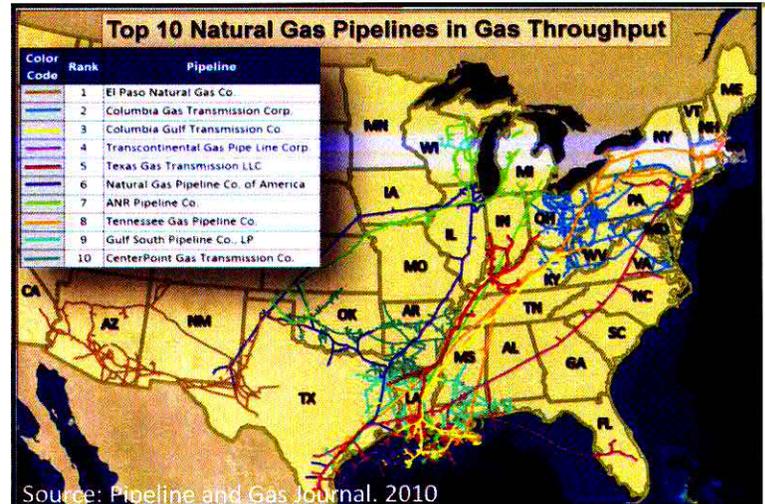
- The Region is rich with natural gas pipelines, including 32 interstate pipelines and 11 intrastate pipelines.

## Interstate Pipelines

- Roughly 60% of the 28 billion cubic feet per day (Bcf/d) of U.S. capacity is concentrated in the Midwest Region. Pipelines with the highest capacities in the Midwest area as follows:
  - Natural Gas Pipeline of America - NGPL (2.7 Bcf/d)
  - Texas Eastern Transmission (2.3 Bcf/d)
  - ANR Pipeline (2.2 Bcf/day)
  - Northern Natural Gas Pipeline (1.5 Bcf/d)
  - Panhandle Eastern Transmission (1.3 Bcf/d)
  - KM Interstate Gas Transmission - KMIGT (0.8 Bcf/d)

## Canadian Inter-regional Pipelines

- Seven interstate pipelines transport Canadian natural gas into the Midwest with a combined capacity of 8.4 Bcf/d (about 30% of total interstate capacity).
  - Northern Border/Plains Pipeline (2.1 Bcf/d) – Interconnects with NGPL and Northern Natural Gas
  - Alliance Pipeline (1.8 Bcf/d)
  - Viking Gas Transmission (0.5 Bcf/d)
  - Great Lakes Transmission (0.5 Bcf/d)



## Natural Gas Import Locations



## Critical Notices for Pipelines

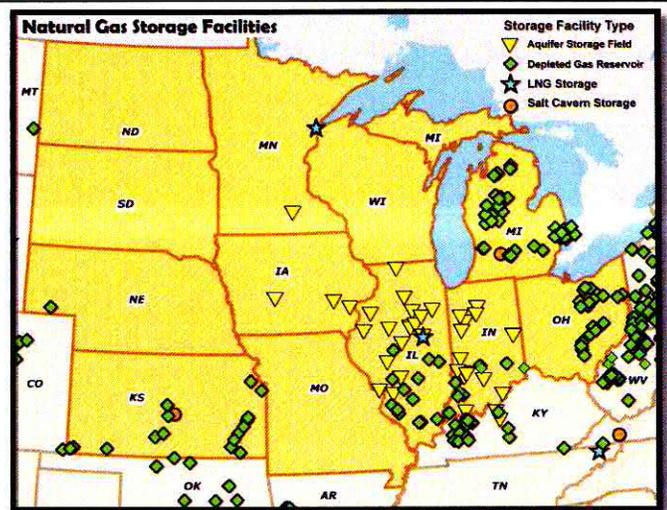
Critical Notices and other information on pipeline operations can be found on pipeline's electronic bulletin board.

EXAMPLE – Kinder Morgan's Natural Gas Pipeline of America:  
<http://pipeline.kindermorgan.com/infoposting/notices.aspx?type=CRIT>

Notice Type Desc	Post Date/Time	Notice Effective Date/Time	Notice End Date/Time	Notice ID	Subject	Notice Sub-Type Desc	Download
CAP. CONSTRAINT	7/25/2011 4:32:27 PM	07/28/2011 4:32:12 PM	12/31/2049 9:00:00 AM	31569	CURRENT PIPELINE CONDITIONS	CURRENT PIPELINE CONDITIONS	<input type="checkbox"/>
MAINTENANCE	7/25/2011 4:05:49 PM	07/25/2011 4:05:49 PM	12/31/2049 9:00:00 AM	31568	STA 305-306 - GC #1 - INSTALL - UEC #1	MAINTENANCE	<input type="checkbox"/>

## Natural Gas Storage

- Midwest has the largest volume of underground (working gas) storage capacity.
  - Total working capacity of 1,453 billion cubic feet (Bcf)
  - Total field capacity of 3,373 Bcf (EIA, 2010).
- Regional storage facilities are concentrated in Michigan (45), Illinois (28) and Indiana (22). The Midwest has 145 active facilities.
  - Deliverability of 34 Bcf/d (EIA, 2010).
  - Many pipelines serving the region provide their shippers/customers access to underground storage
  - Intrastate pipelines and/or local distribution companies, control about 61% of daily deliverability from storage in the Midwest (EIA, 2010).





# Midwest States Regional Energy Assurance Exercise Chicago, Illinois - August 31 & September 1, 2011

Sponsored by the U.S. Department of Energy (DOE) Office of Electricity Delivery and Energy Reliability (OE)

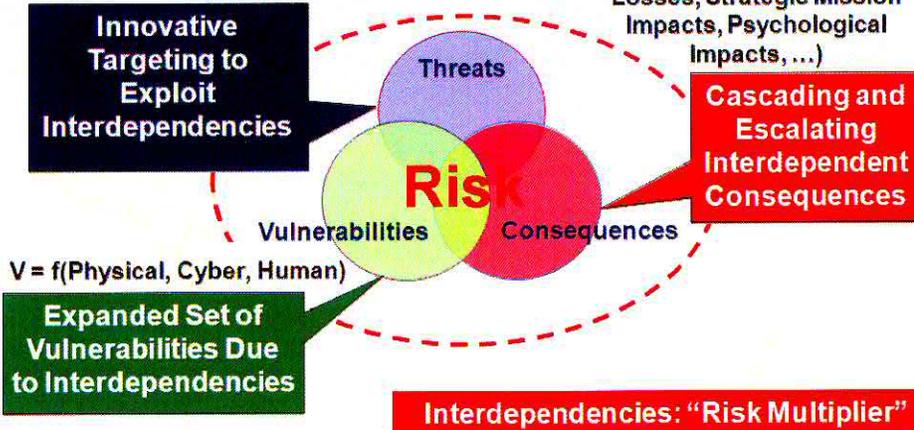
## Interdependencies

### Interdependencies Influence all Components of Risk

$$Risk = f(Threat, Vulnerability, Consequence)$$

$$T = f(Capability, Intent)$$

$$C = f(Deaths, Economic Losses, Strategic Mission Impacts, Psychological Impacts, \dots)$$

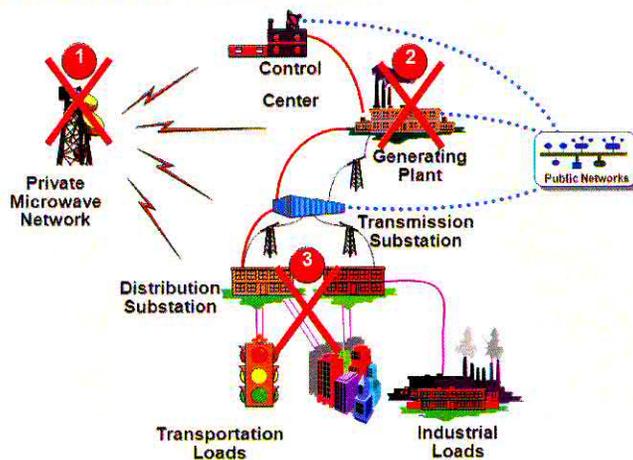


### Three Effects of Interdependency

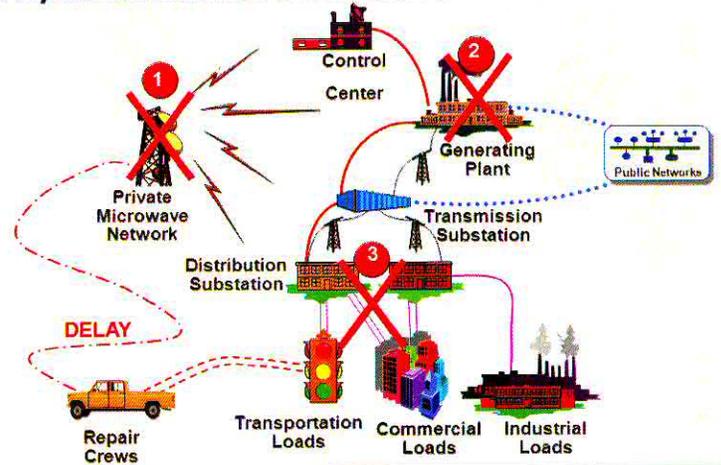
#### Failures:

- *Common cause failure* – A disruption of two or more infrastructures at the same time because of a common cause;
- *Cascading failure* – A disruption in one infrastructure causes a disruption in a second infrastructure;
- *Escalating failure* – A disruption in one infrastructure exacerbates a disruption of a second infrastructure.

### Disruptions Could **CASCADE** Through the Electric Infrastructure



### Disruptions Could **ESCALATE** (Increase) Repair and Restoration Times



#### For more information, please see:

- Argonne National Laboratory, *Infrastructure Interdependencies Associated with the August 14, 2003, Electric Power Blackout*, report prepared by Infrastructure Assurance Center, August 29, 2003.
- Peerenboom, J.P., R.E. Fisher, S. Rinaldi, and T. Kelly, "Studying the Chain Reaction," *Electric Perspectives*, pp. 22-35 (January/February 2002).

