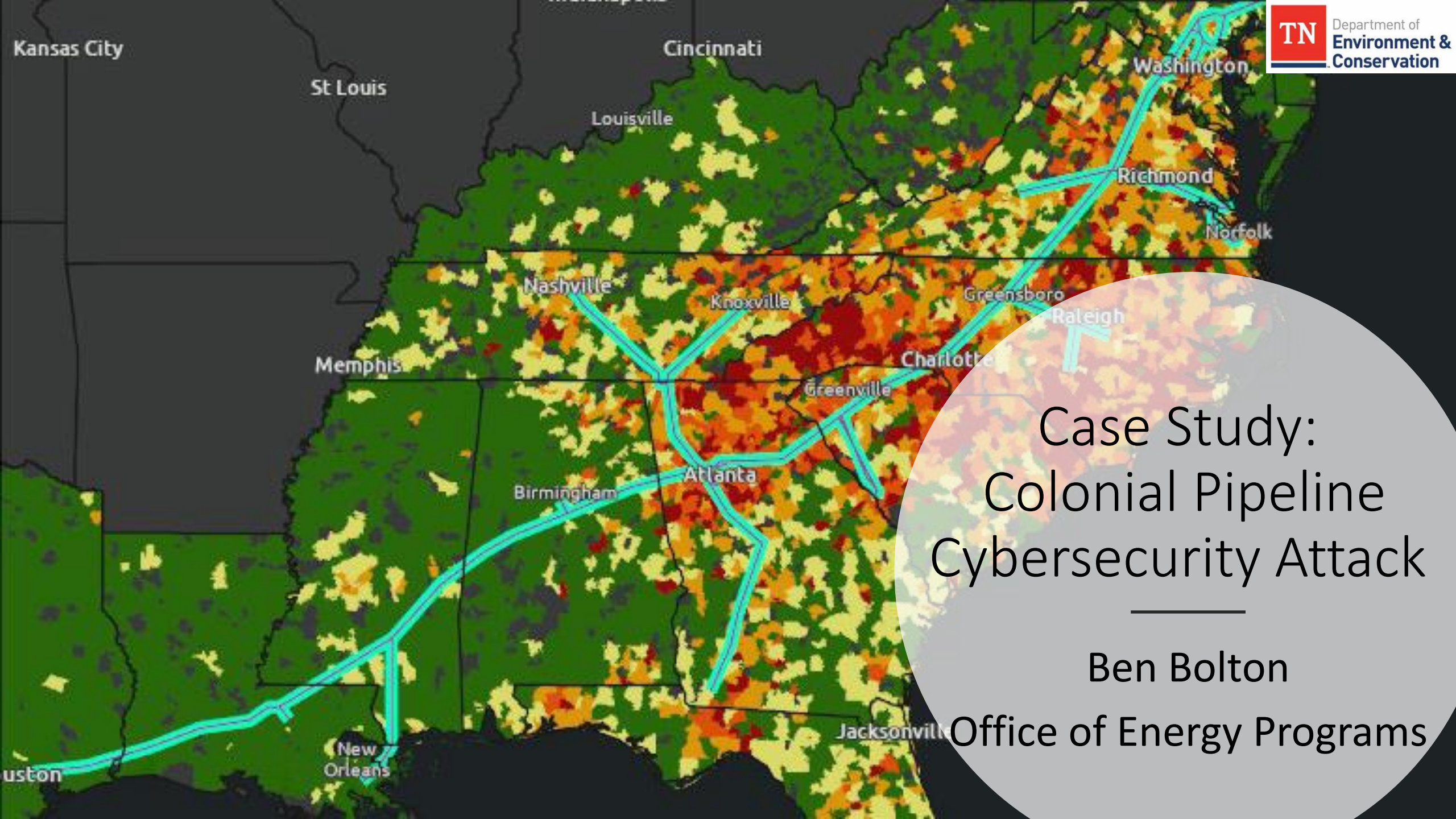


Colonial Pipeline
Ransomware Attack
Are you ready for when it
happens here?



A close-up shot of a person's hands filling a red gas can at a gas station. The person is wearing a dark jacket and blue jeans. The gas can is being held in the left hand, and the nozzle of the gas pump is being inserted into the opening. The background is slightly blurred, showing the gas pump and a white vehicle. The text "© CBS EVENING NEWS" is overlaid in the bottom left corner.

© CBS
EVENING
NEWS



Case Study: Colonial Pipeline Cybersecurity Attack

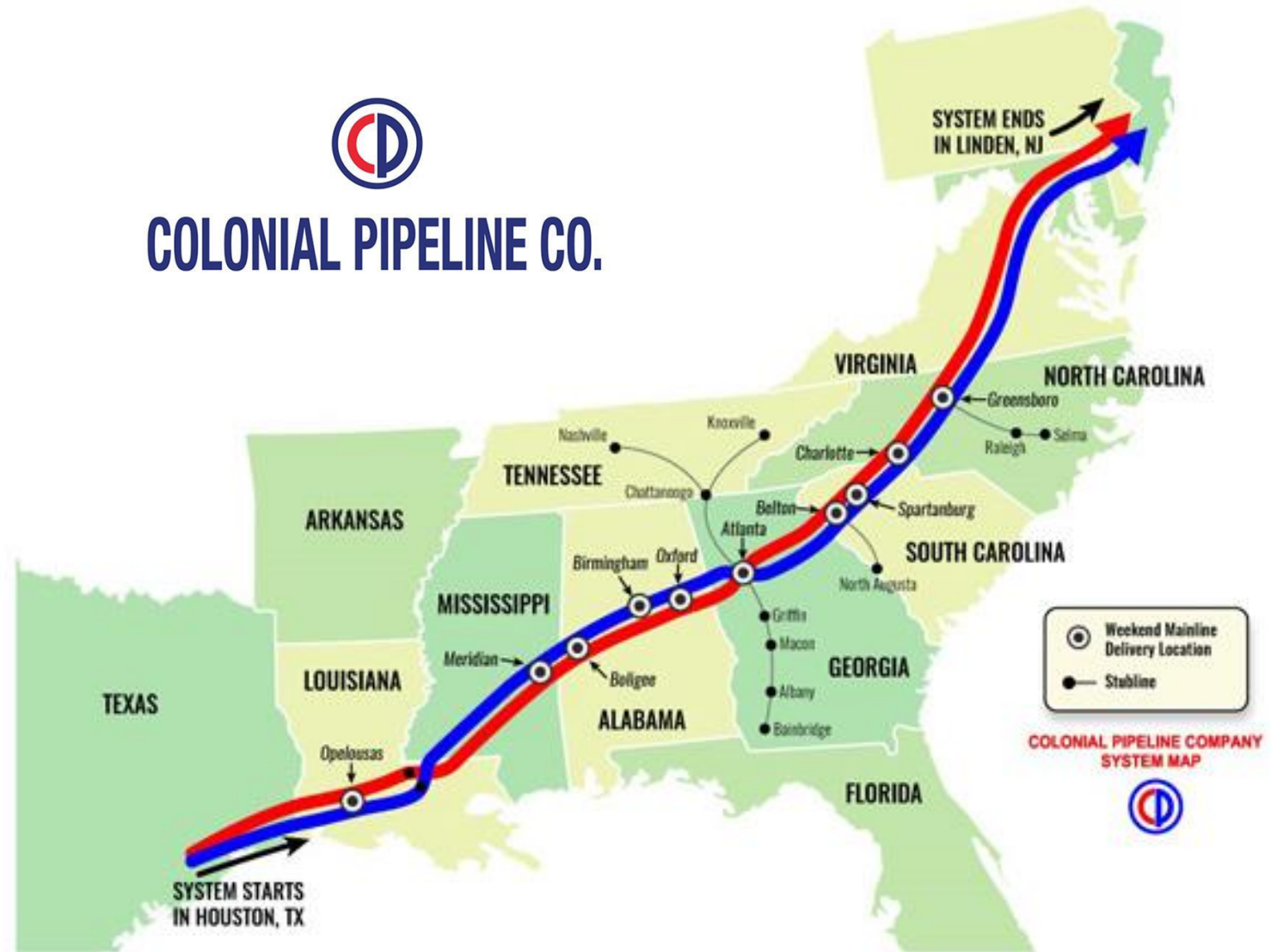
Ben Bolton

Office of Energy Programs

Introduction

Colonial Pipeline

- Built in 1963
- Begins in Houston, TX
- Runs 5,500 miles
- Supplies 7 major airports
- Ends in New York harbor
- Transports 100 million Gallons per day
- Moves ~ 4.5 mph
- >45% East Coast fuel supply