#### August 2003 Regional Blackout illustrated interdependent infrastructure disruption:

- Water supply cut
- Raw sewage dumped
- Traffic jams
- Air traffic halted
- Cell phone towers inoperable
- Emergency dispatchers lost contact
- Perishable groceries lost
- ATMs inoperable
- Hotels closed
- Auto plants shut down
- Chemical plants shut down





# Midwest States Regional Energy Assurance Exercise Chicago, Illinois - August 31 & September 1, 2011

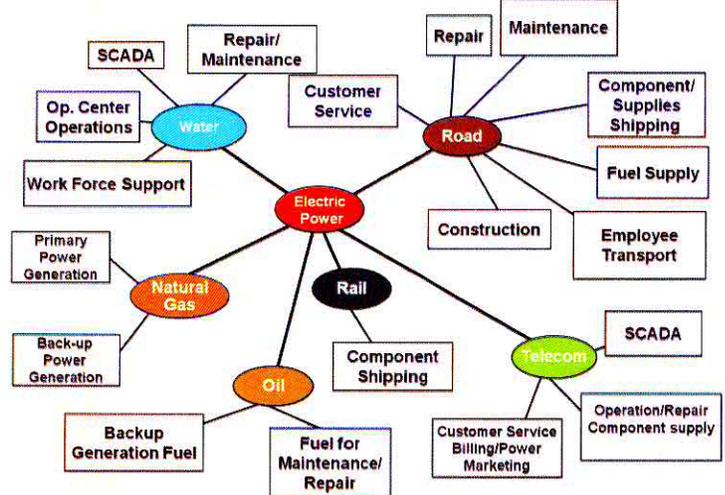
Sponsored by the U.S. Department of Energy (DOE) Office of Electricity Delivery and Energy Reliability (OE)

Interdependencies

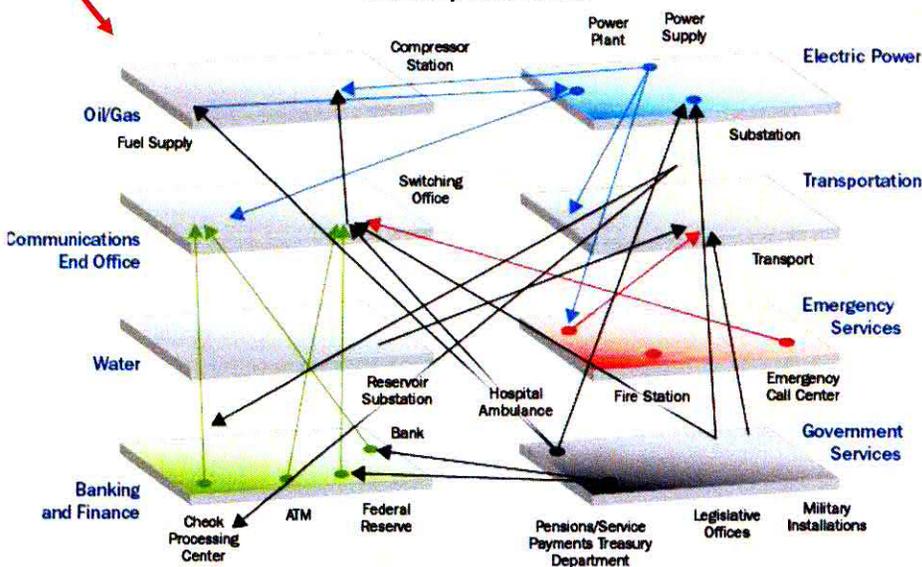
## Infrastructure Interdependencies:

- *Dependency* refers to the linkage or connection between two infrastructures through which the state of one influences the state of the other.
- *Interdependencies* refer to a bidirectional relationship between infrastructures dependent on the other—creating a “systems of systems.”
- Infrastructure linkages vary significantly in scale and complexity.
- The “new economy” (Internet, e-commerce) has important interdependence implications.
- Infrastructure interdependencies are generally not well understood.

## Illustrative Dependencies—Electric Power



## “Systems of Systems” Perspective Needed for Analyzing Interdependencies



## Types of infrastructure interdependencies:

- *Physical* (e.g., output of one infrastructure used by another);
- *Cyber* (e.g., electronic, informational linkages);
- *Geographic* (e.g., common corridor);
- *Logical* (e.g., dependency through financial markets).

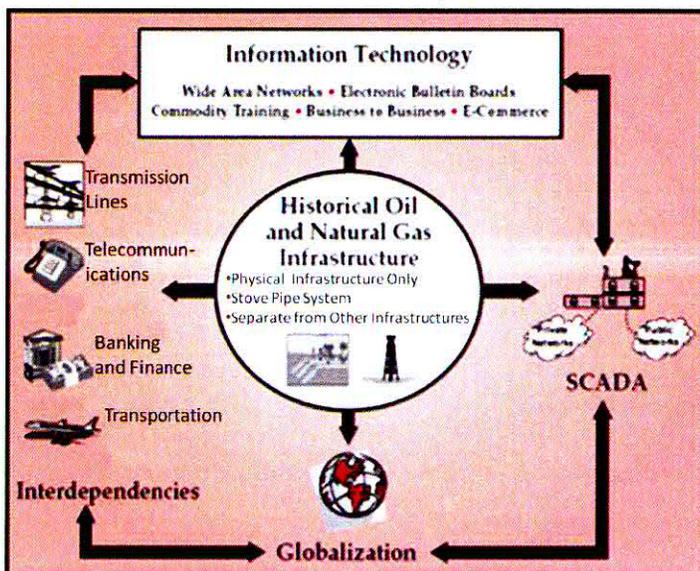
## Physical Interdependency



## Cyber Interdependency



## Geographic Interdependency

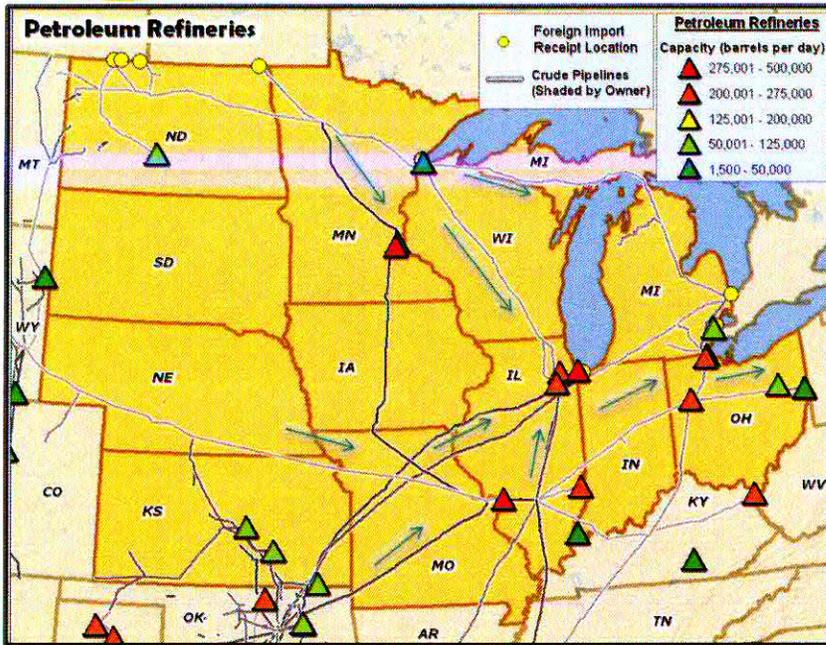




# Midwest States Regional Energy Assurance Exercise Chicago, Illinois - August 31 & September 1, 2011

Sponsored by the U.S. Department of Energy (DOE) Office of Electricity Delivery and Energy Reliability (OE)

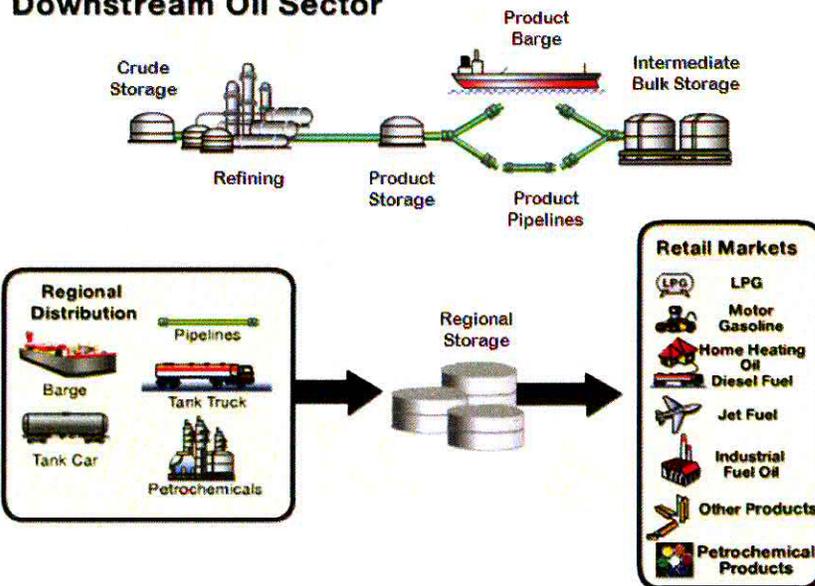
## Petroleum



### Midwest Refineries

- Two principal Refinery clusters located in Midwest:
  - 3 refineries with a combined capacity of 810 MBD (thousand barrels per day) in Chicago Metro Area
  - 3 refineries with a combined capacity of 550 MBD in Detroit-Toledo-Lima Metropolitan Area
- Majority of crude oil consumed by Midwest refineries is delivered by pipeline
  - Region imported 1,206 MBD from PADD 3 in 2010 by pipeline (86%).
- U.S. refineries produced over 90% of the gasoline used in the United States
  - 54% of all gasoline consumed in U.S. was produced in the Gulf Coast, whereas about 20% was produced in the Midwest.