**SORRY
OUT
OF
SERVICE**

The Situation



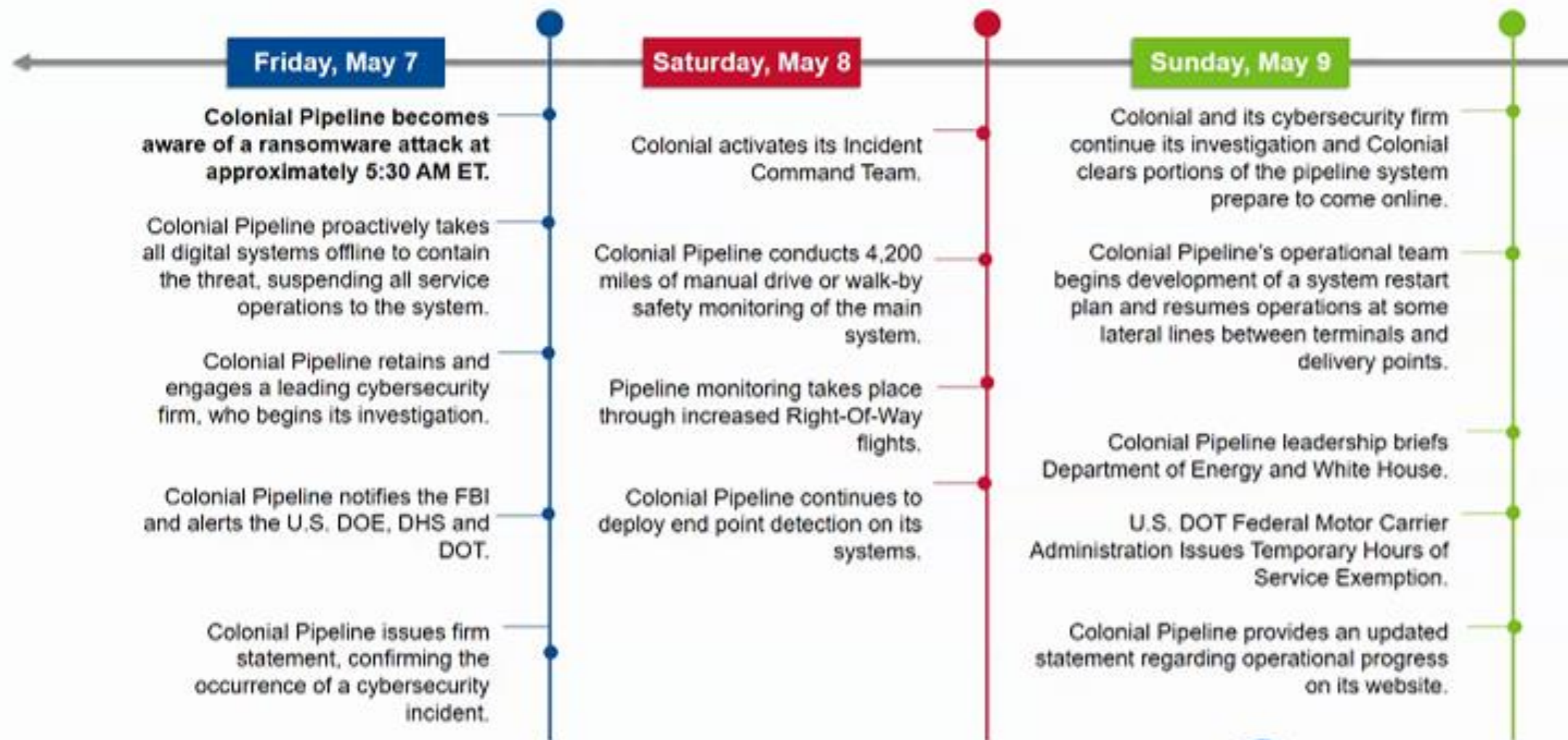
The Situation

- On Thursday, May 7, 2021, Colonial Pipeline announced a shutdown of its main gasoline and its distillate pipelines, citing a network incident on their corporate business network.
- Ransomware attack by cybercrime gang, Darkside.
- The attack targeted Colonial's business systems, not the operating system.
- In an abundance of caution, Colonial shutdown the pipeline as well.
- Vulnerability was traced to a former employee's personal password he had previously used for his VPN password at Colonial.

The Situation

- The result of the shutdown:
 - A significant shortfall in fuel terminals across the East Coast
 - Widespread fuel shortages at retail gas stations in Southeast and Mid-Atlantic
 - Panic buying of fuel and using non-traditional, unsafe vessels
- COVID-19 pandemic: pent up domestic travel demand after first wave of vaccines
- Truck driver shortage compounded by the pandemic.
- Colonial Pipeline indicated they would not pay the \$5 million ransom, which created uncertainty as to the duration of the fuel shortage.

Initial Response





The Challenge



The Challenge





- Policy Considerations
 - State of Emergency
 - Pros/cons of declaration
 - Different state to state
 - Transportation waivers
 - Weight restrictions
 - Hours of service
- Government Operations
 - Fuel planning
 - Travel restrictions
- Public Information
 - Panic buying
 - Social media impacts
 - COVID-19 influence
- Internal Messaging to Employees
 - Consistency in messaging
 - Expect information to become public quickly