### Downstream Oil Sector



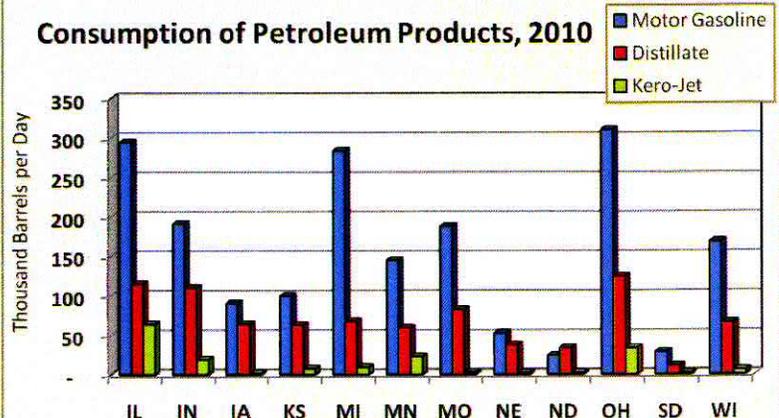
### Crude Oil Supply and Production

- The U.S. produced 5,510 MBD (thousand barrels per day) of crude oil in 2010.
  - The Midwest states produced 490 MBD of crude oil in 2010 - 9% of U.S. total. Of the crude oil produced in the Midwest states, 62% is from North Dakota (305 MBD).
  - By comparison, the Gulf of Mexico accounted for 30% of U.S. crude oil production in 2010.
- Less than 40% of the crude oil used by the refineries was produced in the U.S. Top suppliers in 2009 by country are as follows:
  - Canada (19%), Venezuela (12.7%), Mexico (11.4%), Saudi Arabia (10.8%)
- The U.S. imports 1,970 MBD of crude oil from Canada. Over 61% of the crude oil imports from Canada are imported by refiners in PADD 2.

### Petroleum Demand

- U.S. gasoline consumption in 2010 was about 8.6 MMPD (million barrels per day).
- The Midwest consumed of 1.8 MMBD of gasoline in 2010.
  - Ohio has the highest demand, followed by Illinois and Michigan
- Energy Information Administration (EIA)'s short-term outlook predicts a steady increase in petroleum demand.
  - EIA forecasts an increase of 0.85% each year between 2010 and 2012.

### Consumption of Petroleum Products, 2010



EIA. Prime Supplier Sales Volume.



# Midwest States Regional Energy Assurance Exercise Chicago, Illinois - August 31 & September 1, 2011

Sponsored by the U.S. Department of Energy (DOE) Office of Electricity Delivery and Energy Reliability (OE)

## Petroleum

### Domestic Movements by Mode: Transported to PADD 2 (Thousand Barrels), 2010

Transportation Mode Originating PADD	Pipelines			Tanker / Barge	
	PADD 1	PADD 3	PADD 4	PADD 1	PADD 3
Crude Oil	-	440,480	66,830	275	975
Total Petroleum Products	111,515	266,310	55,895	1,330	34,555
Finished Motor Gasoline	39,530	73,870	6,945	40	3,250
Gasoline Blending Components	33,530	44,880	55	145	2,715
Renewable Fuels (e.g. Fuel Ethanol)	65	-	235	-	915
Kerosene-Type Jet Fuel	2,270	20,300	370	-	220
Distillate Fuel Oil	35,145	47,930	3,680	240	5,185
Other Products	970	79,330	44,975	905	22,265

### Petroleum Administration for Defense Districts



EIA. Movements Between PAD Districts

**Note:** The Midwest states do not equal PADD 2. PADD 2 includes Tennessee, Kentucky and Oklahoma, not otherwise included.

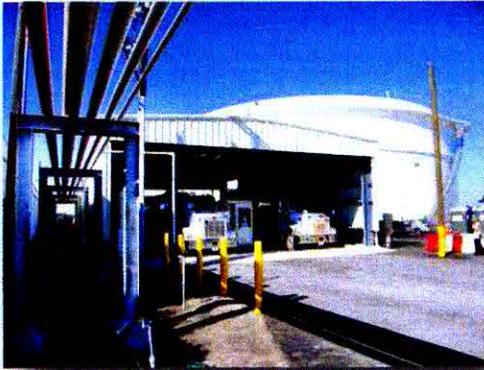
The petroleum infrastructure consists of several interconnected assets operated by a combination of refiner and third party companies, including:

- Refineries
- Pipelines & Breakout Tanks
- Terminals: Inland & Marine
- Railroads

### Important Pipelines Serving PADD II

Origin PADD	Region	Crude Pipelines	Product Pipelines
1	East Coast	Ergon Trucking Pipeline	Sunoco Pipeline, Ohio River Pipeline
3	Gulf Coast	ConocoPhillips, Exxon, Mid-Valley, NuStar Logistics, Plains, Shell, TEPPCO	ConocoPhillips, Explorer, Holly Energy Partners, Magellan, Plantation
4	Rocky Mountains	Enbridge Pipeline (North Dakota), Platte (KM)	ConocoPhillips, Cenex, Rocky Mountains

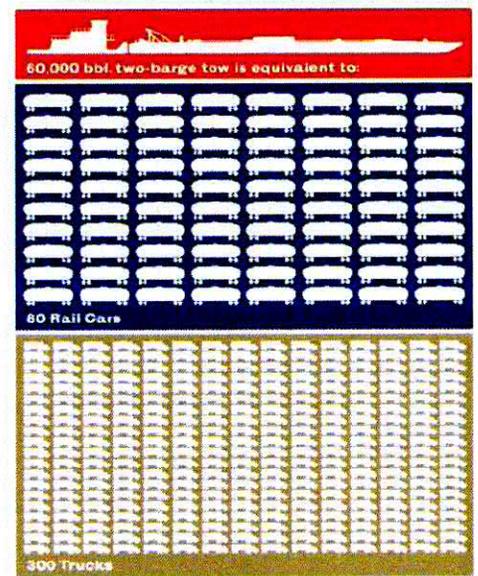
Source: National Pipeline Mapping Service (NPMS)



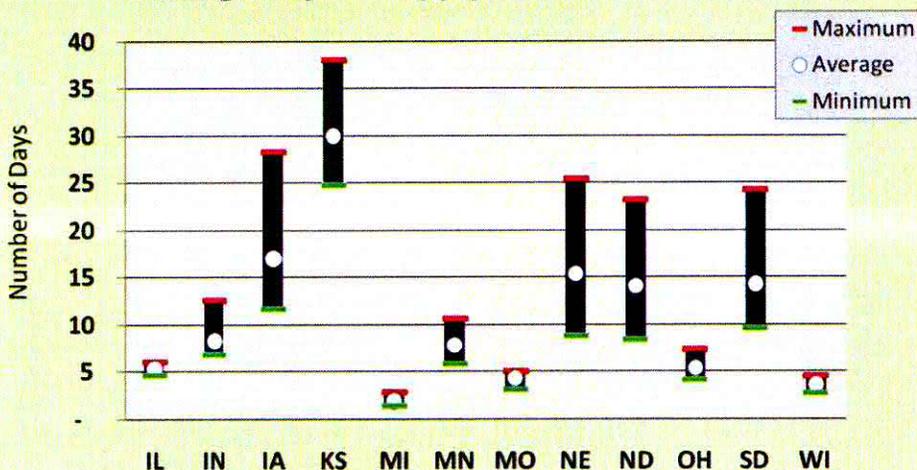
Petroleum terminals or bulk stations receive supplies by tankers, barges and/or pipelines. Two-thirds of petroleum products are delivered by pipeline. A pipeline transporting 1,000 MBD moves the equivalent capacity of over 4,500 tanker trucks.



### Barge / Rail / Truck Comparison



### Average Days of Supply: Motor Gasoline, 2010



Source: EIA. "Stocks" and "Prime Supplier Sales Volume"

Source: <http://news.mongabay.com/bioenergy/>



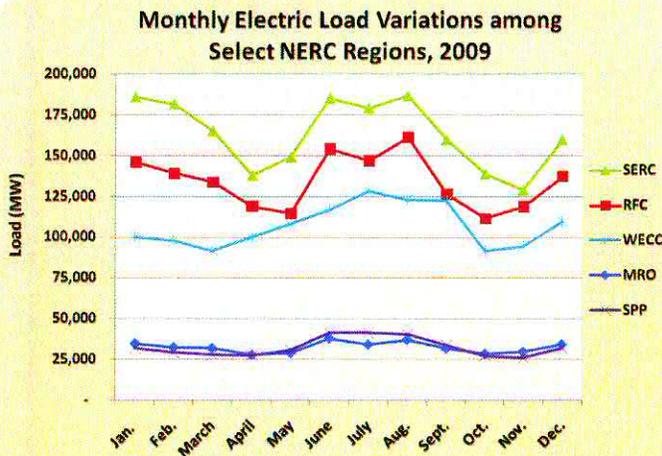
# Midwest States Regional Energy Assurance Exercise Chicago, Illinois - August 31 & September 1, 2011

Sponsored by the U.S. Department of Energy (DOE) Office of Electricity Delivery and Energy Reliability (OE)

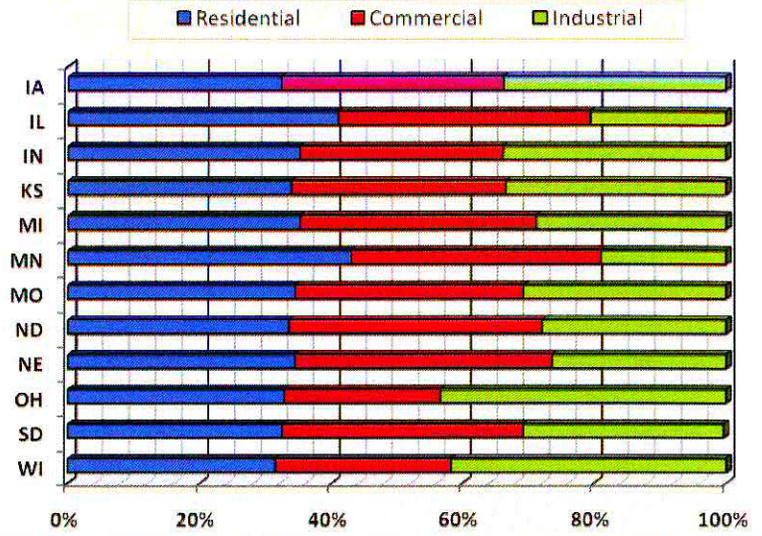
Electricity

## Electricity Consumption

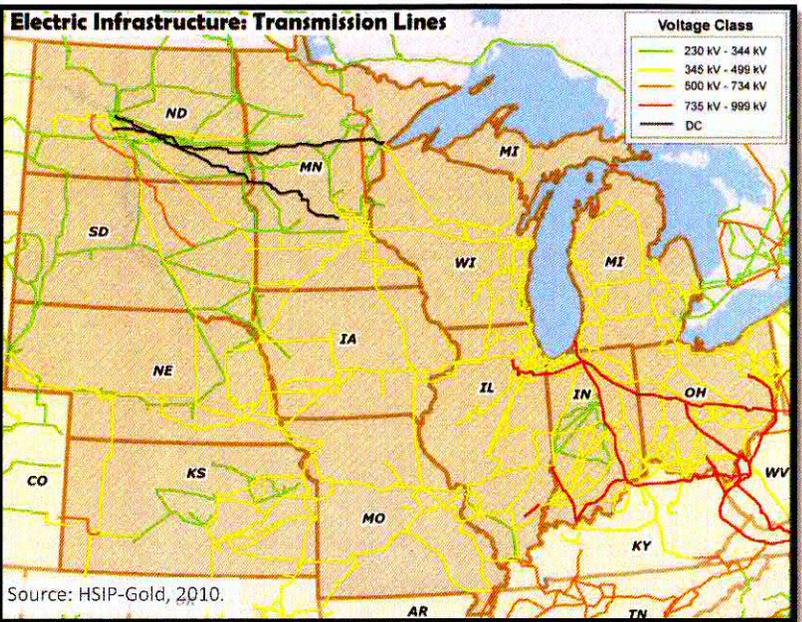
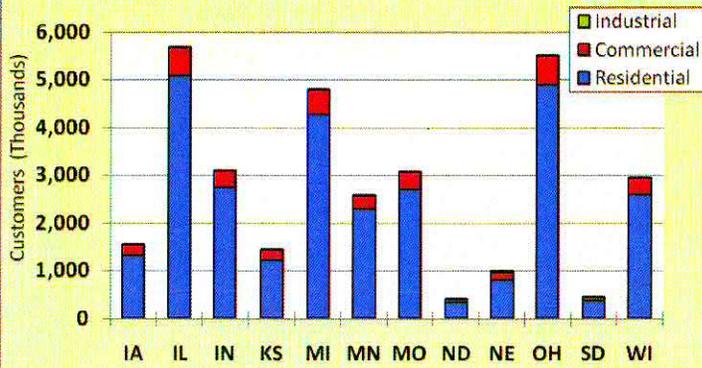
- Monthly MW demand levels among five selected NERC Regions show:
  - June through August is the peak-demand period.
  - RFC and SERC have the highest demand and seasonal variability.
  - WECC is the third highest while MRO is the lowest in term of MW demand.



## Midwest Electricity Sales by State and Sector, 2009



## Midwest Electric Customers by State, 2009



## Electric Transmission

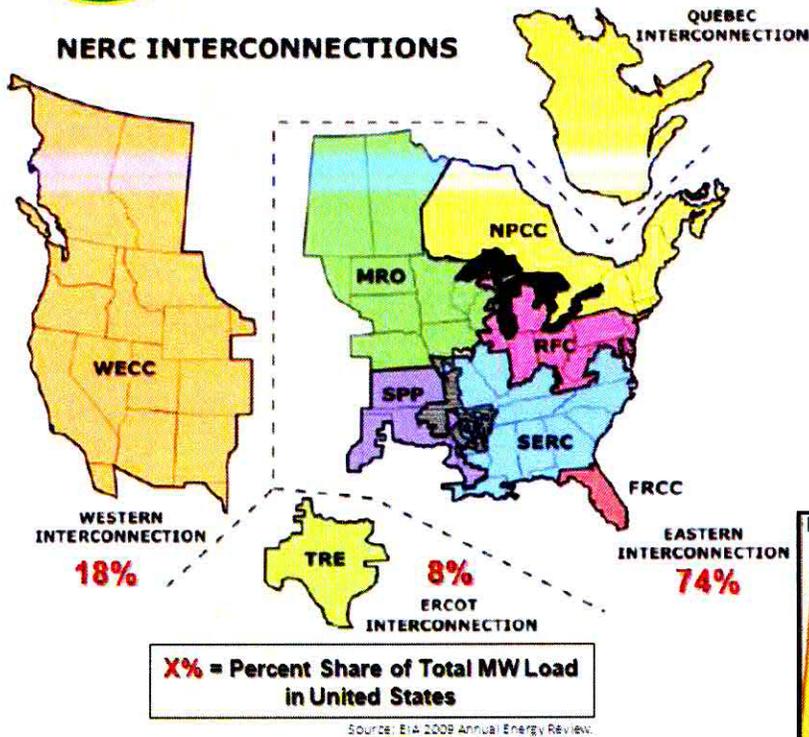
- In 2009, the total length of high voltage (>200 kV) transmission lines in the U.S. was about 202,000 circuit miles.
  - The backbone system in the Midwest consists of 765-, 500-, 345-, and 230-kV networks.
  - Two 1000-kV DC lines run from North Dakota to Minnesota
  - Power market operations in the Midwest is primarily under the purview of the Midwest Independent System Operator (MISO). Some portions are governed by the PJM interconnection.
- In the U.S., about 3,000 circuit miles of new >100 kV transmission lines were added since summer 2009.
  - Bulk-power system reliability is the predominant reason for the addition of new transmission lines and upgrades.



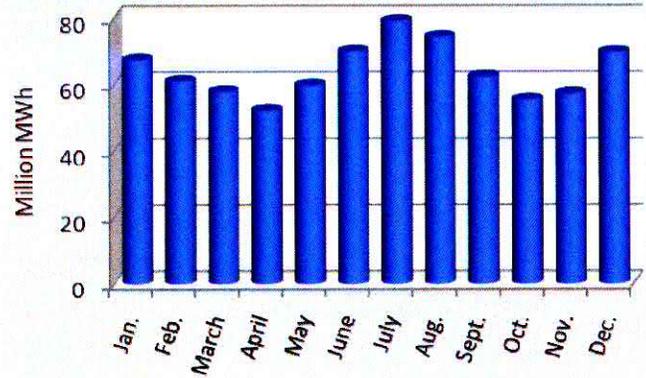
# Midwest States Regional Energy Assurance Exercise Chicago, Illinois - August 31 & September 1, 2011

Sponsored by the U.S. Department of Energy (DOE) Office of Electricity Delivery and Energy Reliability (OE)

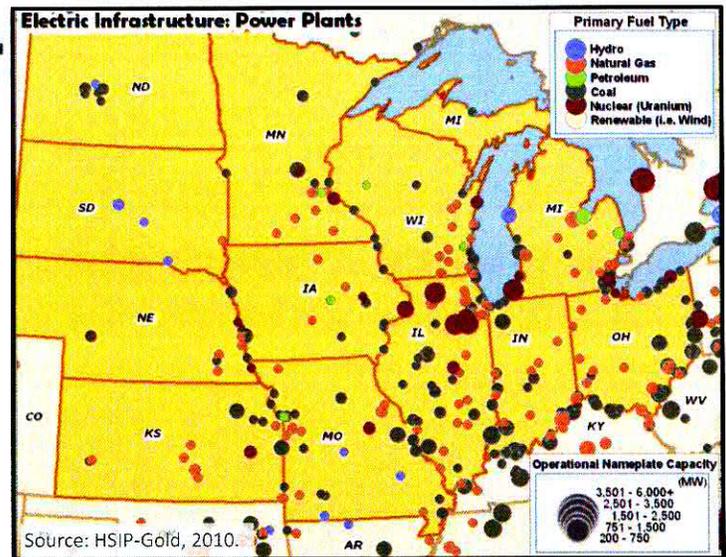
Electricity



## Monthly Net Generation in U.S., 2010



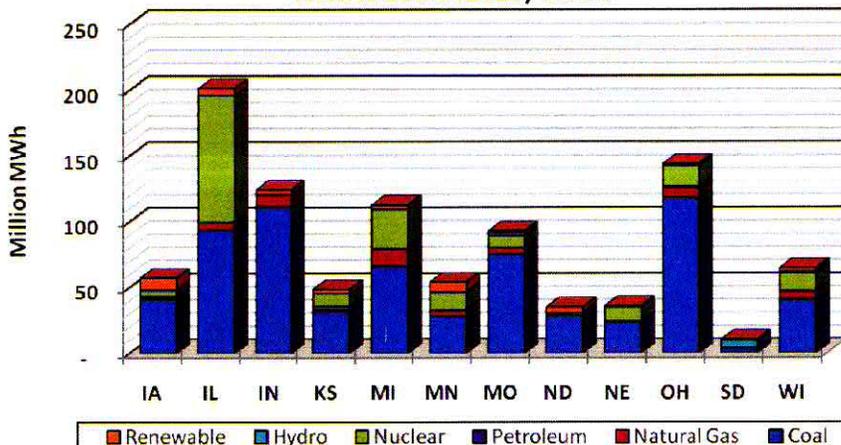
Source: EIA, Form EIA-923.



### Existing and Planned Generating Capacity

- Electric generating plants in the Midwest states are diverse in terms fuel source. The capacity mix with respect to fuel source indicates the dominance of nuclear power in the region.
- Illinois has the highest installed capacity, followed by Ohio, Indiana, and Michigan.
- Electric power producers in the Midwest planned to add 72,157 MW of capacity between 2010 and 2014. Of this, 48% will be natural gas-fired (34,828 MW) and 23% coal-fired (16,685 MW).

### Electricity Net Generation by Fuel: Midwest States, 2009



Source: EIA, Form EIA-923.

### Net Generation by Fuel Type

- Electric energy generation in the Midwest is supported primarily by coal. The second most dominant fuel type is nuclear.
  - Coal-fired plants dominate power generation in Ohio, Indiana and Illinois
  - Illinois ranks #1 in the U.S. in terms of nuclear power plant capacity with a net generation of 95.7 million megawatt-hours (MWh).
  - Minnesota, with the most renewable electric generation, ranks #14 in the U.S. with a net generation of 6.6 million MWh
- Regional dependence on coal-fired power implies regional dependence on rail shipments from Powder River Basin. Logistics issues resulting from a wide range of man-made and natural disruptions can affect movements of coal by rail and potentially result in power plant shutdowns.