The Solution

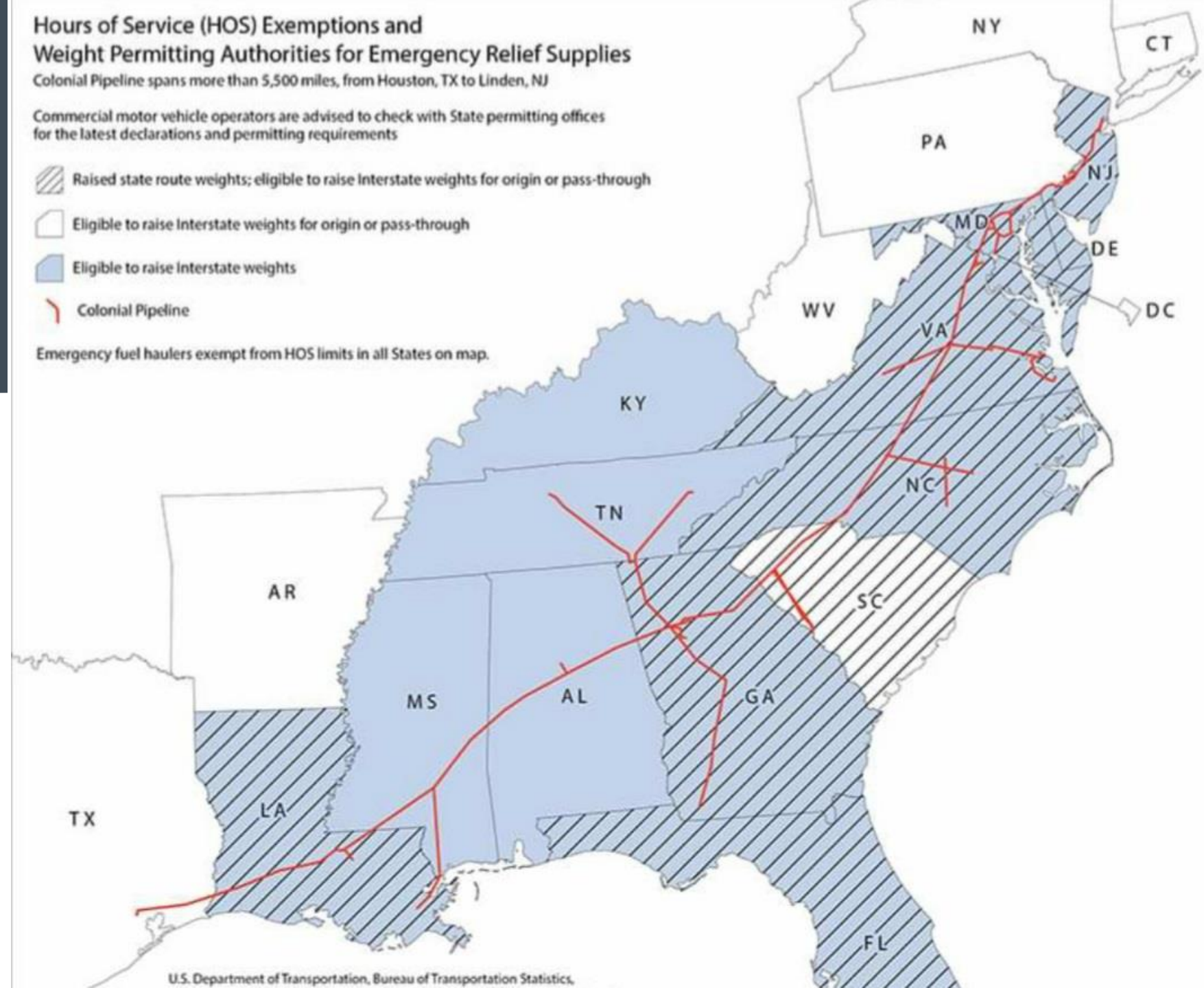
Hours of Service (HOS) Exemptions and Weight Permitting Authorities for Emergency Relief Supplies

Colonial Pipeline spans more than 5,500 miles, from Houston, TX to Linden, NJ

Commercial motor vehicle operators are advised to check with State permitting offices for the latest declarations and permitting requirements

-  Raised state route weights; eligible to raise Interstate weights for origin or pass-through
-  Eligible to raise Interstate weights for origin or pass-through
-  Eligible to raise Interstate weights
-  Colonial Pipeline

Emergency fuel haulers exempt from HOS limits in all States on map.



Public Information

↳ Governor Ralph Northam Retweeted



Virginia Department of Emergency Management @VDEM · 3h

Remember when it wasn't a good idea to panic buy toilet paper last year? Please don't do it with gas now. This can create spot shortages at stations, which is what we DON'T want to happen. Colonial Pipeline hopes to resume normal operations soon.



AAA Mid-Atl VA News and 2 others

77 659 1.1K



T_E_M_A @T_E_M_A · 2h

Please don't panic buy gas. This can create shortages at stations. Only buy what you need and NEVER use unapproved containers for fuel.

US Consumer Product Safety Commission @USCPS · 5h

Do not fill plastic bags with gasoline.

[Show this thread](#)



Governor Roy Cooper @NC_Governor · May 11

I have talked today with federal officials including Energy Secretary Jennifer Granholm and we have a full court press to get the Colonial Pipeline back up and fully operating quickly. Report price gouging and please don't rush to top off your tanks. – RC

Pinned Tweet



GA AG Chris Carr @Georgia_AG · May 11

CONSUMER ALERT

@GovKemp has declared a State of Emergency as a result of the petroleum shortage from the May 7, 2021 cyber-attack on the Colonial Pipeline.



Governor Kay Ivey @GovernorKayIvey · May 11

Spoke w/ @ENERGY earlier re: the #pipelinecyberattack Folks, it should be operational in a few days. Please do not fill up your car unless you need to and do not fill multiple containers. Overreacting creates more of a shortage. Please use common sense and patience! #alpolitics

50 357 726

The Inject

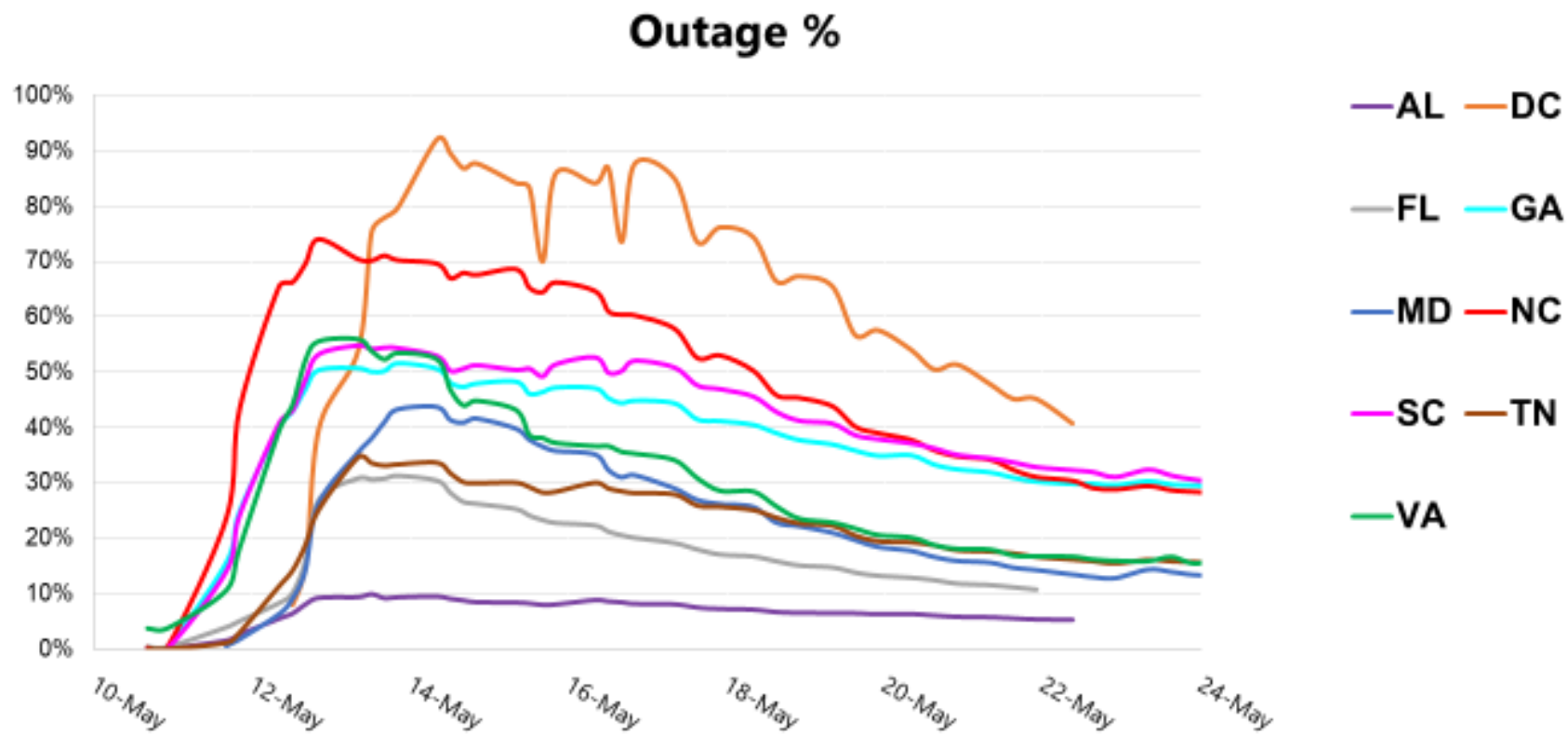
May 11

U.S. One Failed Bridge in Memphis Is Costing Business Millions

Closure of cracked Interstate-40 span clogs local roads, hinders national supply chain



Retail Station Outage % by State



Source: DOE Analysis of GasBuddy's Fuel Availability Tracker

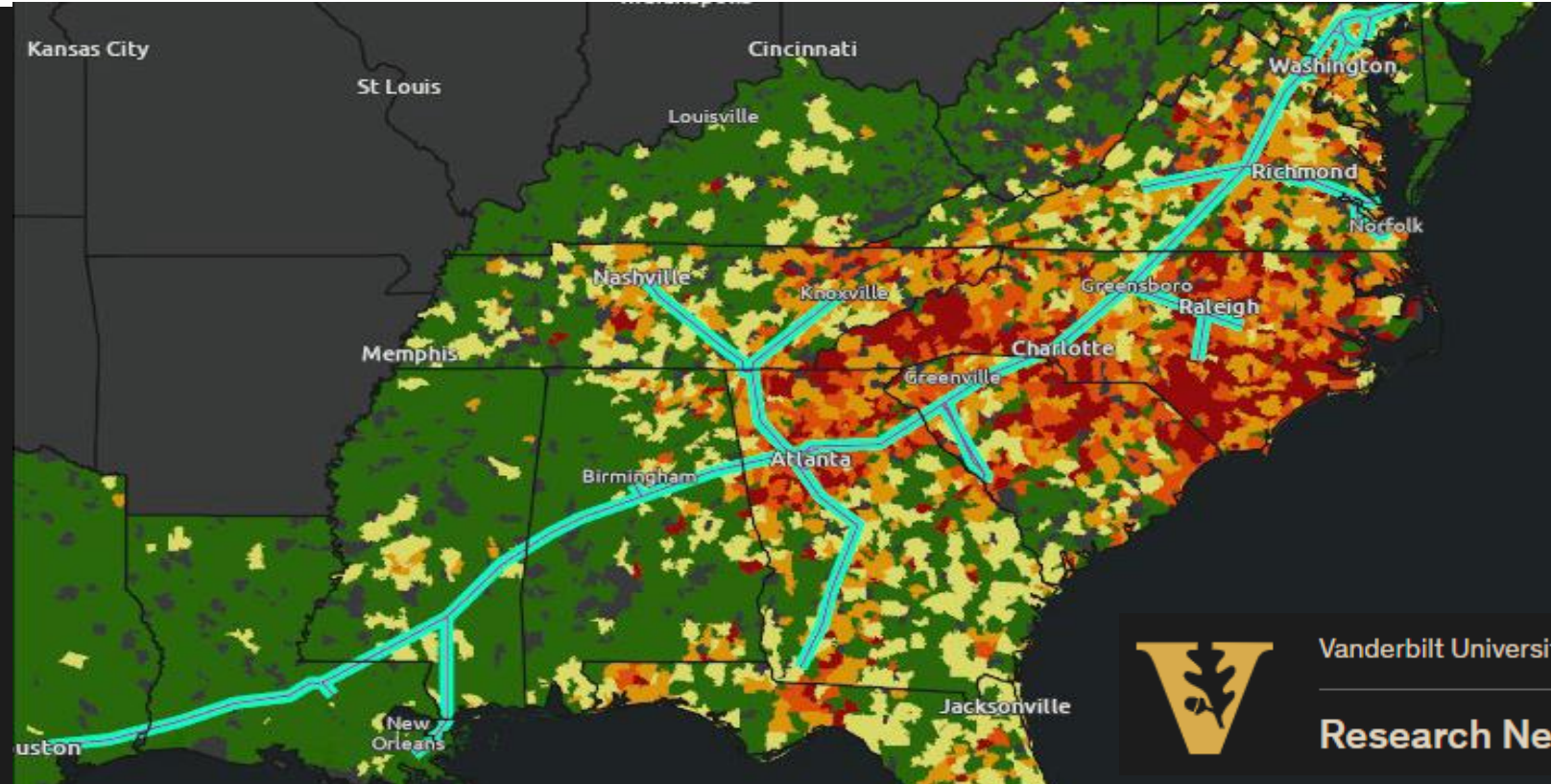
The Outcome

- Restoration of the pipeline 5 days later on May 15, 2021,
- Colonial paid the \$5 million ransom
- Gas stations returned to normal after 6 to 8 weeks in most states.



RESEARCH NEWS

Nashville suffered less than regional cities throughout Colonial Pipeline shutdown due to stronger waterborne petroleum access



Vanderbilt University

Research News

Questions?



Ben Bolton
Senior Energy Programs Administrator
Emergency Services Coordinator 12 for Energy
Office of Energy Programs
(615) 306-5908