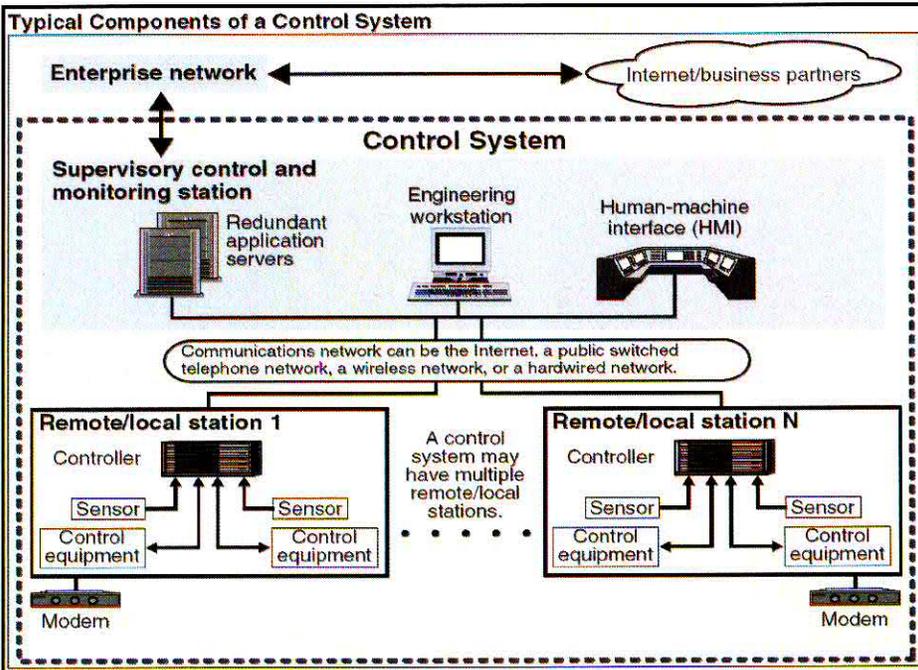
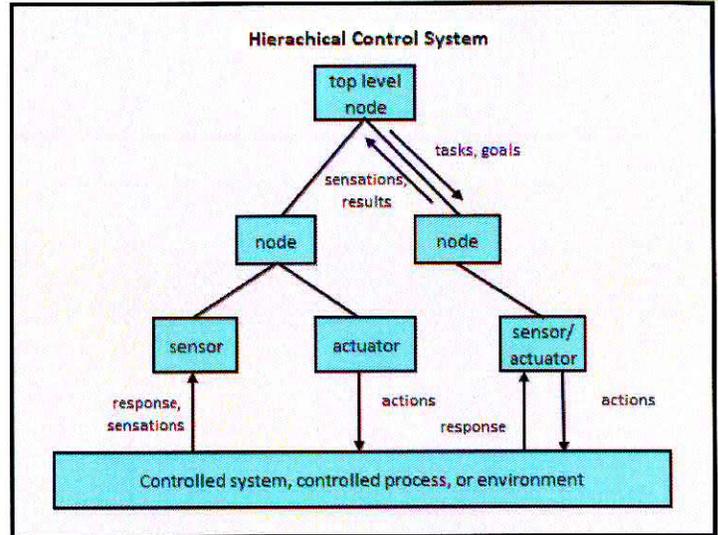
# Midwest States Regional Energy Assurance Exercise Chicago, Illinois - August 31 & September 1, 2011

Sponsored by the U.S. Department of Energy (DOE) Office of Electricity Delivery and Energy Reliability (OE)

Process Control

**Process control** is a system used to automate and control process operations in many sectors:

- Electric power generation, transmission and distribution
- Oil and gas production, pipeline movements, and storage
- Telecommunications
- Water and sewage
- Mass transit and traffic signals
- Food and chemical industry
- Other manufacturing
- Buildings and facilities



Source: GAO (analysis), Art Explosion (clipart).

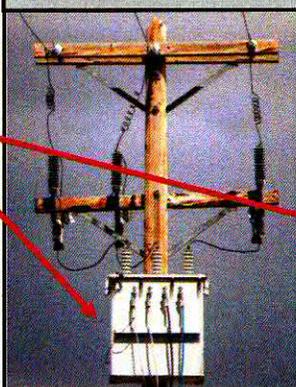
## Control System Definitions:

- **Supervisory Control And Data Acquisition (SCADA)** - A system consisting of a number of remote terminal units (RTUs) collecting field data connected back to a master station via a communications system. The master station displays the data and allows operator performance of remote control operations tasks.
- **Process or Distributed Control System (PCS/DCS)** - A control system where the data acquisition and control functions are performed by a number of distributed microprocessor-based units situated near the field devices being controlled or sensor instruments providing data gathering. The operator interacts with the system through use of a Human-Machine Interface (HMI).
- **Hybrid Systems** - A system of Programmable Logic Controllers (PLC) and/or Intelligent Electronic Devices (IED) that provide flexible configuration of a control system with full programmability, communications and functionality.

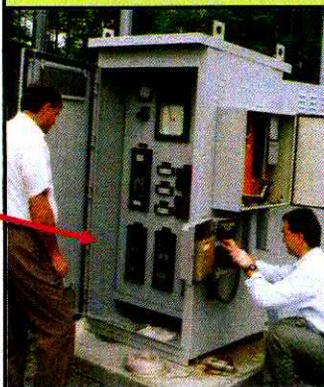
### A SCADA/DCS system performs four functions:

- Data acquisition
- Networked data communication
- Data presentation
- Control

### Recording and Control Terminal Unit



### Controls at an Electric Substation

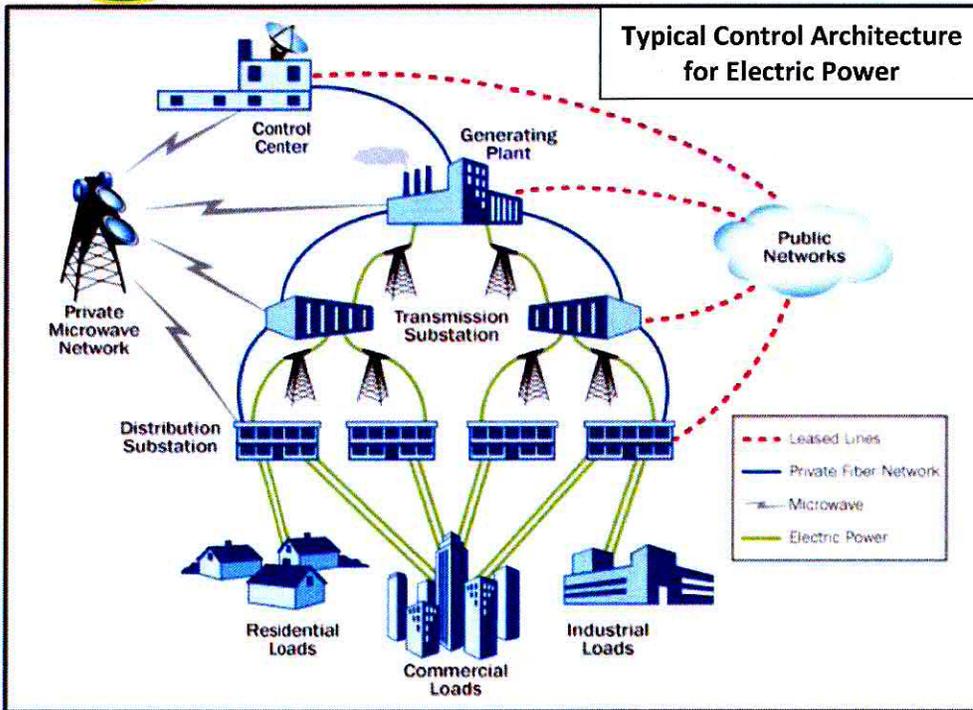




# Midwest States Regional Energy Assurance Exercise Chicago, Illinois - August 31 & September 1, 2011

Sponsored by the U.S. Department of Energy (DOE) Office of Electricity Delivery and Energy Reliability (OE)

Process Control



### Well-Known Incidents:

- A computer worm infecting PLCs known as Stuxnet damages centrifuges at an Iranian uranium enrichment facility (2010).
- Ohio Davis-Besse Nuclear Power Plant safety monitoring system was offline for 5-hours due to Slammer Worm (January 2003)
- Computers and manuals seized in Al Qaeda training camps full of SCADA information related to dams and similar structures (2003).
- Russian government announced that hackers succeeded in gaining control of the world's largest natural gas pipeline network owned by Gazprom (2000).
- Teenager breaks into NYMEX and cuts off Worcester Airport in Massachusetts for 6 hours, affecting both air and ground communications (1997).

### Main elements of a SCADA/DCS system:

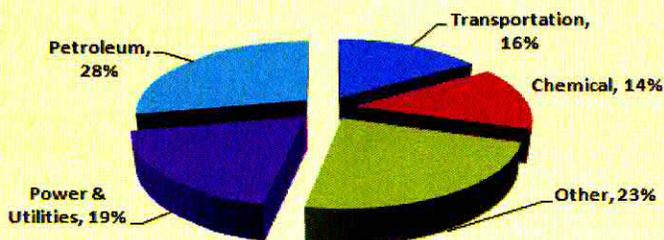
- Master Station/HMI
- Communications
- RTUs or PLCs
- Sensors
- Control Equipment

### Typical Control Room



### Who is Getting Attacked?

(2002 - 2004 data on Industrial Control Systems attacks)



Source: Industrial Security Incident Database

### Top 10 Vulnerabilities of Control Systems

1	Inadequate Policies, Procedures, and Culture Governing Control System Security.
2	Inadequately Designed Control System Networks That Lack Sufficient Defense-In-Depth Mechanisms.
3	Remote Access to the Control System without Appropriate Access Control.
4	Auditable System Administration Mechanisms (System Updates, User Metrics, etc.) are Not Part of Control System Implementation.
5	Inadequately Secured Wireless Communication.
6	Use of a Non-Dedicated Communications Channel for Command and Control, such as Internet Based SCADA, and/or Inappropriate Use of Control System Network Bandwidth for Non-Control Purposes (e.g., VOIP).
7	Lack of Quick and Easy Tools to Detect And Report on Anomalous or Inappropriate Activity. Inadequate or Non-Existent Forensic and Audit Methods.
8	Installation of Inappropriate Applications on Critical Control System Host Computers.
9	Software Used in Control Systems is Not Adequately Scrutinized.
10	Control Systems Command and Control Data Not Authenticated.