Ben.Bolton@tn.gov



[Cumberland Mountain State Park](#), Crossville, TN



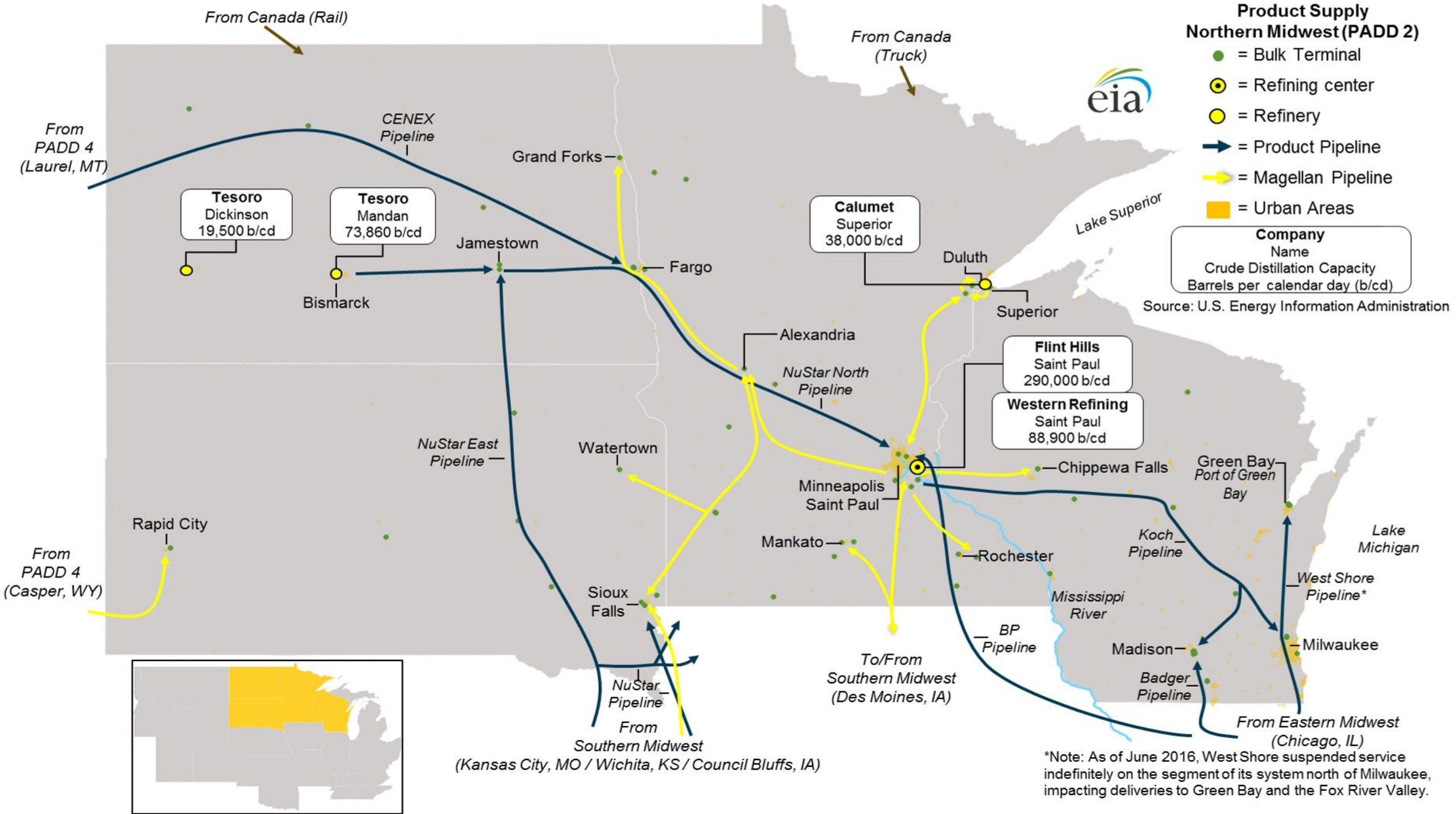
The Situation in Wisconsin

Megan Levy

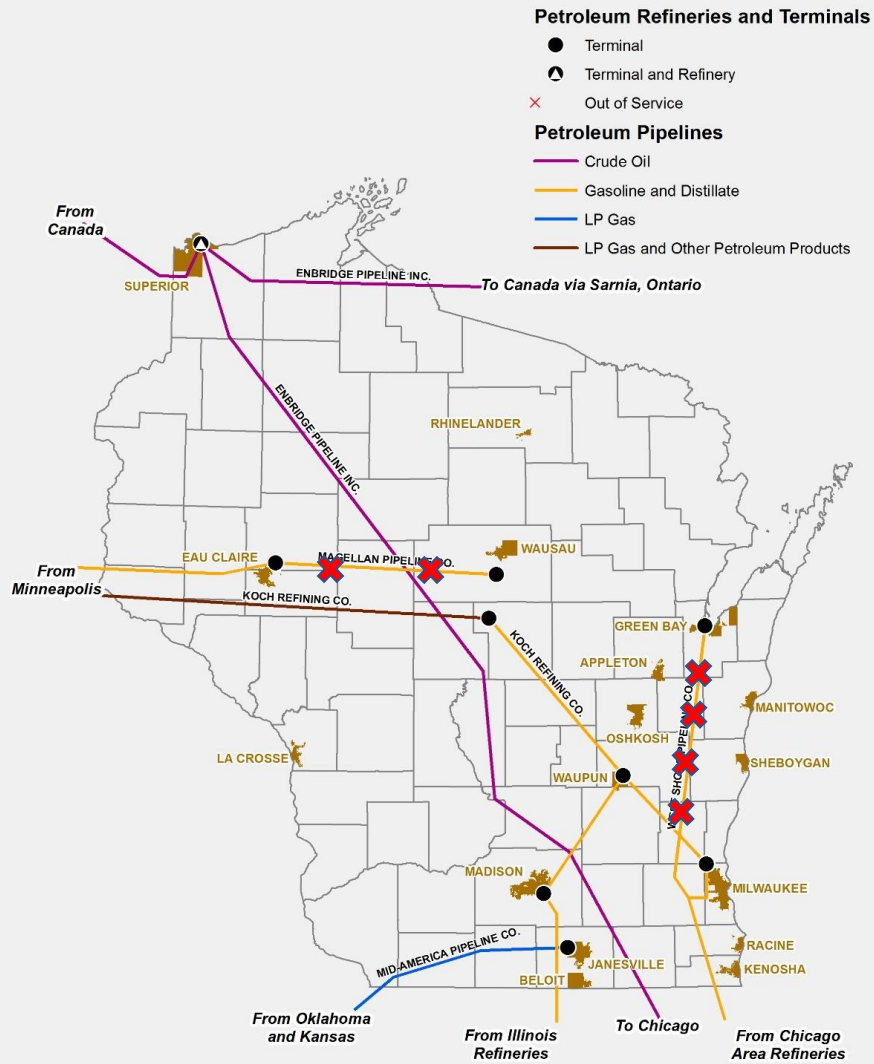
Resilience Strategist and Wisconsin Energy Assurance Coordinator

Wisconsin Office of Energy Innovation

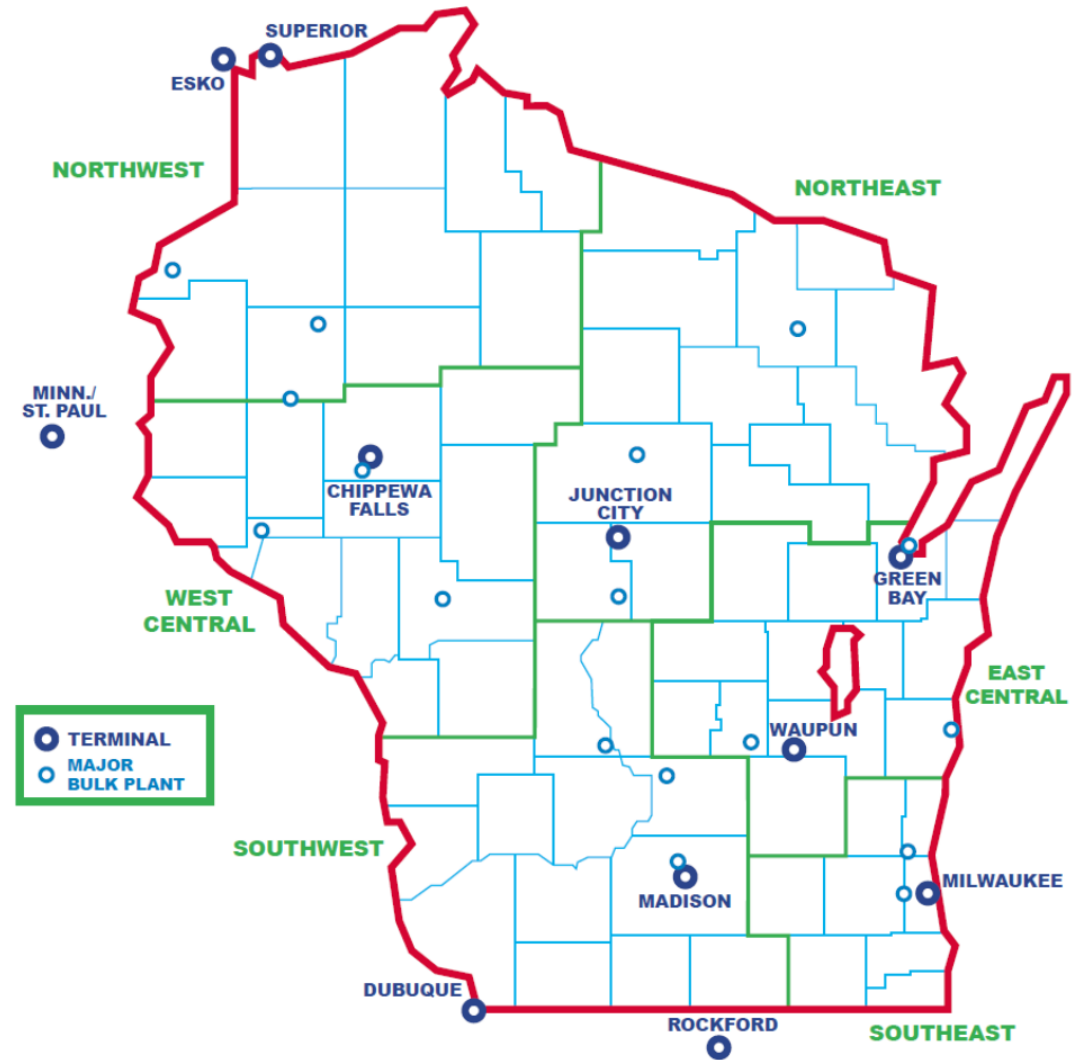




Wisconsin Petroleum Pipelines



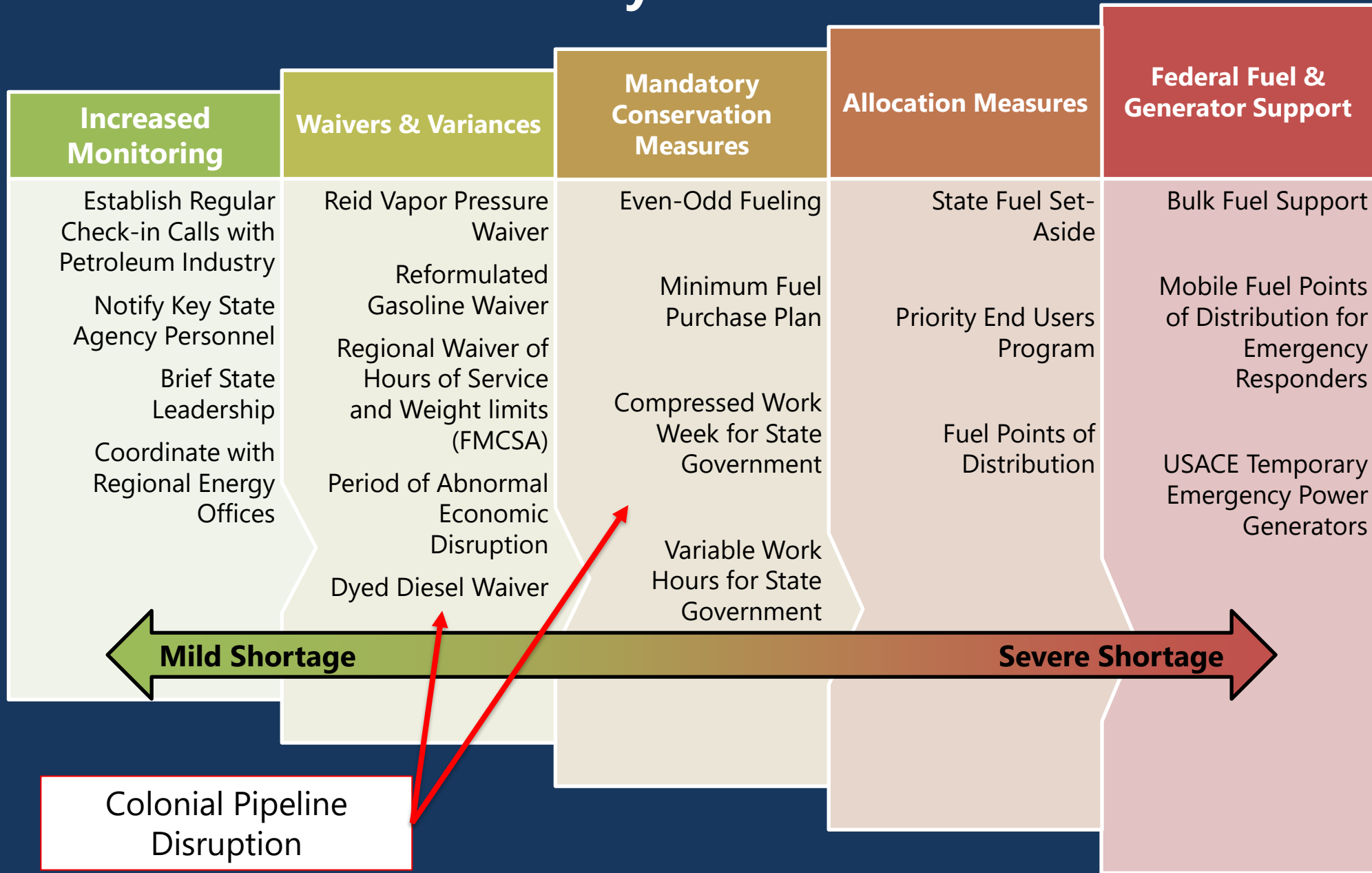
Terminals and Bulk Plants



For discussion purposes only

Wisconsin Petroleum Shortage Contingency Plan

Summary of Measures





Private Sector Fuel Coordination Group

Purpose

- Convened during emergencies to:
 - Obtain industry assessment of the situation
 - Identify ideal response measures
 - Pass information quickly (threat info, state measures, etc.)
 - Relay prioritized resource requests to industry
- Convened outside of emergencies to:
 - Conduct planning
 - Ensure contact information is accurate
 - Exercise and interface with local government

Current Represented Organizations

- Wisconsin Propane Gas Association (WPGA)
- Wisconsin Petroleum Marketers and Convenience Store Association (WPMCA)
- Cooperative Network
- Kwik Trip
- U.S. Venture/U.S. Oil
- Klemm Tank Lines
- Growmark
- CHS Inc
- E.H. Wolf and Sons
- Koch Industries