Source: NERC. "Top 10 Vulnerabilities of Control Systems and Their Associated Mitigations" [http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/Top\\_10\\_vuln\\_2006\\_16\\_mar2006\\_ss.pdf](http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/Top_10_vuln_2006_16_mar2006_ss.pdf)

- U.S. Department of Energy (<http://energy.gov/oe/technology-development/control-systems-security>)
- InfraGard (<http://www.infragard.net/>)
- Multi-State Information Sharing and Analysis Center (<http://msisac.cisecurity.org/>)
- U.S. CERT (<http://www.us-cert.gov/>)

# Timeline – Scenario 1

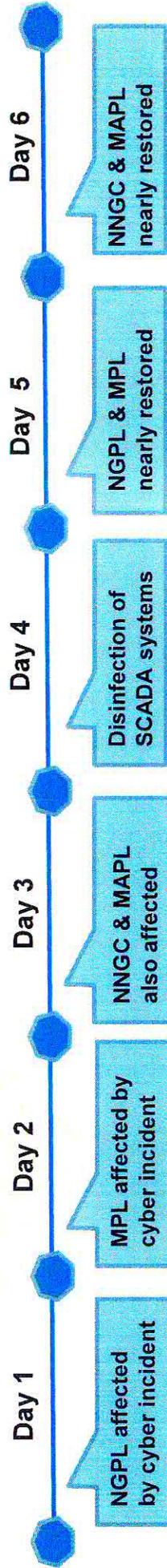
## APPENDIX C Scenario One Timeline

**SEVERE**  
Severe Level of Impacts

**HIGH**  
High Level of Impacts

**ELEVATED**  
Elevated Level of Impacts

**LOW**  
Low Level of Impacts



Day	Description	Midwest Population w/o Electricity	Affected Midwest States															
			IA	IL	IN	KS	KY	MI	MO	ND	NE	OH	SD	WI				
1	Major news organizations reporting natural gas delivery problems for interstate pipelines including Natural Gas Pipeline of America (NGPL): <ul style="list-style-type: none"> <li>* Pipeline switches to manual operation mode</li> <li>* Dispatches all available personnel to the field</li> <li>* Pipeline deliverability reduced</li> </ul>	5,000																
2	Pipeline control issues similar to NGPL experience also occurs today at Marathon Pipeline (MPL): <ul style="list-style-type: none"> <li>* Cyber-related</li> <li>* Safe shutdown performed</li> <li>* Pipeline integrity monitored</li> </ul>	5,000																
3	Conditions similar to NGPL experience occurs at Northern Natural Gas Company (NNGC) and Mid-America Pipeline (MAPL): <ul style="list-style-type: none"> <li>* Also appears to be cyber-related</li> <li>* Similar procedures instituted as previously-affected pipelines</li> <li>* Negative impact on direct-connected power plants and refineries</li> </ul>	24,000																
4	Field workers continue manual operations. Disinfection and restoration of SCADA system resumes: <ul style="list-style-type: none"> <li>* Malware infection appears limited to Control Center</li> <li>* Has not apparently spread to field equipment from audit of PLCs</li> <li>* Additional testing performed to confirm that all SCADA and PLC level software is fully operational</li> </ul>	24,000																
5	Restoration of SCADA system nearly complete for NGPL and MPL: <ul style="list-style-type: none"> <li>* Safety checks and Control Room testing completed</li> <li>* Implemented operating pressure restrictions</li> <li>* Restart of pipeline tightly controlled and closely monitored</li> </ul>	24,000																
6	Restoration of SCADA system nearly complete for NNGC and MAPL: <ul style="list-style-type: none"> <li>* Safety checks and Control Room testing completed</li> <li>* Implemented operating pressure restrictions</li> <li>* Restart of pipeline tightly controlled and closely monitored</li> </ul>	19,000																
7	Pipeline operations returning to normal: <ul style="list-style-type: none"> <li>* Pipelines trying to make up for downtime</li> <li>* General rebuild of petroleum stocks</li> <li>* Disrupted natural gas-fired power plants available for restart</li> </ul>	0																

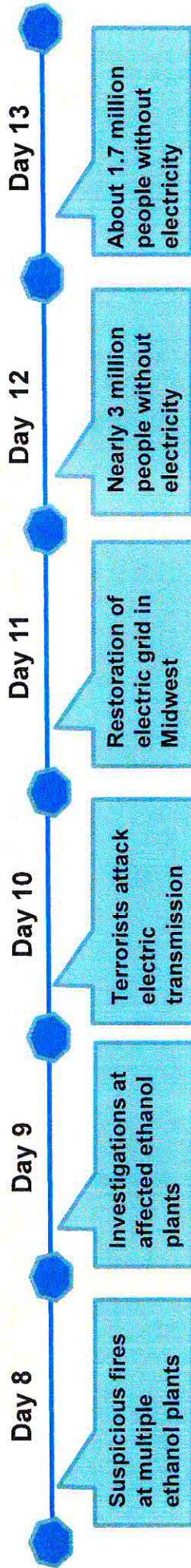
# Timeline – Scenario 2

**SEVERE**  
Severe level of impacts

**HIGH**  
High level of impacts

**ELEVATED**  
Elevated level of impacts

**LOW**  
Low level of impacts



## APPENDIX D Scenario Two Timeline

Day	Description	Midwest Population w/o Electricity	Affected Midwest States													
			IA	IL	IN	KS	KY	MI	MIN	MO	ND	NE	OH	SD	WI	
8	<ul style="list-style-type: none"> <li>Simultaneous fires/explosions at multiple ethanol production plants:                             <ul style="list-style-type: none"> <li>* Eight plants in seven Midwest states</li> <li>* Fire and explosions causing evacuation of nearby facilities</li> </ul> </li> <li>U.S. Government investigating cause:                             <ul style="list-style-type: none"> <li>* Major impact on fuel ethanol production</li> <li>* Security increased at energy facilities</li> <li>* Gasoline prices affected due to psychological factors</li> </ul> </li> </ul>	0														
9	<ul style="list-style-type: none"> <li>Terrorists attack several electric transmission towers:                             <ul style="list-style-type: none"> <li>* Transmission lines extensively damaged</li> <li>* Cascading line overloads and ensuing power swings in MISO territory</li> <li>* Power system collapse affects multiple states from IA to WI</li> </ul> </li> </ul>	0														
10	<ul style="list-style-type: none"> <li>Restoration of the Power Grid continues:                             <ul style="list-style-type: none"> <li>* Power is disrupted periodically as a normal part of balancing the restoration across the electric outage area</li> </ul> </li> </ul>	15,700,000														
11	<ul style="list-style-type: none"> <li>Power restoration continues: conservation still required:                             <ul style="list-style-type: none"> <li>* ISO/RTD officials continue to work closely with state agencies, local distribution companies and external power providers to ensure electricity is returned as soon as possible</li> </ul> </li> </ul>	14,900,000														
12	<ul style="list-style-type: none"> <li>Power situation begins to stabilize:                             <ul style="list-style-type: none"> <li>* Almost all parts of the electric outage area has some power over the next 24 hours as significant load restoration is expected</li> </ul> </li> </ul>	2,900,000														
13	<ul style="list-style-type: none"> <li>Electric sector restoration nearly complete:                             <ul style="list-style-type: none"> <li>* Conservation efforts and imports from neighbouring jurisdictions helped avoid the need for rotating power outages</li> </ul> </li> </ul>	1,700,000														
14		160,000														

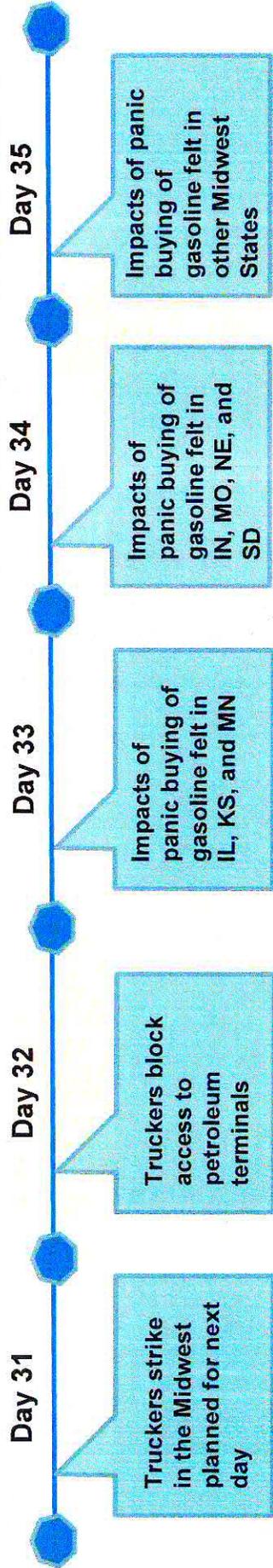
# Timeline – Scenario 3

**SEVERE**  
Severe Level of Impacts

**HIGH**  
High Level of Impacts

**ELEVATED**  
Elevated Level of Impacts

**LOW**  
Low Level of Impacts



## APPENDIX E Scenario Three Timeline

Day	Description	Midwest Population w/o Electricity	Affected Midwest States															
			IA	IL	IN	KS	KY	MI	MN	MO	ND	NE	OH	SD	WI			
31	Truckers Strike in the Midwest: * Independent truckers plan a work stoppage for the next day	0																
32	Truckers block access to petroleum tank farms and petroleum refineries: * Service stations are not being refilled by striking truckers	0																
33	Drivers start panic buying following news of the strike and closures of highways and tunnels: * People refueling frequently, causing local service stations to close	0																
34	Gasoline stations running out of gasoline in IL, KS, and MN: * Motorists traveling out-of-state wherever gasoline stations are open	0																
35	Gasoline stocks extremely low in service stations in IN, MO, NE, and SD: * Employees trying to telecommute instead of driving	0																
36	Gasoline situation serious in IA, ND, and WI: * Gasoline situation becoming grave in IL, KS, and MN	0																
37	Gasoline supplies low throughout the Midwest States: * Business activities grinding to a halt	0																

 <h2 style="text-align: center;">Addressing the Root Causes of Downtime</h2>				
Addressing the Leading Root Causes of Downtime +	Should You Take Your Data Center into the Cloud? +	10 Steps to Increasing Data Center Efficiency and Availability +	Maximizing Data Center Efficiency, Capacity and Availability +	The Four Trends Driving the Future of Data Center Design +



 Print Article  Close Window

From: [www.cio.com](http://www.cio.com)

## Ten Years After 9/11, Cyberattacks Pose National Threat, Committee Says

– Jaikumar Vijayan, Computerworld

September 07, 2011

Ten years after the terrorist attacks of Sept. 11, 2001, the nation faces a critical threat to its security from cyberattacks, a new report by a bipartisan think tank warns.

Slideshow: [What Online News Looked Like on 9/11](#)

The report, released last week by the Bipartisan Policy Center's National Security Preparedness Group (NSPG), offers a broad assessment of the progress that government has made in implementing the security recommendations of the 9/11 Commission. The comments about cyber security are part of broader discussion on nine security recommendations that have yet to be implemented.

The [report](#), the foreword to which is signed by Lee Hamilton, a former Democratic representative from Indiana, and Thomas Kean, former governor of New Jersey, notes that catastrophic cyberattacks against U.S. critical infrastructure targets are not a mere theoretical threat.

"This is not science fiction," the NSPG said its report. "It is possible to take down cyber systems and trigger cascading disruptions and damage. Defending the U.S. against such attacks must be an urgent priority."

The report highlights concerns expressed by the Department of Homeland Security (DHS) and the U.S. intelligence community about terrorists using cyber space to attack the country without physically crossing its borders. "Successive [intelligence chiefs] have warned that the cyber threat to critical infrastructure systems -- to electrical, financial, water, energy, food supply, military, and telecommunications networks -- is grave."

The report makes note of a briefing in which DHS officials described a "nightmare scenario" of terrorists hacking into the U.S. electric grid and shutting down power across large sections of the country for several weeks. "As the current crisis in Japan demonstrates disruption of power grids and basic infrastructure can have devastating effects on society," the report noted.

The committee's report is sure to reinforce perceptions among many within the security industry that critical infrastructure targets remain [woefully underprepared](#) for dealing with cyberattacks. Over the past few years there have been numerous attacks targeting government and military networks. Most of the attacks are believed to be the work of highly organized, well funded, state-sponsored groups.

Despite the attacks, some believe that those within government are not taking the threat seriously enough. Just a few weeks ago for instance, Cofer Black, former director of the CIA's Counterterrorism

Center during the Bush Administration warned about cyber threats [not being taken seriously enough](#) .

Though many security experts agree that future conflicts will likely be fought in cyberspace, military and government officials have shown a hesitancy to act until they see a validation of the threats, Black said during a keynote address at the Black Hat conference in August. It was the same sort of skepticism that many government officials had showed toward the alarms sounded prior to the Sept. 11, 2001, Black had noted.

The Bipartisan Policy Center (BPC) is a Washington-based think tank that was established in 2007 by former Senate Majority leaders Howard Baker, Tom Daschle, Bob Dole and George Mitchell. The NSPG is a group that was established by the BPC to monitor the implementation of the 9/11 Commission's recommendations for bolstering national security in the aftermath of the terrorists attacks.

Last week's report offers an assessment of the progress that the government has made in implementing the commission's recommendations. According to the NSPG the government has made significant progress in addressing many of the 9/11 Commission's 41 recommendations.

However, several crucial ones remain very much a work in progress, the report noted.

One area where little progress has been made, has to do with the recommendation to [increase the availability of radio spectrum for public safety purposes](#), the report noted.

"Incompatible and inadequate communications led to needless loss of life," on 9/11 the BPC said in its report. But plans to address the issue by setting aside more radio spectrum for first responders have "languished" because of a political fight over whether to allocate 10MHz of radio spectrum to first responders or to a commercial wireless bidder.

Another area where progress has been limited has been on the civil rights and privacy fronts, the report noted. Surveillance activities and the use of tools such as National Security Letters to search for terrorists has greatly expanded since the 9/11 attacks. But a recommendation for setting up a Privacy and Civil Liberties Oversight Board with the Executive Branch has yet to be fully implemented.

"If we were issuing grades, the implementation of this recommendation would receive a failing mark," the NSPG said.

Jaikumar Vijayan covers data security and privacy issues, financial services security and e-voting for Computerworld. Follow Jaikumar on Twitter at [@jaivijayan](#) or subscribe to [Jaikumar's RSS feed](#) . His e-mail address is [jvijayan@computerworld.com](mailto:jvijayan@computerworld.com) .

[Read more about security](#) in Computerworld's Security Topic Center.

© 2010 Computerworld Inc.

UNCLASSIFIED



# NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER BULLETIN

A-0010-NCCIC -160020110719

---

**DISTRIBUTION NOTICE (A): THIS PRODUCT IS INTENDED FOR THE CYBERSECURITY, CRITICAL INFRASTRUCTURE AND / OR KEY RESOURCES COMMUNITY AT LARGE.**

---

## **“ANONYMOUS” AND ASSOCIATED HACKER GROUPS CONTINUE TO BE SUCCESSFUL USING RUDIMENTARY EXPLOITS TO ATTACK PUBLIC AND PRIVATE ORGANIZATIONS**

---

### EXECUTIVE SUMMARY

---

(U) This Bulletin is being provided for your Executive Leadership, Operational Management, and Security Administrators situational awareness. The actors who make up the hacker group “Anonymous” and several likely related offshoots like “LulzSec”, continue to harass public and private sector entities with rudimentary exploits and tactics, techniques, and procedures (TTPs) commonly associated with less skilled hackers referred to as “Script Kiddies”<sup>1</sup>. Members of Anonymous routinely claim to have an overt political agenda and have justified at least a portion of their exploits as retaliation for perceived ‘social injustices’ and ‘freedom of speech’ issues. Attacks by associated groups such as LulzSec have essentially been executed entirely for their and their associates’ personal amusement, or in their own hacker jargon “for the lulz”.

(U) Anonymous insist they have no centralized operational leadership, which has been a significant hurdle for government and law enforcement entities attempting to curb their actions. With that being said, we assess with high confidence that Anonymous and associated groups will continue to exploit vulnerable publicly available web servers, web sites, computer networks, and other digital information mediums for the foreseeable future.

(U) So far, Anonymous has not demonstrated any capability to inflict damage to critical infrastructure, instead choosing to harass and embarrass its targets. However, some members of LulzSec have demonstrated moderately higher levels of skill and creativity, evidenced in attacks using combinations of methods and techniques to target multiple networks. To date, their attacks have largely resulted in the release of sensitive documents and personally identifiable information. These attacks have the potential to result in serious harm, particularly to Law Enforcement and other Federal, State and Local Government personnel who may be targeted as a result. Also, this assessment does not take into account the



---

<sup>1</sup> Script Kiddie: Unskilled individuals who use scripts or programs developed by others to attack computer systems and networks and deface websites.

UNCLASSIFIED

UNCLASSIFIED

possibility of a higher-level actor providing Anonymous, LulzSec or a similar group with more advanced capabilities.

BACKGROUND

(U) Anonymous emerged in 2003 on the internet message board / web forum 4chan as a collective group of individuals whose primary purpose was to operate in complete anonymity (as the group name implies), and carry out random acts across the web for their collective amusement. Since then, Anonymous has conducted a number of malicious cyber acts and employed a variety of TTPs (discussed later). In their earlier years, Anonymous' acts seemed to be somewhat random; it wasn't until 2008 that Anonymous became associated with hacktivist<sup>2</sup> activities.



(U) Anonymous' lack of a centralized leadership structure and distributed (often international) personnel poses a significant hurdle for law enforcement organizations hoping to curb the flow of cyber attacks against organizations. Additionally, international law governing cyber crime varies between countries, and often times, attributing malicious activities to cyber operators is difficult.

(U) Though Anonymous' hacktivist activities are commonly reported to have started in 2008, the group has claimed responsibility for several other cyber attacks motivated by "social injustices" as early as 2006. It wasn't until their

distributed denial of service (DDOS) attacks on the Church of Scientology's public facing website (which Anonymous justified as being in retaliation to perceived violations of American's right to freedom of speech) that the group began to garner significant media attention and internet notoriety. Several attacks against other organizations in 2008 followed the attack targeting the Church of Scientology's website, though it is difficult to judge Anonymous's intent behind the attacks<sup>3</sup>. Anonymous also organized several physical protests in response to the alleged Church of Scientology censorship campaign (pictured above).



(U) 2009 brought new opportunities for Anonymous to flex their newfound hacktivism muscle, with at least two attacks targeting organizations that Anonymous viewed as pro-censorship, and involvement in protests in response to the 2009 Iranian elections, where Mahmoud Ahmadinejad was named the winner despite discrepancies in the number of votes. Anonymous, in collaboration

<sup>2</sup> Hacktivist: The nonviolent use of illegal or legally ambiguous digital tools in pursuit of political ends. These tools include web site defacements, redirects, denial-of-service attacks, information theft, web site parodies, virtual sit-ins, and virtual sabotage.<sup>4</sup>

<sup>3</sup> Later 2008 attacks included random acts of malice such as an invasion of a public web forum for the Epilepsy Foundation, and attacks against Support Online Hip Hop/All Hip Hop.

## UNCLASSIFIED

with the Bit Torrent<sup>4</sup> site The Pirate Bay, set up a pro-Iranian Green Party website where internet users could voice support for Iranians who were protesting the election results. In 2009 and early 2010 (respectively), Anonymous also conducted DDOS attacks targeting the Governments of Germany and Australia.