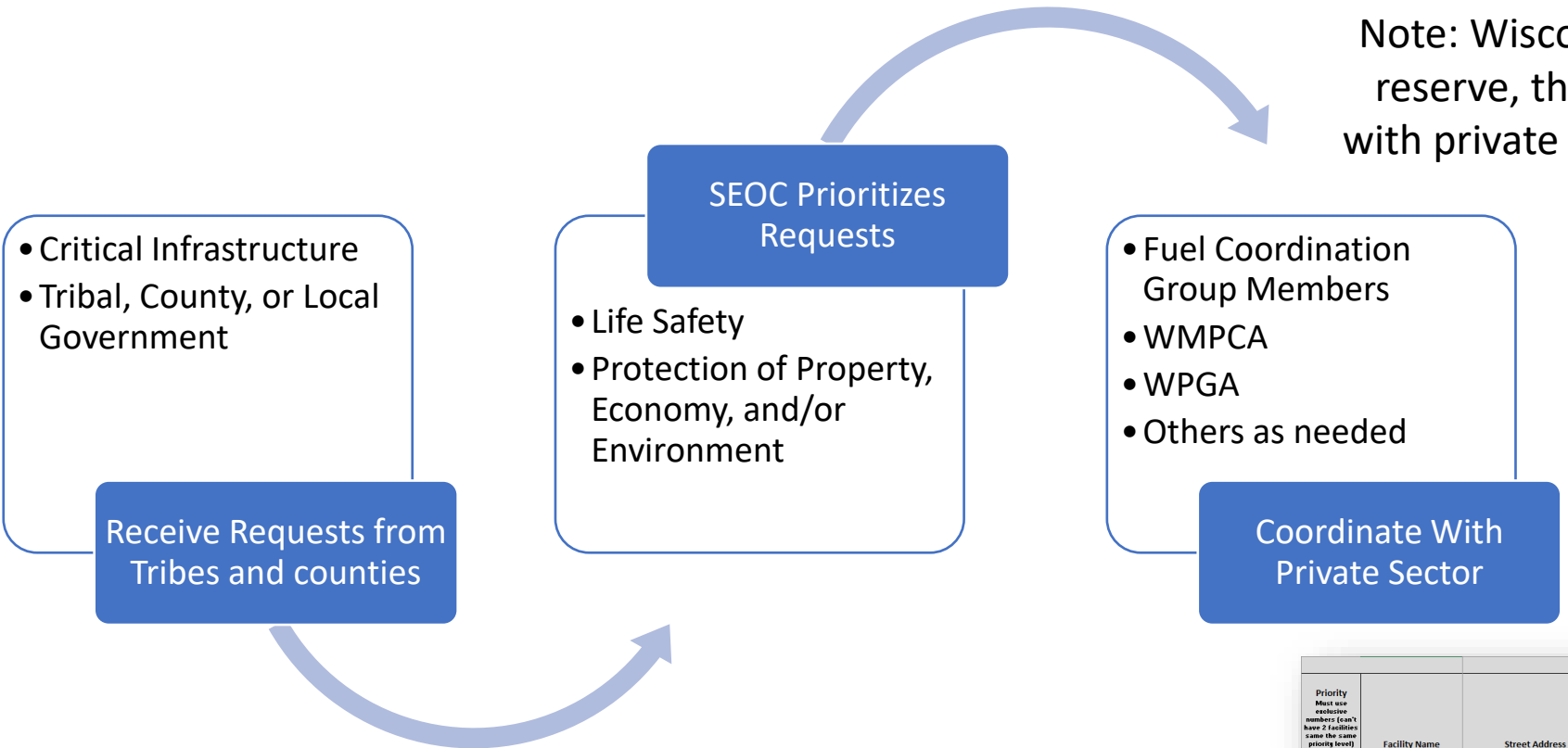


Public Sector Fuel Coordination Group

Agency	Offices	Purpose
Department of Military Affairs	Wisconsin Emergency Management	Emergency response coordination
	Wisconsin National Guard	Situational awareness and emergency response
Public Service Commission	Commission Office	Energy emergency response coordination and energy supply monitoring
	Office of Energy Innovation	
Department of Agriculture Trade and Consumer Protection	Division of Trade and Consumer Protection	Monitor price gouging, announcement of period of abnormal economic disruption
	Bureau of Weights and Measures	Reformulated Gasoline (RFG) variances Reid Vapor Pressure (RVP) variances and EPA waivers
Department of Natural Resources	Air Quality	Reformulated Gasoline (RFG) variances Reid Vapor Pressure (RVP) variances and EPA waivers
Department of Justice	Wisconsin Statewide Intelligence Center	Pass potential threat information and situational awareness
Department of Transportation	Freight Management and Roadside Facilities	Roadway status hours of service and weight limit modifications
	Wisconsin State Patrol	Enforcement of variances and waivers Federal Motor Carrier Safety Administration liaison



Emergency Requests for Fuel



Note: Wisconsin does not have a strategic fuel reserve, therefore the state must coordinate with private sector fuel providers to fill requests

The State Emergency Operations Center Logistics Team will send Fuel Coordination Group members a prioritized list of requests received by the state. Ideally, this would occur at the same time every day throughout an incident

Priority Must use exclusive numbers (can't have 2 facilities same the same priority level)	Facility Name	Street Address	City	Zip Code	County or Tribe	WEM Region	Facility Function Very short description of what the facility is: example: Fire Station, Hospital, Radio Tower, etc.	Facility Description Briefly Describe this facility (Example: 245 bed Level II Trauma Center)	Facility Population How many people live or are staying in the facility?
1	Example: Wisconsin Hospital	100 Miles Ave	City X	33333	La Crosse County	West Central	Hospital	245 Bed Level II Trauma Center	100

Fuel Request Spreadsheet

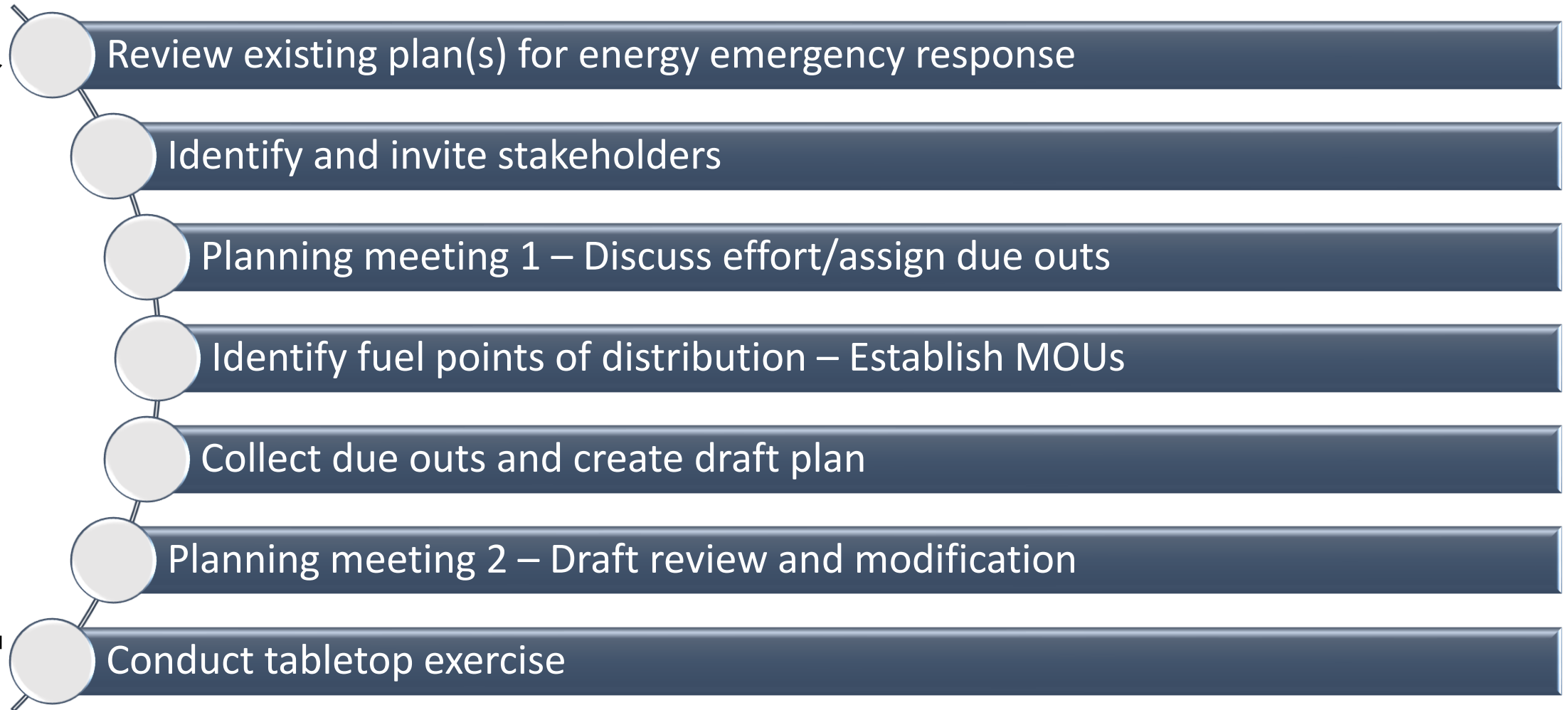


Petroleum Shortage Planning Considerations

- Relationship with fuel vendors and COOPs
- Fuel storage capacity at known fuel sites (Highway shops,
- How full do known fuel sites usually keep their tanks?
- Fuel burn rates for essential services (law enforcement, firefighting, EMS, sanitation, public works)
- Fuel conservation measures
 - Remote work for non-essential functions
 - Acceptable delays in service (example: delay garbage pickup one week)
 - Even-Odd fueling
 - Minimum purchase plans
 - Limiting fill of non-vehicle containers