(U) Anonymous increased its notoriety in 2010 with high-profile attacks motivated by the arrest of U.S. Army Private Bradley Manning in connection to Wikileaks, releasing several thousand classified U.S. government documents on the internet. Though Anonymous's past actions indicate these cyber attacks should have been motivated by Anonymous's views on freedom of speech, their public statements indicated that the intent was to retaliate against mistreatment of Pvt. Manning while he was in U.S. custody.

(U) Anonymous' activities increased throughout 2011 with a number of high-profile attacks targeting both public and private sector entities. Several of these attacks utilized DDoS as their primary tool, while others relied on cross-site scripting exploits to conduct website defacements. Interestingly, Anonymous justified nearly all of their attacks conducted between 2010 and 2011 by citing social or political injustices by each victim organization.

(U) In 2011, a group of relatively more talented individuals spun off from Anonymous to form the hacker group "LulzSec," to which has been attributed several high profile exploitation/attack incidents involving public and private sector organizations. Though LulzSec initially claimed to operate independently of Anonymous, it became clear that the level of coordination between the two groups was greater than initially thought. Upon completing what they termed a "voyage" of hacking for a period of time, it is confirmed that a small cohort of LulzSec returned to Anonymous.



---

### TACTICS, TECHNIQUES, AND PROCEDURES

---

(U) Anonymous utilizes the internet to recruit and train new personnel, conduct reconnaissance on potential targets, exploit vulnerabilities found in information systems, deny access to resources, alter information presented by organizations, and steal sensitive information. Though the TTPs and tools employed by Anonymous are commonly thought to be rudimentary and unsophisticated, their success to date executing operations and gaining media attention is on par with high profile incidents allegedly involving sophisticated "Advanced Persistent Threat" (APT) actors. They have relied on taking advantage of weaknesses in applications, thus allowing them to bypass, at least initially, conventional network defenses such as firewalls and anti-virus applications to access sensitive data. Additionally, Anonymous and closely associated groups appear to be building upon recent successes by conducting highly visible messaging campaigns over publicly available social media forums such as Twitter<sup>(USPER)</sup>, YouTube<sup>(USPER)</sup>, and Facebook<sup>(USPER)</sup>.

(U) Anonymous and associated groups pride themselves on being 'social media' savvy, and routinely use forums such as Twitter, Facebook, and public web pages to announce intended targets, ongoing attack results, and post files stolen from victim computer networks. These announcements can provide

---

<sup>4</sup> Bit Torrent: A Peer-to-Peer File Sharing Protocol.

## UNCLASSIFIED

computer network defenders the opportunity to pro-actively supplement their computer network defenses and provide awareness to management, employees, and partners. For example, cybersecurity experts who have analyzed previous Anonymous attacks have noted there was a significant amount of reconnaissance prior to the attack. Other cybersecurity experts have recommended that public and private sector entities go through the same steps hackers would to determine the extent of attack surface available to a malicious actor. An example of this might entail using internet search engines like Google <sup>(USPER)</sup> to identify sensitive information and computer network vulnerabilities that have been cached as they catalogue the content of the WWW.

---

### ANTICIPATED FUTURE TARGETS

---

(U) Members of the group LulzSec were possibly associated with the 15 June 2011 DDOS attack on the Central Intelligence Agency's (CIA) public-facing website. Although no information was stolen or released to the public, and the website was not defaced, the site was targeted in a manner consistent with other LulzSec and Anonymous attacks. Anonymous also declared that the group was at "war" with the Intelligence Community (IC) and has identified it as a future target. Anonymous is likely targeting the IC because it views it as violating its core belief in total freedom of information. Additionally, following the release of government e-mail account data from the July 2011 Booz Allen compromise, an Anonymous operator stated on Twitter that, "We are working on two of the biggest releases for Anonymous in the last 4 years. Put your helmets on. It is war."

(U) Anonymous has also stated its intent to target companies related to certain Critical Infrastructure / Key Resources sectors. On 12 July 2011, Anonymous released personally identifiable information of approximately 2500 employees of U.S. Agricultural Company Monsanto, and claimed to have taken down corporate web assets and mail servers. Additionally, in a separate statement on 12 July 2011, Anonymous declared their intention to attack several U.S., Canadian, and British companies, including Exxon Mobil and ConocoPhillips, who were associated with development of oil sands in Alberta, Canada.

(U) Future attacks are likely to continue but will likely remain limited in scope due to a lack of advanced capabilities. These attacks are also likely to target the Federal government and critical infrastructure sectors, particularly in response to publicized events relating to civil liberties, cyber security, or allegations of censorship (online or otherwise).

---

### THE WAY AHEAD

---

(U) Some members of LulzSec have demonstrated moderately higher levels of skill and creativity that include using combinations of methods and techniques to target multiple networks. This does not take into account the possibility of a higher-level actor providing LulzSec or Anonymous more advanced capabilities. Therefore, it may be advisable to adjust monitoring of both internal and external resources for indications of a pending or ongoing attack on cyber or telecommunications networks.

(U) The NCCIC recommends that U.S., Federal/State/local/Tribal/Territorial Departments and Agencies, and private sector partners ensure they have processes in place to notify their leadership and network operators if their organization becomes a possible target by hacktivists or other malicious actors, and what notifications they are required or plan to make in the event of an attack.

UNCLASSIFIED

## UNCLASSIFIED

(U) Should a cyber attack occur, ensure backup and recovery procedures are in place and enabled. Be prepared to execute a full spectrum defensive plan that includes contact information for external sources to draw on for assistance. Collect and centrally manage detailed aspects of the attack so you can provide accurate information to Operations, Security, and Law Enforcement personnel as necessary. Such a plan may also include materials identifying who to contact at your Internet service provider, possibly via alternate means, and at any time of day or night to minimize the duration and effect of a cyber attack. Similarly, have contact information readily available for public and private entities to draw on for assistance: the NCCIC, US-CERT, FBI Joint Terrorism Task Force, local FBI Field Office, applicable Information Sharing Analysis Center (ISAC), and Sector Specific Agency.

(U) For the situational awareness of F/S/L/T/T and CIKR partners, below are URLs to the National and Cyber Threat Levels the NCCIC monitors.

- National Terrorism Advisory System: <http://www.dhs.gov/alerts>
- NCRAL: Contact NCCIC Watch & Warning ([NCCIC@HQ.dhs.gov](mailto:NCCIC@HQ.dhs.gov))
- MS-ISAC: <http://www.msisac.org/index.cfm>
- IT-ISAC: <https://www.it-isac.org/>
- ES-ISAC: <http://www.esisac.com/>
- FS-ISAC: <http://www.fsisac.com/>

---

## ADDITIONAL INFORMATION

---

(U) While the U.S. Government doesn't endorse a particular solution, identifying vendors with experience combating such an attack may reduce the time it takes to get assistance mitigating such an attack and restoring service or operations. Additionally, the US-CERT web page offers a wide variety of technical and non-technical information to make use of both before and after an incident:

<http://www.us-cert.gov/nav/t01/>

(U) A variety of documents with information regarding defensive measures to combat a computer network attack are available at:

[http://www.cert.org/tech\\_tips/](http://www.cert.org/tech_tips/)

(U) Many organizations can suffer financial loss as a result of a cyber attack and may wish to pursue criminal or civil charges against the intruder. For legal advice, we recommend that you consult with your legal counsel and law enforcement.

(U) Data breaches which involve a monetary loss or include a financial nexus such as a compromise to your financial, credit or debit accounts, or personal information can be reported to the U.S. Secret Service for criminal investigation. For more information contact your local Secret Service Field Office for assistance.

[http://www.secretservice.gov/field\\_offices.shtml](http://www.secretservice.gov/field_offices.shtml)

(U) U.S. persons and companies interested in pursuing an investigation of a cyber attack can contact their local FBI field office for guidance and information. For contact information for your local FBI field office, please consult your local telephone directory or see the FBI's contact information web page:

<http://www.fbi.gov/contactus.htm>

UNCLASSIFIED

UNCLASSIFIED

(U) Non-U.S. entities may need to discuss malicious cyber activity with their local law enforcement agency to determine the appropriate steps that should be taken with regard to pursuing an investigation.

(U) U.S. Federal Government Departments and Agencies should report cyber attacks and incidents to US-CERT. Non-U.S. F/S/L/T/T Government Departments and Agencies interested in determining the source of certain types of cyber attacks may require the cooperation of your internet service provider and the administrator of the attacked networks. Tracking an intruder this way may not always be possible. If you are interested in trying do to so, contact your service provider directly, as the US-CERT is not able to provide this type of assistance. We do encourage you to report your experiences, however. This helps the NCCIC and US-CERT understand the nature and scope of security incidents on the Internet, and we may be able to relate your report to other activity that has been reported to us.

TERMS OF REFERENCE

---

**(U) Anonymous** - (used as a mass noun) is an Internet meme originating 2003 on the imageboard 4chan, representing the concept of many online community users simultaneously existing as an anarchic, digitized global brain. It is also generally considered to be a blanket term for members of certain Internet subcultures, a way to refer to the actions of people in an environment where their actual identities are not known.

**(U) Lulz** - often used to denote laughter at someone who is the victim of a prank, or a reason for performing an action. This variation is often used on the 'Oh Internet' wiki and '4chan' image boards.

**(U) Distributed Denial of Service (DDoS)** - an attempt to make a computer resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DDoS attack may vary, it generally consists of the concerted efforts of person or persons to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely.

**(U) Hacktivist** - a portmanteau of *hack* and *activism*.

POINTS OF CONTACT

---

(U) This was produced as a collaborative effort between the NCCIC Components and Functional Groups (US-CERT, ICS-CERT, NCS/NCC, I&A/CISD/CTAB).

(U) Please direct questions to the NCCIC Duty Officer (NDO). NCCIC will continue to coordinate with the appropriate component organizations listed below:

<b>NCCIC Duty Officer</b>	<b>US-CERT</b>	<b>NCS/NCC</b>	<b>ICS-CERT</b>
NCCIC@HQ.dhs.gov	SWO@US-CERT.gov	NCS@HQ.dhs.gov	ICS-CERT-SOC@dhs.gov
(703) 235-8831	(703)235-8832/8833	(703) 235-5080	(877) 776-7585