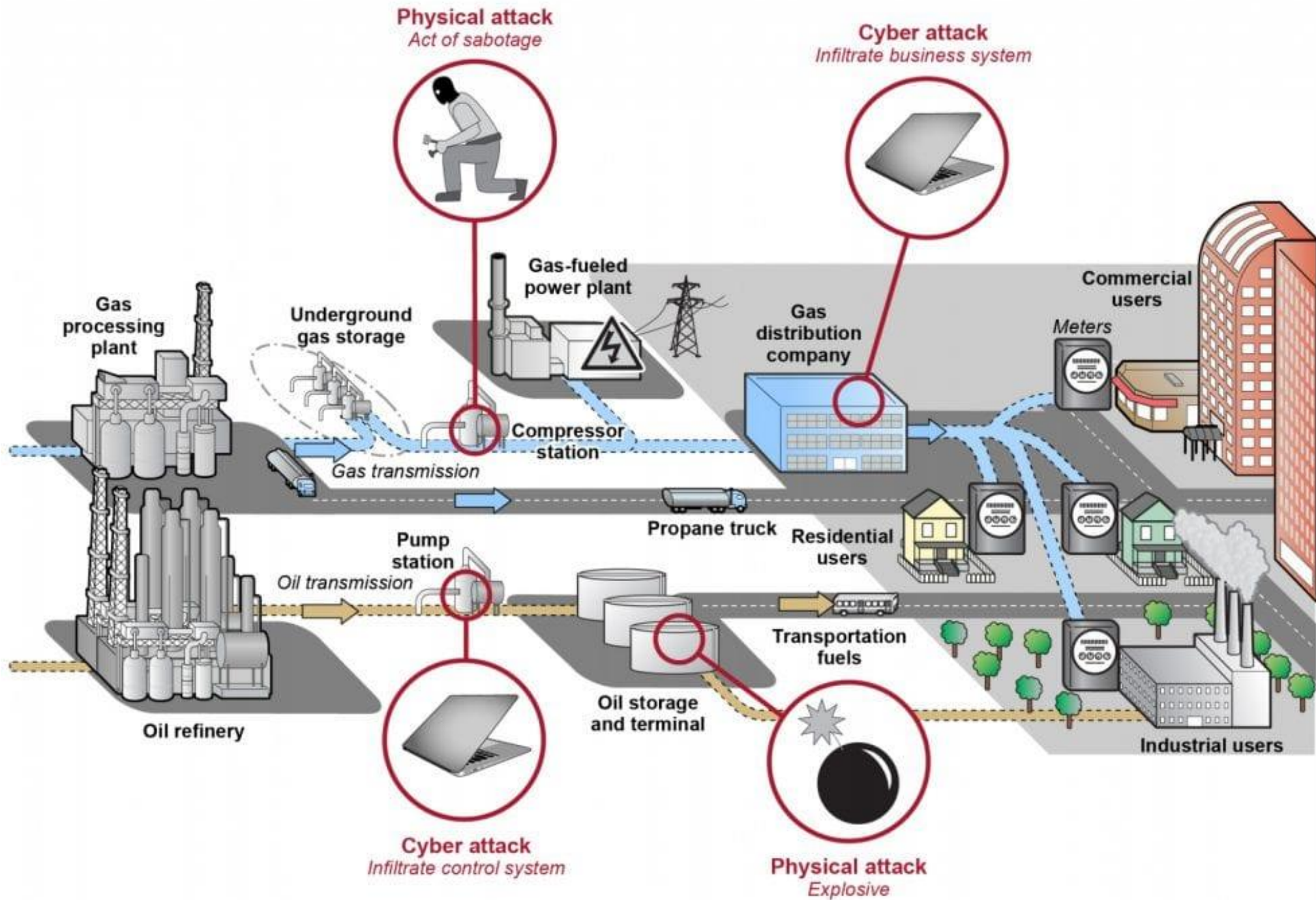
Energy Emergency Plan Development Process



New Transportation Security Administration Requirements

- The May 2021 Security Directive requires critical pipeline owners and operators to:
 - Report confirmed and potential cybersecurity incidents to CISA;
 - Designate a Cybersecurity Coordinator to be available 24 hours a day, seven days a week;
 - Review current practices; and,
 - Identify any gaps and related remediation measures to address cyber-related risks and report the results to TSA and CISA within 30 days
- July 2021 TSA 2 pushed the rules further – Requires Owners/Operators to:
 - Implement specific mitigation measures
 - Protect against ransomware attacks and other threats to IT and OT
 - Develop a cybersecurity contingency and recovery plan
 - Conduct a cybersecurity architecture design review







Cybersecurity Implications in Wisconsin

- If it happens here, we focus on:
 - Responding to the cybersecurity incident
 - Consequence management
- Cyber Incident Response
 - Likely led by private cybersecurity firms with CISA and FBI support.
 - State's goals would be to:
 - Understand what is causing the issue and the **estimated restoration timeline**
 - Remediate any impacts at public infrastructure
 - Share information with mission partners to enable local response
 - Indicators of compromise
 - Restoration timeline
 - Assessments of impacts



Cyber Incident Severity Schema

Rating Color	Score	Required Actions		
		Cyber Response Management Group Level 1 Conference Call	Cyber Response Management Group Level 2 Conference Call	SEOC Activation
Baseline	0-19	X		
	Description: <u>Highly unlikely</u> to affect public health or safety, State security, economic security, civil liberties, or public confidence.			
Baseline (Minor)	20-34	X		
	Description: <u>Highly unlikely</u> to affect public health or safety, State security, economic security, civil liberties, or public confidence. The <u>potential for impact</u> exists and <u>warrants additional scrutiny</u> .			
Low	35-49	X		
	Description: <u>Unlikely</u> to affect public health or safety, State security, economic security, civil liberties, or public confidence.			
Medium	50-64		X	X (potential)
	Description: <u>May</u> affect public health or safety, State security, economic security, civil liberties, or public confidence.			
High	65-74		X	X (potential)
	Description: <u>Likely</u> to result in a <u>demonstrable impact</u> to public health or safety, State security, economic security, civil liberties, or public confidence.			
Severe	75-89		X	X
	Description: Likely to result in a <u>significant impact</u> to public health or safety, State security, economic security, civil liberties, or public confidence.			
Emergency	90-100		X	X
	Description: Imminent threat to the provision of an enterprise wide-scale critical infrastructure services, government stability, or life safety in Wisconsin.			



Want some help with this stuff?

Contact:

Drew Werner
Critical Infrastructure Planner
Wisconsin Emergency Management
Drew.werner@wisconsin.gov
608-888-5348

Megan Levy
Energy Assurance Coordinator
Wisconsin Office of Energy Innovation
Megan.levy@wisconsin.gov
608-266-5054



Questions?

